WiNG™ 5.9.0

Wireless Controller and Service Platform

System Reference Guide

Published June 2017

9035118

Legal Notices

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information about Extreme Networks trademarks, go to: www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/support/

Table of Contents

Chapter 5, Device Configuration

Chapter 6, Wireless Configuration

Chapter 7, Network Configuration

Chapter 8, Profile Configuration

Chapter 9, RF Domains

Chapter 10, Security

Chapter 11, Services

Chapter 12, Management Access

Chapter 13, Diagnostics

Chapter 14, Operations

Chapter 15, Statistics

Chapter 16, Analytics

About This Guide

This manual supports the following Access Point, controller and service platform models:

- Wireless Controller*s* – RFS4000, RFS6000
- *Service Platforms* - NX5500, NX5500E, NX7500, NX75XX, NX7510E, NX9500, NX9510, NX9600, NX9610, VX9000, VX9000E
- Access Point*s* – AP6521, AP6522, AP6522M, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP8122, AP8132, AP8163, AP8232, AP8432 and AP8533.

NOTE: Throughout this guide, unless specific model references are needed, AP8122, AP8132, AP8163 models are referred to as AP81XX.

This section is organized into the following:

Document Convention

The following conventions are used in this manual to draw your attention to important information:

NOTE: Indicates tips or special requirements.

CAUTION: Indicates conditions that can cause equipment damage or data loss.

WARNING! Indicates a condition or procedure that could result in personal injury or equipment damage.

Switch Note: Indicates caveats unique to a particular RFS series controller or NX series service platform.

Notational Conventions

The following notational conventions are used in this document:

- *Italics* are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents
  - Bullets (•) indicate:
    - lists of alternatives
    - lists of required steps that are not necessarily sequential
    - action items
  - Sequential lists (those describing step-by-step procedures) appear as numbered lists

End-User Software License Agreement

This document is an agreement ("Agreement") between You, the end user, and Extreme Networks, Inc., on behalf of itself and its Affiliates ("Extreme") that sets forth your rights and obligations with respect to the "Licensed Materials". BY INSTALLING SOFTWARE AND/OR THE LICENSE KEY FOR THE SOFTWARE ("License Key") (collectively, "Licensed Software"), IF APPLICABLE, COPYING, OR OTHERWISE USING THE LICENSED SOFTWARE AND/OR ANY OF THE LICENSED MATERIALS UNDER THIS AGREEMENT, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES THE LICENSE(S) AND THE LIMITATION(S) OF WARRANTY AND DISCLAIMER(S)/LIMITATION(S) OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, RETURN THE LICENSE KEY (IF APPLICABLE) TO EXTREME OR YOUR DEALER, IF ANY, OR DO NOT USE THE LICENSED SOFTWARE AND/OR LICENSED MATERIALS AND CONTACT EXTREME OR YOUR DEALER WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT TO ARRANGE FOR A REFUND. IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT EXTREME, Attn: LegalTeam@extremenetworks.com.

1 DEFINITIONS. "Affiliates" means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. "Server Application" means the software application associated to software authorized for installation (per License Key, if applicable) on one or more of Your servers as further defined in the Ordering Documentation. "Client Application" shall refer to the application to access the Server Application. "Network Device" for purposes of this Agreement shall mean a physical computer device, appliance, appliance component, controller, wireless access point, or virtual appliance as further described within the applicable product documentation, which includes the Order Documentation. "Licensed Materials" means the Licensed Software (including the Server Application and Client Application), Network Device (if applicable), Firmware, media embodying software, and the accompanying documentation. "Concurrent User" shall refer to any of Your individual employees who You provide access to the Server Application at any one time. "Firmware" refers to any software program or code embedded in chips or other media. "Standalone" software is software licensed for use independent of any hardware purchase as identified in the Ordering Documentation. "Licensed Software" collectively refers to the software, including Standalone software, Firmware, Server Application, Client Application or other application licensed with conditional use parameters as defined in the Ordering Documentation. "Ordering Documentation" shall mean the applicable price quotation, corresponding purchase order, relevant invoice, order acknowledgement, and accompanying documentation or specifications for the products and services purchased, acquired or licensed hereunder from Extreme either directly or indirectly.

2 TERM. This Agreement is effective from the date on which You accept the terms and conditions of this Agreement via click-through, commence using the products and services or upon delivery of the License Key if applicable, and shall be effective until terminated. In the case of Licensed Materials offered on a subscription basis, the term of "licensed use" shall be as defined within Your Ordering Documentation.

3 GRANT OF LICENSE. Extreme will grant You a non-transferable, non-sublicensable, non-exclusive license to use the Licensed Materials and the accompanying documentation for Your own business purposes subject to the terms and conditions of this Agreement, applicable licensing restrictions, and any term, user server networking device, field of use, or other restrictions as set forth in Your Ordering Documentation. If the Licensed Materials are being licensed on a subscription and/or capacity basis, the applicable term and/or capacity limit of the license shall be specified in Your Ordering Documentation. You may install and use the Licensed Materials as permitted by the license type purchased as described below in License Types. The license type purchased is specified on the invoice issued to You by Extreme or Your dealer, if any. YOU MAY NOT USE, COPY, OR MODIFY THE LICENSED MATERIALS, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT.

4 LICENSE TYPES.

- *Single User, Single Network Device*. Under the terms of this license type, the license granted to You by Extreme authorizes You to use the Licensed Materials as bundled with a single Network Device as identified by a unique serial number for the applicable Term, if and as specified in Your Ordering Documentation, or any replacement for that network device for that same Term, for internal use only. A separate license, under a separate License Agreement, is required for any other network device on which You or another individual, employee or other third party intend to use the Licensed Materials. A separate license under a separate License Agreement is also required if You wish to use a Client license (as described below).
- *Single User, Multiple Network Device*. Under the terms of this license type, the license granted to You by Extreme authorizes You to use the Licensed Materials with a defined amount of Network Devices as defined in the Ordering Documentation.
- *Client*. Under the terms of the Client license, the license granted to You by Extreme will authorize You to install the License Key for the Licensed Materials on your server and allow the specific number of Concurrent Users as ordered by you and is set forth in Your Ordering Documentation. A separate license is required for each additional Concurrent User.
- *Standalone*. Software or other Licensed Materials licensed to You for use independent of any Network Device.
- *Subscription*. Licensed Materials, and inclusive Software, Network Device or related appliance updates and maintenance services, licensed to You for use during a subscription period as defined in Your applicable Ordering Documentation.
- *Capacity*. Under the terms of this license, the license granted to You by Extreme authorizes You to use the Licensed Materials up to the amount of capacity or usage as defined in the Ordering Documentation.

5 AUDIT RIGHTS. You agree that Extreme may audit Your use of the Licensed Materials for compliance with these terms and Your License Type at any time, upon reasonable notice. In the event that such audit reveals any use of the Licensed Materials by You other than in full compliance with the license granted and the terms of this Agreement, Extreme reserves the right to charge You for all reasonable expenses related to such audit in addition to any other liabilities and overages applicable as a result of such non-compliance, including but not limited to additional fees for Concurrent Users, excess capacity or usage over and above those specifically granted to You. From time to time, the Licensed Materials may upload information about the Licensed Materials and the associated usage to Extreme. This is to verify the Licensed Materials are being used in accordance with a valid license and/or entitlement. By using the Licensed Materials, you consent to the transmission of this information.

6 RESTRICTION AGAINST COPYING OR MODIFYING LICENSED MATERIALS. Except as expressly permitted in this Agreement, You may not copy or otherwise reproduce the Licensed Materials. In no event does the limited copying or reproduction permitted under this Agreement include the right to decompile, disassemble, electronically transfer, or reverse engineer the Licensed Materials, including the Licensed Software, or to translate the Licensed Materials into another computer language. The media embodying the Licensed Materials may be copied by You, in whole or in part, into printed or machine readable form, in sufficient numbers only for backup or archival purposes, or to replace a worn or defective copy. However, You agree not to have more than two (2) copies of the Licensed Software in whole or in part, including the original media, in your possession for said purposes without Extreme' prior written consent, and in no event shall You operate more copies of the Licensed Software than the specific licenses granted to You. You may not copy or reproduce the documentation. You agree to maintain appropriate records of the location of the original media and all copies of the Licensed Software, in whole or in part, made by You. Any portion of the Licensed Software included in any such modular work shall be used only on a single computer for internal purposes and shall remain subject to all the terms and conditions of this Agreement. You agree to include any copyright or other proprietary notice set forth on the label of the media embodying the Licensed Software on any copy of the Licensed Software in any form, in whole or in part, or on any modification of the Licensed Software or any such modular work containing the Licensed Software or any part thereof.

7 TITLE AND PROPRIETARY RIGHTS

a The Licensed Materials are copyrighted works and are the sole and exclusive property of Extreme, any company or a division thereof which Extreme controls or is controlled by, or which may result from the merger or consolidation with Extreme (its "Affiliates"), and/or their suppliers. This Agreement conveys a limited right to operate the Licensed Materials and shall not be construed to convey title to the Licensed Materials to You. There are no implied rights. You shall not sell, lease, transfer, sublicense, dispose of, or otherwise make available the Licensed Materials or any portion thereof, to any other party.

b You further acknowledge that in the event of a breach of this Agreement, Extreme shall suffer severe and irreparable damages for which monetary compensation alone will be inadequate. You therefore agree that in the event of a breach of this Agreement, Extreme shall be entitled to monetary damages and its reasonable attorney's fees and costs in enforcing this Agreement, as well as injunctive relief to restrain such breach, in addition to any other remedies available to Extreme.

8 PROTECTION AND SECURITY. In the performance of this Agreement or in contemplation thereof, You and your employees and agents may have access to private or confidential information owned or controlled by Extreme relating to the Licensed Materials supplied hereunder including, but not limited to, product specifications and schematics, and such information may contain proprietary details and disclosures. All information and data so acquired by You or your employees or agents under this Agreement or in contemplation hereof shall be and shall remain Extreme' exclusive property, and You shall use all commercially reasonable efforts to keep, and have your employees and agents keep, any and all such information and data confidential, and shall not copy, publish, or disclose it to others, without Extreme' prior written approval, and shall return such information and data to Extreme at its request. Nothing herein shall limit your use or dissemination of information not actually derived from Extreme or of information which has been or subsequently is made public by Extreme, or a third party having authority to do so

You agree not to deliver or otherwise make available the Licensed Materials or any part thereof, including without limitation the object or source code (if provided) of the Licensed Software, to any party other than Extreme or its employees, except for purposes specifically related to your use of the Licensed Materials on a single computer as expressly provided in this Agreement, without the prior written consent of Extreme. You acknowledge that the Licensed Materials contain valuable confidential information and trade secrets, and that unauthorized use, copying and/or disclosure thereof are harmful to Extreme or its Affiliates and/or its/their software suppliers.

9 MAINTENANCE AND UPDATES. Except as otherwise defined below, updates and certain maintenance and support services, if any, shall be provided to You pursuant to the terms of an Extreme Service and Maintenance Agreement, if Extreme and You enter into such an agreement. Except as specifically set forth in such agreement, Extreme shall not be under any obligation to provide updates, modifications, or enhancements, or maintenance and support services for the Licensed Materials to You. If you have purchased Licensed Materials on a subscription basis then the applicable service terms for Your Licensed Materials are as provided in Your Ordering Documentation. Extreme will perform the maintenance and updates in a timely and professional manner, during the Term of Your subscription, using qualified and experienced personnel. You will cooperate in good faith with Extreme in the performance of the support services including, but not limited to, providing Extreme with: (a) access to the Extreme Licensed Materials (and related systems); and (b) reasonably requested assistance and information. Further information about the applicable maintenance and updates terms can be found on Extreme's website at http://www.extremenetworks.com/company/legal/terms-of-support

10 DEFAULT AND TERMINATION. In the event that You shall fail to keep, observe, or perform any obligation under this Agreement, including a failure to pay any sums due to Extreme, or in the event that you become insolvent or seek protection, voluntarily or involuntarily, under any bankruptcy law, Extreme may, in addition to any other remedies it may have under law, terminate the License and any other agreements between Extreme and You.

a Immediately after any termination of the Agreement, Your licensed subscription term, or if You have for any reason discontinued use of Licensed Materials, You shall return to Extreme the original and any copies of the Licensed Materials and remove the Licensed Materials, including an Licensed Software, from any modular

works made pursuant to Section 3, and certify in writing that through your best efforts and to the best of your knowledge the original and all copies of the terminated or discontinued Licensed Materials have been returned to Extreme

b Sections 1, 7, 8, 10, 11, 12, 13, 14 and 15 shall survive termination of this Agreement for any reason.

11 EXPORT REQUIREMENTS. You are advised that the Licensed Materials, including the Licensed Software is of United States origin and subject to United States Export Administration Regulations; diversion contrary to United States law and regulation is prohibited. You agree not to directly or indirectly export, import or transmit the Licensed Materials, including the Licensed Software to any country, end user or for any Use that is prohibited by applicable United States regulation or statute (including but not limited to those countries embargoed from time to time by the United States government); or contrary to the laws or regulations of any other governmental entity that has jurisdiction over such export, import, transmission or Use

12 UNITED STATES GOVERNMENT RESTRICTED RIGHTS. The Licensed Materials (i) were developed solely at private expense; (ii) contain “restricted computer software” submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Extreme and/or its suppliers. For Department of Defense units, the Licensed Materials are considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the U.S. Government is subject to restrictions set forth herein.

13 LIMITED WARRANTY AND LIMITATION OF LIABILITY. Extreme warrants to You that (a) the initially-shipped version of the Licensed Materials will materially conform to the Documentation; and (b) the media on which the Licensed Software is recorded will be free from material defects for a period of ninety (90) days from the date of delivery to You or such other minimum period required under applicable law. Extreme does not warrant that Your use of the Licensed Materials will be error-free or uninterrupted.

NEITHER EXTREME NOR ITS AFFILIATES MAKE ANY OTHER WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, WITH RESPECT TO THE LICENSED MATERIALS, WHICH ARE LICENSED "AS IS". THE LIMITED WARRANTY AND REMEDY PROVIDED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE EXPRESSLY DISCLAIMED, AND STATEMENTS OR REPRESENTATIONS MADE BY ANY OTHER PERSON OR FIRM ARE VOID. IN NO EVENT WILL EXTREME OR ANY OTHER PARTY WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THE LICENSED MATERIALS BE LIABLE FOR SPECIAL, DIRECT, INDIRECT, RELIANCE, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING LOSS OF DATA OR PROFITS OR FOR INABILITY TO USE THE LICENSED MATERIALS, TO ANY PARTY EVEN IF EXTREME OR SUCH OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL EXTREME OR SUCH OTHER PARTY'S LIABILITY FOR ANY DAMAGES OR LOSS TO YOU OR ANY OTHER PARTY EXCEED THE LICENSE FEE YOU PAID FOR THE LICENSED MATERIALS.

Some states do not allow limitations on how long an implied warranty lasts and some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation and exclusion may not apply to You. This limited warranty gives You specific legal rights, and You may also have other rights which vary from state to state.

14 JURISDICTION. The rights and obligations of the parties to this Agreement shall be governed and construed in accordance with the laws and in the State and Federal courts of the State of California, without regard to its rules with respect to choice of law. You waive any objections to the personal jurisdiction and venue of such courts. None of the 1980 United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement

15 FREE AND OPEN SOURCE SOFTWARE. Portions of the Software (Open Source Software) provided to you may be subject to a license that permits you to modify these portions and redistribute the modifications (an Open Source License). Your use, modification and redistribution of the Open Source Software are governed by the

terms and conditions of the applicable Open Source License. More details regarding the Open Source Software and the applicable Open Source Licenses are available at www.extremenetworks.com/services/SoftwareLicensing.aspx. Some of the Open Source software may be subject to the GNU General Public License v.x (GPL) or the Lesser General Public Library (LGPL), copies of which are provided with the Licensed Materials and are further available for review at www.extremenetworks.com/services/SoftwareLicensing.aspx, or upon request as directed herein. In accordance with the terms of the GPL and LGPL, you may request a copy of the relevant source code. See the Software Licensing web site for additional details. This offer is valid for up to three years from the date of original download of the software.

16 GENERAL.

a This Agreement is the entire agreement between Extreme and You regarding the Licensed Materials, and all prior agreements, representations, statements, and undertakings, oral or written, are hereby expressly superseded and canceled.

b This Agreement may not be changed or amended except in writing signed by both parties hereto.

c You represent that You have full right and/or authorization to enter into this Agreement.

d This Agreement shall not be assignable by You without the express written consent of Extreme. The rights of Extreme and Your obligations under this Agreement shall inure to the benefit of Extreme' assignees, licensors, and licensees.

e Section headings are for convenience only and shall not be considered in the interpretation of this Agreement

f The provisions of the Agreement are severable and if any one or more of the provisions hereof are judicially determined to be illegal or otherwise unenforceable, in whole or in part, the remaining provisions of this Agreement shall nevertheless be binding on and enforceable by and between the parties hereto

g Extreme's waiver of any right shall not constitute waiver of that right in future. This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof, and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and canceled. No purchase order shall supersede this Agreement.

h Should You have any questions regarding this Agreement, You may contact Extreme at the address set forth below. Any notice or other communication to be sent to Extreme must be mailed by certified mail to the following address:

Extreme Networks, Inc.
16480 Via Del
San Jose, CA 95119 United States
Tel: +1 408-579-2800
Toll-free: +1 888-257-3000

1 Overview

Extreme Networks' WiNG 5 operating system is the next generation in the evolution of WLAN architectures. WiNG 5 OS is designed to scale efficiently from the smallest networks to large, geographically dispersed deployments. The co-operative, distributed control plane innovation in the WiNG 5 architecture offers a software-defined networking (SDN)-ready operating system that can distribute controller functionality to every Access Point in your network. Now, every Access Point is network aware, providing the intelligence required to truly unleash optimal performance, all wireless LAN infrastructure can work together to ensure every transmission is routed through the most efficient path, every time.

WiNG 5 brings you the resiliency of a standalone Access Point network without the vulnerability of a centralized controller, with advancements that take performance, reliability, security, scalability and manageability to a new level. The result? Maximum network uptime and security with minimal management. And true seamless and dependable mobility for your users.

WiNG 5 advances the following technology:

Comprehensive Wi-Fi support - WiNG supports all Wi-Fi protocols, including 802.11a/b/g/n/ac, allowing you to create a cost-effective migration plan based on the needs of your business.

Extraordinary scalability - With WiNG, you can build any size network, from a small WLAN network in a single location to a large multi-site network that reaches all around the globe.

Extraordinary flexibility - No matter what type of infrastructure you deploy, WiNG 5 delivers intelligence to all: standalone independent Access Points or adaptive Access Points that can be adopted by a controller but can switch to independent mode; virtual controllers; physical controllers in branch offices, the *network operating center* (NOC) or the cloud.

The power of distributed intelligence - WiNG distributes intelligence right to the network edge, empowering every controller and Access Point with the intelligence needed to be network-aware, able to identify and dynamically route traffic over the most efficient path available at that time.

Extraordinary network flexibility and site survivability - WiNG provides the best of both worlds: true hierarchical management that delivers a new level of management simplicity and resiliency by enabling controllers to adopt and manage other controllers and Access Points, while allowing adopted infrastructure to also stand on its own.

Gap-free security - When it comes to security, there can be no compromises. WiNG's comprehensive security capabilities keep your network and your data safe, ensuring compliance with PCI, HIPAA and other government and industry security regulations.

Connectivity for the largest indoor and outdoor spaces - In addition to enabling a robust indoor WLAN, our patented MeshConnex™ technology enables the extension of Wi-Fi networks to the largest of outdoor spaces from an expansive outdoor campus environment to an entire city.

Powerful centralized management - With WiNG you get complete control over every aspect of your WLAN. This single powerful windowpane enables zero touch infrastructure deployment, rich analytics that can help you recognize and correct brewing issues before they impact service quality and user connectivity, along with centralized and remote troubleshooting and issue resolution of the entire network.

Application Visibility and Control - With WiNG you get visibility & control over Layer-7 applications with an embedded DPI engine at the Access Point. Extreme Networks NSight (An add-on module to WiNG)

provides real-time visibility and in-depth insight into every dimension of the network including layer-7 application visibility, client devices, device & OS types and users. At a glance the administrator can discern the top applications by usage or by count at every level of the network from site level to Access Points and clients. This is achieved by *Deep Packet Inspection* (DPI) of every flow of every user at the Access Point. The embedded DPI engine in the WiNG OS can detect and identify thousands of applications real time and report to NSight. In addition to detection, firewall and QOS policies can leverage the application context to enforce policies.

1.1 Distributed Intelligence

WiNG 5 enables all WLAN infrastructure with the intelligence required to work together to determine the most efficient path for every transmission. The need to route all traffic through a controller is eliminated, along with the resulting congestion and latency, resulting in higher throughput and superior network performance. Since all features are available at the access layer, they remain available even when the controller is offline, for example, due to a WAN outage, ensuring site survivability and extraordinary network resilience. In addition, you get unprecedented scalability, large networks can support as many as 10,000 nodes without impacting throughput or manageability, providing unprecedented scalability.

1.2 High Availability Networks

WiNG 5 enables the creation of highly reliable networks, with several levels of redundancy and failover mechanisms to ensure continuous network service in case of outages. APs in remote sites coordinate with each other to provide optimized routing and self-healing, delivering a superior quality of experience for business critical applications. Even when WiNG 5 site survivable APs lose communication with the controller, they continue to function, able to bridge traffic while still enforcing QoS and security policies, including stateful inspection of Layer2 (locally bridged) or Layer 3 traffic.

1.3 Gap Free Security

When it comes to wireless security, one size does not fit all. A variety of solutions are required to meet the varying needs and demands of different types of organizations. Regardless of the size of your WLAN or your security requirements, our tiered approach to security allows you to deploy the features you need to achieve the right level of security for your networks and your data. And where a hub-and-spoke architecture can't stop threats until they reach the controller inside your network, WiNG 5 distributes security features to every access point, including those at the very edge of your network, creating an around-the-clock constant network perimeter guard that prevents threats from entering your network for unprecedented gap free security.

1.4 Outdoor Wireless and Mesh Networking

When you need to extend your wireless LAN to outdoor spaces, our patented MeshConnex technology combines with comprehensive mesh networking features to enable you to create secure, high performance, flexible and scalable mesh networks. With our mesh technology, you can cover virtually any area without installing cabling, enabling the creation of cost-effective outdoor wireless networks that can provide

coverage to enterprise workers in vast campus-style environments as well as public safety personnel in patrol cars.

1.5 Network Services, Routing and Switching

WiNG 5 integrates network services like built-in DHCP server, AAA server and routing protocols like policy based routing and OSPF, Layer 2 protocols like MSTP and Link Aggregation. Integration of services and routing/ switching protocols eliminates the need for additional servers or other networking gear in small offices thereby reducing Total Cost of Ownership (TCO). In large networks, where such services are deployed on a dedicated server/ router at the NOC, this provides a backup solution for remote sites when the WAN link to the NOC is temporarily lost. Integrating also provides the added benefit of coordination across these services on failover from primary to standby, assisting a more meaningful behavior, rather than when each fails over independently of the other for the same root cause.

1.6 Management, Deployment and Troubleshooting

WiNG's comprehensive end-to-end management capabilities cover deployment through day-to-day management. You get true zero-touch deployment for access points located anywhere in the world, the simplicity of a single window into the entire network, plus the ability to remotely troubleshoot and resolve issues. And since our management technology is manufacturer-agnostic, you can manage your Extreme Networks WLAN infrastructure as well as any legacy equipment from other manufacturers, allowing you to take advantage of our advanced WLAN infrastructure without requiring a costly rip and replace of your existing WLAN.

2 Web UI Features

The WiNG software contains a Web UI allowing network administrators to manage and view Access Point, controller and service platform settings, configuration data and status. This *Graphical User Interface* (GUI) allows full control of all administration features.

Access Points, controllers and service platforms also share a *Command Line Interface* (CLI) for managing and viewing settings, configuration and status. For more information on the command line interface and a full list of available commands, refer to the *Wireless Services CLI Reference Guide* available at www.extremenetworks.com/support.

For information on how to access and use the Web UI, see:

- *Accessing the Web UI*
- *Glossary of Icons Used*

2.1 Accessing the Web UI

Access Points, controllers and service platforms use a UI accessed using any supported Web browser on a client connected to the subnet the Web UI is configured on.

2.1.1 Browser and System Requirements

To access the GUI, a browser supporting Flash Player 11 is recommended. The system accessing the GUI should have a minimum of 1 GB of RAM for the UI to display and function properly, with the exception of NX service platforms which require 4 GB of RAM. The Web UI is based on Flex, and does not use Java as the underlying UI framework. A resolution of 1280 x 1024 pixels for the GUI is recommended.

The following browsers are required to access the WiNG Web UI:

- Firefox 3.5 or higher
- Internet Explorer 7 or higher
- Google Chrome 2.0 or higher
- Safari 3 and higher
- Opera 9.5 and higher

NOTE: Throughout the Web UI leading and trailing spaces are not allowed in any text fields. In addition, the "?" character is also not supported in text fields.

2.1.2 Connecting to the Web UI

1 Connect one end of an Ethernet cable to a LAN port on the front of the controller or service platform and connect the other end to a computer with a working Web browser.

2 Set the computer to use an IP address between 192.168.0.10 and 192.168.0.250 on the connected port. Set a subnet/network mask of 255.255.255.0.

Once the computer has an IP address, point the browser to: https://192.168.0.1/ and the following login screen will display.

Figure 2-1 *Web UI Login Screen*

3 Enter the default username *admin* in the **Username** field.
Enter the default password *admin123* in the **Password** field.

4 Click the Login button to load the management interface.

5 If this is the first time the UI has been accessed on RFS4011 model controllers and NX4500 and NX6500 model service platforms, a dialogue displays to begin an initial setup wizard. For more information on using the initial setup wizard on these models see *Using the Initial Setup Wizard*.

2.2 Glossary of Icons Used

The UI uses a number of icons used to interact with the system, gather information, and obtain status for the entities managed by the system. This chapter is a compendium of the icons used. This chapter is organized as follows:

- *Global Icons*
- *Dialog Box Icons*
- *Table Icons*
- *Status Icons*
- *Configurable Objects*
- *Configuration Objects*
- *Configuration Operation Icons*
- *Access Type Icons*
- *Administrative Role Icons*
- *Device Icons*

2.2.1 Global Icons

Glossary of Icons Used

This section lists global icons available throughout the interface.

	*Logout*– Select this icon to log out of the system. This icon is always available and is located at the top right corner of the UI.
	*Add* – Select this icon to add a row in a table. When selected, a new row is created in the table or a dialog box displays where you can enter values for a particular list.
	Delete – Select this icon to remove a row from a table. When selected, the selected row is deleted.
	*More Information* – Select this icon to display a pop up with supplementary information that may be available for an item.
	*Trash* – Select this icon to remove a row from a table. When selected, the row is immediately deleted.
	*Create new policy* – Select this icon to create a new policy. Policies define different configuration parameters that can be applied to individual device configurations, profiles and RF Domains.
	*Edit policy* – Select this icon to edit an existing configuration item or policy. To edit a policy, select a policy and this icon.

2.2.2 Dialog Box Icons

Glossary of Icons Used

These icons indicate the current state of various controls in a dialog. These icons enables you to gather the status of all the controls in a dialog. The absence of any of these icons next to a control indicates the value in that control has not been modified from its last saved configuration.

	*Entry Updated* – Indicates a value has been modified from its last saved configuration.
	*Entry Update* – States that an override has been applied to a device profile configuration.

	*Mandatory Field* – Indicates this control value is a mandatory configuration item. You are not allowed to proceed further without providing all mandatory values in this dialog.
	*Error in Entry* – Indicates there is an error in a supplied value. A small red popup provides a likely cause of the error.

2.2.3 Table Icons

Glossary of Icons Used

The following two override icons are status indicators for transactions:

	*Table Row Overridden* – Indicates a change (profile configuration override) has been made to a table row and the change will not be implemented until saved. This icon represents a change from this device's profile assigned configuration.
	*Table Row Added* – Indicates a new row has been added to a table and the change is not implemented until saved. This icon represents a change from this device's profile assigned configuration.

2.2.4 Status Icons

Glossary of Icons Used

These icons indicate device status, operations, or any other action that requires a status returned to the user.

	*Fatal Error* – States there is an error causing a managed device to stop functioning.
	*Error* – Indicates an error exits requiring intervention. An action has failed, but the error is not system wide.
	*Warning* – States a particular action has completed, but errors were detected that did not prevent the process from completing. Intervention might still be required to resolve subsequent warnings.
	*Success* – Indicates everything is well within the network or a process has completed successfully without error.
	Information – This icon always precedes information displayed to the user. This may either be a message displaying progress for a particular process, or just be a message from the system.

2.2.5 Configurable Objects

Glossary of Icons Used

These icons represent configurable items within the UI.

	*Device Configuration* – Represents a configuration file supporting a device category (Access Point, wireless controller etc.).
	*Auto Provisioning Policy* – Represents a provisioning policy. Provisioning policies are a set of configuration parameters that define how Access Points and wireless clients are adopted and their management configuration supplied.
	*Critical Resource Policy* – States a critical resource policy has been applied. Critical resources are resources whose availability is essential to the network. If any of these resources is unavailable, an administrator is notified.
	*Wireless LANs* – States an action impacting a managed WLAN has occurred.
	*WLAN QoS Policy* – States a *quality of service policy* (QoS) configuration has been impacted.
	*Radio QoS Policy* – Indicates a radio's QoS configuration has been impacted.
	*AAA Policy* – Indicates an *Authentication, Authorization and Accounting* (AAA) policy has been impacted. AAA policies define RADIUS authentication and accounting parameters.
	*Association ACL* – Indicates an *Access Control List* (ACL) configuration has been impacted. An ACL is a set of configuration parameters either allowing or denying access to network resources.
	*Smart RF Policy* – States a Smart RF policy has been impacted. Smart RF enables neighboring Access Point radios to take over for an Access Point radio if it becomes unavailable. This is accomplished by increasing the power of radios on nearby Access Points to compensate for the coverage hole created by the non-functioning Access Point.
	*Profile* – States a device profile configuration has been impacted. A profile is a collection of configuration parameters used to configure a device or a feature.

	*Bridging Policy* – Indicates a bridging policy configuration has been impacted. A bridging policy defines which VLANs are bridged, and how local VLANs are bridged between the wired and wireless sides of the network.
	*RF Domain* – States an RF Domain configuration has been impacted.
	*Firewall Policy* – Indicates a firewall policy has been impacted. Firewalls provide a barrier that prevents unauthorized access to resources while allowing authorized access to external and internal resources.
	*IP Firewall Rules* – Indicates an IP firewall rule has been applied. An IP based firewall rule implements restrictions based on the IP address in a received packet.
	*MAC Firewall Rules* – States a MAC based firewall rule has been applied. A MAC based firewall rule implements network allowance restrictions based on the MAC address in a received data packet.
	*Wireless Client Role* – Indicates a wireless client role has been applied to a managed client. The role could be either sensor or client.
	*WIPS Policy* – States the conditions of a WIPS policy have been invoked. WIPS prevents unauthorized access to the network by checking for (and removing) rogue Access Points and wireless clients.
	*Device Categorization* – Indicates a device categorization policy has been applied. This is used by the intrusion prevention system to categorize Access Points or wireless clients as either sanctioned or unsanctioned devices. This enables devices to bypass the intrusion prevention system.
	*Captive Portals* – States a captive portal is being applied. Captive portal is used to provide temporary controller, service platform or Access Point access to requesting wireless clients.
	*DNS Whitelist* – A DNS whitelist is used in conjunction with captive portal to provide access to requesting wireless clients.
	*DHCP Server Policy* – Indicates a DHCP server policy is being applied. DHCP provides IP addresses to wireless clients. A DHCP server policy configures how DHCP provides IP addresses.
	*RADIUS Group* – Indicates the configuration of RADIUS group has been defined and applied. A RADIUS group is a collection of RADIUS users with the same set of permissions.

	*RADIUS User Pools* – States a RADIUS user pool has been applied. RADIUS user pools are a set of IP addresses that can be assigned to an authenticated RADIUS user.
	*RADIUS Server Policy* – Indicates a RADIUS server policy has been applied. A RADIUS server policy is a set of configuration attributes used when a RADIUS server is configured for AAA.
	*Smart Caching Policy* – Smart Caching enables NX4500 and NX6500 series service platforms to temporarily store frequently accessed Web content on network infrastructure devices.
	*Management Policy* – Indicates a management policy has been applied. Management policies configure access control, authentication, traps and administrator permissions.
	*BGP – Border Gateway Protocol* (BGP) is an inter-ISP routing protocol which establishes routing between ISPs. ISPs use BGP to exchange routing and reachability information between *Autonomous Systems* (AS) on the Internet. BGP makes routing decisions based on paths, network policies and/or rules configured by network administrators.

2.2.6 Configuration Objects

- *Glossary of Icons Used*

These configuration icons are used to define the following:

	*Configuration* – Indicates an item capable of being configured by an interface.
	*View Events / Event History* – Defines a list of events. Click this icon to view events or view the event history.
	*Core Snapshots* – Indicates a core snapshot has been generated. A core snapshot is a file that records status events when a process fails on a wireless controller or Access Point.
	*Panic Snapshots* – Indicates a panic snapshot has been generated. A panic snapshot is a file that records status when a wireless controller or Access Point fails without recovery.

	*UI Debugging* – Select this icon/link to view current NETCONF messages.
	*View UI Logs* – Select this icon/link to view the different logs generated by the UI, FLEX and the error logs.

2.2.7 Configuration Operation Icons

Glossary of Icons Used

The following operations icons are used to define configuration operations:

	*Revert* – When selected, any unsaved changes are reverted to their last saved configuration settings.
	*Commit* – When selected, all changes made to the configuration are written to the system. Once committed, changes cannot be reverted.
	*Commit and Save* – When selected, changes are saved to the configuration.

2.2.8 Access Type Icons

Glossary of Icons Used

The following icons display a user access type:

	*Web UI* – Defines a Web UI access permission. A user with this permission is permitted to access an associated device's Web UI.
	*Telnet* – Defines a TELNET access permission. A user with this permission is permitted to access an associated device using TELNET.
	*SSH* – Indicates a SSH access permission. A user with this permission is permitted to access an associated device using SSH.
	*Console* – Indicates a console access permission. A user with this permission is permitted to access an associated device using the device's serial console.

2.2.9 Administrative Role Icons

Glossary of Icons Used

The following icons identify the different administrative roles allowed on the system:

	*Superuser* – Indicates superuser privileges. A superuser has complete access to all configuration aspects of the connected device.
	*System* – States system user privileges. A system user is allowed to configure general settings, such as boot parameters, licenses, auto install, image upgrades etc.
	*Network* – Indicates network user privileges. A network user is allowed to configure wired and wireless parameters, such as IP configuration, VLANs, L2/L3 security, WLANs and radios.
	*Security* – Indicates security user privileges. A security level user is allowed to configure all security related parameters.
	*Monitor* – Defines a monitor role. This role provides no configuration privileges. A user with this role can view the system configuration but cannot modify it.
	*Help Desk* – Indicates help desk privileges. A help desk user is allowed to use troubleshooting tools like sniffers, execute service commands, view or retrieve logs and reboot the controller or service platform.
	*Web User* – Indicates a web user privilege. A Web user is allowed accessing the device's Web UI.

2.2.10 Device Icons

Glossary of Icons Used

The following icons represent the different device types managed by the system:

	*System* – This icon represents the entire WiNG supported system, and all of its member controller, service platform or Access Points that may be interacting at any one time.
	*Cluster* – This icon represents a cluster. A cluster is a set of wireless controllers or service platforms working collectively to provide redundancy and load sharing amongst its members.

	*Service Platform* – This icon indicates an NX45xx, NX65xx or NX9000 series service platform that's part of the managed network
	Wireless Controller – This icon indicates a RFS6000 or a RFS4000 wireless controller that's part of the managed network.
	Wireless Controller – This icon indicates a RFS4000 wireless controller that's part of the managed network.
	Access Point – This icon lists any Access Point that's part of the managed network.
	*Wireless Client* – This icon defines any wireless client connection within the network.

3 Quick Start

RFS4011 model controllers and NX4500 and NX6500 model service platforms utilize an initial setup wizard to streamline getting on the network for the first time. This wizard configures location, network and WLAN settings and assists in the discovery of Access Points and their connected clients.

3.1 Using the Initial Setup Wizard

Once deployed and powered on, complete the following to get the controller or service platform up and running and access more advanced user interface functions:

1 Connect one end of an Ethernet cable to a port on the front of the controller or service platform, and connect the other end to a computer with a working Web browser.

2 Set the computer to use an IP address between 192.168.0.10 and 192.168.0.250 on the connected port. Set a subnet/network mask of 255.255.255.0.

3 Once the computer has an IP address, point the Web browser to: https://192.168.0.1/. The following login screen displays.

Figure 3-1 *Web UI Login Screen*

4 Enter the default username **admin** in the **Username** field.

5 Enter the default password **admin123** in the **Password** field.

6 Select the preferred language to display for the *graphical user interface* (GUI).

7 Select the **Login** button to load the management interface.

NOTE: When logging in for the first time, you are prompted to change the password to enhance device security in subsequent logins.

NOTE: If you get disconnected when running the wizard, you can connect again and resume the wizard setup.

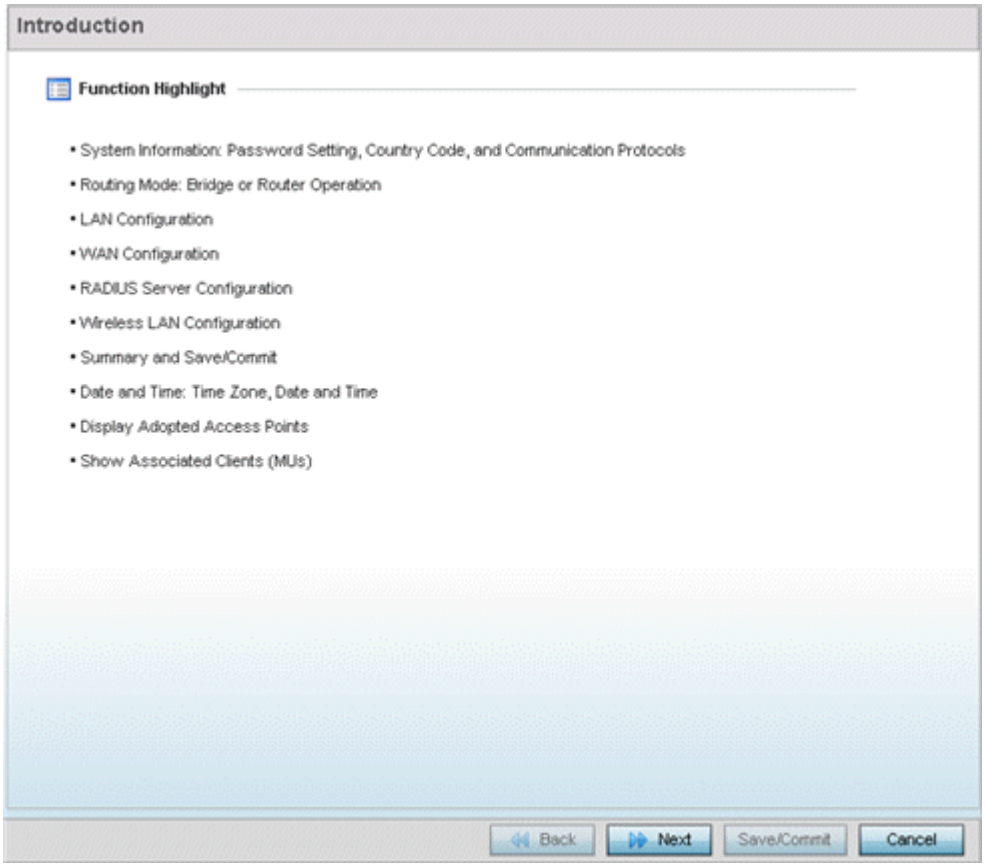


Figure 3-2 *Initial Setup Wizard - Introduction*

The **Introduction** screen displays first (on the right-hand side of the screen), and lists the various actions that can be performed using the setup wizard.

The wizard displays a **Navigation Panel** on the left-hand side of each screen to assist the administrator in assessing which tasks still require completion before the RFS4011, NX4500 or NX6500 can be deployed.

Figure 3-3 *Initial Setup Wizard - Navigation Panel*

A green checkmark to the left of an item in the Navigation Panel defines the task as having its minimum required configuration set correctly. A red X defines a task as still requiring at least one parameter be defined correctly.

8 Select **Save/Commit** within each page to save the updates made to that page's configuration.

9 Select **Next** to proceed to the next page listed in the Navigation Panel.

10 Select **Back** to revert to the previous screen in the Navigation Panel without saving your updates. Selecting **Cancel** closes the wizard without committing any updates.

NOTE: While you can scroll to any page in the Navigation Panel at any time, you cannot complete the wizard until each task in the Navigation Panel has a green checkmark displayed to the left of the task.

11 Select **Next.** The wizard displays the **Networking Mode** screen to define routing or bridging functionality.

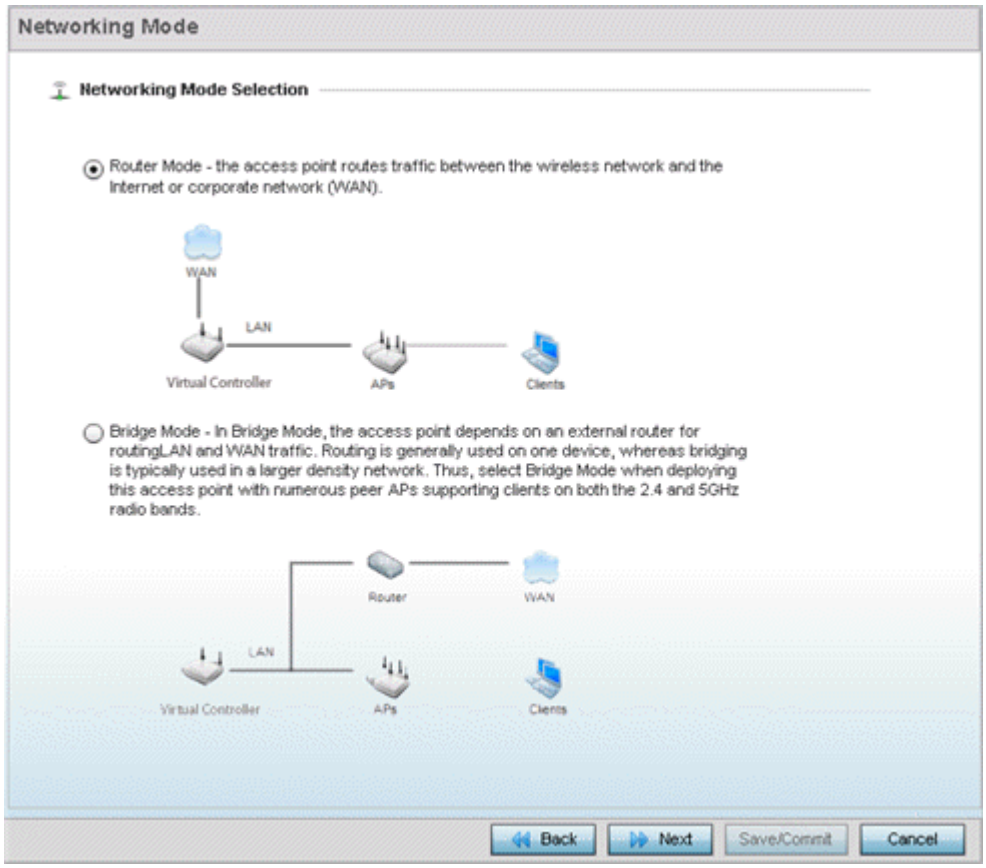


Figure 3-4 *Initial Setup Wizard - Networking Mode*

12 Select one of the following network mode options:

- *Router Mode* - In Router Mode, connected Access Points route traffic between the *local network* (LAN) and the Internet or *external network* (WAN). Router mode is recommended in a deployment supported by just a single Access Point. When Router Mode is selected, an additional WAN screen is available in wizard screen flow to configure interface settings for an Access Point's WAN port.
- *Bridge Mode* - In Bridge Mode, connected Access Points depend on an external router for routing LAN and WAN traffic. Routing is generally used on one device, whereas bridging is typically used in a larger network. Thus, select Bridge Mode when deploying numerous peer Access Points supporting clients on both the 2.4 and 5GHz radio bands.

13 Select **Next**. The wizard displays the **LAN Configuration** screen to set the LAN interface configuration.

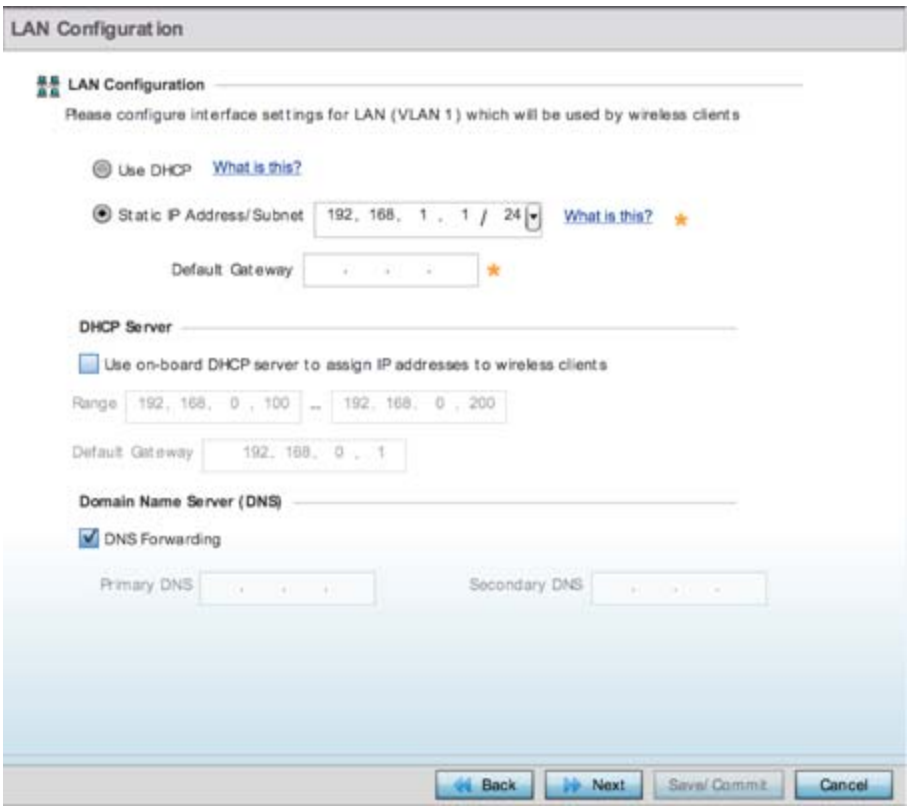


Figure 3-5 *Initial Setup Wizard - LAN Configuration*

14 Set the following DHCP information for the LAN interface:

- *Use DHCP* - Select Use DHCP to enable an automatic network address configuration using local DHCP server resources.
- *Static IP Address/Subnet* - Enter an IP Address and a subnet for the LAN interface. If Use DHCP is selected, this field is not available. When selecting this option, define the following DHCP Server and *Domain Name Server* (DNS) resources, as those fields are enabled on the bottom portion of the screen.
  - *Use on-board DHCP server to assign IP addresses to wireless clients* - Select this option to enable the DHCP server to provide IP and DNS support to requesting clients on the LAN interface.
  - *Range* - Enter a starting and ending IP Address range for client assignments on the LAN interface. Avoid assigning IP addresses from x.x.x.1 - x.x.x.10 and x.x.x.255, as they are often reserved for standard network services. This is a required parameter.
  - *Default Gateway* - Define a default an address for use with the default gateway. This is a required parameter.
- *DNS Forwarding* - Select this option to allow a DNS server to translate domain names into IP addresses. If this option is not selected, a primary and secondary DNS resource must be specified. DNS forwarding is useful when a request for a domain name is made but the DNS server, responsible for converting the name into its corresponding IP address, cannot locate the matching IP address.
  - Primary DNS - Enter an IP Address for the main Domain Name Server providing DNS services for the LAN interface.
  - Secondary DNS - Enter an IP Address for the backup Domain Name Server providing DNS services for the LAN interface.

15 Select **Next**. If Router was selected as the Access Point mode the wizard displays the **WAN Configuration** screen. If Bridge was selected, the wizard proceeds to the **Wireless LAN Setting** screen.

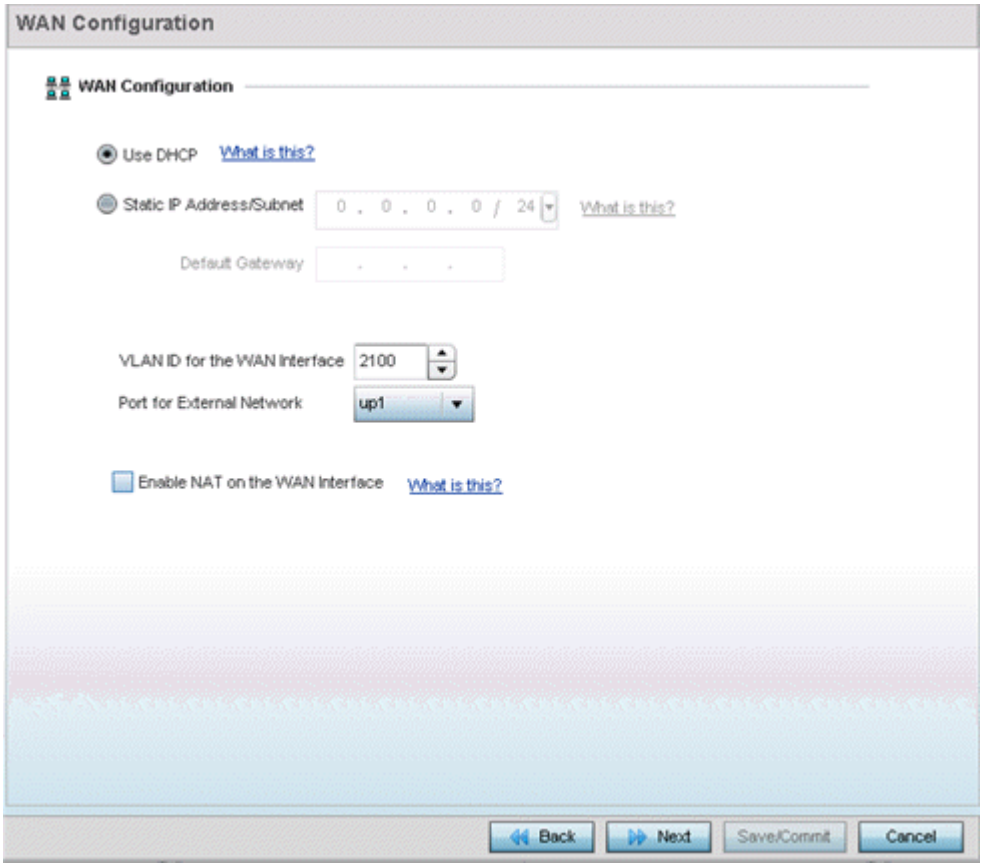


Figure 3-6 *Initial Setup Wizard - WAN Configuration*

16 Set the following DHCP and Static IP Address/Subnet information to define how traffic is routed between the *local network* (LAN) and the Internet or *external network* (WAN).

- *Use DHCP* - Select Use DHCP to enable an automatic network address configuration using local DHCP server resources.
- *Static IP Address/Subnet* - Enter an IP Address/Subnet and gateway for the WAN interface. These are required fields
  - *Default Gateway* -Enter an IP Address for the default gateway on the WAN interface. If Use DHCP is enabled, this field is not configurable.
  - *VLAN ID for the WAN Interface* - Set the VLAN ID (virtual interface) to associate with the physical WAN Interface. The default setting is VLAN 2100.
  - *Port for External Network* - Select the physical port connected to the WAN interface. The list of available ports varies based on the RFS4011 controllers or NX4500 and NX6500 service platform model.
  - *Enable NAT on the WAN Interface* - Select the option to allow traffic to pass between WAN and LAN interfaces.

17 Select **Next**. The wizard displays the **Wireless LAN Setting** screen to define up to four WLAN configurations for the controller or service platform.

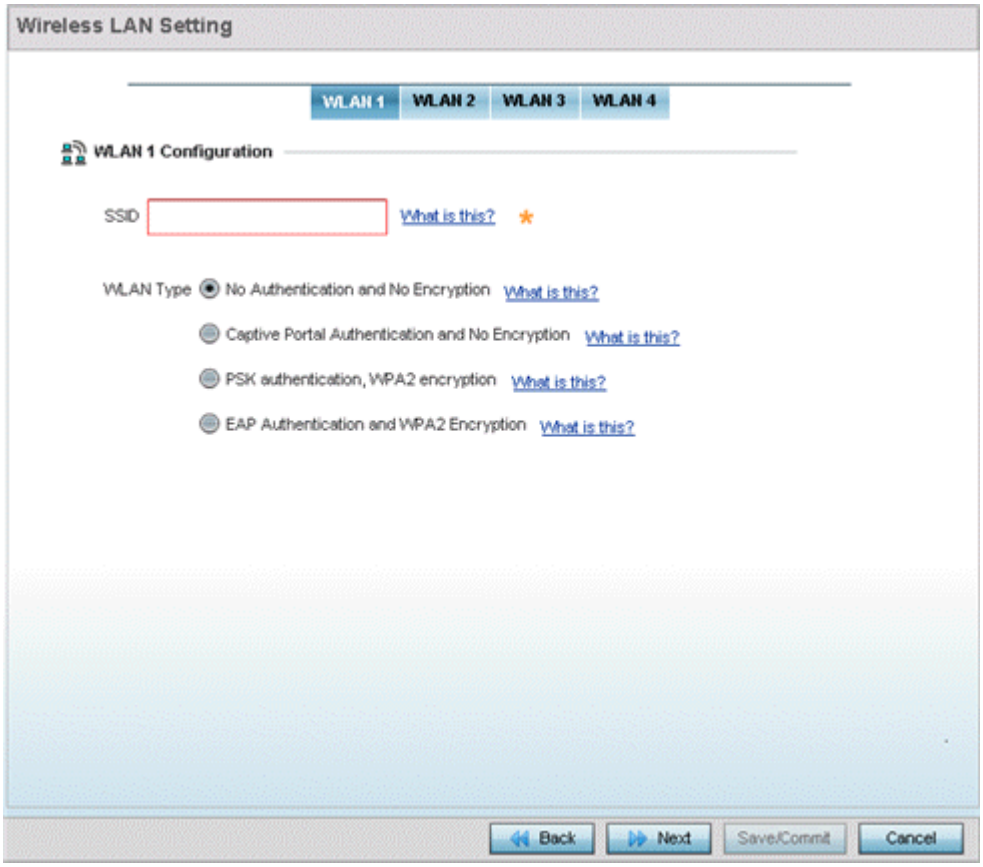


Figure 3-7 *Initial Setup Wizard - Wireless LAN Settings*

18 Set the following parameters for up to four WLAN configurations:

- *SSID* - Enter or modify the *Services Set Identification* (SSID) associated with the WLAN. The WLAN name is auto-generated using the SSID until changed by the administrator. The maximum number of characters is 32. Do not use any of these characters (< > | " & \ ? ,).
- *WLAN Type* - Select a basic authentication and encryption scheme for the WLAN. Available options include:
  - *No Authentication and No Encryption* (provides no security at all)
  - *Captive Portal Authentication and No Encryption*
  - *PSK authentication, WPA2 encryption*
  - *EAP Authentication and WPA2 Encryption*

19 Select **Next.** The wizard displays the **System Information** screen to set device deployment, administrative contact and system time information. The system time can either be set manually or be supplied by a dedicated *Network Time Protocol (NTP)* resource.

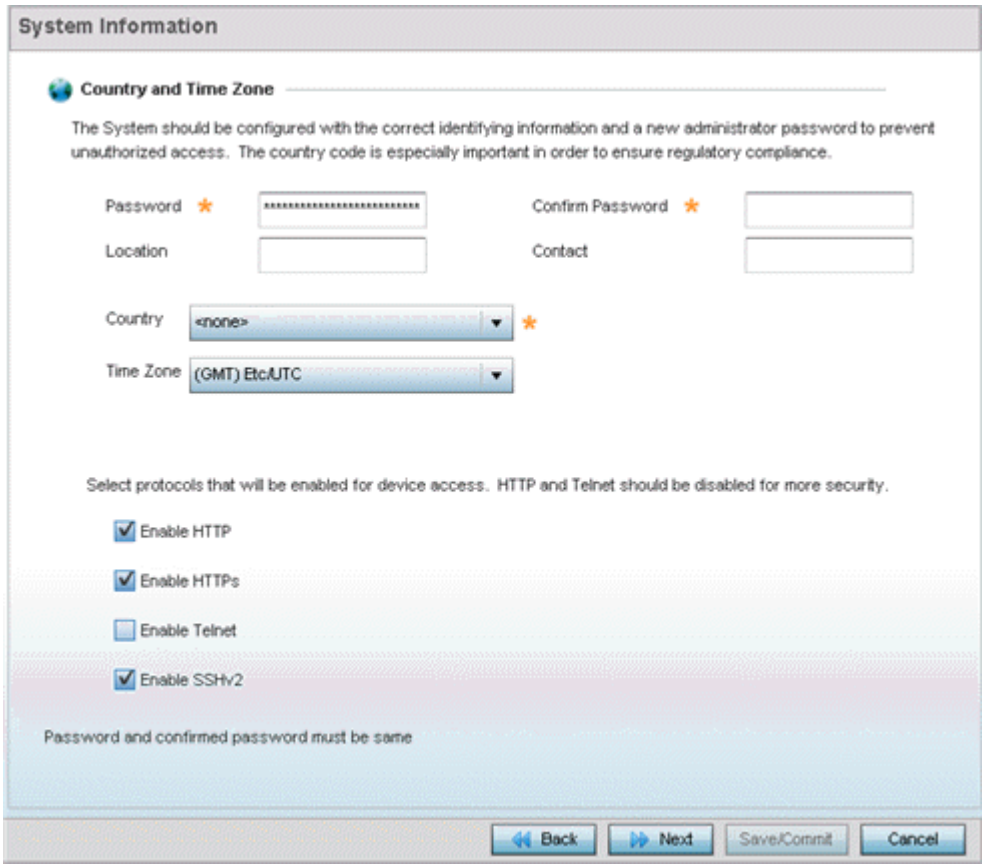


Figure 3-8 *Initial Setup Wizard - System Information*

20 Refer to the **Country and Time Zone** field to set the following deployment information:

- *Password* - Enter and confirm a system password used to login into the controller or service platform on subsequent login attempts.Changing the default system password is strongly recommended to secure the proprietary configuration data maintained on the controller or service platform.
- *Location* - Define the location of the controller or service platform deployment.
- *Contact* - Specify the contact information for the administrator. The credentials provided should accurately reflect the individual responding to service queries.
- *Country* - Select the country where the controller or service platform is deployed. The controller or service platform prompts for the correct country code on the first login. A warning message also displays stating an incorrect country setting may result in illegal radio operation. Selecting the correct country is central to legal operation. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted.
- *Time Zone* - Set the time zone where the controller or service platform is deployed. This is a required parameter. The setting should be complimentary with the selected deployment country.

Refer to the **Select protocols that will be enabled for device access** area and enable those controller or service platform interfaces for accessing the controller or service platform. HTTP and Telnet are considered relatively insecure and only should be enabled is necessary.

21 Select **Next.** The wizard displays the **Summary and Commit** screen to summarize the screens (pages) and settings updated using the wizard.

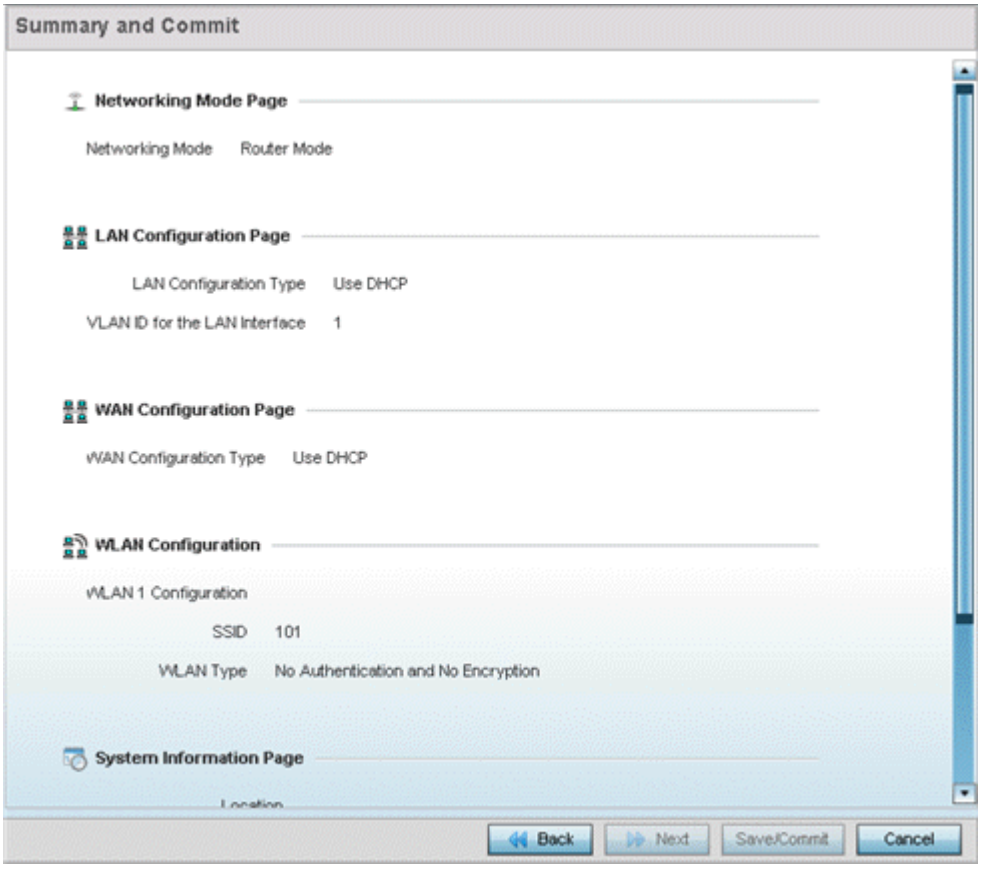


Figure 3-9 *Initial Setup Wizard - Summary and Commit*

No user intervention or additional settings are required within this screen. Its an additional means of validating the Access Point's updated configuration before it's deployed. However, if a screen displays settings not intended as part of the initial configuration, the any screen can be selected again from within the Navigation Panel and its settings modified accordingly.

22 If the configuration displays as intended, select **Save/Commit** to implement these settings to the controller or service platform configuration. If additional changes are warranted based on the summary, either select the target page from the Navigational Panel, or use the **Back** and **Next** buttons to scroll to the target screen.

4 Dashboard

The dashboard enables administrators to review and troubleshoot network device operation. Additionally, the dashboard allows an administrative review of the network's topology, an assessment of network's component health and a diagnostic review of device performance.

By default, the **Dashboard** displays the **System** screen, which is the top level in the device hierarchy. To view information for **Access Points**, **RF Domains** or **Controllers** select the associated item in the tree.

For more information, refer to the following:

- *Summary*
- *System Screen*
- *RF Domain Screen*
- *Controller*
- *Access Point Screen*
- *Network View*
- *Debug Wireless Clients*
- *Debug Captive Portal Clients*
- *Packet Capture*

4.1 Summary

The **Dashboard** displays information organized by device association and inter-connectivity between the connected Access Points and wireless clients.

1 To review dashboard information, select **Dashboard**.

2 Select **Summary** if it's not already selected by default.
The Dashboard displays the **Health** tab by default.

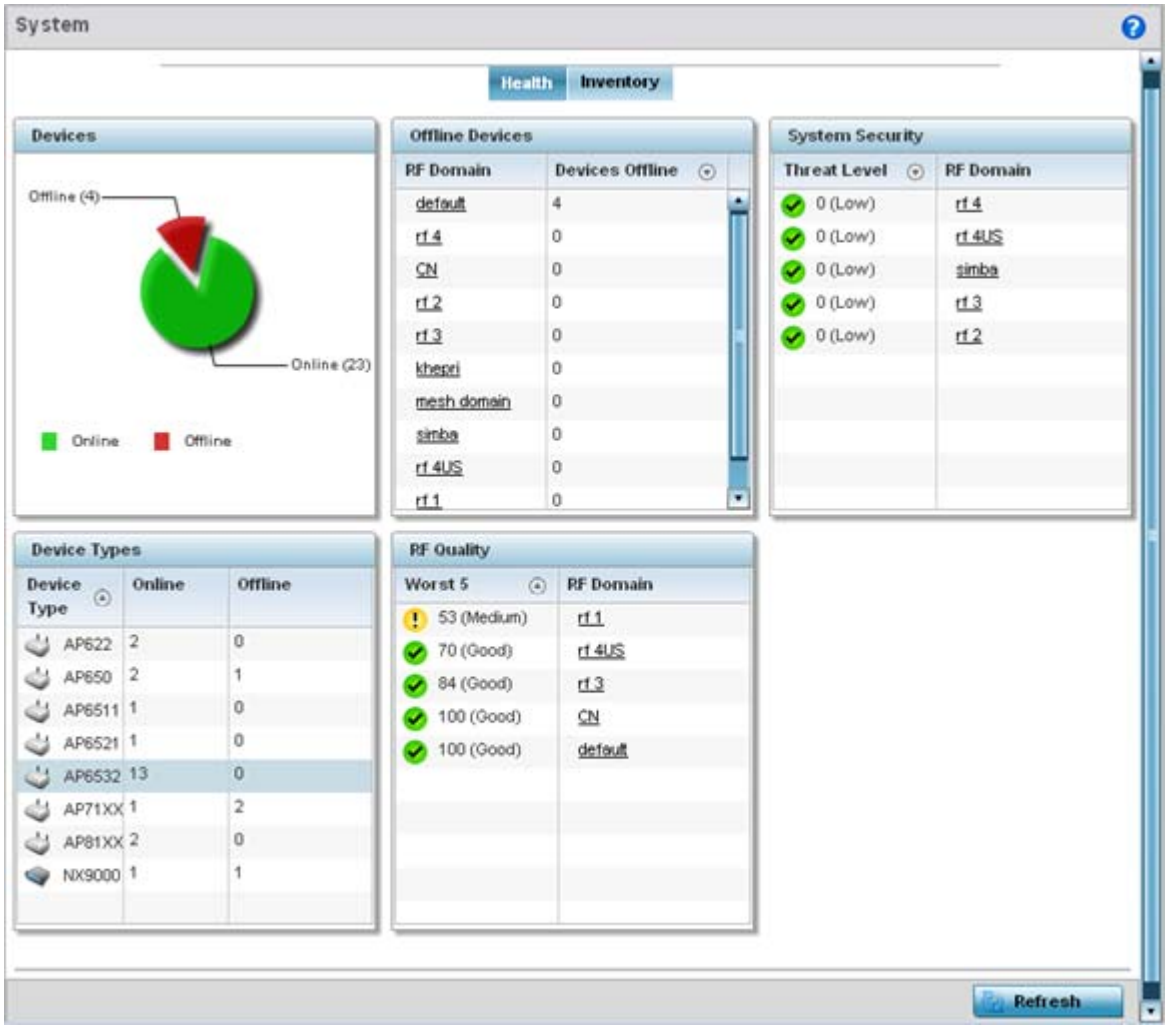


Figure 4-1 *System Dashboard screen - Health tab*

4.1.1 Device Listing

Summary

The device menu displays information as a hierarchical tree, comprised of system, controller/service platform and Access Point connection relationships.

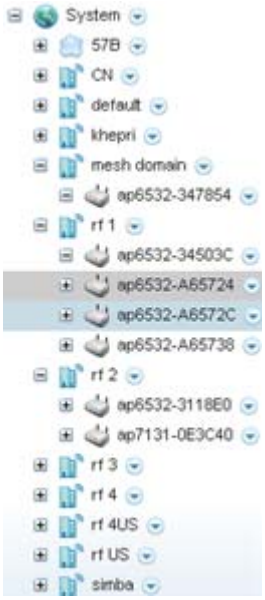


Figure 4-2 *Dashboard Menu Tree*

The **Search** option, at the bottom of the screen, enables you to filter (search amongst) RF Domains. The **By** drop-down menu refines the search. You can further refine a search using the following:

- *Auto* – The search is automatically set to device type.
- *Name* – The search is performed for the device name specified in the **Search** text box.
- *WLAN* – The search is performed for the WLAN specified in the **Search** text box.
- *IP Address* – The search is performed for the IP Address specified in the **Search** text box.
- *MAC Address* – The search is performed for the MAC Address specified in the **Search** text box.

4.2 System Screen

The **System** screen displays system-wide network status. The screen is partitioned into the following tabs:

- *Health* – The Health tab displays information about the state of the WiNG device managed system.
- *Inventory* – The Inventory tab displays information on the physical devices managed within the WiNG wireless network.

4.2.1 Health

Health

The **Health** tab displays device performance status for managed devices, and includes their RF Domain memberships.

To assess system health:

1 Select **Dashboard**.

2 Select **Summary** if it's not already selected by default.

3 Select **System**. The **Health** tab displays by default.

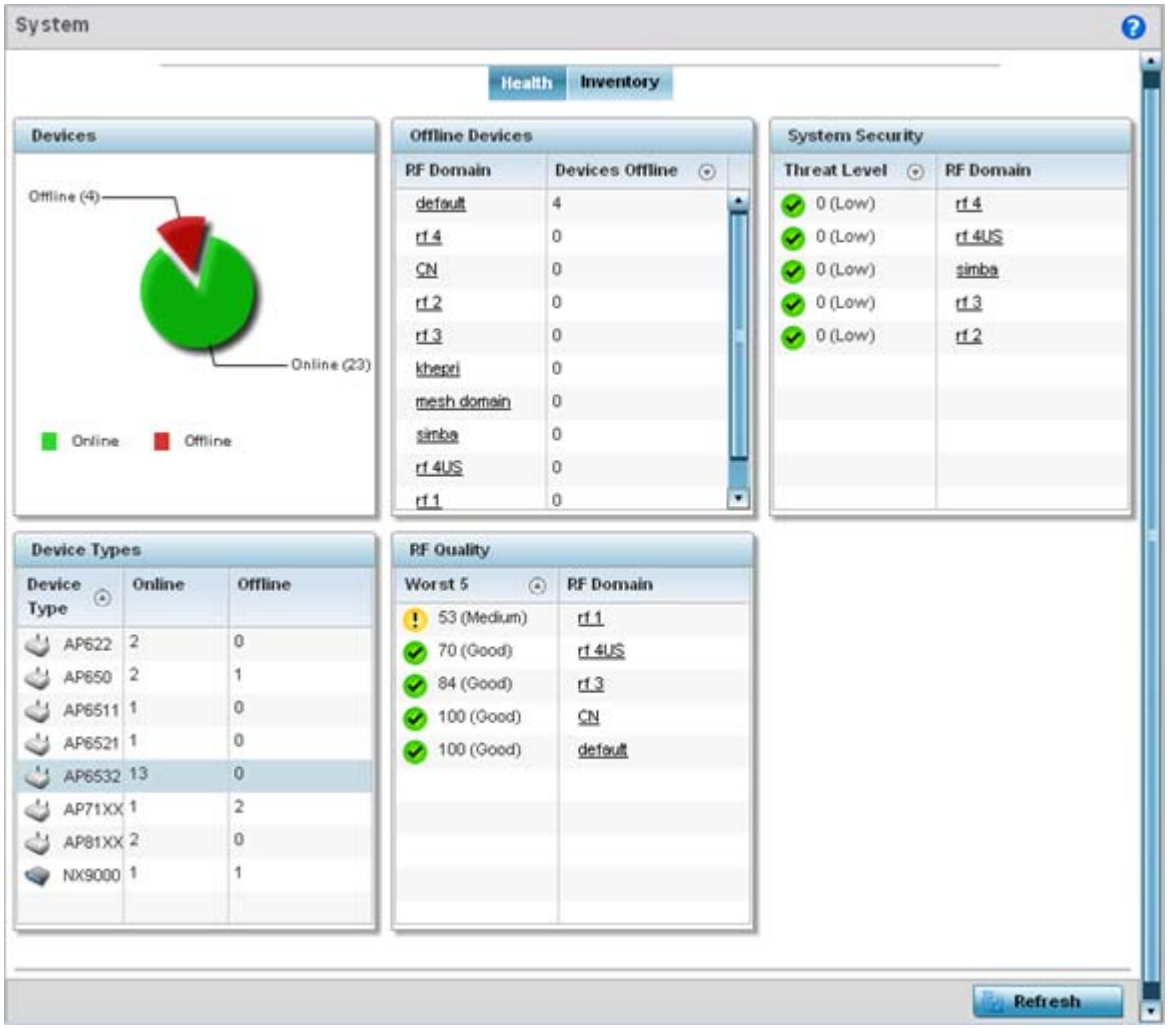


Figure 4-3 *System Dashboard screen - Health tab*

The **Health** screen is partitioned into the following fields:

- The **Devices** field displays a ratio of offline versus online devices within the system. The information is displayed in pie chart format to illustrate device support ratios.
- The **Device Type** field displays a numerical representation of the different controller, service platform and Access Point models in the current system. Their online and offline device connections are also displayed. Does this device distribution adequately support the number and types of Access Point radios and their client load requirements.
- The **Offline Devices** field displays a table of supported RF Domains within the system, with each RF Domain listing the number offline devices within that RF Domain. Listed RF Domains display as individual links that can be selected to RF Domain information in greater detail.
- The **RF Quality Index** displays RF quality per RF Domain. It's a measure of the overall effectiveness of the RF environment displayed in percentage. It's a function of the connect rate in both directions, retry rate and error rate.

The RF Quality field displays an average quality index supporting each RF Domain. The table lists the bottom five (5) RF quality values for RF Domains. Listed RF Domains display as individual links that can be selected to RF Domain information in greater detail. Use this diagnostic information to determine what measures can be taken to improve radio performance in respect to wireless client load and the radio bands supported.

The quality is measured as:

- 0-20 – *Very poor quality*

- 20-40 – *Poor quality*
- 40-60 – *Average quality*
- 60-100 – *Good quality*

The **System Security** field displays RF intrusion prevention stats and their associated threat level. The greater the number of unauthorized devices, the greater the associated threat level. The System Security field displays a list of up to five RF Domains in relation to the number of associated wireless clients. The RF Domains appear as links that can be selected to display RF Domain information in greater detail.

4.2.2 Inventory

System Screen

The system screen's **Inventory** tab displays granular data on specific devices supported within the network. The screen provides a complete overview of the number and state WiNG managed devices. Information is displayed in easy to read tables and graphs. This screen also provides links for more detailed information.

To assess the system inventory:

1 Select **Dashboard**.

2 Select **Summary** if it's not already selected by default.

3 Select **System**.

4 Select the **Inventory** tab.

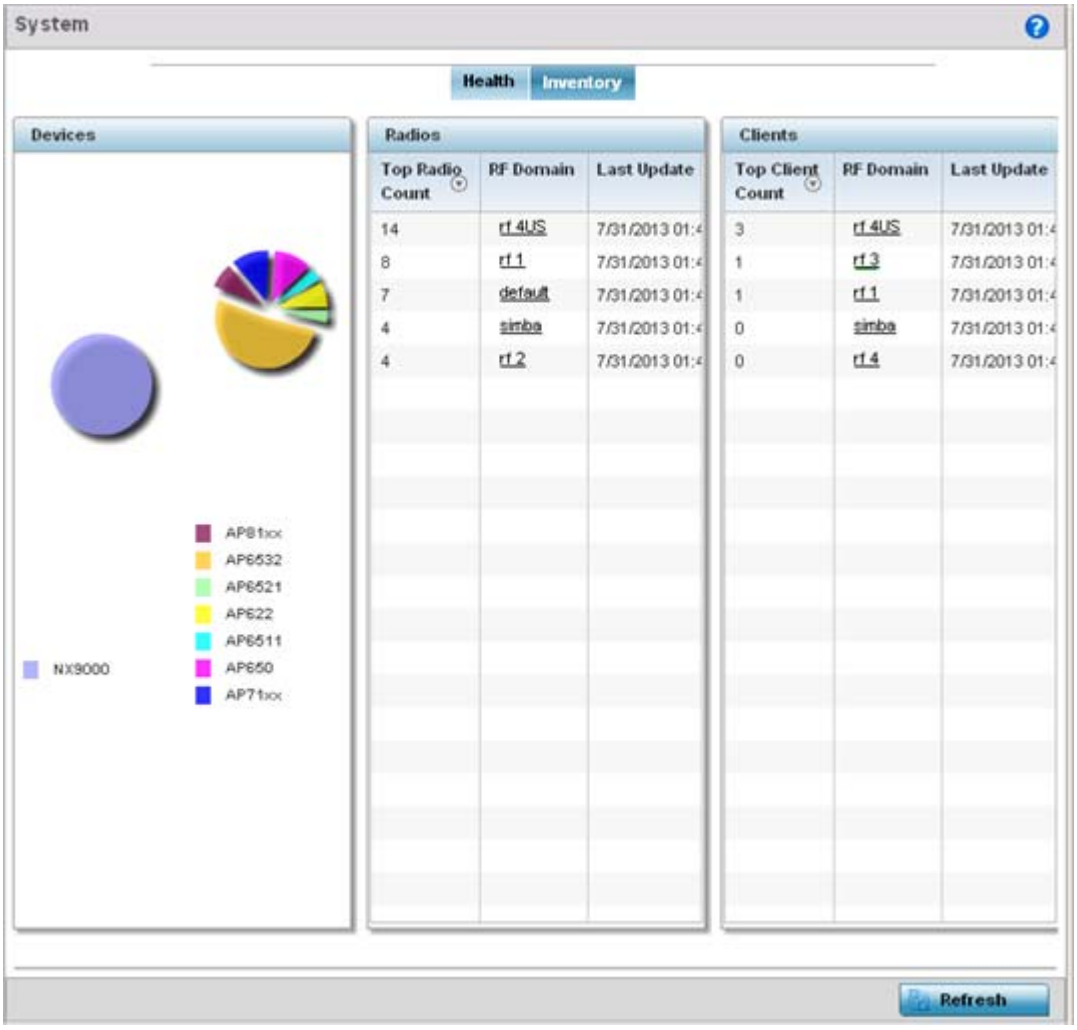


Figure 4-4 *System screen - Inventory tab*

The information within the Inventory tab is partitioned into the following fields:

- The **Devices** field displays a ratio of peer controllers and service platforms as well as their managed Access Point radios. The information is displayed in pie chart format. The Device Type field displays a numerical representation of the different controller models and connected Access Points in the current system.
- The **Radios** field displays top performing radios, their RF Domain memberships and a status time stamp. RF Domain information can be selected to review RF Domain membership information in greater detail.Information in the Radio area is presented in two tables. The first lists the total number of Radios managed by this system, the second lists the top five RF Domains in terms of the number of available radios.Information in the Radio area is presented in two tables. The first lists the total number of Radios managed by this system, the second lists the top five RF Domains in terms of the number of available radios.
- The wireless **Clients** field lists the top five RF Domains with the highest total number of clients managed by connected devices in this system. RF Domain information can be selected to review RF Domain membership information in greater detail. Select **Refresh** as needed update the screen to its latest values.

4.3 RF Domain Screen

RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building or site. Each RF Domain contains policies that can determine a Smart RF or WIPS configuration.RF Domains enable administrators to override WLAN SSID name and VLAN assignments. This enables the deployment of a global WLAN across multiple sites and unique SSID name or VLAN assignments to groups of Access Points servicing the global WLAN. This WLAN override technique eliminates the requirement for defining and managing a large number of individual WLANs and profiles.

A configuration contains (at a minimum) one default RF Domain and can optionally use additional user defined RF Domains:

- *Default RF Domain* - Automatically assigned to each controller or service platform and associated Access Point by default.
- *User Defined RF Domains* - Created by administrators and manually assigned to individual controller or service platforms, but can be automatically assigned to Access Points using adoption policies.

Each controller and service platform is assigned to only one RF Domain at a time. However, a user defined RF Domain can be assigned to multiple controllers or service platforms as required. User defined RF Domains can be manually assigned or automatically assigned to Access Points using an AP provisioning policy.

The **RF Domain** screen displays system-wide network status. The screen is partitioned into the following tabs:

- *RF Domain Health* – The Health tab displays information about the state of the RF Domain and network performance as tallied from its collective device members.
- *RF Domain Inventory* – The Inventory tab displays information on the physical devices comprising the RF Domain.

4.3.1 RF Domain Health

The **Health** tab displays the status of the RF Domain's device membership.

To assess the RF Domain health:

1 Select **Dashboard**.

2 Select **Summary** if it's not already selected by default.

3 Expand the **System** node to display RF Domains.

4 Select a **RF Domain**. The **Health** tab displays by default.

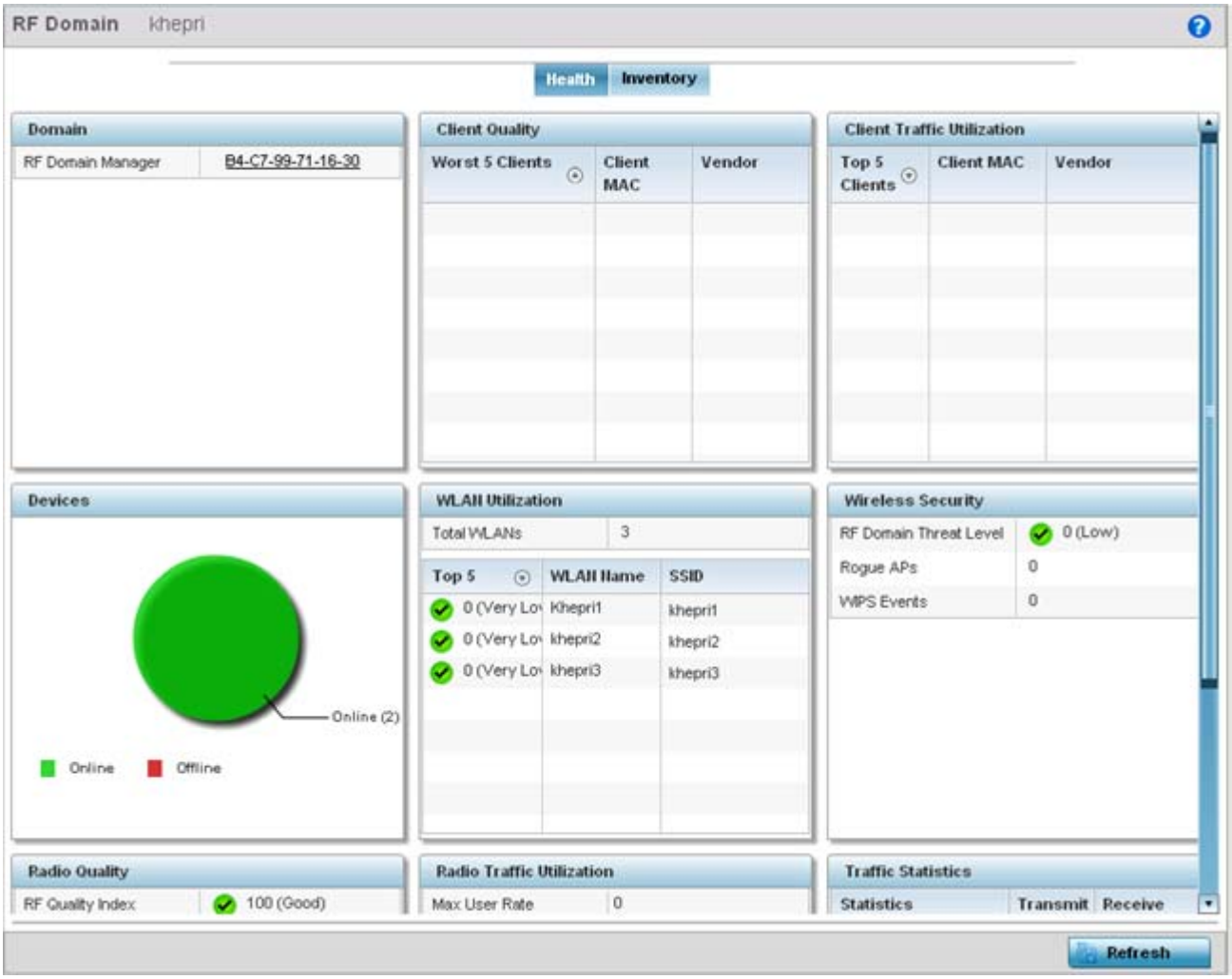


Figure 4-5 *RF Domain screen - Health tab*

Refer to the following RF Domain health information for member devices:

- The **Domain** field lists the RF Domain manager reporting utilization statistics. The MAC address displays as a link that can be selected to display RF Domain information in at more granular level. A RF Domain manager can retain and store new firmware images for RF Domain member Access Points.
- The **Devices** field displays the total number of devices and the status of the devices in the network as a graph. This area displays the total device count managed by this device and their status (online vs. offline) as a pie graph.
- The **Radio Quality** table displays a table of RF quality on a per radio basis. It is a measure of the overall effectiveness of the RF environment displayed in percentage. It is a function of the transmit retry rate in both directions and the error rate. This area of the screen displays the average quality index across all the defined RF Domain on the wireless controller. The table lists worst five of the RF quality values of all the radios defined on the wireless controller. The quality is measured as:
  - 0-20 - *Very poor quality*
  - 20-40 - Poor quality
  - 40-60 - *Average quality*
  - 60-100 - *Good quality*

5 Select a **Radio Id** to view all the statistics for the selected radio in detail.

- The Client Quality table displays RF quality for the worst five performing clients.It is a function of the transmit retry rate in both directions and the error rate. This area of the screen displays the average quality index across all the defined RF Domain on the wireless controller. The quality is measured as:
  - 0-20 - *Very poor quality*
  - 20-40 - Poor quality
  - 40-60 - *Average quality*
  - 60-100 - *Good quality*

6 Select a client to view its statistics in greater detail.

- **WLAN Utilization** displays how efficiently the WLANs are used. Traffic utilization is defined as the percentage of current throughput relative to the maximum possible throughput for the WLAN. The total number of WLANs is displayed above the table. The table displays a list of the top five WLANs in terms of overall traffic utilization. It displays the utilization level names, WLAN name and SSIDs for each of the top five WLANs.
- **Radio Traffic Utilization** displays how efficiently the RF medium is used. Traffic utilization is defined as the percentage of current throughput relative to the maximum possible throughput for the RF Domain. The Traffic Index area displays an overall quality level for radio traffic and the Max User Rate displays the maximum data rate of associated radios. The table displays a list of the top five radios in terms of overall traffic utilization quality. It displays the radio names, MAC Addresses and radio types for each of the top five radios.
- **Client Traffic Utilization** displays how efficiently the RF medium is utilized for connected clients. Traffic utilization is defined as the percentage of current throughput relative to the maximum possible throughput for the clients in the RF Domain. The table displays a list of the top five performing clients in respect to overall traffic utilization. It displays the client names, MAC Addresses and vendor for each of the top five clients.
- **Wireless Security** displays the overall threat index for the system. This index is based on the number of Rogue/Unsanctioned APs and Wireless Intrusion Protection System (WIPS) events detected. The index is in the range 0 - 5 where 0 indicates there are no detected threats. An index of 5 indicates a large number of intrusion detection events or rogue/unsanctioned APs detected.
- **Traffic Statistics** include transmit and receive values for Total Bytes, Total Packets, User Data Rate, Broadcast/Multicast Packets, Management Packets, Tx Dropped Packets and Rx Errors.

4.3.2 RF Domain Inventory

Refer to the following RF Domain inventory data collected by member controllers, service platforms or Access Points:

To review the RF Domain inventory:

1 Select **Dashboard**.

2 Select **Summary** if it's not already selected by default.

3 Expand the **System** node to display RF Domains.

4 Select a **RF Domain**.

5 Select the **Inventory** tab.

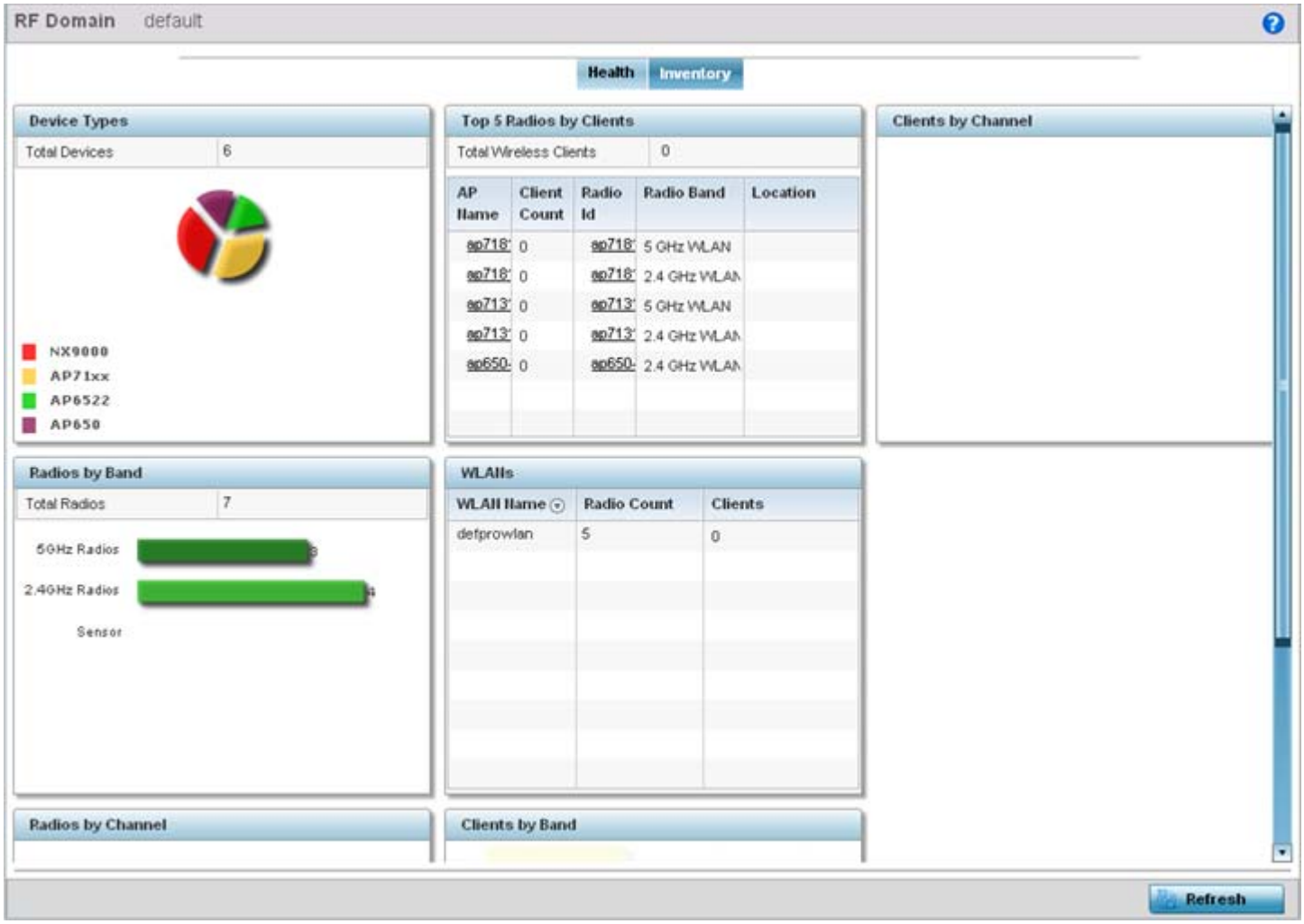


Figure 4-6 *RF Domain screen - Inventory tab*

- The **Inventory** tab displays information on the devices managed by RF Domain member devices in the controller, service platform or Access Point managed network. The Inventory screen enables an administrator to overview of the number and state of the devices in the selected RF Domain. Information is displayed in easy to read tables and graphs.
- The **Device Types** table displays the devices types populating the RF Domain. The Device Type area displays an exploded pie chart that displays the type of device and their numbers in the RF Domain.
- The **Radios by Band** table displays a bar graph of RF Domain member device radios classified by their radio band or sensor dedication. Review this information to assess whether RF Domain member radios adequately support client device traffic requirements.
- The **Radios by Channel** table displays pie charts of the different channels utilized by RF Domain member radios. These dedicated channels should be as segregated as possible from one another to avoid interference. If too many radios are utilizing a single channel, consider off-loading radios to non utilized channels to improve RF Domain performance.
- The **Top 5 Radios by Clients** table displays a list of radios with the highest number of clients. This list displays the radio IDs as links that can be selected to display individual radio information in greater detail.
- The **WLANs** table displays a list of WLANs utilized by RF Domain member devices. The table is ordered by WLAN member device radio count and their number of connected clients. Use this information to assess whether the WLAN is overly populated by radios and clients contributing to congestion.

- The **Clients by Band** table displays the radio band utilization of connected RF Domain member clients. Assess whether the client band utilization adequately supports the intended radio deployment objectives of the connected RF Domain member Access Point radios.
- The **Clients of Channel** table displays a bar-graph of wireless clients classified by their frequency. Information for each channel is further classified by their 802.11x band. In the 5GHz channel, information is displayed classified under 802.11a and 802.11an bands. In the 2.4 GHz channel, information is displayed classified under 802.11b, 802.11bg, and 802.11bgn band.

4.4 Controller

The **Wireless Controller** screen displays system collected network status for controllers and service platforms. The screen is partitioned into two tabs:

- *Controller Health* – The Health tab displays information about the state of the controller or service platform managed wireless network.
- *Controller Inventory* – The Inventory tab displays information on the physical devices managed by the controller or service platform.

NOTE: A T5 controller can also be selected from the dashboard's controller level to display a set of unique T5 dashboard screens. A T5 controller uses a different operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. For information on enabling controller adoption of external devices (for T5 support specifically) refer to, *Adoption Overrides (Controllers Only) on page 5-48*.

4.4.1 Controller Health

To assess the controller or service platform's network health:

1 Select **Dashboard**.

2 Select **Summary** if it's not already selected by default.

3 Expand the **System** node to display RF Domains.

4 Select and expand a **RF Domain** to expose its member controllers or service platforms.

5 Select a controller or service platform. The **Health** tab display by default.

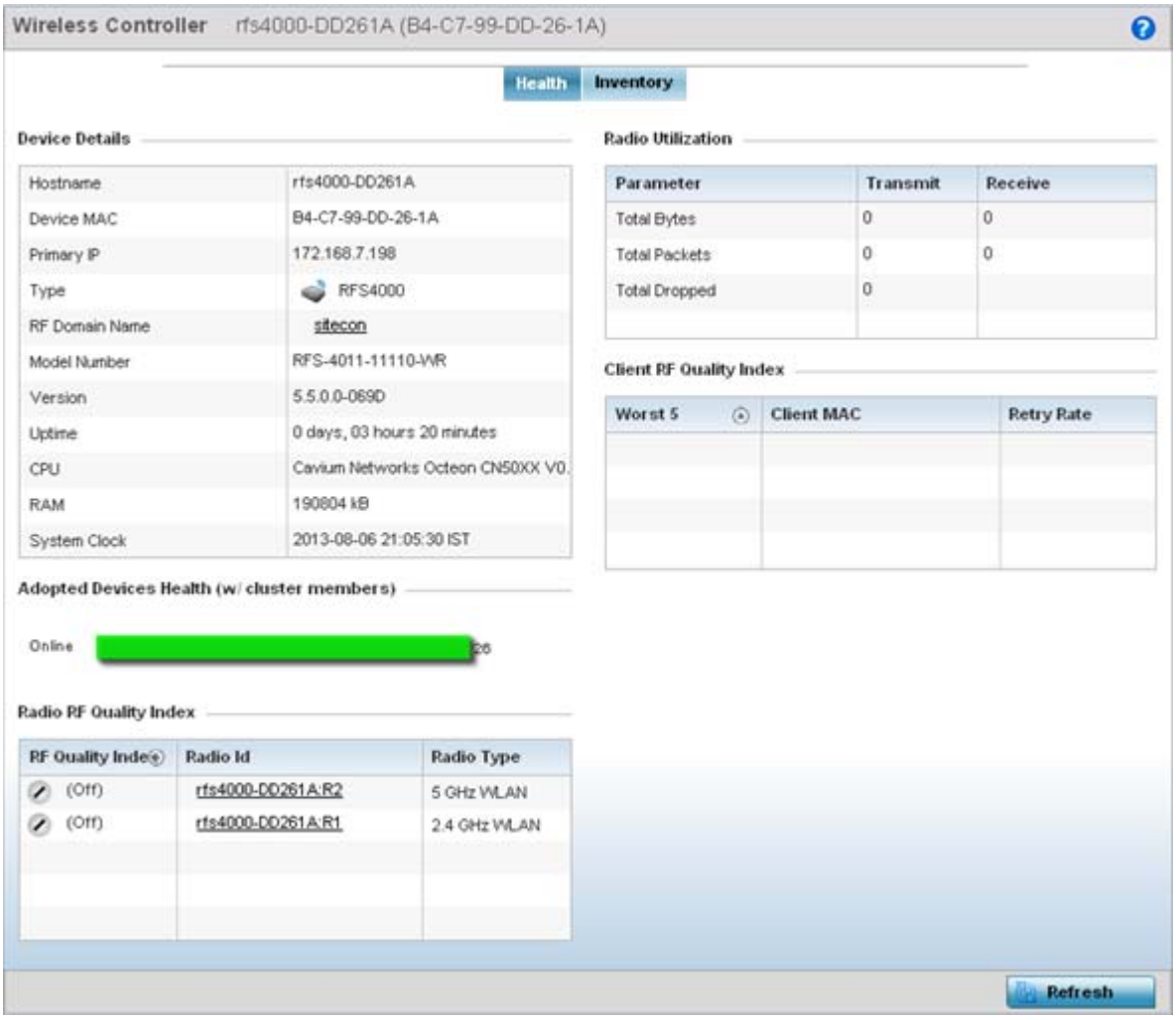


Figure 4-7 *Wireless Controller screen - Health tab*

Refer to the **Device Details** table for information about the selected controller or service platform The following information is displayed:

- **Hostname** - Lists the administrator assigned name of the controller or service platform.
- **Device MAC** - Lists the factory encoded MAC address of the controller or service platform.
- **Type** - Indicates the type of controller or service platform. An icon representing the RFS controller or NX service platform device type is displayed along with the model number.
- **RF Domain Name** - Lists the RF Domain to which the controller or service platform belongs. The RF Domain displays as a link that's selectable to display RF Domain data in greater detail.
- **Model Number** - Lists the model number and hardware SKU information of the selected controller or service platform to refine its intended deployment region.
- **Version** - Lists the firmware version currently running on the controller or service platform. Compare this version against the version currently on the support site to ensure the controller or service platform has the latest feature set available.
- **Uptime** - Displays the duration the controller or service platform has been running since it was last restarted.
- **CPU** - Displays the CPU installed on this controller or service platform.
- **RAM** - Displays the amount of RAM available for use in this system.
- **System Clock** - Displays the current time set on the controller or service platform.

The **Adopted Devices Health (w/ cluster members)** displays a graph of Access Points in the system with the available Access Points in green and unavailable Access Points in red.

The **Radio RF Quality Index** provides a table of RF quality on a per radio basis. It is a measure of the overall effectiveness of the RF environment displayed in percentage. It is a function of the connect rate in both directions, the retry rate and the error rate. The screen displays the average quality index within the Access Point single radio. The table lists bottom five (5) of the RF quality values by Access Point radio. The quality is measured as:

- 0-20 - *Very poor quality*
- 20-40 - *Poor quality*
- 40-60 - *Average quality*
- 60-100 - *Good quality*

6 Select a radio Id to view statistics in greater detail.

The **Radio Utilization** table displays how efficiently the RF medium is used. Radio utilization is defined as the percentage of current throughput relative to the maximum possible throughput for the radio. The Radio Utilization table displays the Access Point radios in terms of the number of associated wireless clients and the percentage of utilization. It also displays a table of packets types transmitted and received.

The **Client RF Quality Index** displays a table of RF quality on a per client basis. It is a measure of the overall effectiveness of the RF environment displayed in percentage. It is a function of the connect rate in both directions, the retry rate and the error rate. This area of the screen displays the average quality index for a client. The table lists bottom five (5) of the RF quality values by a client. Quality is measured as:

- 0-20 - *Very poor quality*
- 20-40 - *Poor quality*
- 40-60 - *Average quality*
- 60-100 - *Good quality*

7 Select a client MAC to view all the statistics for the selected client in greater detail.

4.4.2 Controller Inventory

The **Inventory** tab displays information for the devices managed by the system. This screen enables a system administrator to have a complete overview of the number and state of managed devices. Information is displayed in easy to read tables and graphs. The Inventory screen also provides links for the system administrator to get more detailed information.

To assess the controller or service platform inventory:

1 Select **Dashboard**.

2 Select **Summary** if it's not already selected by default.

3 Expand the **System** node to display RF Domains.

4 Select and expand a **RF Domain** to expose its member controllers or service platforms.

5 Select a controller or service platform.

6 Select the **Inventory** tab.

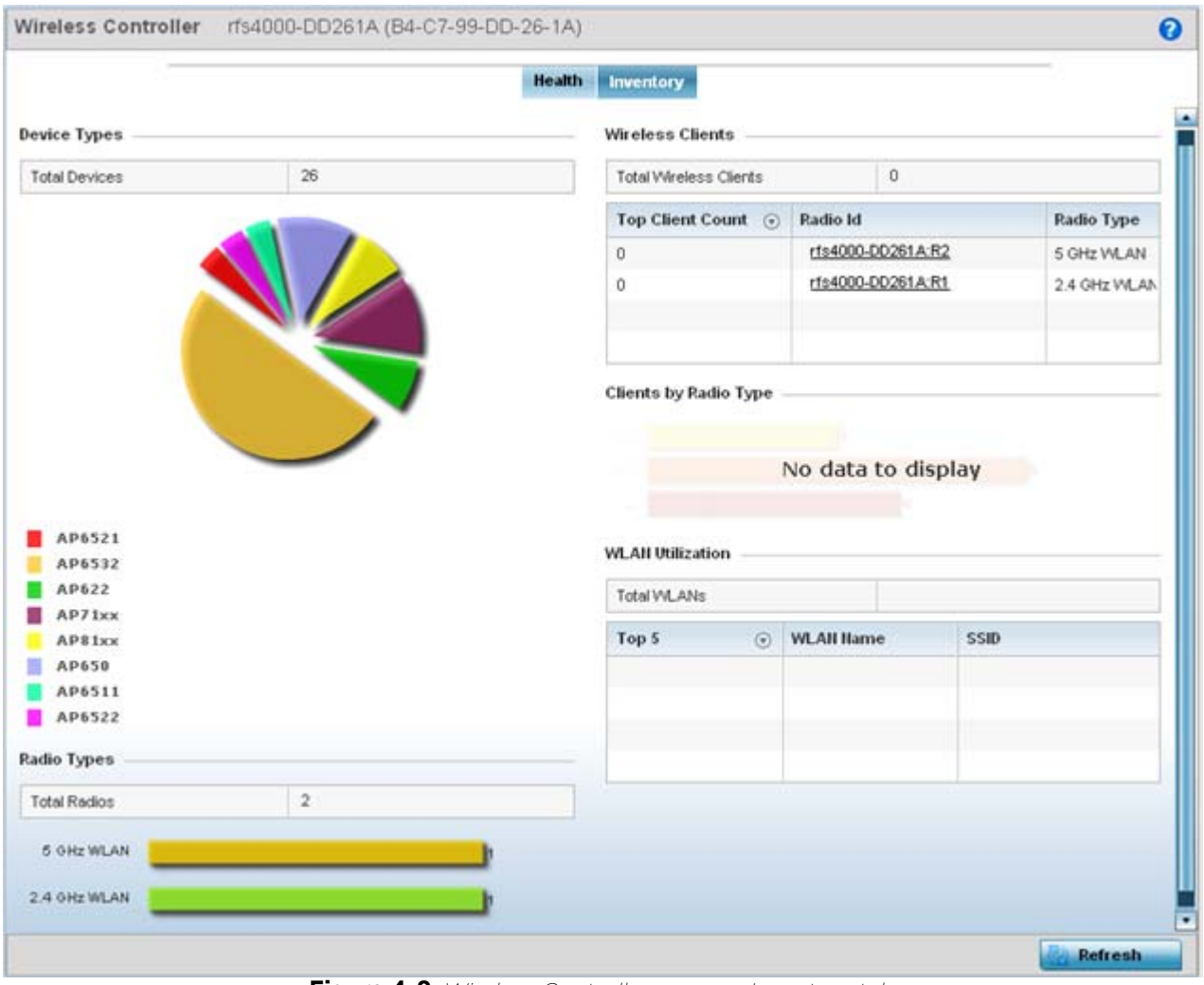


Figure 4-8 *Wireless Controller screen - Inventory tab*

The **Inventory** tab displays information on the devices managed by the controller or service platform. The Inventory screen enables an administrator to overview of the number and state of controller or service platform managed devices and their utilization. Refer to the following Inventory data:

- The **Device Types** field displays a ratio of devices managed by this controller or service platform in pie chart format. The Device Type area displays an exploded pie chart that displays the type of device and their numbers in the current system.
- The **Radios Type** field displays the total number of radios managed by this controller or service platform. The graph lists the number of radios in both the 2.4 GHz and 5 GHz radio bands.
- The **Wireless Clients** table lists clients managed by this controller or service platform by connected client count. Information is presented in two (2) tables and a graph. The first table lists the total number of clients managed by the listed controller or service platform. The second lists the top five (5) radios in terms of the number of connected clients. The graph just below the table lists the number of clients by radio type.
- The **WLAN Utilization** table displays utilization statistics for controller or service platform WLAN configurations. Information displays in two tables. The first table lists the total number of WLANs managed by this system. The second table lists the top five (5) WLANs in terms of the usage percentage along with the name and network identifying SSID.

4.4.3 T5 Controller Dashboard

A T5 controller can be selected from the dashboard's controller level to display a set of unique T5 dashboard screens. A T5 controller uses a different operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices.

To review a T5's controller dashboard:

1 Select **Dashboard**.

2 Select **Summary** if it's not already selected by default.

3 Expand the **System** node to display RF Domains.

4 Select and expand a **RF Domain** to expose its member controllers or service platforms.

5 Select a T5 controller from amongst the devices listed at the dashboard's controller level. T5 devices will not appear at any other level in the dashboard's device tree.

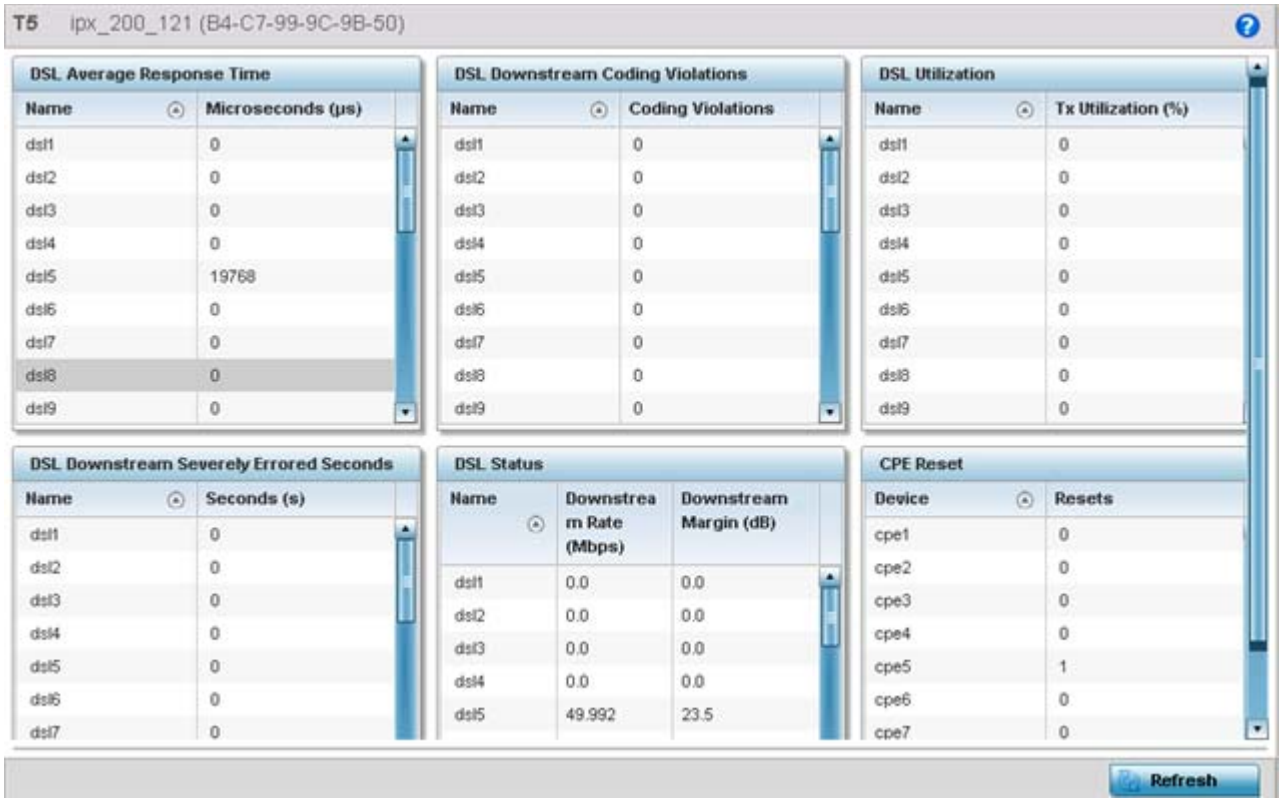


Figure 4-9 *T5 Dashboard tab*

6 Refer to the following T5 specific dashboard stats to assess whether a CPE's DLS connection is problematic and has excessive device rests (rendering the T5 device temporarily offline).

The *Customer Premises Equipment* (CPEs) are the T5 managed radio devices. These CPEs use *Digital Subscriber Line* (DSL) as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

DSL Average Response Time	Lists each CPE's DSL name and its average response time in microseconds. Use this data to assess whether a specific DSL is experiencing response latency negatively impacting performance.
DSL Downstream Coding Violations	Displays each listed DSL's number of coding violations as a measure of erroneous data degrading the DSL's performance within the T5's network coverage area.
DSL Utilization	Lists each CPE's DSL name and its transmit utilization by percentage of overall load.
DSL Downstream Severely Eroded Seconds	Displays each listed DSL's eroded seconds, as a negative measure of delivery latency degrading the DSL's performance within the T5's network coverage area.
DSL Status	Lists the name of the DSL utilized on T5 managed CPE devices, and their downstream (transmit) data rate (in Mbps) and downstream throughput margin (in dB).
CPE Reset	The a selected CPE's number of resets. A reset renders the CPE offline until completed, and consequently should be carefully tracked to ensure consistent online availability amongst CPEs in the same radio coverage area.

7 Select a T5 device from amongst the devices listed in the dashboard's controller level, and right click the arrow to the right to list an additional menu of diagnostic activities that can be administrated for the selected T5 device.

Figure 4-10 *T5 Dashboard Menu Path*

Use these additional T5 configuration items to optionally upgrade T5 managed device firmware, reload configurations, upgrade the T5 CPE and manage T5 managed device LED status.

8 Select **Firmware Upgrade** to conduct firmware updates for T5 managed devices.

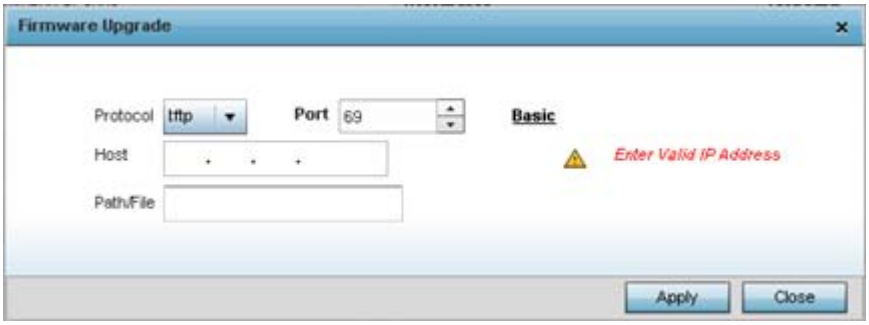


Figure 4-11 *T5 Dashboard Firmware Upgrade*

By default, the **Firmware Upgrade** screen displays the tftp server parameters for the target T5 device firmware file.

9 Provide the following information to accurately define the location of the T5 device firmware file.

Protocol	Select the FTP or TFTP protocol used for updating T5 device firmware.
Port	Use the spinner control, or manually set, the T5 device port used by the selected transfer protocol for firmware updates.
Host	Provide the numeric IP address of the resource used to update the firmware.
User Name	Define the user name used to access either a FTP or TFTP resource.
Password	Specify the password for the user account to access a FTP or a TFTP resource.
Path/File	Specify the correct directory path to the firmware file. Enter the complete relative path to the file on the server.

10 Select **Apply** to save the T5 device firmware connection protocol settings. Select **Close** to exit the Firmware Upgrade popup.

11 Select **Reload** to administrate current and next boot version available to the selected T5 device.

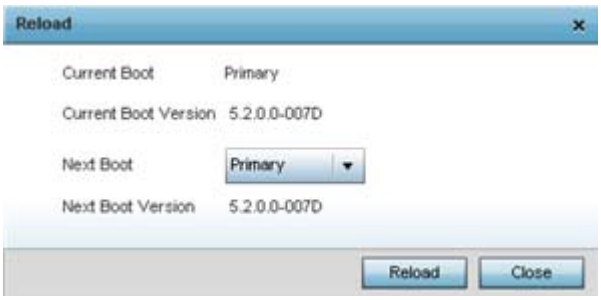


Figure 4-12 *T5 Dashboard Device Reload*

12 Review the following **Current** and **Next Boot Versions** and optionally apply a *primary* or *secondary* designation to the next boot version used in pending T5 managed device updates:

Current Boot	Lists whether the firmware image for a current T5 managed device boot is the *primary* or *secondary* firmware image.
Current Boot Version	Lists the firmware version currently utilized with T5 managed device boots.

Next Boot	Use the drop-down menu to specify whether the next boot is the *primary* or *secondary* firmware image.
Next Boot Version	Lists this version used the next time the T5 managed radio device is booted.

13 Select **Reload** to apply the current and next boot settings to a T5 update. Select **Close** to exit the Reload popup.

14 Expand the **CPE Management** item from the T5 dashboard and select **CPE Reload**. *Customer Premises Equipment* (CPE) are the T5 managed radio devices.

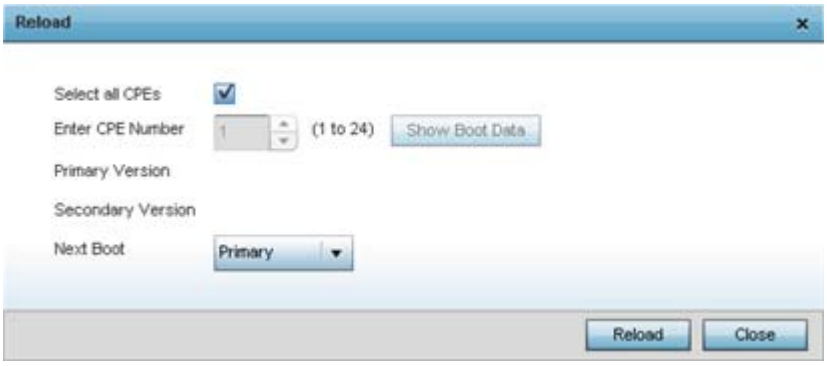


Figure 4-13 *T5 Dashboard CPE Management Reload*

15 Use the **Reload** screen to specify the CPEs to target for a T5 managed device firmware upgrade.

Select all CPEs	Select this option to use the settings specified in the *Firmware Upgrade* and *Reload* screens to update all the selected T5's managed CPE devices.
Enter CPE Number	If wanting to administrate an update to a specific T5 managed CPE, use the spinner control to select a specific CPE (1 - 24) for update. This option is enabled only when Select all CPEs is disabled. Select *Show Boot Data* to supply display the *Primary* and *Secondary* firmware versions utilized in the update.
Primary Version	When *Show Boot Data* is selected, this column lists the *Primary Version* utilized for the selected T5 managed CPE device update.
Secondary Version	When *Show Boot Data* is selected, this column lists the *Secondary Version* utilized for the selected T5 managed CPE device update.
Next Boot	Use the drop-down menu to specify whether the next boot is the *primary* or *secondary* firmware image utilized for the selected T5 managed CPE device update.

16 Select **Reload** to make available the selected firmware images(s) to the T5 in advance of initiating device upgrades. Select **Close** to exit the Reload popup.

17 Expand the **CPE Management** item from the T5 dashboard and select **Firmware Upgrade** to apply the defined upgrade settings to the selected T5's managed CPE devices.

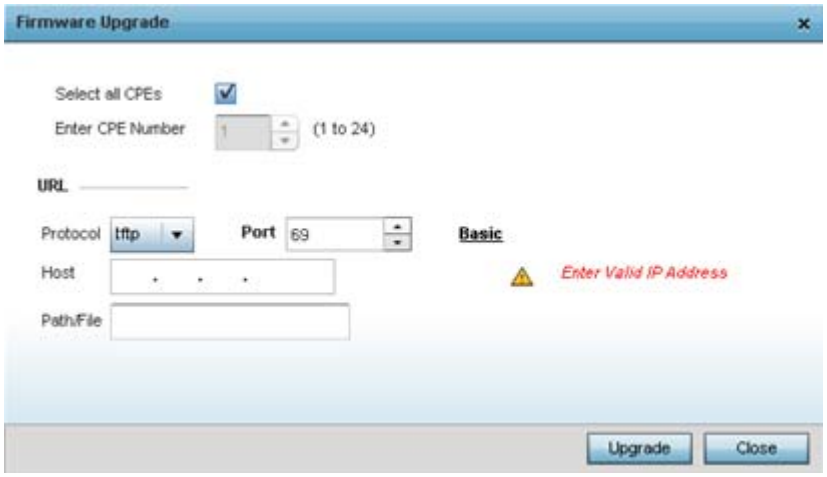


Figure 4-14 *T5 Dashboard CPE Reload*

18 Use the **Reload** screen to specify the CPEs to target for a T5 managed device firmware upgrade.

Select all CPEs	Select this option to use the settings specified in the *Firmware Upgrade* and *Reload* screens to update all T5's managed CPE devices.
Enter CPE Number	If wanting to administrate an update to a specific T5 managed CPE, use the spinner control to select a specific CPE (1 - 24) for update. This option is enabled only when *Select all CPEs* is disabled. Select *Show Boot Data* to supply display the *Primary* and *Secondary* firmware versions utilized in the update.
Protocol	Select the FTP or TFTP communication protocol used for updating T5 managed CPE device firmware.
Port	Use the spinner control, or manually set, the T5 device port used by the selected transfer protocol for CPE device firmware updates.
Host	Provide the numeric IP address of the resource used to update the CPE device firmware.
Path/File	Specify the correct directory path to the T5 managed CPE device firmware file. Enter the complete relative path to the file.

19 Select **Upgrade** to initiate the update from the T5 to the selected CPE device(s). Select **Close** to exit the Firmware Upgrade popup.

20 Expand the **CPE Management** item from the T5 dashboard and select **Set LED State** to administrate the LED behavior of the T5 managed CPE devices.

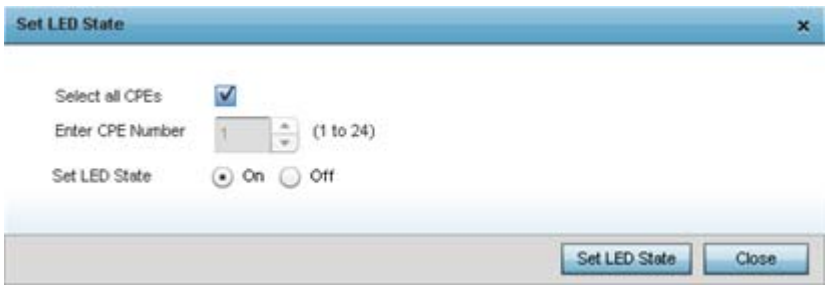


Figure 4-15 *T5 Dashboard Set LED State*

21 Use the **Set LED State** screen to set the LED behavior T5 managed CPE devices.

Select all CPEs	Select this option to apply the administrated LED state to each T5 managed CPE device.
Enter CPE Number	If wanting to set a specific T5 managed CPE LED, use the spinner control to set the CPE to be impacted by the ELD state setting. This setting could be quite useful in deployments where a specific CPE's LED illumination could be disruptive (such as a hospital etc.). This option is enabled only when *Select all CPEs* is disabled.
Set LED State	Define whether the LEDs remain on or off for the selected T5 managed CPE devices. The default setting is On.

22 Select **Start LED State** to initiate the LED behavior updates to the selected T5 managed CPE device(s). Select **Close** to exit the Set LED State popup.

23 Select **T5 File Management** to set the *Source* and *Destination* addresses used for T5 device configuration file updates.

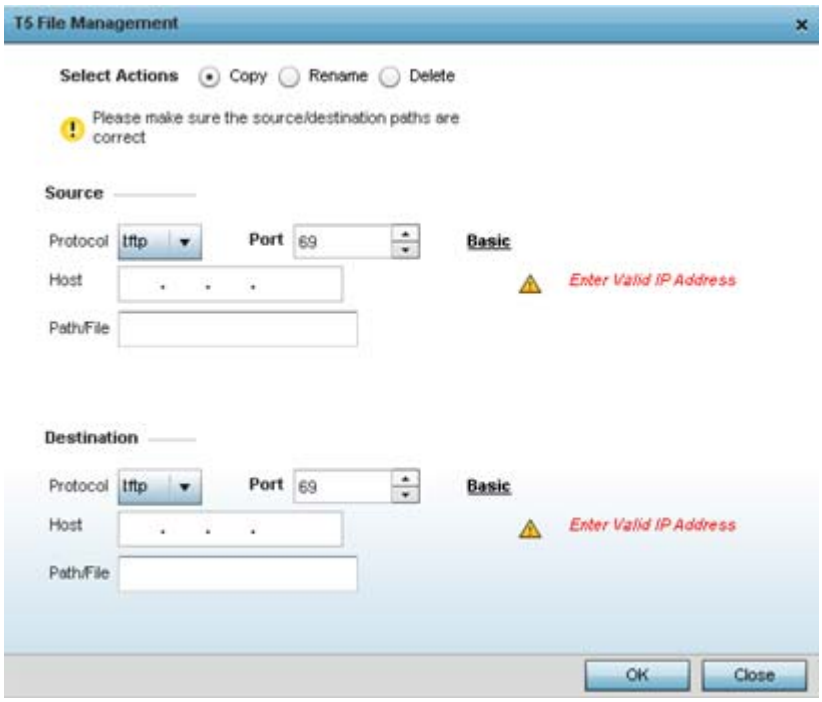


Figure 4-16 *T5 Dashboard T5 File Management*

NOTE: The configuration parameters displayed within the T5 File Management screen differ (increase or reduce) depending on whether *Copy*, *Rename* or *Delete* is selected as the management action. When **Copy** is selected, both source and destination protocols, ports, host addresses and paths are required for transfers. If the action is to **Rename** a configuration, both source and destination paths are required for name update. If the action is to **Delete**, only the path to the target file is required. All supplied paths and addresses must be set correctly for the selected action to be successful.

24 Set the following **T5 File Management** *Source* and/or *Destination* transfer protocols and address information. Options differ depending on selected **Copy**, **Rename** or **Delete** file management action.

Selected Action	Select *Copy* to enable parameters where the correct source and destination T5 device port, host IP address and directory path must be specified. Select *Rename* to correctly provide the source and destination directory paths of a renamed T5 configuration file. Select *Delete* to define the correct directory path of a target T5 configuration file to delete and remove. The default setting is Copy.
Protocol	Select the FTP or TFTP communication protocol used for updating T5 file transfers. This option is only available when *Copy* is the selected action.
Port	Use the spinner control, or manually set, the T5 device port used by the selected transfer protocol. This option is only available when *Copy* is the selected action.
Host	Provide the numeric IP address of the resource used to update the CPE device firmware. This option is only available when *Copy* is the selected action.
Path/File	Specify the correct directory path to the location(s) of the source and destination T5 device addresses. This option is only available when *Copy* is the selected action.
Source	If *Renaming* or *Deleting* a T5 configuration file, correctly enter the directory path of the target file to be renamed or deleted.
Destination	If Renaming a T5 configuration file, correctly enter the directory path of the target file to be renamed.

25 Select **OK** to apply the selected file management action. Select **Close** to exit the T5 File Management popup.

4.4.4 EX3500 Switch Dashboard

The EX3500 series switch is a Gigabit Ethernet Layer 2 switch with either 24 or 48 10/100/1000-BASE-T ports, and four *small form factor pluggable* (SFP) transceiver slots for fiber connectivity. Each 10/100/1000 Mbps port supports both the IEEE 802.3af and IEEE 802.3at-2009 PoE standards. Each EX3500 series switch includes an SNMP-based management agent, which provides both in-band and out-of-band access for management. An EX3500 series switch utilizes an embedded HTTP Web agent and command line interface (CLI) somewhat different from the WiNG operating system, while still enabling the EX3500 series switch to provide WiNG controllers PoE and port management resources.

Going forward NX9600, NX9500, NX7500, NX6500, NX5500, NX4500 WiNG managed services platforms and WiNG VMs can discover, adopt and partially manage EX3500 series Ethernet switches, as DHCP option 193 has been added to support external device adoption. DHCP option 193 is a simplified form of DHCP options 191 and 192 used by WiNG devices currently. DHCP option 193 supports pool1, hello-interval and adjacency-hold-time parameters.

When adopted to a managing controller or service platform, an EX3500 switch can display a unique dashboard helpful to administrators to better assess the interoperability of the selected EX3500 with its connected controller or service platform.

NOTE: To enable the adoption of an EX3500 switch, the **Allow Adoption of External Devices** option must be enabled. For more information, refer to *Adoption Overrides (Controllers Only) on page 5-48*.

To review an EX3500 switch dashboard:

1 Select **Dashboard**.

2 Select **Summary** if it's not already selected by default.

3 Expand the **System** node to display RF Domains.

4 Select and expand a **RF Domain** to expose its member controllers or service platforms.

5 Select an EX3500 switch from amongst the devices listed.

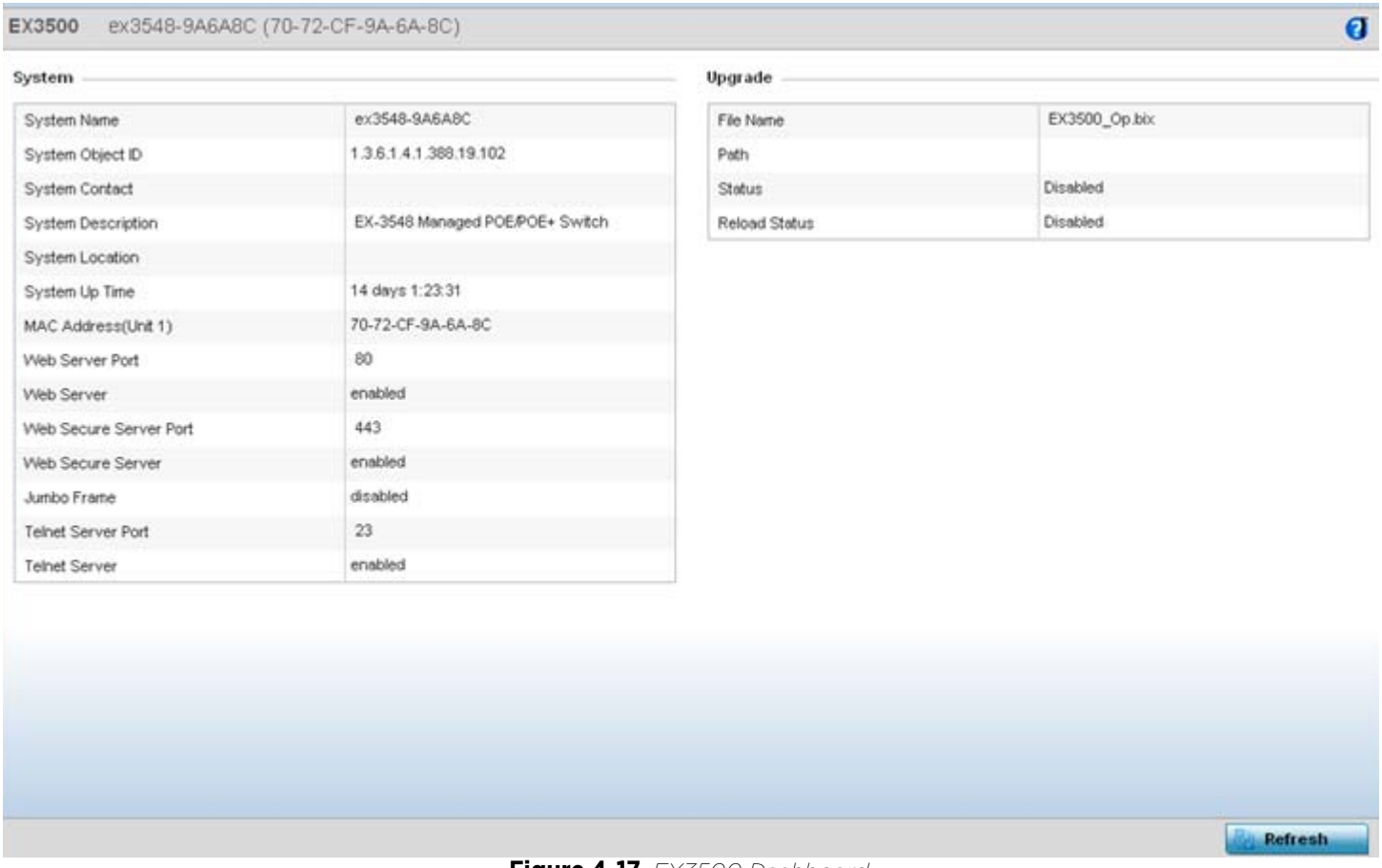


Figure 4-17 *EX3500 Dashboard*

6 Refer to the following **System** information to assess dashboard information for the selected EX3500 switch.

System Name	Displays the administrator assigned system name of the selected EX3500 switch.

System Object ID	Lists the numeric ID used to determine the monitoring capabilities of the EX3500 switch.
System Contact	Lists the EX3500 switch administrative contact assigned to respond to events created by, or impacting, this selected EX3500 switch and the RF Domain devices it helps support.
System Description	Displays the administrator defined system description provided by the administrator upon initial deployment of this particular EX3500 switch.
System Location	Lists a 255 character maximum EX3500 switch location reflecting the switch's physical deployment location.
System Up Time	Displays the cumulative time since this EX3500 was last rebooted or lost power.
MAC Address (Unit 1)	Lists the factory encoded MAC address of the selected EX3500 as its hardware identifier.
Web Server Port	Displays the Web server port the EX3500 is using. Port 80 is the default port the Web server expects to listen to.
Web Server	Lists whether the Web server facility is *enabled/disabled* between this selected EX3500 switch and its connected controller or service platform. A Web server is a program using a client/server model and the *Hypertext Transfer Protocol* (HTTP) to serve files forming Web pages to Web resource requesting clients.
Web Secure Server Port	Lists the numeric virtual server port providing secure Web resources with the selected EX3500. Any system with multiple open ports, multiple services and multiple scripting languages is vulnerable simply because it has so many points of entry to watch. The secure open port has been specifically designated and utilizes the latest security patches and updates.
Web Secure Server	Lists whether the secure Web server functionality has been *enabled* or *disabled* for the selected EX3500's management session with the WiNG controller or service platform.
Jumbo Frame	Lists whether support for jumbo Ethernet frames with more than 1500 bytes of payload has been *enabled* or *disabled*. Jumbo frames support up to 9000 bytes, but variations must be accounted for. Many Gigabit Ethernet switches and Gigabit Ethernet network interface cards support jumbo frames. Some Fast Ethernet switches and Fast Ethernet network interface cards also support jumbo frames.
Telnet Server Port	Lists the numeric Telnet server port used with the selected EX3500's session with the WiNG controller or service platform to test for open ports. The listed port is the port number where the server is listening.
Telnet Server	Displays whether Telnet functionality is currently *enabled* or *disabled* for the selected EX3500 switch.

7 Refer to the **Upgrade** field to assess the EX3500's current firmware and upgrade configuration status.

Filename	Lists the target firmware file queued for subsequent uploads to the selected EX3500 switch.
Path	Lists the complete relative path to the EX3500 switch firmware file defined for subsequent upgrades.
Status‘	Lists whether a device firmware upgrade is currently *enabled* and queued for the selected EX3500 or is currently *disabled*.

Reload Status	Displays the selected EX3500's current firmware reload status.

8 Periodically select **Refresh** to update the statistics counters to their latest values.

4.5 Access Point Screen

The **Access Point** screen displays system-wide network status for standalone or controller connected Access Points. The screen is partitioned into the following tabs:

- *Access Point Health* – The Health tab displays information about the state of the Access Point managed network.
- *Access Point Inventory* – The Inventory tab displays information on the physical devices managed within the Access Point managed network.

4.5.1 Access Point Health

To assess Access Point network health:

1 Select **Dashboard**.

2 Select **Summary** if it's not already selected by default.

3 Expand the **System** node to display RF Domains.

4 Select and expand a **RF Domain** to expose its member controllers or service platforms.

5 Select a controller or service platform and expand the menu item to display connected Access Points.

6 Select an Access Point. The **Health** tab display by default.

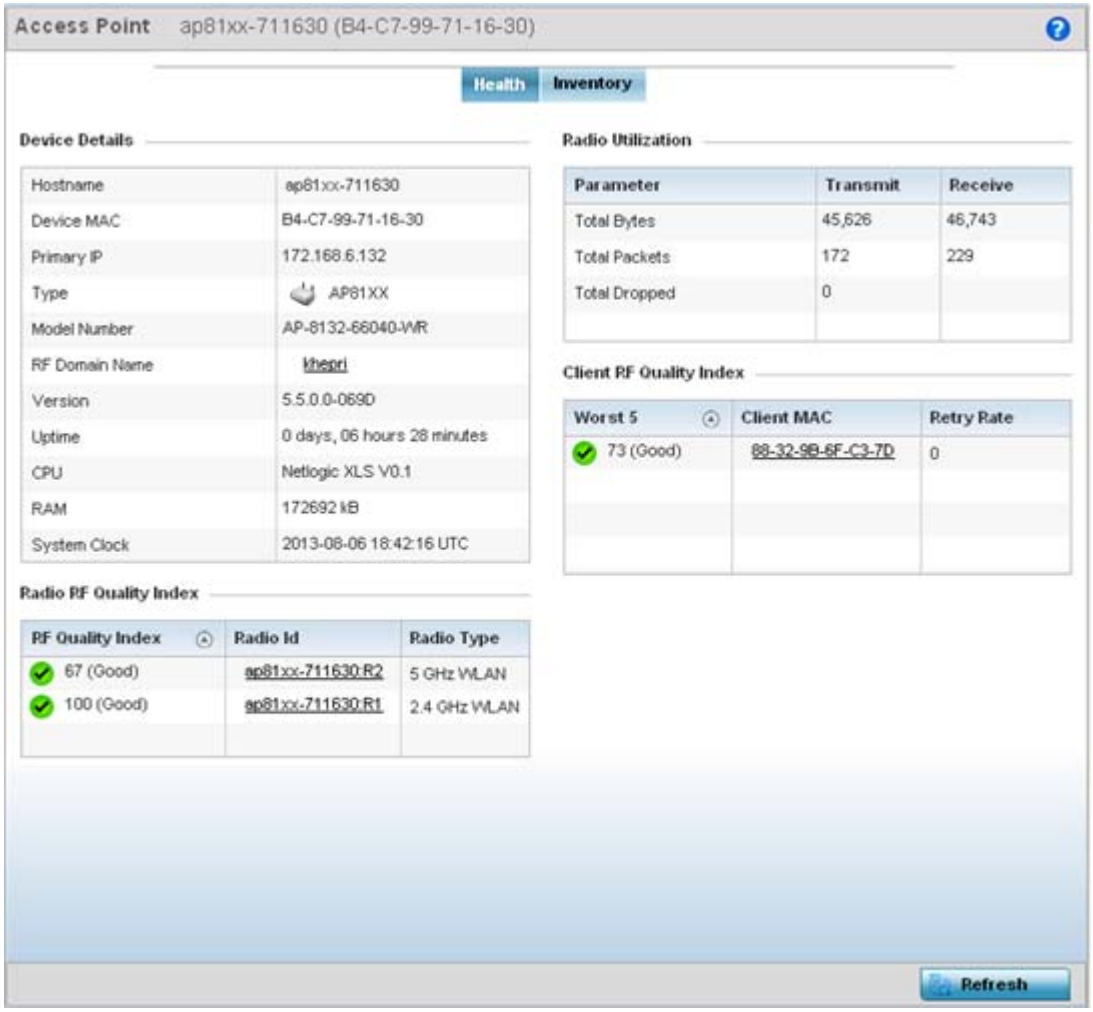


Figure 4-18 *Access Point screen - Health tab*

- The **Device Detail** field displays the following information about the selected Access Point:
- **Hostname** - Lists the administrator assigned name of the selected Access Point.
- **Device MAC** - Lists the factory encoded MAC address of the selected Access Point.
- **Primary IP Address** - Lists the IP address assigned to the Access Point as a network identifier.
- **Type** - Indicates the Access Point model type. An icon representing the Access Point is displayed along with the model number.
- **RF Domain Name** - Lists the RF Domain to which the Access Point belongs. The RF Domain displays as a link that can be selected to display Access Point RF Domain membership data in greater detail.
- **Model Number** - Lists the specific model number of the Access Point.
- **Version** - Lists the version of the firmware running on the Access Point. Compare this version against the version currently on the support site to ensure the Access Point has the latest feature set available.
- **Uptime** - Displays the duration the Access Point has been running from the time it was last restarted.
- **CPU** - Displays the CPU installed on this Access Point.
- **RAM** - Displays the amount of RAM available for use in this system.
- **System Clock** - Displays the current time on the Access Point.
- The **Radio RF Quality Index** displays a table of RF quality per radio. It is a measure of the overall effectiveness of the RF environment displayed in percentage. It is a function of the connect rate in both directions, the retry rate and error rate. The quality is measured as:
  - 0-20 - *Very poor quality*

  - 20-40 - *Poor quality*
  - 40-60 - *Average quality*
  - 60-100 - *Good quality*
- The **Radio Utilization** Index area displays how efficiently the RF medium is used. Radio utilization is defined as the percentage of current throughput relative to the maximum possible throughput for the radio. The Radio Utilization displays radios in terms of the number of associated wireless clients and percentage of utilization. It also lists packets types transmitted and received.
- The **Client RF Quality** Index displays a table of RF quality on a per client basis. It is a measure of the overall effectiveness of the RF environment displayed in percentage. It is a function of the connect rate in both directions, the retry rate and the error rate. This area of the screen displays the average quality index for a client. The table lists bottom five (5) of the RF quality values by client. The quality is measured as:
  - 0-20 - *Very poor quality*
  - 20-40 - *Poor quality*
  - 40-60 - *Average quality*
  - 60-100 - *Good quality*

4.5.2 Access Point Inventory

The Access Point **Inventory** tab displays granular data on devices managed by the selected Access Point. Information is displayed in easy to read tables and graphs.

To assess Access Point network health:

1 Select **Dashboard.**

2 Select **Summary** if it's not already selected by default.

3 Expand the **System** node to display RF Domains.

4 Select and expand a **RF Domain** to expose its member controllers or service platforms.

5 Select a controller or service platform and expand the menu item to display connected Access Points.

6 Select an **Access Point.**

7 Select the **Inventory** tab.

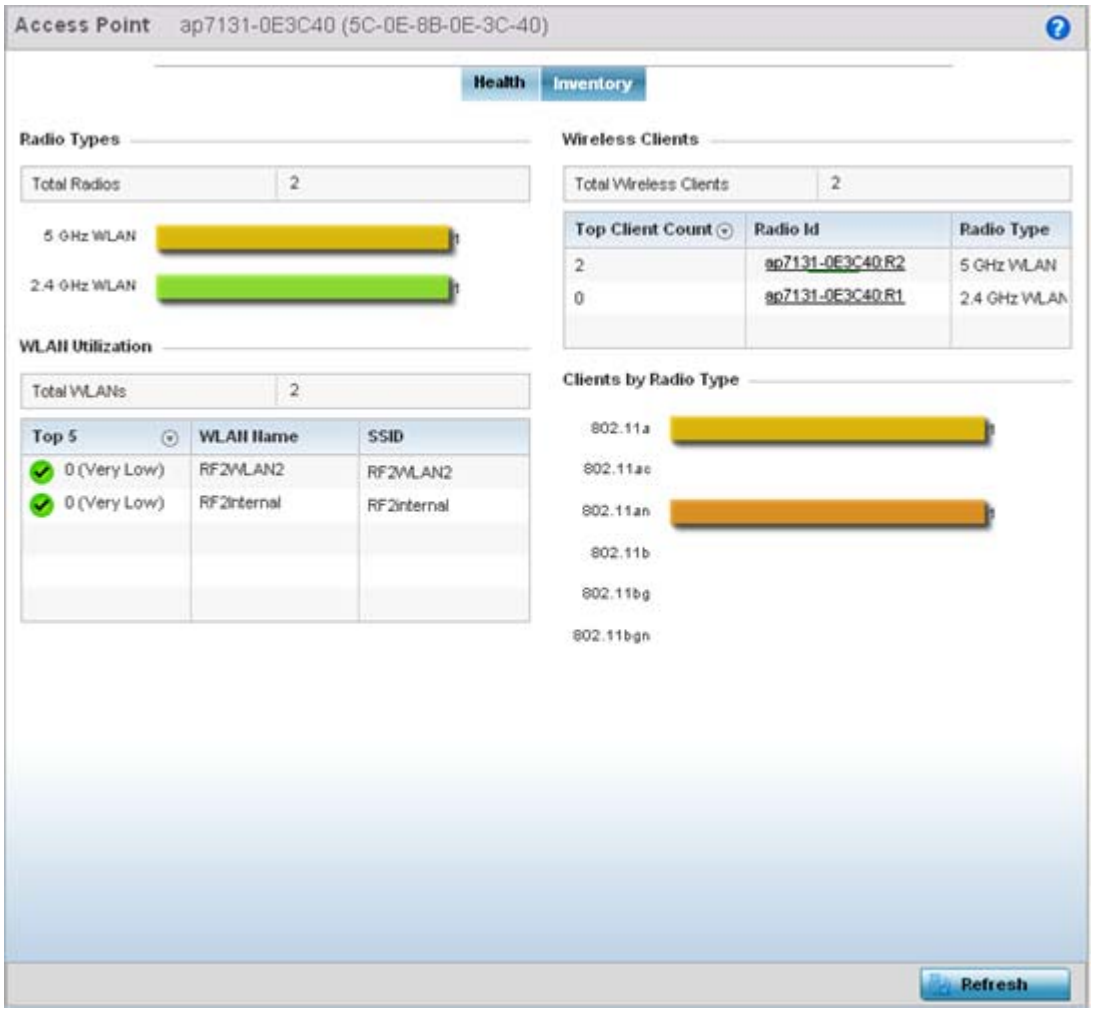


Figure 4-19 *Access Point screen - Inventory tab*

The information within the **Inventory** tab is partitioned into the following fields:

- The **Radios Type** field displays the total number of radios utilized by this Access Point. The graph lists the number of radios in the 2.4 GHz and 5 GHz radio bands and funtioning as a sensor.
- The **WLAN Utilization** table displays utilization statistics for controller or service platform WLAN configurations. Information displays in two tables. The first table lists the total number of WLANs managed by this system. The second table lists the top five (5) WLANs in terms of the usage percentage along with their name and network identifying SSID.
- The **Wireless Clients** table lists clients managed by this Access Point by connected client count. Information is presented in two (2) tables and a graph. The first table lists the total number of clients managed by the listed Access Point. The second lists the top five (5) radios in terms of the number of connected clients. The graph just below the table lists the number of clients by radio type.

4.6 Network View

The **Network View** functionality displays device association connectivity amongst controllers, service platforms, Access Point radios and wireless clients. This association is represented by a number of different graphs.

To review the wireless controller's Network Topology, select **Dashboard > Network View**.

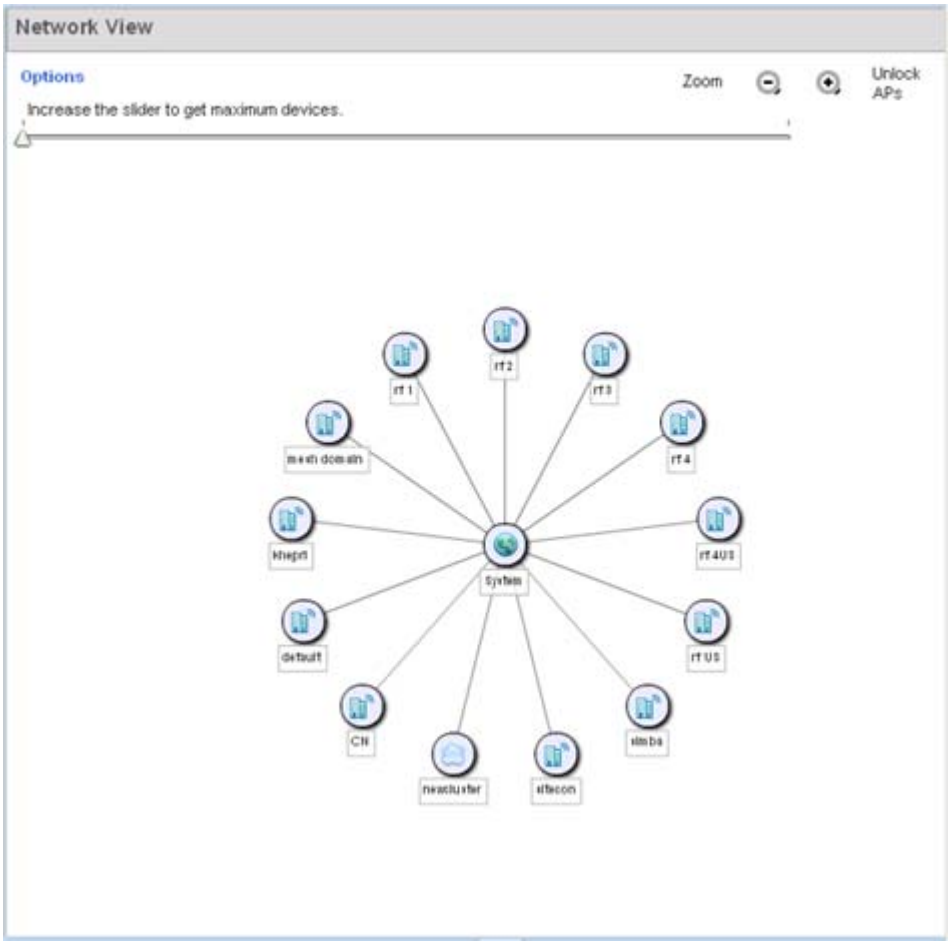


Figure 4-20 *Network View Topology*

- The screen displays icons for the different views available to the system. Apart from device specific icons, the following three icons are available:
  - *default* – Displays information about the default RF Domain.
  - *system* – Displays information about the current system.
  - *cluster* – Displays information about clusters managed by this system.

Use the icons to navigate quickly within top level groupings.

The middle field displays a Network View, or graphical representation of the network. Nodes display whether or not they are members of a cluster or mesh domain. Use this information to assess whether the topology of the network has changed in such a manner that devices need to be added or moved. This field changes to display a graphical network map.

Use the Lock / Unlock icon in the upper right of the screen to prevent users from moving APs around within the specified area.

4.7 Debug Wireless Clients

An administrator has the ability to select a RF Domain and capture connected client debug messages at an administrator assigned interval and location. Client debug information can either be collected historically or in real-time.

To troubleshoot issues with wireless client connectivity within a controller, service platform or Access Point managed RF Domain:

1 Select **Dashboard.**

2 Expand the **System** node to display controller, service platform or Access Point managed RF Domains.

3 Select and expand a RF Domain and click on the down arrow to the right of the RF Domain's name

4 Select **Troubleshooting**.

5 Select **Debug Wireless Clients.**

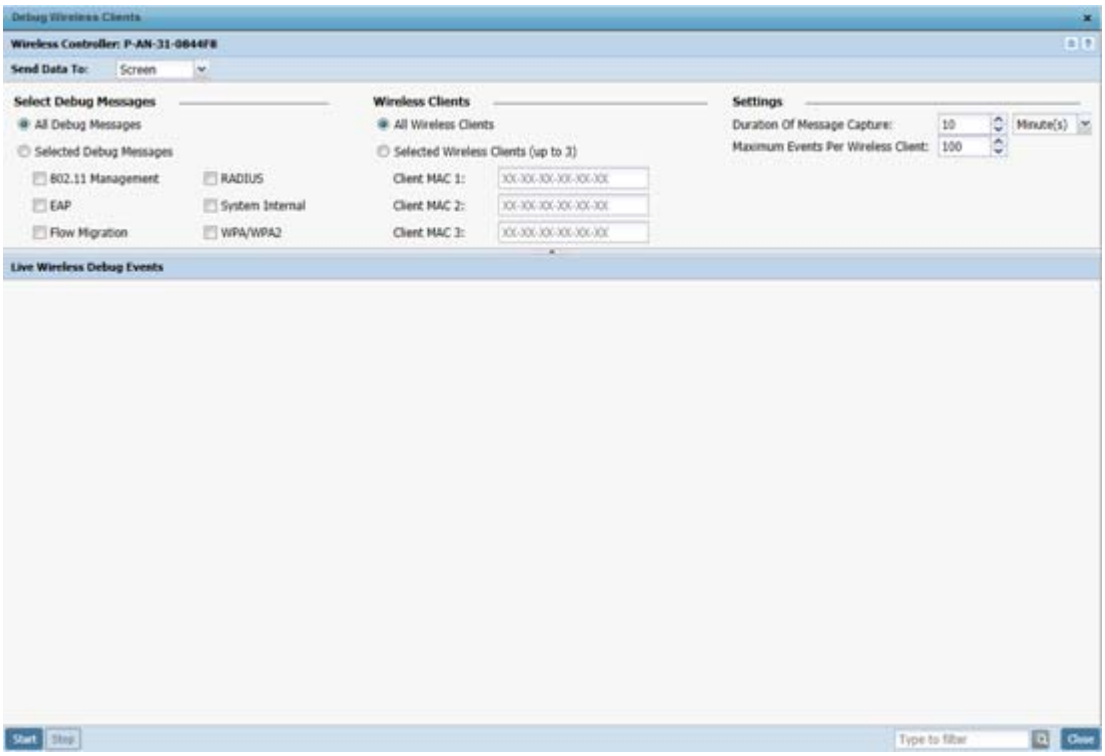


Figure 4-21 *Debug Wireless Clients screen*

6 Refer to the following remote debug information for RF Domain member connected wireless clients:

RF Domain	Displays the administrator assigned name of the selected RF Domain used for wireless client debugging. RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building or site.
Send Data To	Use the *Send Data To* drop-down menu to select where wireless client debug messages are collected. If Screen is selected the wireless client debug information is sent to the *Live Wireless Debug Events* window at the bottom of the dialog window. If *File* is selected, the file location must be specified in the *File Location* section of the window.

Select Debug Messages	Select *All Debug Messages*, to display all wireless client debug information for the selected wireless clients on the current RF Domain. Choose *Selected Debug Messages to* specify which types of wireless client debug messages to display. If the *Selected Debug Messages* radio button is selected, you can display information for any combination of the following: - *802.11 Management* - *EAP* - Flow Migration - RADIUS - System Internal - WPA/WPA2
Wireless Clients	Select *All Wireless Clients* to display debug information for all wireless clients currently associated to the current RF Domain. Choose *Selected Wireless Clients* to display information only for specific wireless clients (between 1 and 3). If the Selected Wireless Clients radio button is selected enter the MAC address for up to three wireless clients. The information displayed or logged to the file will only be from the specified wireless clients.
Duration of Message Capture	Use the spinner controls to select how long to capture wireless client debug information. This can range between 1 second and 24 hours, with the default value being 1 minute.
Maximum Events Per Wireless Client	Use the spinner controls to select the maximum number of debug messages displayed per wireless client. Set the number of messages from 1 - 9999 events with the default value being 100 events.
File Location	When the *Send Data To* field is set to *File*, the *File Location* configuration displays below the configuration section. If *Basic* is selected, enter the URL in the following format: URL Syntax: tftp://<hostname|IP>[:port]/path/file ftp://<user>:<passwd>@<hostname|IP>[:port]/path/file IPv6 URL Syntax: tftp://<hostname|[IPv6]>[:port]/path/file *ftp://<user>:<passwd>@<hostname|[IPv6]>[:port]/path/file* If *Advanced* is selected, configure the Target, Port, Host/IP, User, Password and optionally the path for the wireless client debug log file you wish to create.
Live Wireless Debug Events	When the *Send Data To* field is set to *Screen,* this area displays live debug information for connected wireless clients in the selected RF Domain.

When all configuration fields are complete, select **Start** to start the wireless client debug capture. If information is being sent to the screen it displays in the Live Wireless Debug Events section. If the data is being sent to a file,

that file populates with remote debug information. If you have set a long message capture duration and wish to end the capture early, select **Stop**.

4.8 Debug Captive Portal Clients

An administrator can select a RF Domain and capture captive portal client and authentication debug messages at an administrator assigned interval and location. Captive portal debug information can either be collected historically or in real-time.

To troubleshoot captive portal client debug messages:

1 Select **Dashboard.**

2 Expand the **System** node to display controller, service platform or Access Point managed RF Domains.

3 Select and expand a RF Domain and click on the down arrow to the right of the RF Domain's name

4 Select **Troubleshooting**.

5 Select **Captive Portal Clients.**

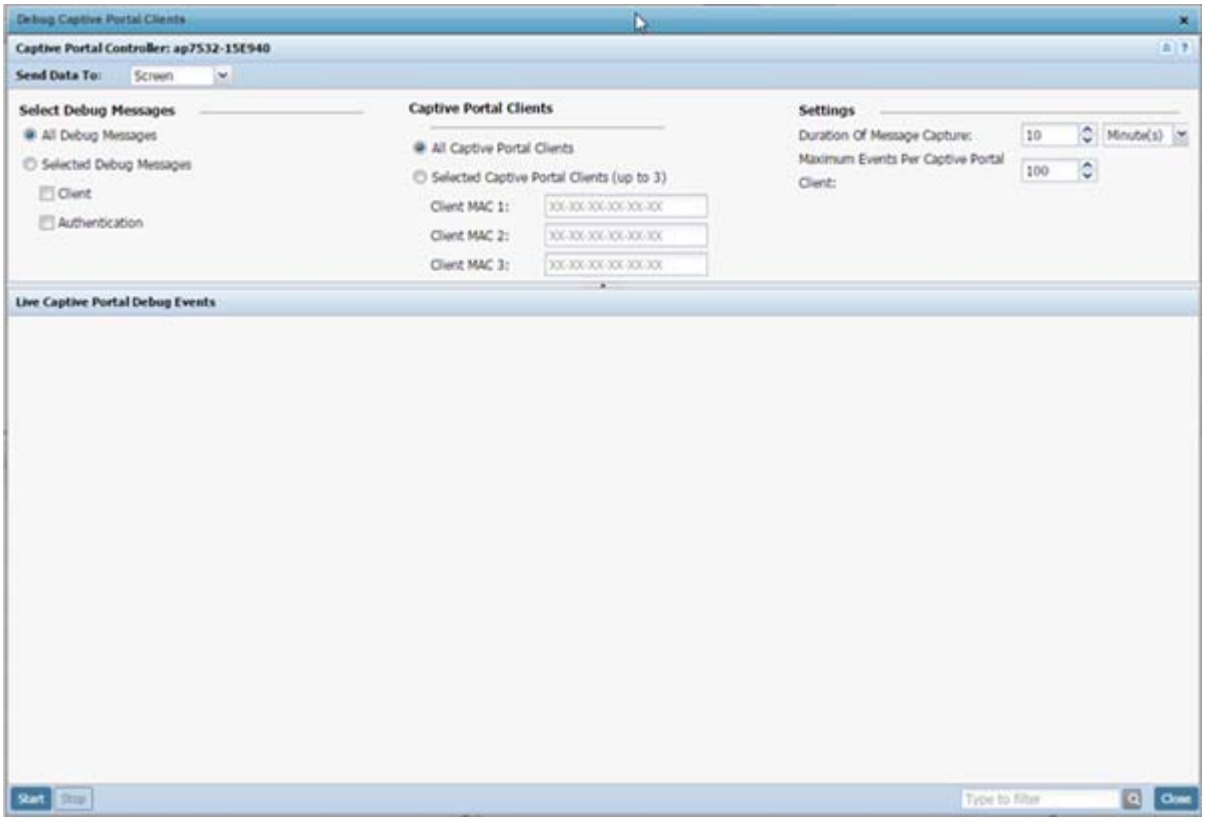


Figure 4-22 *Debug Wireless Clients screen*

6 Use the **Send Data To** drop-down menu to select where captive portal debug messages are collected. If *Screen* is selected, information is sent to the *Live Wireless Debug Events* window at the bottom of the screen. If *File* is selected, the file location must be specified in the *File Location* field.

7 Select **Debug Message** settings to refine how captive portal client debug messages are trended:

All Debug Messages	Select this option to capture all captive portal client and captive portal authentication request events collectively without filtering by type.
Select Debug Messages	Choose *Selected Debug Messages* to specify the type of captive portal event messages to display. Options include captive portal client events and events specific to captive portal authentication requests.

8 Set **Captive Portal Clients** filter options to refine which clients are included in the debug messages.

All Captive Portal Clients	Select *All Captive Portal Clients* to display debug information for each client utilizing a captive portal for network access within the selected RF Domain.
Select Captive Portal Clients (up to 3)	Optionally display captive portal debug messages for specific clients (1 - 3). Enter the MAC address for up to three wireless clients. The information displayed or logged to the file is only from the specified wireless clients. Change the client MAC addresses as needed when clients are no longer utilizing the RF Domain's captive portal resources.

9 Define the following captive portal client **Settings** to determine how messages are trended:

Duration of Message Capture	Use the spinner controls to set the message capture interval for captive portal debug information. This can range between 1 second and 24 hours.
Maximum Events Per Captive Portal Client	Use the spinner controls to select the maximum number of captive portal event messages displayed per RF Domain member client. Set the number of messages from 1 - 9999 events with the default value being 100 events.

10 When all configuration fields are complete, select **Start** to start the captive portal client debug message capture. Information sent to the screen displays in the **Live Captive Portal Debug Events** field. If you have set a long message capture duration and wish to end the capture early, select **Stop**.

4.9 Packet Capture

An administrator can capture connected client packet data based on the packet's address type or port on which received. Dropped client packets can also be trended to assess RF Domain client connectivity health.

To administrate RF Domain packet captures:

1 Select **Dashboard.**

2 Expand the **System** node to display controller, service platform or Access Point managed RF Domains.

3 Select and expand a RF Domain and click on the down arrow to the right of the RF Domain's name

4 Select **Troubleshooting**.

5 Select **Packet Capture.**

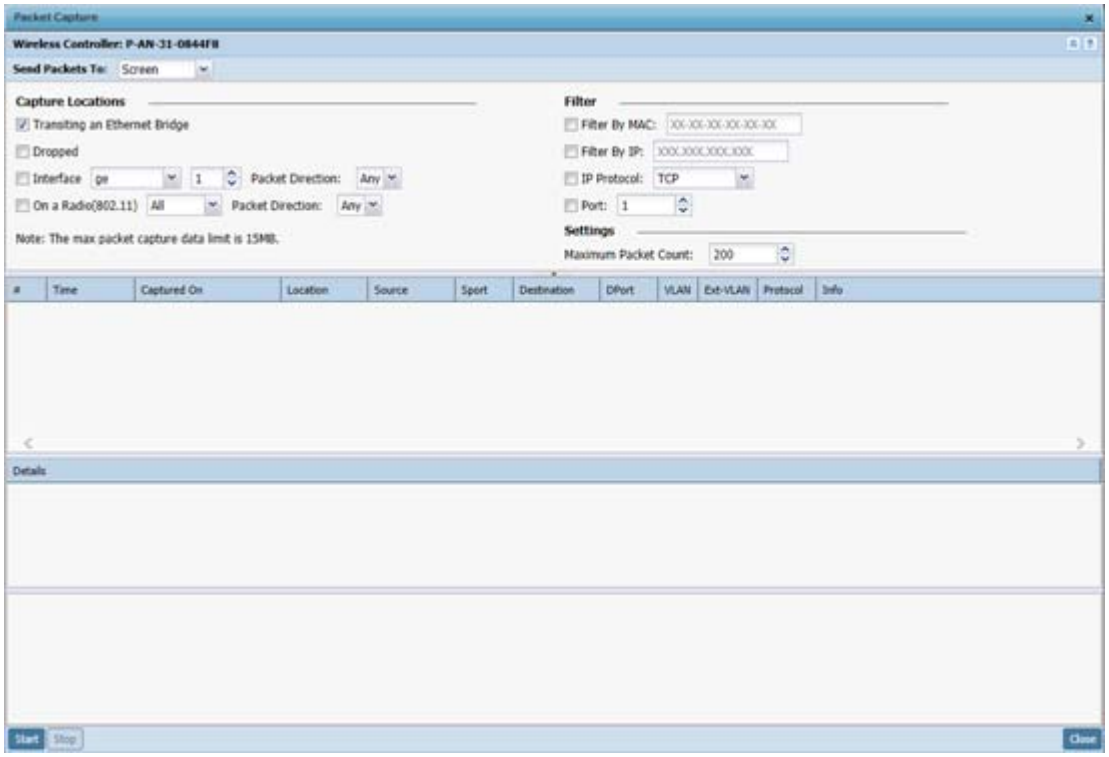


Figure 4-23 *Packet Capture screen*

6 Refer to the following packet capture data for RF Domain member connected wireless clients:

RF Domain	Displays the administrator assigned name of the selected RF Domain used for wireless client packet captures. RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building or site.
Send Data To	Use the *Send Data To* drop-down menu to select where wireless client packet capture messages are collected. If *Screen* is selected client packet capture data is sent to the *Live Wireless Debug Events* window at the bottom of the dialog window. If *File* is selected, the file location must be specified in the *File Location* section of the window.
Dropped	Select *Dropped* to create an event entry each time a packet is dropped from a client connected to a RF Domain member device. Use this information to assess whether a particular RF Domain is experiencing high levels of dropped packets that may require administration to distribute client connections more evenly.
Interface	Select Interface to specify packet capture on a specific interface on the current RF Domain. If Interface is selected, specify the interface name and number and specify a Packet Direction
On a Radio (802.11)	Select *On a Radio (802.11)* to capture packets only on 802.11 radios. If selecting this option, specify which radios should be used and specify a *Packet Direction*.

Filter (MAC, IP, Protocol, Port)	Filter packet captures based on specific criteria. Select one or more of the following and specify the relevant information: - *Filter by MAC* - Filter By IP - IP Protocol - Port
Maximum Packet Count	Set the *Maximum Packet Count* to limit the number of packets captured for trending. Set this value between 1 - 10000 packets, with a default value of 200.

7 Select **Start** to begin the packet capture. Information sent to the screen displays in the lower portion of the window. If the data is being sent to a file, that file populates with the packet capture information. If you have set a long message capture duration and wish to end the capture early, select **Stop.**

5 Device Configuration

Managed devices can either be assigned unique configurations or have existing RF Domain or Profile configurations modified (overridden) to support a requirement that dictates a device's configuration be customized from the configuration shared by its profiled peer devices.

When a device is initially managed by the controller or service platform, it requires several basic configuration parameters be set (system name, deployment location etc.). Additionally, the number of permitted device licenses needs to be accessed to determine whether a new Access Point can be adopted.

Refer to the following to set a device's basic configuration, license and certificate usage:

- *Basic Configuration*
- *Basic Device Configuration*
- *Auto Provisioning Policies*
- *Managing an Event Policy*
- *Managing MINT Policies*

RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area (floor, building or site). In such instances, there's many configuration attributes these devices share as their general client support roles are quite similar. However, device configurations may need periodic refinement (overrides) from their original RF Domain administered design. For more information, see RF Domain Overrides on page 5-32.

Profiles enable administrators to assign a common set of configuration parameters and policies to controller or service platforms and Access Points. Profiles can be used to assign shared or unique network, wireless and security parameters to wireless controllers and Access Points across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support. The controller and service platform supports both default and user defined profiles implementing new features or updating existing parameters to groups of controllers, service platforms or Access Points.

However, device profile configurations may need periodic refinement from their original administered configuration. Consequently, a device profile could be applied an override from the configuration shared amongst numerous peer devices deployed within a particular site. For more information, see Profile Overrides on page 5-38.

Adoption is the process an Access Point uses to discover controller or service platforms available in the network, pick the most desirable, establish an association, obtain its configuration and consider itself provisioned.

At adoption, an Access Point solicits and receives multiple adoption responses from available controllers or service platforms on the network. Modify existing adoption policies or create a new one as needed to meet the adoption requirements of a device and its assigned profile. For more information, see Auto Provisioning Policies on page 5-268.

Lastly, use **Configuration** > **Devices** to define and manage a critical resource policy. A critical resource policy defines a list of device IP addresses on the network (gateways, routers etc.). The support of these IP address is interpreted as critical to the health of the network. These devices addresses are pinged regularly by the controller or service platform. If there's a connectivity issue, an event is generated stating a critical resource is unavailable. For more information, see Overriding a Profile's Critical Resource Configuration on page 5-233.

5.1 Basic Configuration

Device Configuration

To assign a Basic Configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the Configuration tab.
The Device Configuration screen displays a list of devices.

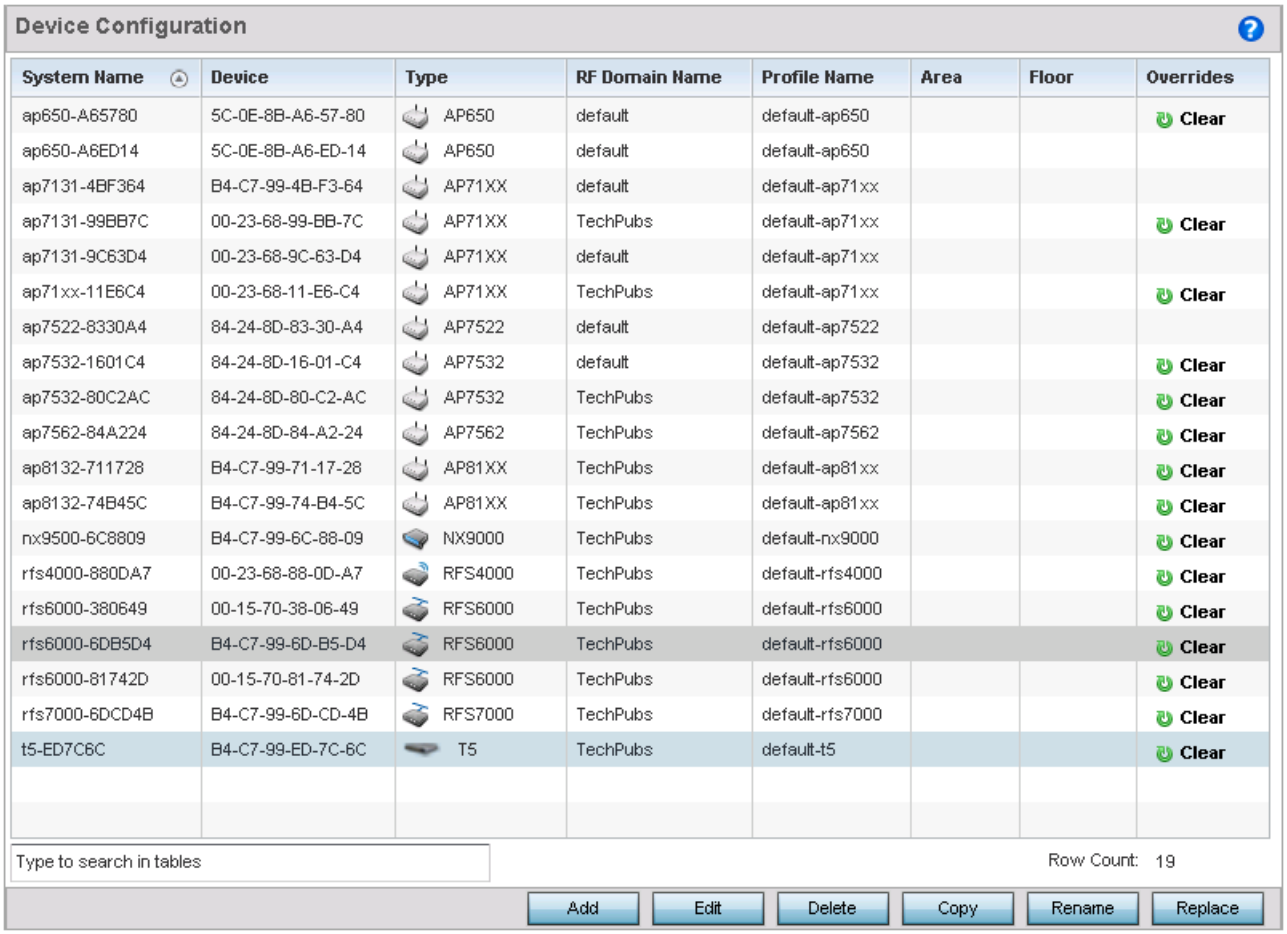


Figure 5-1 *Device Configuration screen*

Refer to the following device settings to determine whether a configuration update or RF Domain or Profile change is warranted:

System Name	Displays the name assigned to the device when the basic configuration was defined. This is also the device name that appears within the RF Domain or Profile the device supports.
Device	Displays the device's factory assigned MAC address used as hardware identifier. The MAC address cannot be revised with the device's configuration.
Type	Displays the device model for the listed controller, service platform or Access Point.

RF Domain Name	Lists RF Domain memberships for each listed device. Devices can either belong to a default RF Domain based on model type, or be assigned a unique RF Domain supporting a specific configuration customized to that device model.
Profile Name	Lists the profile each listed device is currently a member of. Devices can either belong to a default profile based on model type, or be assigned a unique profile supporting a specific configuration customized to that model.
Area	List the physical area where the controller or service platform is deployed. This can be a building, region, campus or other area that describes the deployment location.
Floor	List the building Floor name representative of the location within the area or building the controller or service platform was physically deployed. Assigning a building Floor name is helpful when grouping devices in RF Domains and Profiles, as devices on the same physical building floor may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location.
Overrides	The Overrides column contains an option to clear all profile overrides for any devices that contain overrides. To clear an override, select the clear button to the right of the device.

3 Select **Add** to create a new device, select **Edit** to modify an existing device or select **Delete** to remove an existing device.Optionally **Copy** or **Rename** a device as needed.

4 Use the **Replace** button to replace an existing Access Point with another Access Point. The Replace feature enable you to swap an existing Access Point with a new one without disrupting normal operations. The configuration of the old Access Point is automatically copied to the newly added Access Point. The following screen is displayed.

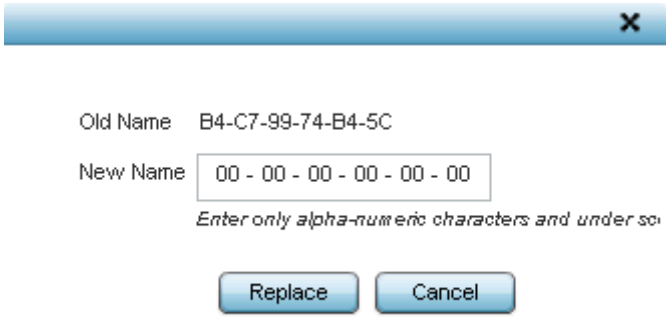


Figure 5-2 *Device Configuration screen - Replace*

5 Enter the MAC address of the new Access Point in the **New Name** field and select the **Replace** button. The new Access Point is added to the list of devices and the configuration from the old Access Point is applied to it. The old Access Point is then removed from the device list.

5.2 Basic Device Configuration

Device Configuration

Setting a device's Basic Configuration is required to assign a device *name,* deployment *location*, and system *time*. Similarly, the Basic Configuration screen is where Profile and RF Domain assignments are made. RF Domains allow

administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building or site. Each RF Domain contains policies that can determine a Smart RF or WIPS configuration.

Profiles enable administrators to assign a common set of configuration parameters and policies to controllers, service platforms and Access Points. Profiles can be used to assign common or *unique* network, wireless and security parameters to wireless controllers and Access Points across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support. A controller and service platform support both default and user defined profiles implementing new features or updating existing parameters to groups of peer devices and Access Points. The central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations one at a time.

NOTE: Once devices have been assigned membership in either a profile or RF Domain, an administrator must be careful not to assign the device a configuration update that removes it from membership from a RF Domain or profile. A RF Domain or profile configuration must be re-applied to a device once its configuration has been modified in a manner that differentiates it from the configuration shared by the devices comprising the RF Domain or profile.

To assign a device a Basic Configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the Configuration tab.

The *Device Configuration* screen displays a list of managed devices or peer controllers, service platforms or Access Points.

3 Select a target device (by double-clicking it) from amongst those displayed.

Devices can also be selected directly from the *Device Browser* in the lower, left-hand, side of the UI.

The **Basic Configuration** screen displays by default.

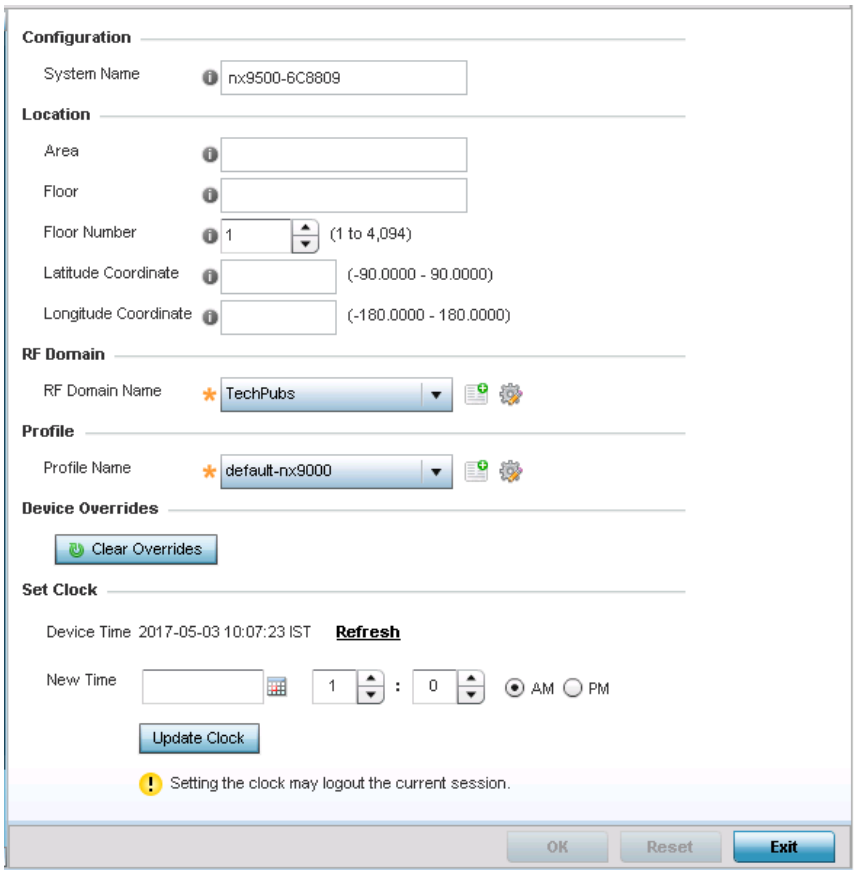


Figure 5-3 *Basic Configuration screen*

4 Set the following **Configuration** settings for the target device:

System Name	Provide the selected device a system name up to 64 characters. This is the device name that appears within the RF Domain or Profile the device supports.
Area	Assign the device an *Area* name representative of the location the controller or service platform was physically deployed. The name cannot exceed 64 characters. Assigning an area name is helpful when grouping devices in RF Domains and profiles, as devices in the same physical deployment location may need to share specific configuration parameters in respect to radio transmission and interference requirements specific to that location.
Floor	Assign the target a device a building *Floor* name representative of the location the Access Point was physically deployed. The name cannot exceed 64 characters. Assigning a building Floor name is helpful when grouping devices within the same general coverage area.
Floor Number	Use the spinner control to assign a numerical floor designation in respect to the floor's actual location within a building. Set a value from 1 - 4094. The default setting is the 1st floor.

Latitude Coordinate	Set the latitude coordinate where devices are deployed within a floor. When looking at a floor map, latitude lines specify the *east-west* position of a point on the Earth's surface. The exact location of a device deployment can be ascertained by aligning the latitude and longitude points on the earth's surface.
Longitude Coordinate	Set the longitude coordinate where devices are deployed within a floor. When looking at a floor map, longitude lines specify the *north-south* position of a point on the Earth's surface. The exact location of a device deployment can be ascertained by aligning the longitude and latitude points on the earth's surface.

5 Use the **RF Domain** drop-down menu to select an existing RF Domain for device membership.

6 If a RF Domain configuration does not exist suiting the deployment requirements of the target device, select the **Create** icon to create a new RF Domain configuration, or select the **Edit** icon to modify the configuration of a selected RF Domain. For more information, see About RF Domains on page 9-1 or Managing RF Domains on page 9-2.

7 Use the **Profile** drop-down menu to select an existing device profile for multiple device deployment uniformity.

8 If a profile configuration does not exist suiting the deployment requirements of the target device, select the **Create** icon to create a new profile configuration, or select the **Edit** icon to modify the configuration of a selected profile. For more information, see General Profile Configuration on page 8-5.

9 If necessary, select the **Clear Overrides** button to remove all existing overrides from the device.

10 Refer to the **Set Clock** parameter to update the system time of the target device.

11 Refer to the **Device Time** parameter to assess the device's current time, or whether the device time is unavailable. Select **Refresh** as required to update the device's reported system time.

12 Use the **New Time** parameter to set the calendar day, hour and minute for the target device. Use the *AM* and *PM* radio buttons to refine whether the updated time is for the morning or afternoon/evening.

13 When completed, select **Update Clock** to commit the updated time to the target device.

14 If a T5 controller is deployed, select it from the **Type** drop-down menu and configure CPE VLAN Settings, in addition to the other parameters described in this section.

A T5 controller uses the a somewhat different operating system to manage its connected radio devices, as opposed to the WiNG operating used by RFS controllers and NX service platforms. However, a T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The *Customer Premises Equipment* (CPEs) are the T5 controller managed radio devices. These CPEs use a *Digital Subscriber Line* (DSL) as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

VLAN	Set a VLAN from 1 - 4,094 used as a virtual interface for connections between the T5 controller and its managed CPE devices.
Start IP	Set a starting IP address used in a range of addresses available to T5 controller connecting CPE devices.
End IP	Set an end IP address used in a range of addresses available to T5 controller connecting CPE devices.

15 Select **OK** to save the changes made to the screen. Selecting Reset reverts the screen to its last saved configuration.

5.2.1 License Configuration

Basic Device Configuration

Licenses are purchased directly for the number of permissible adoptions per controller, service platform or managed cluster.

NOTE: The Licenses screen is only available to wireless controllers capable of sustaining device connections, and thus requires license support to set the maximum number of allowed device connections. The License screen is not available for Access Points.

Managing infrastructure devices requires a license key to enable software functionality or define the number of adoptable devices permitted. My Licenses is a Web based online application enabling you to request a license key for license certificates for products.

NOTE: For detailed instructions on using My Licenses to add hardware or software licenses and register certificates, refer to the My Licenses Users Guide, available at www.extremenetworks.com/support.

The Licenses screen also contains a facility where new licenses can be applied to increase the number of device adoptions permitted, or to allow the use of the advanced security features.

Each controller and service platform family has multiple models to choose from that range from zero licenses to the maximum number that can be loaded for that specific SKU.

To configure a device's a license configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the Configuration tab.

The *Device Configuration* screen displays a list of managed devices or peer controllers, service platforms or Access Points.

3 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

4 Select **Licenses** from the Device menu options.

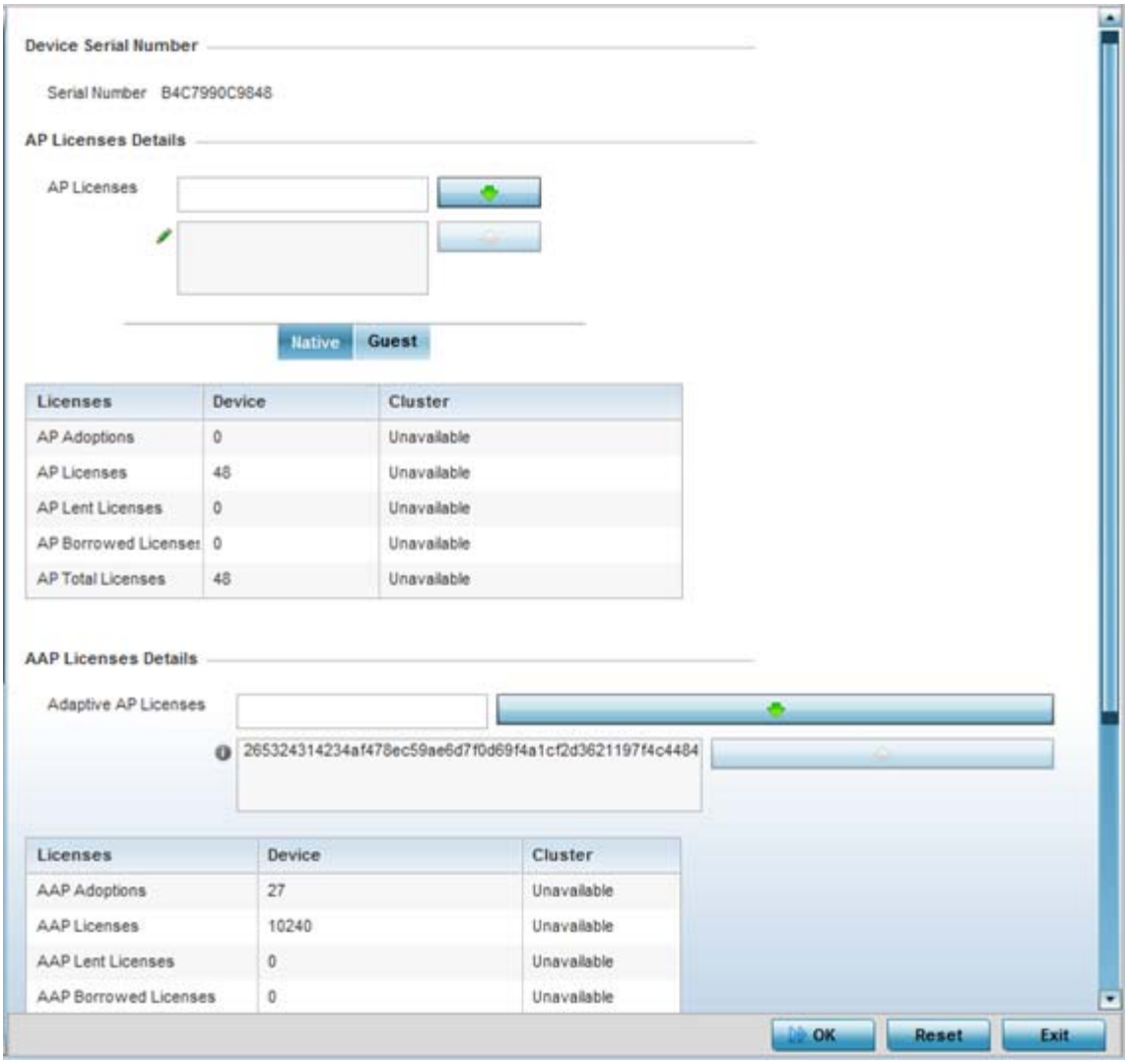


Figure 5-4 *Device Licenses screen*

The License screen displays the **Device Serial Number** of the controller or service platform generating the license key.

NOTE: When assessing *lent* and *borrowed* license information, its important to distinguish between site controllers and NOC controllers.

NOC controllers are NX9000, NX9500, NX9510, NX7500, NX6500, NX6524 and RFS6000.

Site controllers are NX4500, NX4524, NX5500, NX6500, NX6524, NX7500, RFS4000 and RFS6000.

5 Review the **AP Licenses** table to assess the specific number of adoptions permitted, as dictated by the terms of the current license. The **Native** tab displays by default. Select the **Guest** tab to display guest licenses.

AP Adoptions	The *Device* column Lists the total number of AP adoptions made by the controller or service platform. If the installed license count is 10 APs and the number of AP adoptions is 5, 5 additional APs can still be adopted under the terms of the license. The total number of APs adoptions varies by platform, as well as the terms of the license. The *Cluster* column lists the total number of AP adoptions made by the cluster membership (all members). If the installed license count is 100 APs and the number of AP adoptions is 50, 50 additional APs can still be adopted under the terms of the AP licenses, pooled by the cluster members.
AP Licenses	The *Device* column lists the number of APs available for adoption under the restrictions of the license. This number applies to dependent mode adaptive APs only, and not independent mode APs. The *Cluster* column lists the number of APs available for adoption by cluster members under the restrictions of the licenses, as pooled amongst the cluster members.
AP Lent Licenses	Lent licenses are the total number of AP licenses the NOC controller lends (if needed) to its site controllers so site controllers can adopt APs in excess of its own installed AP license count. AP lent licenses can be non-zero only in controllers currently configured as the NOC (NOC controller). Lent Licenses is always zero in controllers configured as the site (site controller).
AP Borrowed Licenses	Borrowed licenses are the total number of AP licenses borrowed by the site controller from the NOC controller (NOC controllers if a NOC controller is in a cluster). AP borrowed licenses are always zero in the NOC controller. AAP borrowed licenses can be non-zero only on site controllers.
AP Total Licenses	Lists the cumulative number of both *Device* and *Cluster* AP licenses supported by the listed controller or service platform.

NOTE: The following is a licensing example: Assume there are two site controllers (S1 and S2) adopted to a NOC controller (N1). S1 has 3 installed AP licenses, and S2 has 4 installed AP licenses. Eight APs seek to adopt on S1, and ten APs seek to adopt on S2. N1 has 1024 installed licenses. N1 lends 5 (8-3) AP licenses to S1, and 6 (10-4) AP licenses to S2.

N1 displays the following in the Device column: AP Adoptions: 2 (site controllers S1 and S2) AP Licenses: 1024 AP Lent Licenses: 11 (5 to S1 + 6 to S2) AP Borrowed Licenses: 0 AP Total Licenses: 1013 (1024 – 11 lent) S1 displays the following in the Device column: AP Adoptions: 8 AP Licenses: 3 AP Lent Licenses: 0 AP Borrowed Licenses: 5 AP Total Licenses: 8 (3 + 5 borrowed). S2 displays the following in the Device column: AP Adoptions: 10 AP Licenses: 4 AP Lent Licenses: 0 AP Borrowed Licenses: 6 AP Total Licenses: 10 (4 + 6 borrowed).

6 Review the **AAP Licenses** table to assess the specific number of adoptions permitted, as dictated by the terms of the current license.

AAP Adoptions	The *Device* column Lists the total number of AAP adoptions made by the controller or service platform. If the installed license count is 10 APs and the number of AAP adoptions is 5, 5 additional AAPs can still be adopted under the terms of the license. The total number of AAPs adoptions varies by platform, as well as the terms of the license. The *Cluster* column lists the total number of AAP adoptions made by the cluster membership (all members). If the installed license count is 100 APs and the number of AAP adoptions is 50, 50 additional AAPs can still be adopted under the terms of the AAP licenses, pooled by the cluster members.
AAP Licenses	The *Device* column lists the number of AAPs available for adoption under the restrictions of the license. This number applies to dependent mode adaptive AAPs only, and not independent mode AAPs. The *Cluster* column lists the number of AAPs available for adoption by cluster members under the restrictions of the licenses, as pooled amongst the cluster members.
AAP Lent Licenses	Lent licenses are the total number of AAP licenses the NOC controller lends (if needed) to its site controllers so site controllers can adopt adaptive APs in excess of its own installed AAP license count. AAP lent licenses can be non-zero only in controllers currently configured as the NOC (NOC controller). Lent Licenses is always zero in controllers configured as the site (site controller).
AAP Borrowed Licenses	Borrowed licenses are the total number of AAP licenses borrowed by the site controller from the NOC controller (NOC controllers if a NOC controller is in a cluster). AAP borrowed licenses are always zero in the NOC controller. AAP borrowed licenses can be non-zero only on site controllers.
AAP Total Licenses	Lists the cumulative number of both *Device* and *Cluster* AAP licenses supported by the listed controller or service platform.

7 Refer to the **Feature Licenses** field to apply licenses and provision advanced security and analytics features:

Advanced Security	Enter the provided license key required to install the Role Based Firewall feature and increase the number of IPSec VPN tunnels. The number of IPSec tunnels varies by platform.
Analytics Licenses	Enter the provided license key required to install Analytics (an enhanced statistical management tool) for NX4500, NX6500, NX7500 and NX9000 series service platforms.

8 Refer to the **Web Filtering License** field if required to provide a 256 character maximum license string for the Web filtering feature. Web filtering is used to restrict access to specific resources on the Internet.

9 Select **OK** to save the changes made to the applied licenses. Selecting **Reset** reverts the screen to its last saved configuration.

5.2.2 Assigning Certificates

Basic Device Configuration

A certificate links identity information with a public key enclosed in the certificate. A *certificate authority* (CA) is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the

certificate and is called a CA certificate. A browser must contain the CA certificate in its Trusted Root Library so it can trust certificates *signed* by the CA's private key.

Depending on the public key infrastructure, the digital certificate includes the owner's public key, the certificate expiration date, the owner's name and other public key owner information. Each certificate is digitally signed by a *trustpoint*. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.

SSH keys are a pair of cryptographic keys used to authenticate users instead of, or in addition to, a username/password. One key is private and the other is public key. *Secure Shell* (SSH) public key authentication can be used by a requesting client to access resources, if properly configured. A RSA key pair must be generated on the client. The public portion of the key pair resides with the controller or service platform, while the private portion remains on a secure local area of the client.

To configure certificate usage:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the Configuration tab.

The *Device Configuration* screen displays a list of managed devices or peer controllers, service platforms or Access Points.

3 Select **Certificates** from the Device menu.

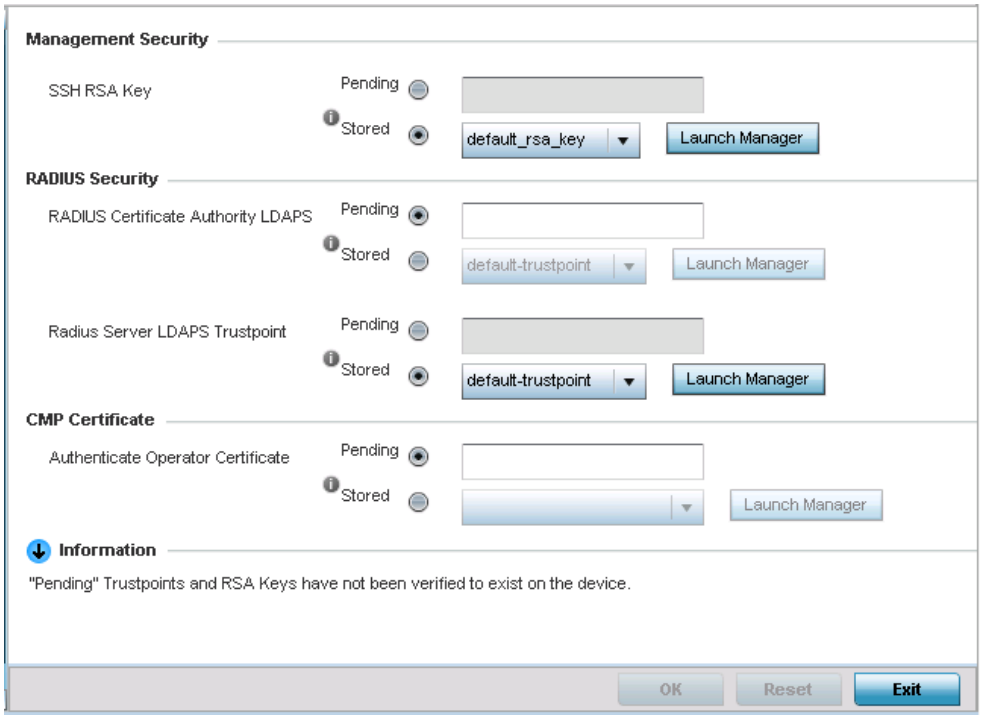


Figure 5-5 *Device Certificates screen*

4 Set the following **Management Security** certificate configurations:

SSH RSA Key	Either use the default_rsa_key or select the Stored radio button to enable a drop-down menu where an existing certificate can be used. To leverage an existing key, select the Launch Manager button. For more information, see RSA Key Management on page 5-21.

NOTE: Pending trustpoints and RSA keys are typically not verified as existing on a device.

5 Set the following **RADIUS Security** certificate configurations:

RADIUS Certificate Authority	Either use the default-trustpoint or select the *Stored* radio button to enable a drop-down menu where an existing certificate can be leveraged. To leverage an existing certificate, select the *Launch Manager* button.
RADIUS Server Certificate	Either use the default-trustpoint or select the *Stored* radio button to enable a drop-down menu where an existing certificate/trustpoint can be used. To leverage an existing trustpoint, select the *Launch Manager* button.
RADIUS Certificate Authority LDAPS	Either use the LDAP server default-trustpoint or select the *Stored* radio button to enable a drop-down menu where an existing certificate can be leveraged. To leverage an existing certificate, select the *Launch Manager* button.
Radius Server LDAPS Trustpoint	Either use the LDAP server default-trustpoint or select the *Stored* radio button to enable a drop-down menu where an existing certificate/ trustpoint can be used. To leverage an existing trustpoint, select the *Launch Manager* button.

6 Refer to the **CMP Certificate** field to optionally use *Certificate Management Protocol* (CMP) as an Internet protocol to obtain and manage digital certificates in a *Public Key Infrastructure* (PKI) network. A *Certificate Authority* (CA) issues the certificates using the defined CMP. Using CMP, a device can communicate to a CMP supported CA server, initiate a certificate request and download the required certificates from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting the certificates from the server. It can also auto update the certificates which are about to expire.

Either use the server default-trustpoint or select the *Stored* radio button to enable a drop-down menu where an existing certificate/trustpoint can be selected. To leverage an existing trustpoint, select the **Launch Manager** button.

7 Select **OK** to save the changes made to the certificate configurations. Selecting **Reset** reverts the screen to its last saved configuration.

For more information on the certification activities supported, refer to the following:

- *Certificate Management*
- *RSA Key Management*
- *Certificate Creation*
- *Generating a Certificate Signing Request*

5.2.2.1 Certificate Management

- *Assigning Certificates*

A *stored* certificate can be leveraged from a different managed device if not wanting to use an existing certificate or key. Device certificates can be imported and exported to and from the controller or service platform to a secure remote location for archive and retrieval as required for other managed devices.

To configure trustpoints for use with certificates:

1 Select **Launch Manager** from either the *HTTPS Trustpoint*, *SSH RSA Key*, *RADIUS Certificate Authority* or *RADIUS Server Certificate* parameters.

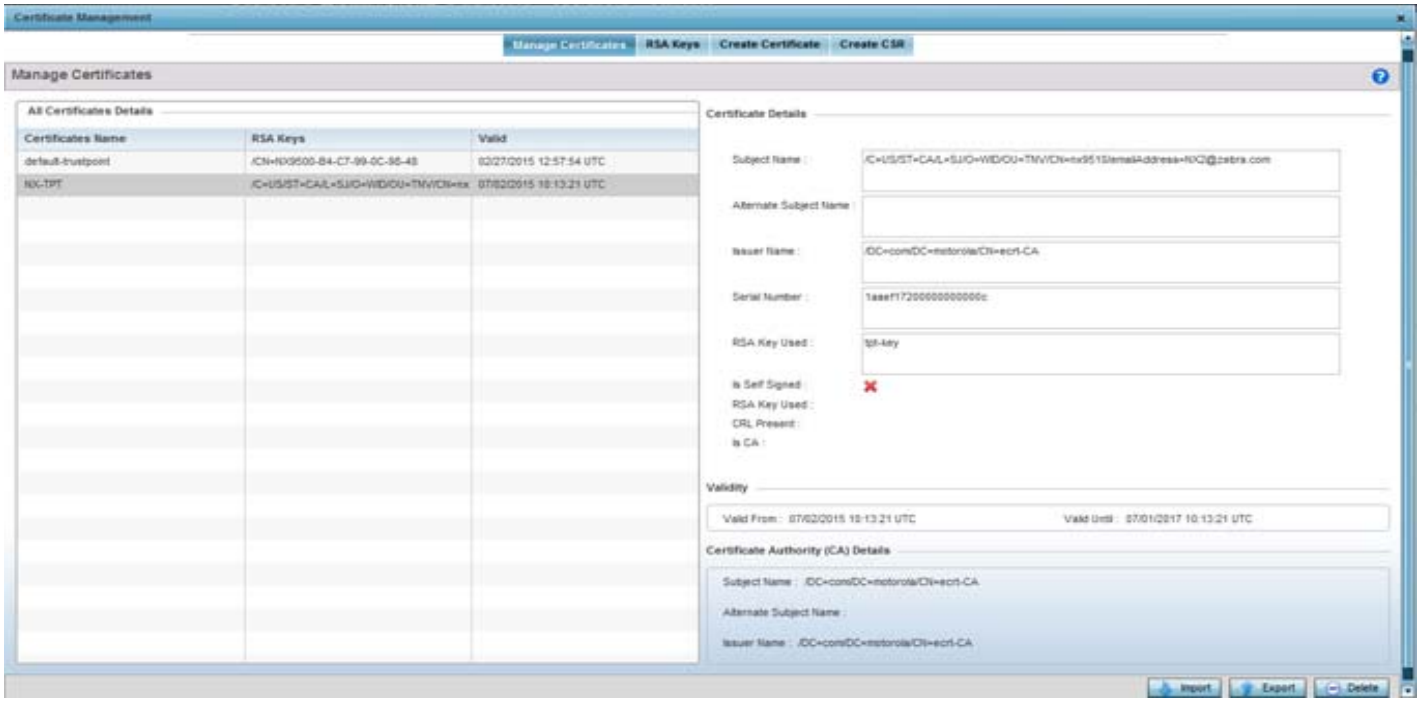


Figure 5-6 *Certificate Management - Manage Certificates screen*

The Certificate Management screen displays with the **Manage Certificates** tab displayed by default.

2 Select a device from amongst those displayed to review its certificate information.

3 Refer to the **All Certificates Details** to review the certificate's properties, self-signed credentials, validity duration and CA information.

4 To optionally import a certificate, select the **Import** button from the Certificate Management screen.

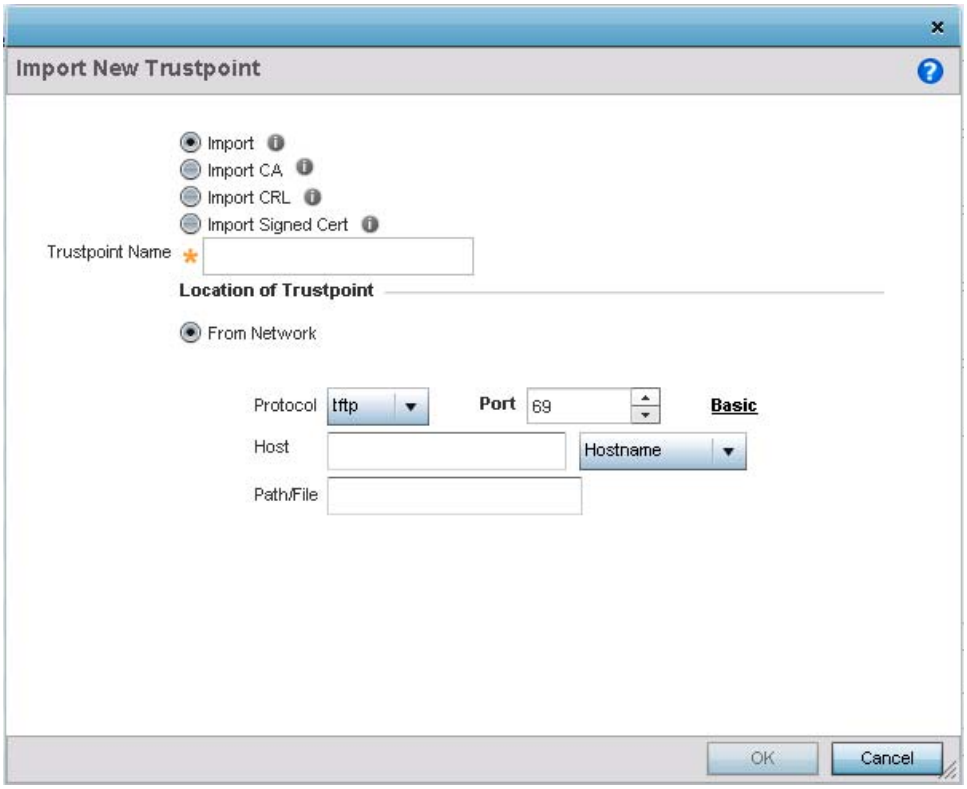


Figure 5-7 *Certificate Management - Import New Trustpoint screen*

5 Define the following configuration parameters required for the **Import** of the trustpoint.

Trustpoint Name	Enter the 32 character maximum name assigned to the target trustpoint. The trustpoint signing the certificate can be a *certificate authority*, *corporation* or *individual*.
URL	Provide the complete URL to the location of the trustpoint. If needed, select *Advanced* to expand the dialog to display network address information to the location of the target trustpoint. The number of additional fields that populate the screen is also dependent on the selected protocol.
Protocol	Select the protocol used for importing the target trustpoint. Available options include: tftp ftp sftp http cf usb1-4
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1-4*.

Host	Provide the hostname string or numeric IP address of the server used to import the trustpoint. Hostnames cannot include an underscore character. This option is not valid for *cf* and *usb1-4.* Select *IPv4 Address* to use an IPv4 formatted address as the host. Select IPv6 Address to use an IPv6 formatted address as the host. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Path/File	Specify the path to the trustpoint file. Enter the complete relative path to the file on the server.

6 Select **OK** to import the defined trustpoint. Select **Cancel** to revert the screen to its last saved configuration.

7 To optionally import a CA certificate, select the **Import CA** button from the Certificate Management screen.

A CA is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate.

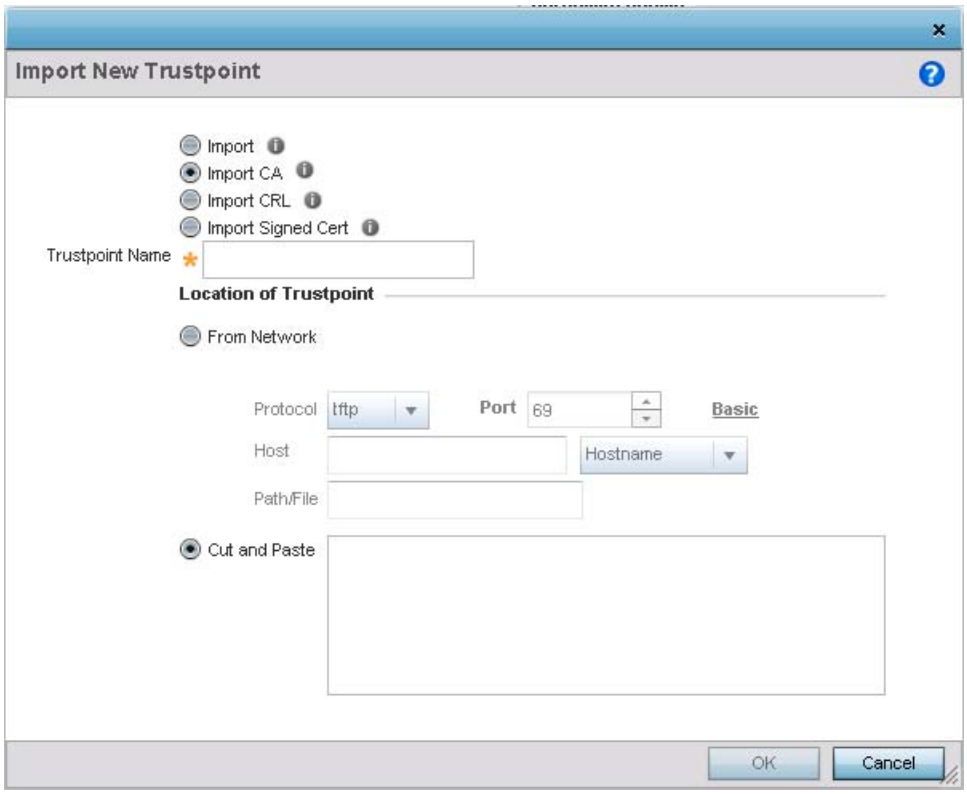


Figure 5-8 *Certificate Management - Import CA Certificate screen*

8 Define the following configuration parameters required for the **Import** of the CA certificate:

Trustpoint Name	Enter the 32 character maximum name assigned to the target trustpoint signing the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA specific configuration parameters, and an association with an enrolled identity certificate.
URL	Provide the complete URL to the location of the trustpoint. If needed, select *Advanced* to expand the dialog to display network address information to the location of the target trustpoint. The number of additional fields populating the screen is dependent on the selected protocol.
Advanced / Basic	Click the *Advanced* or *Basic* link to switch between a basic URL and an advanced location to specify trustpoint location.
Protocol	Select the protocol used for importing the target CA certificate. Available options include: tftp ftp sftp http cf usb1-4
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1-4*.
Host	Provide the hostname string or numeric IP address of the server used to import the CA. Hostnames cannot include an underscore character. This option is not valid for *cf* and *usb1-4*. Select *IPv4 Address* to use an IPv4 formatted address as the host. Select IPv6 Address to use an IPv6 formatted address as the host. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Path/File	Specify the path to the CA file. Enter the complete relative path to the file on the server.
Cut and Paste	Select the *Cut and Paste* radio button to simply copy an existing CA into the cut and paste field. When pasting, no additional network address information is required.

9 Select **OK** to import the defined CA certificate. Select **Cancel** to revert the screen to its last saved configuration.

10 Select the **Import CRL** button from the Certificate Management screen to optionally import a CRL to a controller or service platform.

If a certificate displays within the Certificate Management screen with a CRL, that CRL can be imported. A *certificate revocation list* (CRL) is a list of certificates that have been revoked or are no longer valid. A certificate can be revoked if the CA had improperly issued a certificate, or if a private-key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.

For information on creating a CRL to use with a trustpoint, refer to Setting the Profile's Certificate Revocation List (CRL) Configuration on page 8-166.

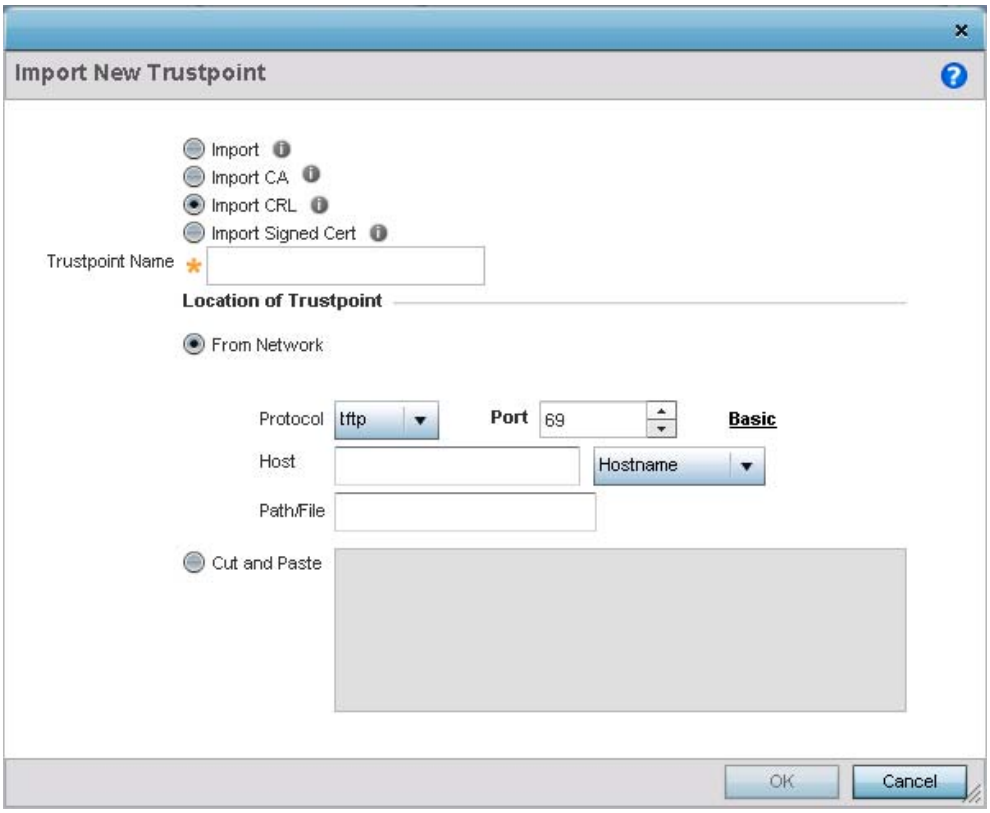


Figure 5-9 *Certificate Management - Import CRL screen*

11 Define the following configuration parameters required for the **Import** of the CRL

Trustpoint Name	Enter the 32 character maximum name assigned to the target trustpoint signing the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.
From Network	Select the *From Network* radio button to provide network address information to the location of the target CRL. The number of additional fields that populate the screen is also dependent on the selected protocol. This is the default setting.
URL	Provide the complete URL to the location of the CRL. If needed, select *Advanced* to expand the dialog to display network address information to the location of the CRL. The number of additional fields that populate the screen is also dependent on the selected protocol.
Protocol	Select the protocol used for importing the CRL. Available options include: tftp ftp sftp http cf usb1-4
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1-4*.

Host	Provide the hostname string or numeric IP address of the server used to import the CRL. Hostnames cannot include an underscore character. This option is not valid for *cf* and *usb1-4*. Select *IPv4 Address* to use an IPv4 formatted address as the host. Select *IPv6 Address* to use an IPv6 formatted address as the host. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Path/File	Specify the path to the CRL file. Enter the complete relative path to the file on the server.
Cut and Paste	Select the *Cut and Paste* radio button to simply copy an existing CRL into the cut and paste field. When pasting, no additional network address information is required.

12 Select **OK** to import the CRL. Select **Cancel** to revert the screen to its last saved configuration.

13 To import a signed certificate, select the **Import Signed Cert** button from the Certificate Management screen.

Signed certificates (or root certificates) avoid the use of public or private CAs. A self-signed certificate is an identity certificate signed by its own creator, thus the certificate creator also signs off on its legitimacy. The lack of mistakes or corruption in the issuance of self signed certificates is central.

Self-signed certificates cannot be revoked which may allow an attacker who has already gained access to monitor and inject data into a connection to spoof an identity if a private key has been compromised. However, CAs have the ability to revoke a compromised certificate, preventing its further use.

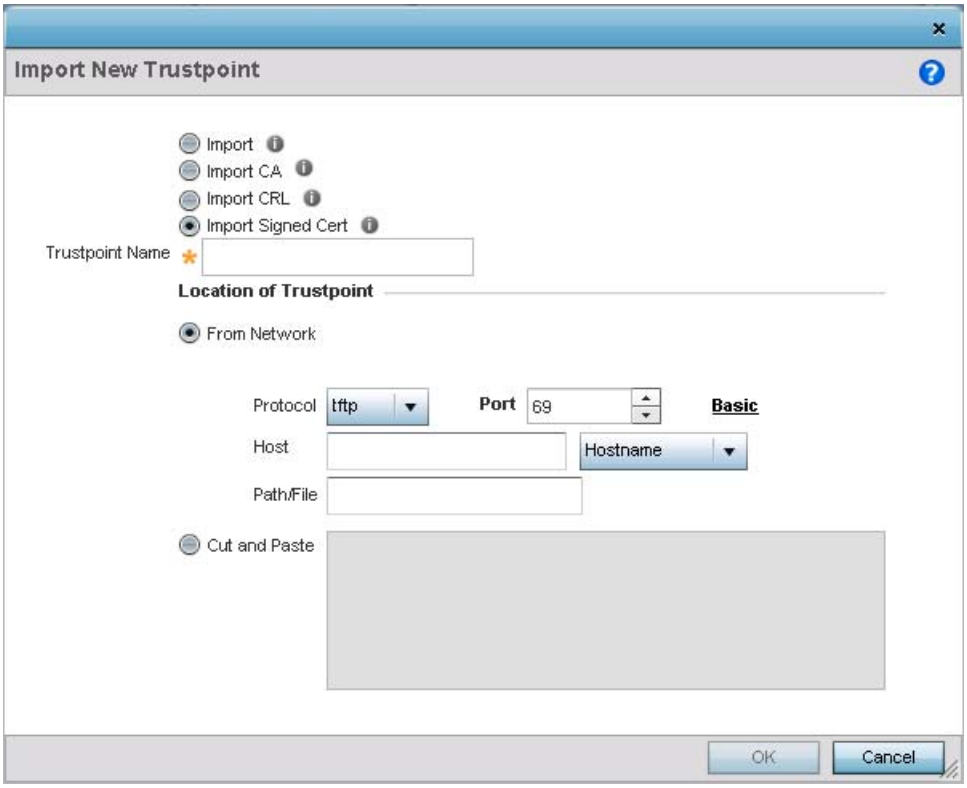


Figure 5-10 *Certificate Management - Import Signed Cert screen*

14 Define the following parameters required for the **Import** of the CA certificate:

Certificate Name	Enter the 32 character maximum trustpoint name with which the certificate should be associated.
From Network	Select the *From Network* radio button to provide network address information to the location of the signed certificate. The number of additional fields that populate the screen is dependent on the selected protocol. From Network is the default setting.
URL	Provide the complete URL to the location of the signed certificate. If needed, select *Advanced* to expand the dialog to display network address information to the location of the signed certificate. The number of additional fields populating the screen is dependent on the selected protocol.
Protocol	Select the protocol for importing the signed certificate. Available options include: tftp ftp sftp http cf usb1-4
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1-4*.
Host	Provide the hostname string or numeric IP address of the server used to import the signed certificate. Hostnames cannot include an underscore character. This option is not valid for *cf* and *usb1-4*. Select *IPv4 Address* to use an IPv4 formatted address as the host. Select *IPv6 Address* to use an IPv6 formatted address as the host. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Path/File	Specify the path to the signed certificate file. Enter the complete relative path to the file on the server.
Cut and Paste	Select the *Cut and Paste* radio button to simply copy an existing certificate into the cut and paste field. When pasting, no additional network address information is required.

15 Select **OK** to import the signed certificate. Select **Cancel** to revert the screen to its last saved configuration.

16 To optionally export a trustpoint to a remote location, select the **Export** button from the Certificate Management screen.

Once a certificate has been generated on the controller or service platform's authentication server, export the self signed certificate. A digital CA certificate is different from a self signed certificate. The CA certificate contains the public and private key pairs. The self certificate only contains a public key. Export the self certificate for publication on a Web server or file server for certificate deployment or export it in to an active directory group policy for automatic root certificate deployment.

17 Additionally export the key to a redundant RADIUS server so it can be imported without generating a second key. If there's more than one RADIUS authentication server, export the certificate and don't generate a second key unless you want to deploy two root certificates.

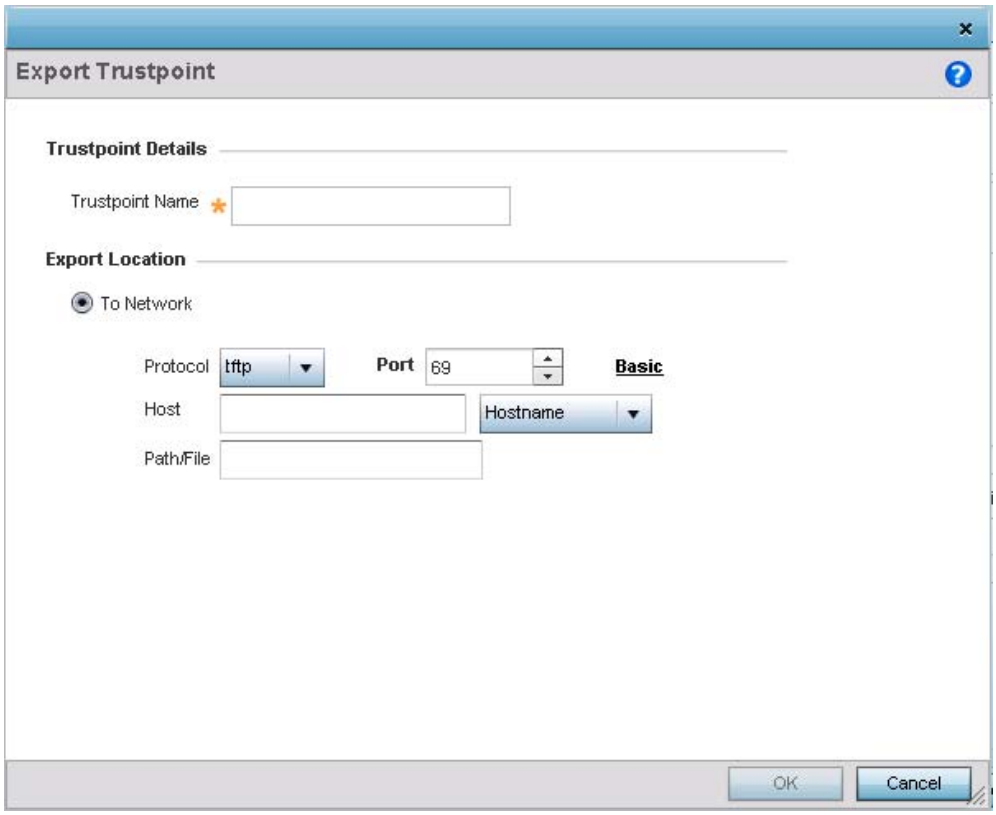


Figure 5-11 *Certificate Management - Export Trustpoint screen*

18 Define the following configuration parameters required for the **Export** of the trustpoint.

Trustpoint Name	Enter the 32 character maximum name assigned to the trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual.
URL	Provide the complete URL to the location of the trustpoint. If needed, select *Advanced* to expand the dialog to display network address information to the location of the trustpoint. The number of additional fields that populate the screen is dependent on the selected protocol.
Protocol	Select the protocol used for exporting the target trustpoint. Available options include: tftp ftp sftp http cf usb1-4
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1-4*.

Host	Provide the hostname string or numeric IP address of the server used to export the trustpoint. Hostnames cannot include an underscore character. This option is not valid for *cf* and *usb1-4*. Select *IPv4 Address* to use an IPv4 formatted address as the host. Select *IPv6 Address* to use an IPv6 formatted address as the host. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Path/File	Specify the path to the signed trustpoint file. Enter the complete relative path to the file on the server.
Cut and Paste	Select the *Cut and Paste* radio button to simply copy an existing trustpoint into the cut and paste field. When pasting, no additional network address information is required.

19 Select **OK** to export the defined trustpoint. Select **Cancel** to revert the screen to its last saved configuration.

20 To optionally delete a trustpoint, select the **Delete** button from within the Certificate Management screen. Provide the trustpoint name within the **Delete Trustpoint** screen and optionally select **Delete RSA Key** to remove the RSA key along with the trustpoint. Select **OK** to proceed with the deletion, or **Cancel** to revert to the Certificate Management screen

5.2.2.2 RSA Key Management

- *Assigning Certificates*

Refer to the RSA Keys screen to review existing RSA key configurations that have been applied to managed devices. If an existing key does not meet the needs of a pending certificate request, generate a new key or import/export an existing key to and from a remote location.

Rivest, Shamir, and Adleman (RSA) is an algorithm for public key cryptography. It's an algorithm that can be used for certificate signing and encryption. When a device trustpoint is created, the RSA key is the private key used with the trustpoint.

To review existing device RSA key configurations, generate additional keys or import/export keys to and from remote locations:

1 Select the **Launch Manager** button from either the SSH RSA Key, RADIUS Certificate Authority or RADIUS Server Certificate parameters (within the Certificate Management screen).

2 Select **RSA Keys** from the Certificate Management screen.

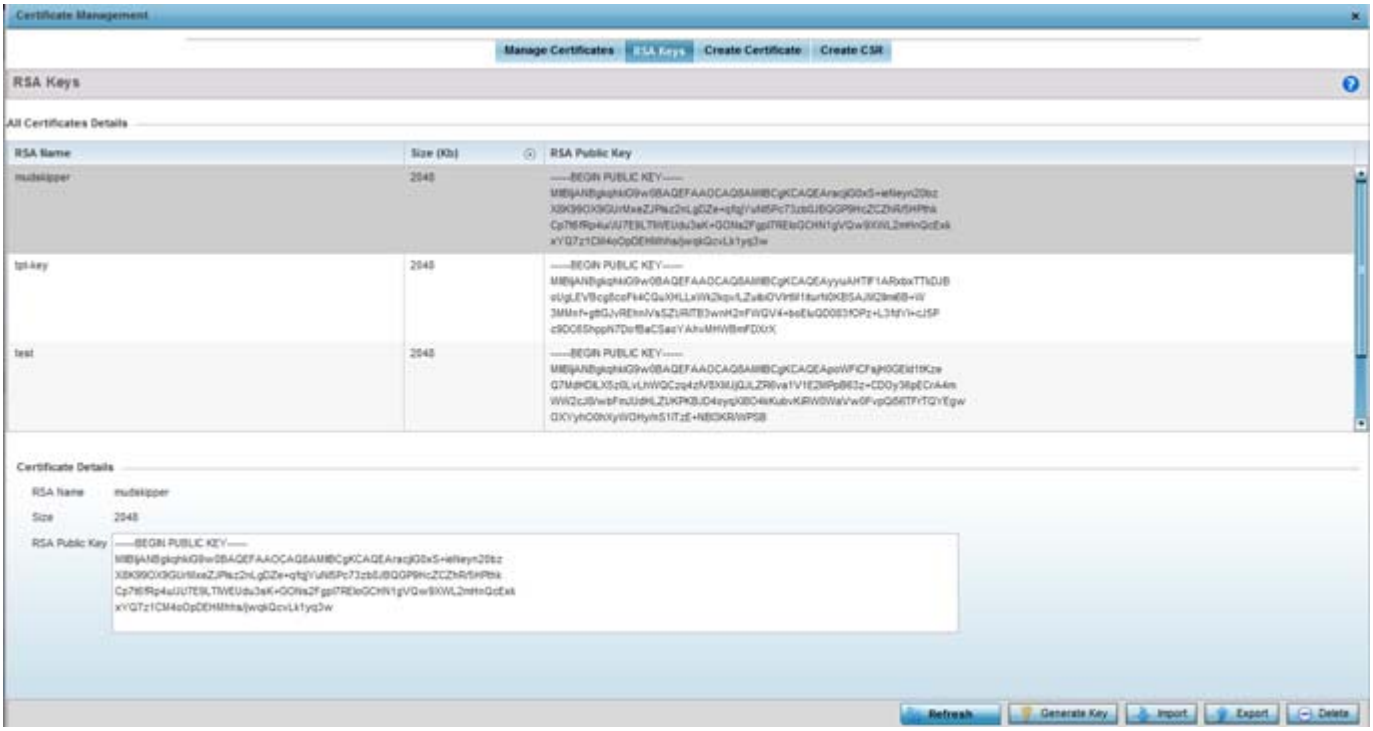


Figure 5-12 *Certificate Management - RSA Keys screen*

3 Select a listed device to review its current RSA key configuration.

Each key can have its size and character syntax displayed. Once reviewed, optionally generate a new RSA key, import a key from a selected device, export a key to a remote location or delete a key from a selected device.

4 Select **Generate Key** to create a new key with a defined size.

Figure 5-13 *Certificate Management - Generate RSA Keys screen*

5 Define the following configuration parameters required for the **Import** of the key:

Key Name	Enter the 32 character maximum name assigned to the RSA key.
Key Size	Set the size of the key as either 2048 (bits) or 4096 (bits). Leaving this value at the default setting of 2048 is recommended to ensure optimum functionality.

6 Select **OK** to generate the RSA key. Select **Cancel** to revert the screen to its last saved configuration.

7 To optionally import a CA certificate, select the **Import** button from the Certificate Management > RSA Keys screen.

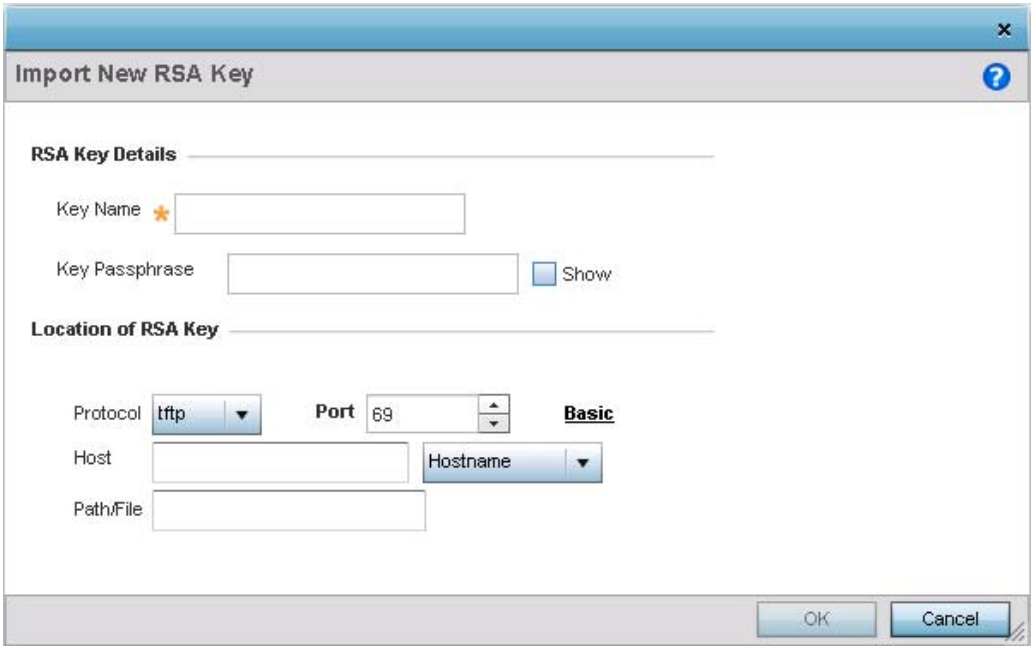


Figure 5-14 *Certificate Management - Import New RSA Key screen*

8 Define the following parameters required for the **Import** of the RSA key:

Key Name	Enter the 32 character maximum name assigned to identify the RSA key.
Key Passphrase	Define the key used by both the controller or service platform and the server (or repository) of the target RSA key. Select the *Show* to expose the actual characters used in the passphrase. Leaving the Show unselected displays the passphrase as a series of asterisks "*".
URL	Provide the complete URL to the location of the RSA key. If needed, select *Advanced* to expand the dialog to display network address information to the location of the target key. The number of additional fields that populate the screen is dependent on the selected protocol.
Advanced or **Basic**	Select either the *Advanced* or *Basic* link to switch between a basic URL and an advanced location to specify key location.
Protocol	Select the protocol used for importing the target key. Available options include: tftp ftp sftp http cf usb1-4
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1-4*.

Host	Provide a text string hostname or numeric IP address of the server used to import the RSA key. Hostnames cannot include an underscore character. This option is not valid for *cf* and *usb1-4*. Select *IPv4 Address* to use an IPv4 formatted address as the host. Select *IPv6 Address* to use an IPv6 formatted address as the host. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Path/File	Specify the path to the RSA key. Enter the complete relative path to the key on the server.

9 Select **OK** to import the defined RSA key. Select **Cancel** to revert the screen to its last saved configuration.

10 To optionally export a RSA key to a remote location, select the **Export** button from the Certificate Management > RSA Keys screen.

Export the key to a redundant RADIUS server to import it without generating a second key. If there's more than one RADIUS authentication server, export the certificate and don't generate a second key unless you want to deploy two root certificates.

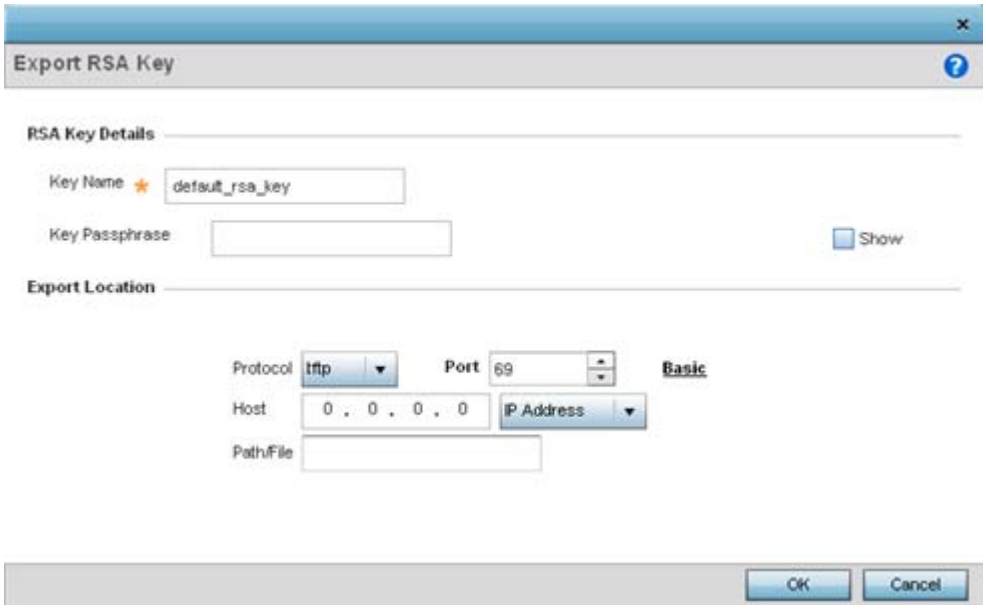


Figure 5-15 *Certificate Management - Export RSA Key screen*

11 Define the following configuration parameters required for the **Export** of the RSA key.

Key Name	Enter the 32 character maximum name assigned to the RSA key.
Key Passphrase	Define the key passphrase used by both the controller or service platform and the server. Select *Show* to expose the actual characters used in the passphrase. Leaving the Show unselected displays the passphrase as a series of asterisks "*".
URL	Provide the complete URL to the location of the key. If needed, select *Advanced* to expand the dialog to display network address information to the location of the target key. The number of additional fields that populate the screen is dependent on the selected protocol.

Protocol	Select the protocol used for exporting the RSA key. Available options include: tftp ftp sftp http cf usb1-4
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1-4*.
Host	Provide a text string hostname or numeric IP address of the server used to export the RSA key. Hostnames cannot include an underscore character. This option is not valid for cf and usb1-4. Select *IPv4 Address* to use an IPv4 formatted address as the host. Select *IPv6 Address* to use an IPv6 formatted address as the host. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Path / File	Specify the path to the key. Enter the complete relative path to the key on the server.

12 Select **OK** to export the defined RSA key. Select **Cancel** to revert the screen to its last saved configuration.

13 To optionally delete a key, select the **Delete** button from within the Certificate Management > RSA Keys screen. Provide the key name within the **Delete RSA Key** screen and select **Delete Certificates** to remove the certificate. Select **OK** to proceed with the deletion, or **Cancel** to revert back to the Certificate Management screen.

5.2.2.3 Certificate Creation

Assigning Certificates

The Certificate Management screen provides the facility for creating new self-signed certificates. Self signed certificates (often referred to as root certificates) do not use public or private CAs. A self signed certificate is a certificate signed by its own creator, with the certificate creator responsible for its legitimacy.

To create a self-signed certificate that can be applied to a managed device:

1 Select the **Launch Manager** button from either the SSH RSA Key, RADIUS Certificate Authority or RADIUS Server Certificate parameters (within the Certificate Management screen).

2 Select **Create Certificate** from the upper, left-hand, side of the Certificate Management screen.

Figure 5-16 *Certificate Management - Create Certificate screen*

3 Define the following configuration parameters required to **Create New Self-Signed Certificate**:

Certificate Name	Enter the 32 character maximum name assigned to identify the name of the trustpoint associated with the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.
RSA Key	Select a radio button and use the drop-down menu to set the key used by both the controller or service platform and the server (or repository) of the target RSA key. Optionally select *Create New* and enter a 32 character name used to identify the RSA key. Set the size of the key to either 2,048 or 4,096 bits. Leaving this value at the default setting of 2,048 is recommended to ensure optimum functionality.

4 Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

Certificate Subject Name	Select either *auto-generate* to automatically create the certificate's subject credentials or *user-configurable* to manually enter the credentials of the self signed certificate. The default setting is auto-generate.
Country (C)	Define the *Country* used in the certificate. The field can be modified by the user to other values. This is a required field and must not exceed 2 characters.
State (ST)	Enter a *State/Prov.* for the state or province name used in the certificate. This is a required field.
City (L)	Enter a *City* to represent the city used in the certificate. This is a required field.
Organization (O)	Define an *Organization* for the organization represented in the certificate. This is a required field.
Organizational Unit (OU)	Enter an *Org. Unit* for the organization unit represented in the certificate. This is a required field.
Common Name (CN)	If there's a common name (IP address) for the organizational unit issuing the certificate, enter it here.

5 Select the following **Additional Credentials** required for the generation of the self signed certificate:

Email Address	Provide an *Email Address* used as the contact address for issues relating to this certificate request.
Domain Name	Enter a *fully qualified domain name* (FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely. To distinguish an FQDN from a regular domain name, a trailing period is added. For example, *somehost.example.com*. An FQDN differs from a regular domain name by its absoluteness, since a suffix is not added.
IP Address	Specify the IP address used as the destination for certificate requests.Only IPv4 formatted IP addresses are permitted, not IPv6 formatted addresses.

6 Select the **Generate Certificate** button at the bottom of the Certificate Management > Create Certificate screen to produce the certificate.

5.2.2.4 Generating a Certificate Signing Request

Assigning Certificates

A *certificate signing request* (CSR) is a request to a certificate authority to apply for a digital identity certificate. The CSR is a block of encrypted text generated on the server the certificate is used on. It contains the organization name, common name (domain name), locality and country.

A RSA key must be either created or applied to the certificate request before the certificate can be generated. A private key is not included in the CSR, but is used to digitally sign the completed request. The certificate created with a particular CSR only works with the private key generated with it. If the private key is lost, the certificate is no longer functional.The CSR can be accompanied by other identity credentials required by the certificate authority, and the certificate authority maintains the right to contact the applicant for additional information.

If the request is successful, the CA sends an identity certificate digitally signed with the private key of the CA.

To create a CSR:

1 Select the **Launch Manager** button from either the SSH RSA Key, RADIUS Certificate Authority or RADIUS Server Certificate parameters (within the Certificate Management screen).

2 Select **Create CSR** from the upper, left-hand, side of the Certificate Management screen.

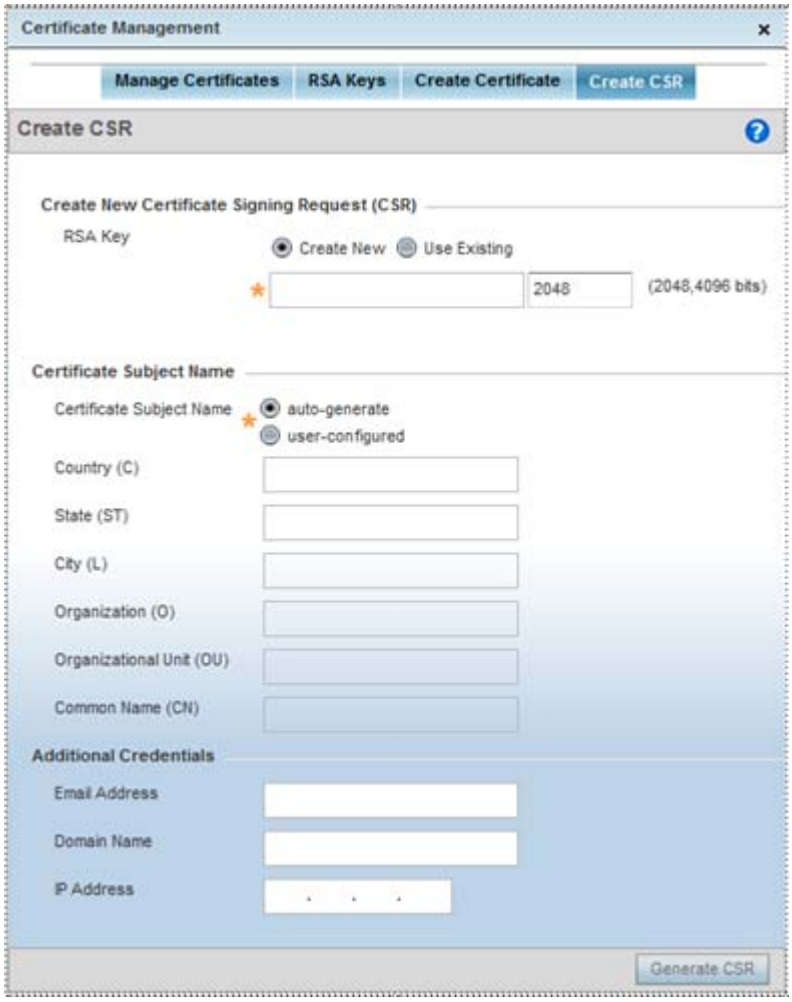


Figure 5-17 *Certificate Management - Create CSR screen*

3 Define the following configuration parameters required to **Create New Certificate Signing Request (CSR)**:

RSA Key	Select a radio button and use the drop-down menu to set the key used by both the controller or service platform and the server (or repository) of the target RSA key. Optionally select *Create New* to use new RSA key and provide a 32 character name used to identify the RSA key. Set the size of the key to either 2,048 or 4,096 bits. Leaving this value at the default setting of 2,048 is recommended to ensure optimum functionality.

4 Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

Certificate Subject Name	Select either the *auto-generate* radio button to automatically create the certificate's subject credentials or *user-configurable* to manually enter the credentials of the self signed certificate. The default setting is auto-generate.
Country (C)	Define the *Country* used in the CSR. The field can be modified by the user to other values. This is a required field and must not exceed 2 characters.

State (ST)	Enter a *State/Prov.* for the state or province name represented in the CSR. This is a required field.
City (L)	Enter a *City* represented in the CSR. This is a required field.
Organization (O)	Define the *Organization* represented in the CSR. This is a required field.
Organizational Unit (OU)	Enter the *Org. Unit* represented in the CSR. This is a required field.
Common Name (CN)	If there's a common name (IP address) for the organizational unit issuing the certificate, enter it here.

5 Select the following **Additional Credentials** required for the generation of the CSR:

Email Address	Provide an email address used as the contact address for issues relating to this CSR.
Domain Name	Enter a *fully qualified domain name* (FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely. To distinguish an FQDN from a regular domain name, a trailing period is added. ex: somehost.example.com. An FQDN differs from a regular domain name by its absoluteness; as a suffix is not added.
IP Address	Specify the IP address used as the destination for certificate requests.Only IPv4 formatted IP addresses are permitted, not IPv6 formatted addresses.

6 Select the **Generate CSR** button to produce the CSR.

5.2.3 Port Mirroring (NX4524 and NX6524 Service Platforms only)

Basic Device Configuration

NX4524 and NX6524 model service platforms have the ability to mirror data packets transmitted or received on any of their GE ports (GE port 1 - 24). Both transmit and receive packets can be mirrored from a source to a destination port as needed to provide traditional *spanning* functionality on the 24 GE ports.

NOTE: Port mirroring is not supported on NX4500 or NX6500 models, as they only utilize GE ports 1 - 2. Additionally, port mirroring is not supported on uplink (up) ports or wired ports on any controller or service platform model.

To set a NX4524 or NX6524 service platform port mirror configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

3 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

4 Select **Mirroring** from the Device menu options.

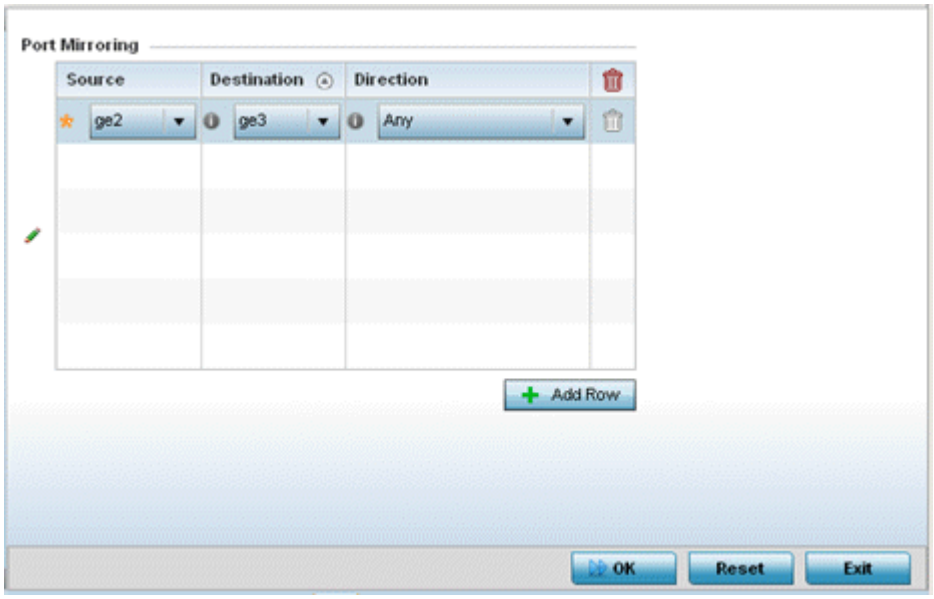


Figure 5-18 *Port Mirroring screen*

5 Set the following **Port Mirroring** values to define the ports and directions data is spanned on the NX4524 or NX6524 model service platform:

Source	Select the GE port (1 - 24) used as the data source to span packets to the selected destination port. The packets spanned from the selected source to the destination depend on whether *Inbound, Outbound* or *Any* is selected as the direction. A source port cannot be a destination port.
Destination	Select the GE port (1 - 24) used as the port destination to span packets from the selected source. The destination port serves as a duplicate image of the source port and can be used to send packets to a network diagnostic without disrupting the behavior on the original port. The destination port transmits only mirrored traffic and does not forward received traffic. Additionally, address learning is disabled on the destination port.
Direction	Define the direction data packets are spanned from the selected source to the defined destination. Packets spanned from the source to the destination depend on whether *Inbound* (received packets only), *Outbound* (transmitted packets only) or *Any* (packets in either direction) is selected.

6 Select **+ Add Row** to add different sources, destinations and directions for additional GE port spanning configurations.

7 Select **OK** to save the changes made to the NX4524 or NX6524 port mirroring configuration. Selecting **Reset** reverts the screen to its last saved configuration.

5.2.4 Wired 802.1x Configuration

Basic Device Configuration

802.1X is an IEEE standard for media-level (Layer 2) access control, providing the capability to *permit* or *deny* connectivity based on user or device identity. 802.1X allows port based access using authentication. An 802.1X enabled port can be dynamically *enabled* or *disabled* depending on user identity or device connection.

Before authentication, the endpoint is unknown, and traffic is blocked. Upon authentication, the endpoint is known and traffic is allowed. The controller or service platform uses source MAC filtering to ensure only the authenticated endpoint is allowed to send traffic.

To configure a device's wired 802.1x configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the Configuration tab.
The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

3 Select a device (by double-clicking it) from amongst those displayed within the Device Configuration screen. Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

4 Select **Wired 802.1x** from the Device menu options.

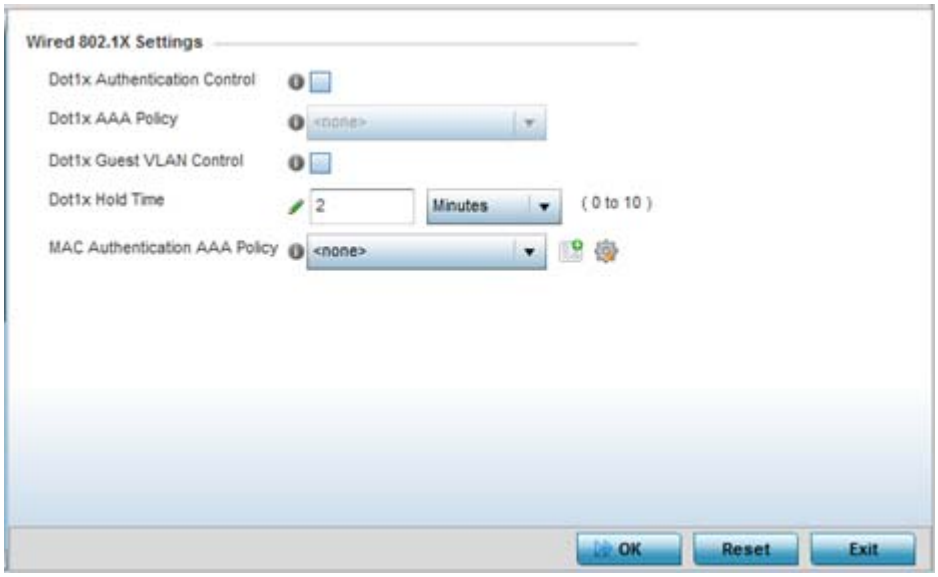


Figure 5-19 *Device Wired 802.1x screen*

5 Review the **Wired 802.1x Settings** area to configure the following parameters:

Dot1x Authentication Control	Select this option to globally enable 802.1x authentication. 802.1x authentication is disabled by default.
Dot1x AAA Policy	Use the drop-down menu to select a AAA policy to associate with wired 802.1x traffic. If a suitable AAA policy does not exist, select the *Create* icon to create a new policy or the *Edit* icon to modify an existing policy.
Dot1x Guest VLAN Control	Select this option to globally enable the use of 802.1x guest VLANs.
Dot1x Hold Time	Set a hold time value (after the last hello packet) in either *Seconds* (0 - 600) or *Minutes* (0 - 10). When exceeded, the controller's 802.1X enabled port and its destination end-point connection is defined as lost and the connection must be re-established.
MAC Authentication AAA Policy	Use the drop-down menu to select an AAA authentication policy for MAC address authentication. If a suitable MAC AAA policy does not exist, click the *Create* icon to create a new policy or the *Edit* icon to modify an existing policy.

6 Select **OK** to save the changes made to the 802.1x configurations. Selecting **Reset** reverts the screen to its last saved configuration.

5.2.5 RF Domain Overrides

Basic Device Configuration

Use **RF Domain Overrides** to define configurations overriding the configuration set by the target device's original RF Domain assignment.

RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area (floor, building or site). In such instances, there's many configuration attributes these devices share, since their general client support roles are quite similar. However, device configurations may need periodic refinement from their original RF Domain administered design.

A controller or service platform configuration contains (at a minimum) one default RF Domain, but can optionally use additional user defined RF Domains:

- *Default RF Domain* - Automatically assigned to each controller, service platform and associated Access Points by default. A default RF Domain is unique to a specific model.
- *User Defined RF Domains* - Created by administrators and manually assigned to individual controllers, service platforms or Access Points, but can be automatically assigned to Access Points using adoption policies.

Each controller, service platform and Access Point is assigned one RF Domain at a time. However, a user defined RF Domain can be assigned to multiple devices as required. User defined RF Domains can be manually assigned or automatically assigned to Access Points using an auto provisioning policy. The more devices assigned a single RF Domain, the greater the likelihood one of the device's configurations will require an override deviating that device's configuration from the original RF Domain assignment shared by the others.

To review the RF Domain's original configuration requirements and the options available for a target device, refer to Managing RF Domains on page 9-2.

To define a device's RF Domain override configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

3 Select a device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

4 Expand the **RF Domain Overrides** menu option to display its sub-menu options.

5 Select **RF Domain**.

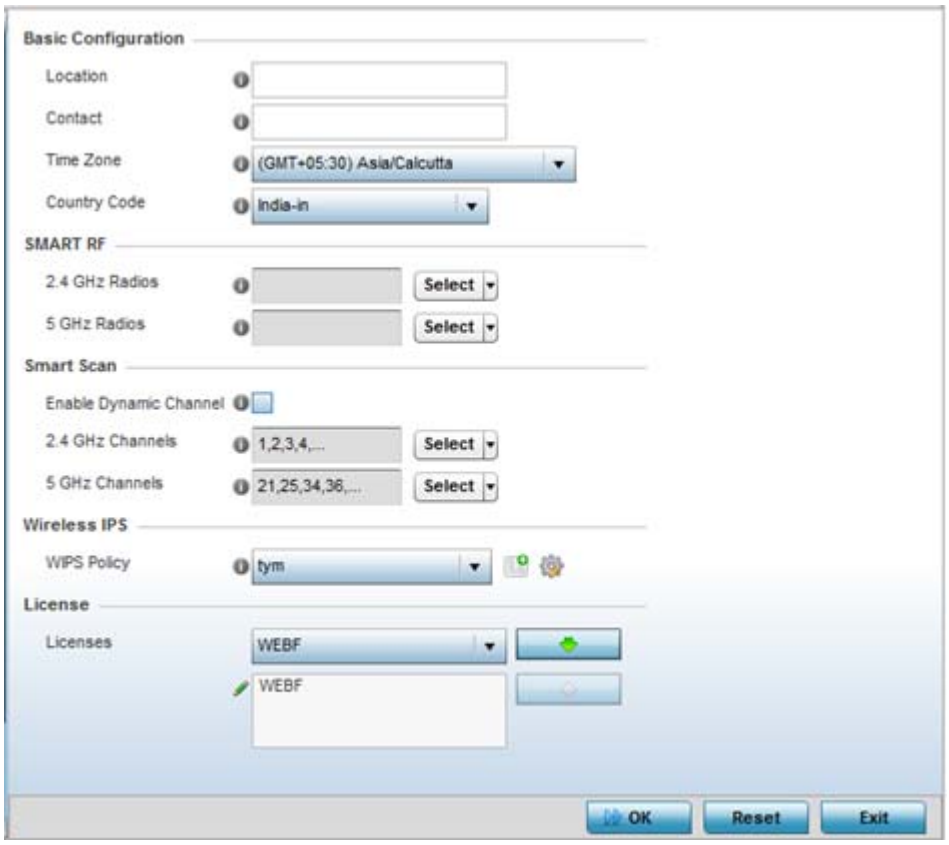


Figure 5-20 *RF Domain Overrides - Basic Configuration screen*

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

6 Refer to the **Basic Configuration** field to review the basic settings defined for the target device's RF Domain configuration, and optionally assign/remove overrides to and from specific parameters.

Location	Provide the 64 character maximum deployment location set for the controller or service platform as part of its RF Domain configuration.
Contact	Enter the 64 character maximum administrative contact for the controller or service platform as part of its RF Domain configuration.
Time Zone	Set the time zone utilized by the selected device as part of its RF Domain configuration.
Country Code	Set the country code utilized by the device as part of its RF Domain configuration. Selecting the correct country is central to legal operation. Each country has its own regulatory restrictions concerning electromagnetic emissions and the maximum RF signal strength that can be transmitted.

7 Refer to the **Smart RF** section to configure Smart RF policy and dynamic channel settings.

2.4 GHz Radios	Select an override group of channels Smart RF can use for channel compensation adjustments in the 2.4 GHz band.
5 GHz Radios	Select an override group of channels Smart RF can use for channel compensation adjustments in the 5 GHz band.

8 Refer to the **Smart Scan** section to configure Smart RF policy and dynamic channel settings.

Enable Dynamic Channel	Select this option to enable dynamic channel switching for Smart RF radios.
2.4 GHz Channels	Select legal channels (device radios transmit in specific channels unique to their country of operation) from the drop-down menu for 2.4GHz Smart RF radios.
5 GHz Channels	Select legal channels (device radios transmit in specific channels unique to their country of operation) from the drop-down menu for 5GHz Smart RF radios.

9 Use the **WIPS Policy** drop-down menu to apply a WIPS policy to the RF Domain.

The *Wireless Intrusion Protection System* (WIPS) provides continuous protection against wireless threats and act as an additional layer of security complementing wireless VPNs and encryption and authentication policies. Controllers and service platforms support WIPS through the use of dedicated sensor devices, designed to actively detect and locate unauthorized AP devices. After detection, they use mitigation techniques to block devices using manual termination, air lockdown or port suppression.

Select the **Create** icon to define a new WIPS policy that can be applied to the RF Domain, or select the **Edit** icon to modify or override an existing WIPS policy.

For an overview of WIPS and instructions on how to create a WIPS policy that can be used with a RF Domain, see Intrusion Prevention on page 10-51.

10 Use the **Licenses** drop-down menu to obtain and leverage feature licenses from RF Domain member devices.

11 Select **OK** to save the changes and overrides made to the RF Domain configuration. Selecting **Reset** reverts the screen to its last saved configuration.

12 Select **Sensor** from within the expanded RF Domain Overrides menu to define ADSP server credentials for WiNG controller or service platform data exchanges.

Controllers and service platforms support dedicated sensor devices, designed to actively detect and locate unauthorized AP devices. After detection, they use mitigation techniques to block devices using manual termination, air lockdown or port suppression.

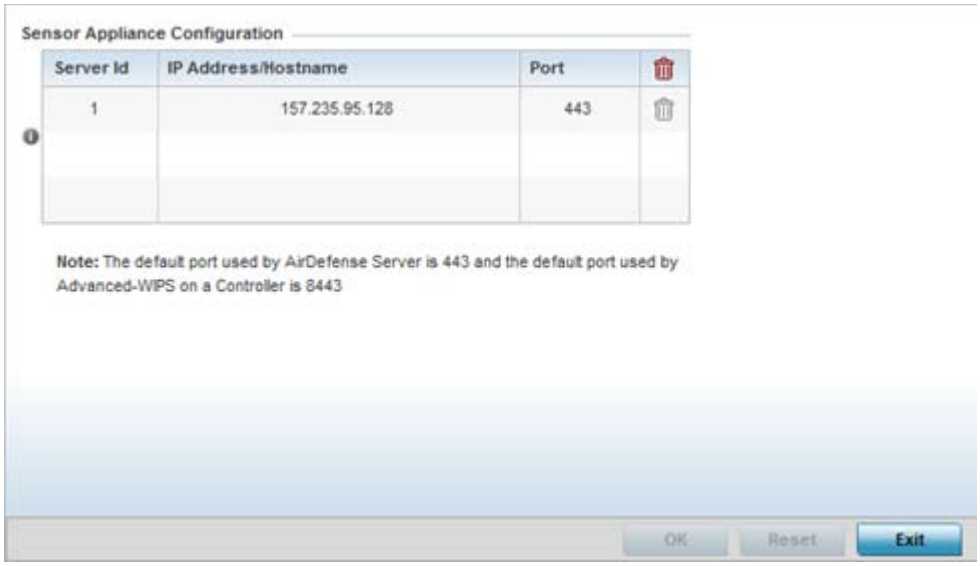


Figure 5-21 *RF Domain - Sensor screen*

13 Select the **+ Add Row** button to populate the **Server Appliance Configuration** field with up to three rows for ADSP server credentials:

Server Id	Use the spinner control to assign a numerical ID for up to three WIPS server resources. The server with the lowest defined ID is the first reached by the controller or service platform. The default ID is 1.
IP Address/Hostname	Provide the numerical (non DNS) IP address or hostname of each server used as a WIPS sensor server by RF Domain member devices. A hostname cannot exceed 64 characters or contain an underscore.
Port	Use the spinner control to specify the port of each WIPS sensor server utilized by RF member devices. The default port is 443.

14 Select **OK** to save the changes to the ADSP appliance sensor configuration, or select **Reset** to revert to the last saved configuration.

15 Select **Client Name** from within the expanded RF Domain Overrides:

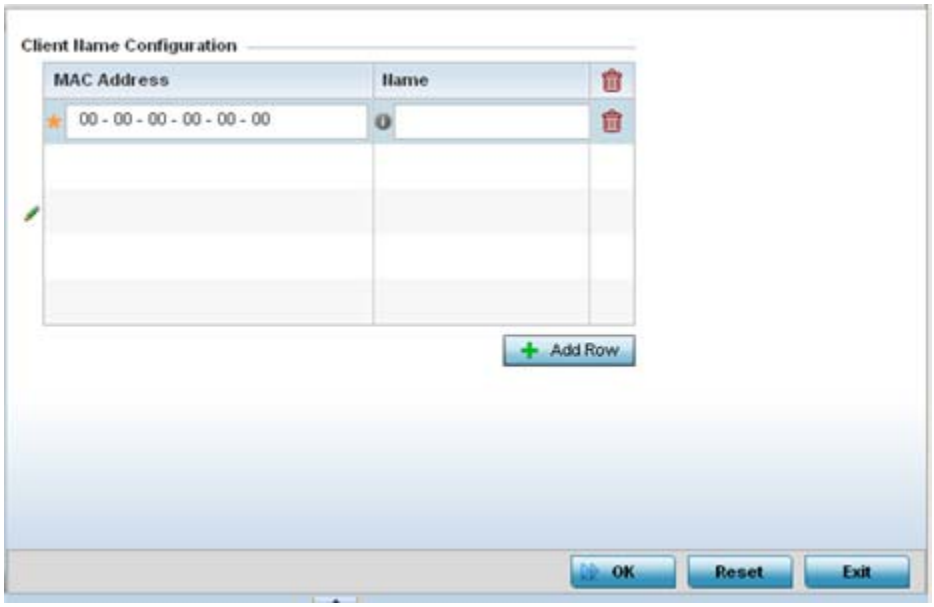


Figure 5-22 *Client Name screen*

16 Click **+ Add Row** to add client name information to the table.

MAC Address	Enter the MAC address of the device assigned a client name for controller, service platform or Access Point management.
Name	Enter the name assigned to this client.

17 Select **OK** to save the changes and overrides made to the Client Name Configuration. Selecting **Reset** reverts the screen to its last saved configuration.

18 Select **WLAN Override** from within the expanded RF Domain Overrides menu.

NOTE: The WLAN Override option does not appear as a sub menu option under RF Domain Overrides for either controllers or service platforms, just Access Points.

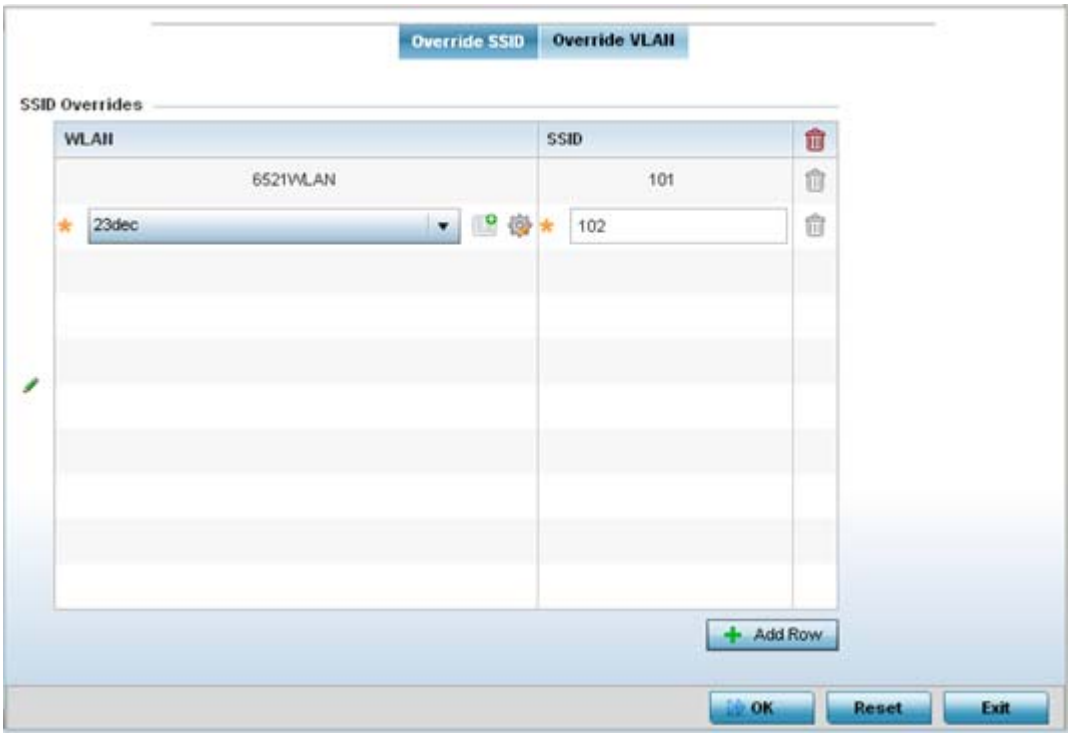


Figure 5-23 *WLAN Override screen - Override SSID tab*

The WLAN Override screen displays with the **Override SSID** tab displayed by default.

19 Optionally define up to 3 overrides for the listed WLAN SSID assignment:

WLAN	Optionally use the drop-down menu to change the WLAN assignment for the listed Access Point. Select either the *Create* icon to define a new WLAN configuration, or select the *Edit* icon to modify an existing WLAN configuration.
SSID	Optionally change the SSID associated with the WLAN. The WLAN name is auto-generated using the SSID until changed (overridden). The maximum number of characters used for the SSID is 32.

20 Select the **Add Row** button as needed to add additional WLAN SSID overrides.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

21 Select **OK** to save the changes and overrides. Selecting **Reset** reverts the screen to its last saved configuration.

22 Select the **Override VLAN** tab to review any VLAN assignment overrides that may have been or optionally add or edit override configurations.

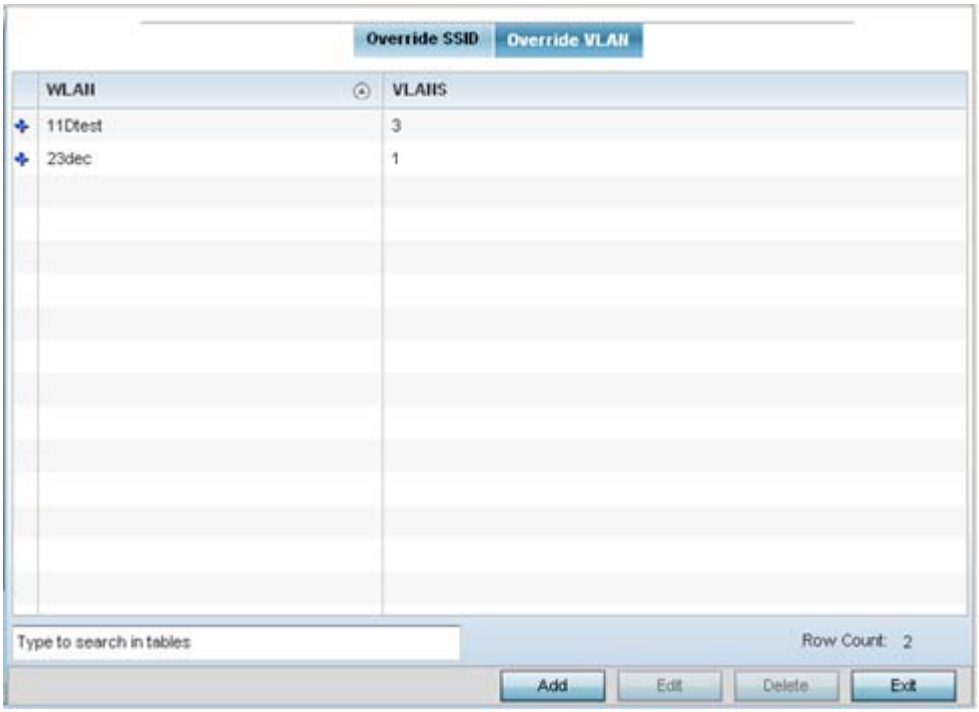


Figure 5-24 *WLAN Override screen - Override VLAN tab*

The Override VLAN tab displays VLANs assigned to the Access Point's WLAN. Select **Add** to create a new client limit for a specific WLAN and VLAN or **Edit** to modify an existing configuration.

23 Optionally define a VLAN's wireless client limit override configuration.

VLANS	Use the spinner control to set a virtual interface ID (1 - 4094).
Wireless Client Limit	Use the spinner control to set the number of users permitted on the VLAN. Set the value to 0 to have an unlimited number of users.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

24 Select **OK** to save the changes and overrides. Selecting **Reset** reverts the screen to its last saved configuration.

5.2.6 Profile Overrides

Basic Device Configuration

Profiles enable administrators to assign a common set of parameters and policies to controllers, service platforms and Access Points. Profiles can be used to assign shared or *unique* network, wireless and security parameters to wireless controllers and Access Points across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support. Controllers and service platforms support both default and user defined profiles implementing new features or updating existing parameters to groups of devices. The central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations. Power and Adoption overrides apply specifically to Access Points, while Cluster configuration overrides apply to only controller or service platform configurations.

However, device profile configurations may need periodic refinement from their original administered design. Consequently, a device profile could require modification from a profile configuration shared amongst numerous devices deployed within a particular site.

Use Profile Overrides to define configurations overriding the parameters set by the target device's original profile assignment.

To review a profile's original configuration requirements and the options available for a target device, refer to General Profile Configuration on page 8-5.

To define a device's general profile override configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the Configuration tab.
The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

3 Select a device (by double-clicking it) from amongst those displayed within the Device Configuration screen. Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

4 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

5 Select **General** if it doesn't display by default.

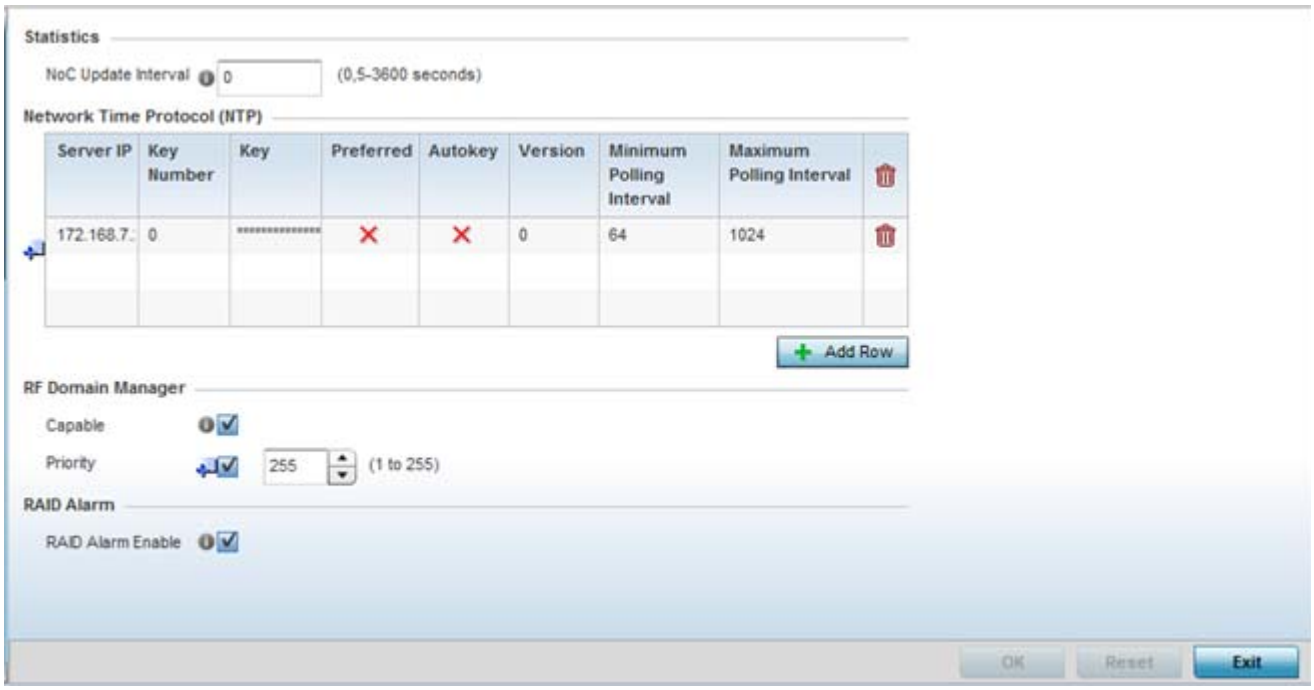


Figure 5-25 *Profile Overrides - General screen*

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

6 Select the **IP Routing** option (within the **Settings** field) to enable routing for the device.

7 Set a **NoC Update Interval** of 0, or from 5-3600 seconds for updates from the RF Domain manager to the controller or service platform.

8 Select **+ Add Row** below the **Network Time Protocol (NTP)** table to launch a screen used to define (or override) the configurations of NTP server resources the controller or service platform uses it obtain its system time. Set the following parameters to define the NTP configuration:

Server IP	Set the IP address of each server as a potential NTP resource. Provide either a hostname or an IPv4 formatted IP address. Hostnames cannot include an underscore character.
Key Number	Select the number of the associated *Authentication Key* for the NTP resource.
Key	If an autokey is not being used, manually enter a 64 character maximum key the controller or service platform and NTP resource share to securely interoperate.
Preferred	Select the radio button to designate this particular NTP resource as preferred. If using multiple NTP resources, preferred resources are given first opportunity to connect to the controller or service platform and provide NTP calibration.
AutoKey	Select the radio button to enable an *Autokey* configuration for the controller or service platform and NTP resource. The default setting is disabled.
Version	Use the spinner control to specify the version number used by this NTP server resource. The default setting is 0.
Minimum Polling Interval	Use the drop-down menu to select the minimum polling interval. Once set, the NTP resource is polled no sooner then the defined interval. Options include *64*, *128*, *256*, *512* or *1024* seconds. The default setting is 64 seconds.
Maximum Polling Interval	Use the drop-down menu to select the maximum polling interval. Once set, the NTP resource is polled no later then the defined interval. Options include *64*, *128*, *256*, *512* or *1024* seconds. The default setting is 1024 seconds.

9 Refer to the **RF Domain Manager** field to elect RF Domain Manager devices and assign them a priority in the election process:

Capable	Select this option to elect this controller a RF Domain manager capable of storing and provisioning configuration and firmware images for other members of the RF Domain. The RF-domain-manager updates any state changes to the rest of the devices in the RF Domain. This setting is enabled by default.
Priority	Select this option to set the priority of this device becoming the RF Domain Manager versus other capable RF Domain members. The higher the value (1 - 255) the higher priority assigned to the device in the RF Domain Manager election process.

10 Refer to the **RAID Alarm** field to either *enable* or *disable* the chassis alarm that sounds when events are detected that degrade RAID support (drive content mirroring) on a service platform.

NOTE: RAID controller drive arrays are available within NX7530 and NX9000 series service platforms (NX9000, NX9500 and NX9510 models) only. However, they can be administrated on behalf of a profile by a different model service platform or controller.

Service platforms include a single Intel MegaRAID controller (virtual drive) with RAID-1 mirroring support enabled. The online virtual drive supports up to two physical drives that could require hot spare substitution if a drive were to fail. An administrator can manage the RAID controller event alarm and syslogs supporting the array hardware from the service platform user interface and is not required to reboot the service platform BIOS.

For information on setting the service platform drive array configuration and diagnostic behavior of its member drives, refer to RAID Operations on page 14-12. To view the service platform's current RAID array status, drive utilization and consistency check information, refer to RAID Statistics on page 15-114.

11 Select **OK** to save the changes and overrides made to the general profile configuration. Select **Reset** to revert to the last saved configuration.

5.2.6.1 Cluster Configuration Overrides (Controllers and Service Platforms Only)

Profile Overrides

A redundancy group (cluster) is a set of controllers or service platforms (nodes) uniquely defined by a profile configuration. Within the redundancy group, members discover and establish connections to other peers and provide wireless self-healing support in the event of cluster member failure.

A cluster's AP load balance is typically distributed evenly amongst the controllers or service platforms in the cluster. Define how often this profile is load balanced for AP radio distribution as often as you feel required, as radios can come and go and members can join and exit the cluster. For information on setting a profile's original cluster configuration (before applying an override), see Profile Cluster Configuration (Controllers and Service Platforms) on page 8-8.

As cluster memberships increase or decrease and their load requirements change, a profile may need an override applied to best suit a site's cluster requirements.

To apply an override (if required) to a profile cluster configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of devices or peer controllers service platforms or Access Points.

3 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

4 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

5 Select **Cluster**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

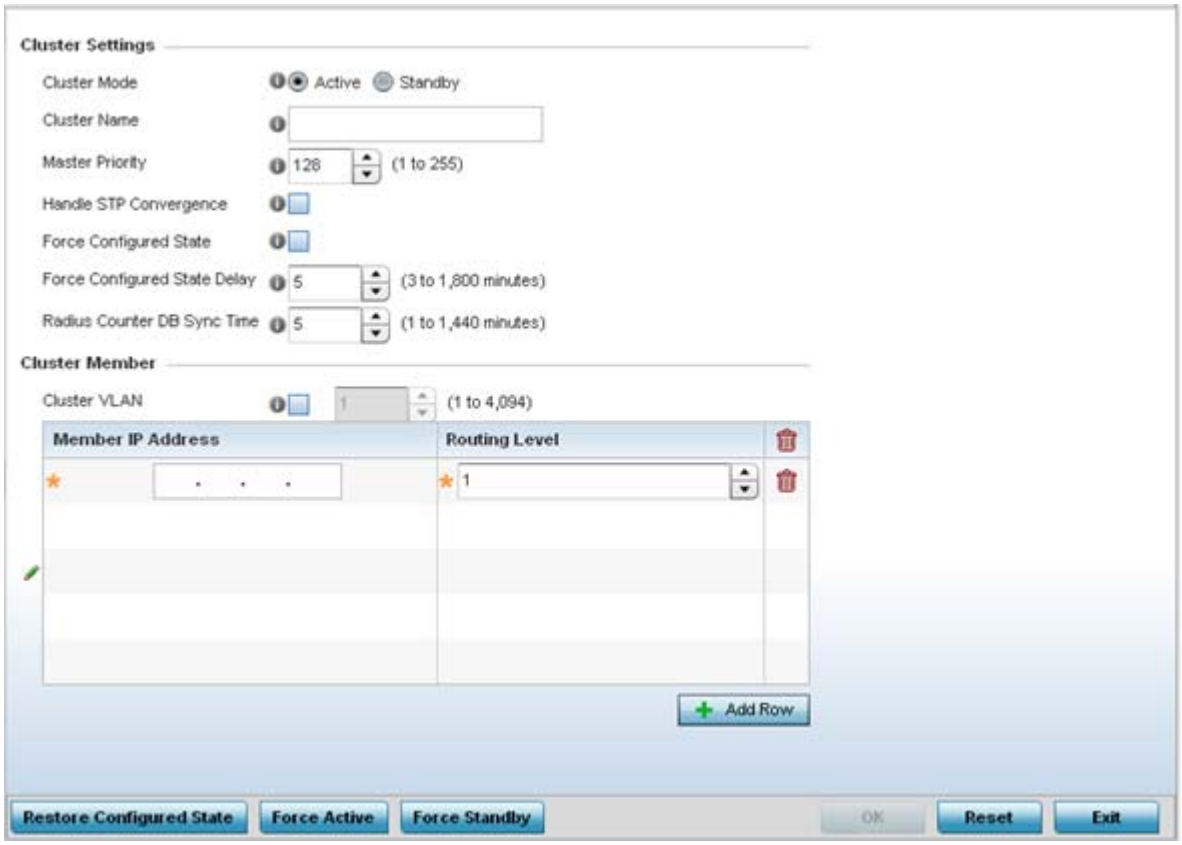


Figure 5-26 *Profile Overrides - Cluster screen*

6 Optionally define the following **Cluster Settings** and overrides:

Cluster Mode	A member can be in either an *Active* or *Standby* mode. All active member controllers or service platforms can adopt Access Points. Standby members only adopt Access Points when an active member has failed or sees an Access Point that's not yet adopted. The default cluster mode is Active and enabled for use with the profile.
Cluster Name	Define a name for the cluster name unique to its configuration or profile support requirements. The name cannot exceed 64 characters.
Master Priority	Set a priority value from 1 and 255 with the higher value being given higher priority. This configuration is the device's priority to become cluster master. In cluster environment one device from cluster members is elected as cluster master. This configuration is the device's priority to become cluster master. The default is 128.

Handle STP Convergence	Select the radio button to enable *Spanning Tree Protocol* (STP) convergence for the controller or service platform. In general, this protocol is enabled in layer 2 networks to prevent network looping. Spanning Tree is a network layer protocol that ensures a loop-free topology in a mesh network of inter-connected layer 2 controller or service platform. The spanning tree protocol disables redundant connections and uses the least costly path to maintain a connection between any two controllers or service platforms in the network. If enabled, the network forwards data only after STP convergence. Enabling STP convergence delays the redundancy state machine execution until the STP convergence is completed (the standard protocol value for STP convergence is 50 seconds). Delaying the state machine is important to load balance APs at startup. The default setting is disabled.
Force Configured State	Select the radio button to allow this controller or service platform to take over for an active member if it were to fail. A standby controller or service platform in the cluster takes over APs adopted by the failed active member. If the failed active member were to come back up, the active member starts a timer based on the Auto Revert Delay interval. At the expiration of the Auto Revert Delay, the standby member releases all adopted APs and goes back to a monitoring mode. The Auto Revert Delay timer is stopped and restarted if the active member goes down and comes up during the Auto Revert Delay interval. The default value is disabled.
Force Configured State Delay	Specify a delay interval in minutes (3 - 1,800). This is the interval a standby member waits before releasing adopted APs and goes back to a monitoring mode when an active cluster member becomes active again after a failure. The default interval is 5 minutes.
Radius Counter DB Sync Time	Specify a sync time (from 1 - 1,440 minutes) a RADIUS counter database uses as its synchronization interval with the dedicated NTP server resource. The default interval is 5 minutes.

7 Within the **Cluster Member** field, select **Cluster VLAN** to enable a spinner control to designate the VLAN where cluster members are reachable. Specify a VLAN from 1 - 4094.

Specify the IP addresses of the VLAN's cluster members using the **Member IP Address** table.

8 Select **Restore Configured State** to restore this cluster member back into role of taking over for an active member if it were to fail.

9 Select **Force Active** to revert this cluster member back into its default active state and provide the ability to adopt Access Points.

10 Select **Force Standby** to only adopt Access Points when an active member has failed or sees an Access Point that's not yet adopted.

11 Select **OK** to save the changes and overrides made to the profile's cluster configuration. Select **Reset** to revert to the last saved configuration.

5.2.6.2 Access Point Radio Power Overrides (Access Points Only)

Profile Overrides

A profile can manage the transmit output power of the Access Point radios it supports within the network.

NOTE: The Power option only appears within the Profile Overrides menu tree if an Access Point is selected from within the main Devices screen. Power management is configured differently for controllers or service platforms, so the Power screen only displays for Access Points.

Use the **Power** screen to set or override one of two power modes (3af or Auto) for a managed Access Point. When automatic is selected, the Access Point safely operates within available power. Once the power configuration is determined, the Access Point configures its operating power characteristics based on its model and power configuration.

An Access Point uses a *complex programmable logic device* (CPLD). The CPLD determines proper supply sequencing, the maximum power available and other status information. One of the primary functions of the CPLD is to determine the Access Point's maximum power budget. When an Access Point is powered on (or performing a cold reset), the CPLD determines the maximum power provided by the POE device and the budget available to the Access Point. The CPLD also determines the Access Point hardware SKU and the number of radios. If the Access Point's POE resource cannot provide sufficient power (with all intended interfaces enabled), some of the following interfaces could be disabled or modified:

- The Access Point's transmit and receive algorithms could be negatively impacted
- The Access Point's transmit power could be reduced due to insufficient power
- The Access Point's WAN port configuration could be changed (either enabled or disabled)

To define an Access Point's power configuration or apply an override to an existing parameter:

1 Select the Devices tab from the Web UI.

2 Select **Profile Overrides** to expand its sub menu items.

3 Select **Power.**

A screen displays where an Access Point's power configuration can be defined or overridden for a profile.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

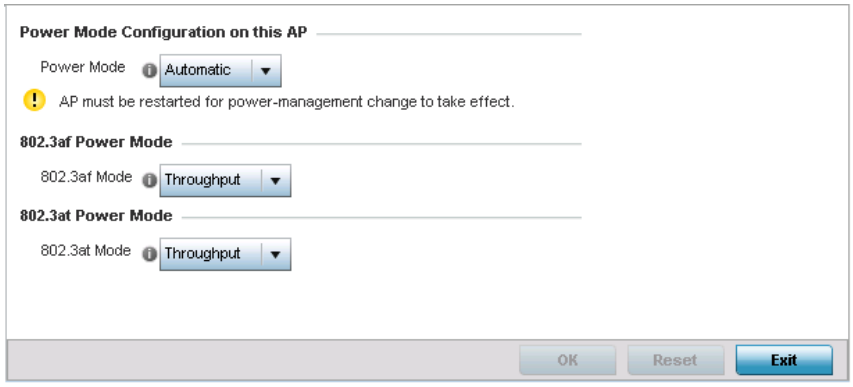


Figure 5-27 *Access Point Profile Power Override screen*

4 Use the **Power Mode** drop-down menu to set or override the **Power Mode Configuration on this AP**.

> **NOTE:** Single radio model Access Point's always operate using a full power configuration. The power management configurations described in this section do not apply to single radio models.

When an Access Point is powered on for the first time, the system determines the power budget available to the Access Point. Using the **Automatic** setting, the Access Point automatically determines the best power configuration based on the available power budget. Automatic is the default setting.

If 802.3af is selected, the Access Point assumes 12.95 watts are available. If the mode is changed, the Access Point requires a reset to implement the change. If 802.3at is selected, the Access Point assumes 23 - 26 watts are available.

5 Set or override the Access Point radio's **802.3af Power Mode** and the radio's **802.3at Power Mode**.

Use the drop-down menu to define a mode of either **Range** or **Throughput**.

Select **Throughput** to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where the transmission range is secondary to broadcast/multicast transmission performance. Select **Range** when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates. Throughput is the default setting for both 802.3af and 802.3at.

6 Select **OK** to save the changes and overrides made to the Access Point power configuration. Select **Reset** to revert to the last saved configuration.

5.2.6.3 Access Point Adoption Overrides (Access Points Only)

Profile Overrides

Adoption is the process an Access Point uses to discover available controllers or service platforms, pick the most desirable one, establish an association and optionally obtain an image upgrade and configuration. Adoption is configurable and supported within a device profile and applied to other Access Points supported by the profile. Individual attributes of an Access Point's auto provisioning policy can be overridden as specific parameters require modification.

At adoption, an Access Point solicits and receives multiple adoption responses from controllers and service platforms available on the network. These adoption responses contain loading policy information the Access Point uses to select the optimum controller or service platform for adoption. By default, an auto provisioning policy generally distributes AP adoption evenly amongst available controllers and service platforms. Modify existing adoption policies or create a new one as needed to meet the adoption requirements of a device and their assigned profile.

> **NOTE:** A device configuration does not need to be present for an auto provisioning policy to take effect. Once adopted, and the device's configuration is defined and applied by the controller or service platform, the auto provisioning policy mapping does not have impact on subsequent adoptions by the same device.

An auto provisioning policy enables an administrator to define adoption rules for the supported Access Points capable of being adopted by a wireless controller.

To define an Access Point's adoption configuration or apply an override:

1 Select the **Devices** from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Profile Overrides** to expand its sub-menu items.

4 Select **Adoption**.

A screen displays where an Access Point's adoption configuration can be defined and overridden for a profile.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

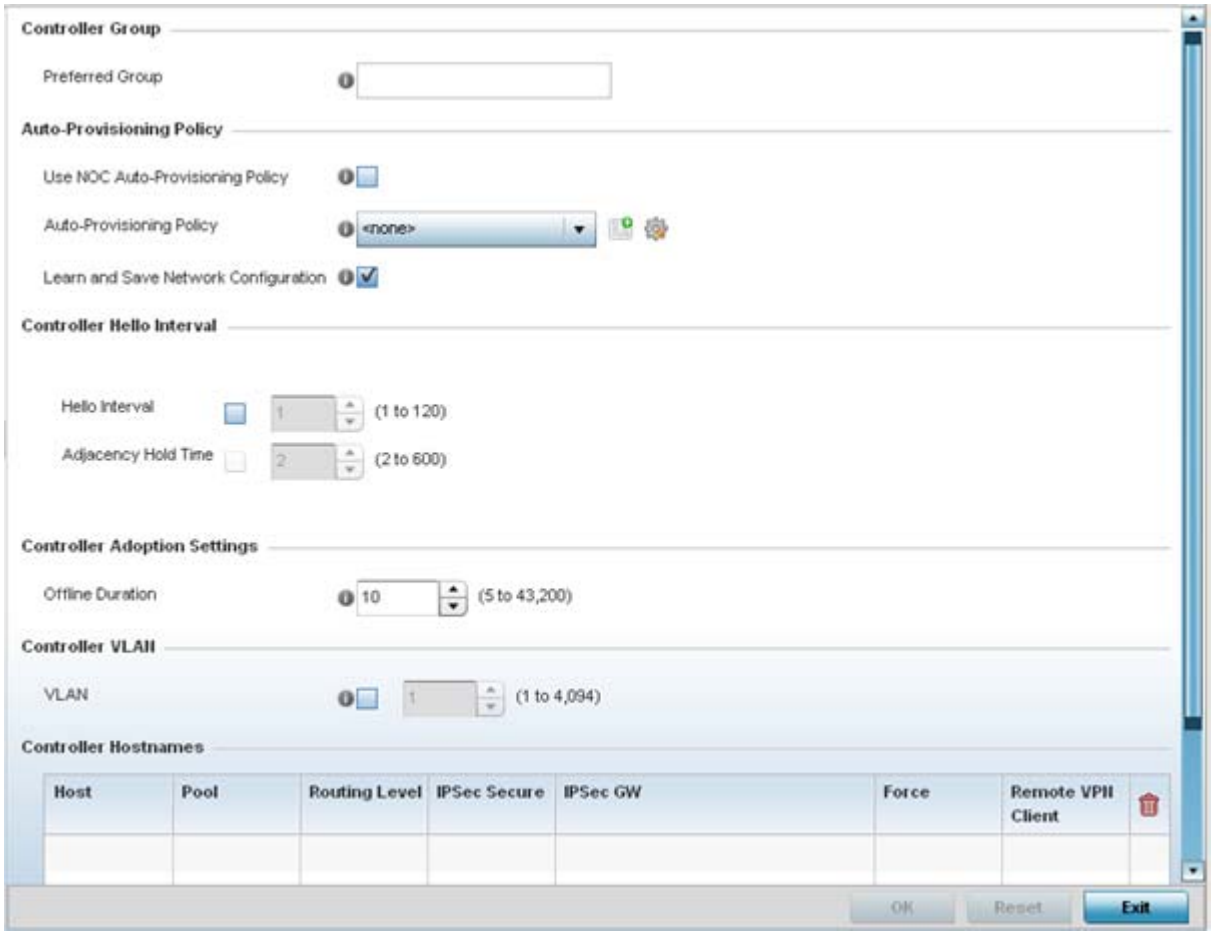


Figure 5-28 *Access Point Adoption Override screen*

5 Define or override the **Preferred Group** used as optimal group for the Access Point's adoption. The name of the preferred group cannot exceed 64 characters.

6 Set the following **Auto-Provisioning Policy** settings for Access Point adoptions:

Use NOC Auto-Provisioning Policy	Select this option to use the NOC controller's auto provisioning policy and not the policy maintained locally. The NOC is an elected controller or service platform capable of provisioning all of its peer controllers, service platforms and adopted devices. This setting is disabled by default. NOC controllers are NX9000, NX9500, NX9510, NX7500, NX6500, NX6524 and RFS6000 models.

Auto-Provisioning Policy	Select an auto provisioning policy from the drop-down menu. To create a new auto provisioning policy, select the *Create* icon or modify an existing one by selecting the *Edit* icon.
Learn and Save Network Configuration	Select this option to learn and save the configuration of any device requesting adoption. This setting is enabled by default.

7 Set the following **Controller Hello Interval** settings manage message exchanges and connection re-establishments between adopting devices:

Hello Interval	Define an interval (from 1 - 120 seconds) between hello keep alive messages exchanged with the adopting device. These messages serve as a connection validation mechanism to ensure the availability of the adopting resource.
Adjacency Hold Time	Set the time (from 2 - 600 seconds) after the last hello packet after which the connection between the controller and Access Point is defined as lost and their connection is re-established. When a hello interval is set, an adjacency hold time is mandatory and should be higher then the hello interval.

8 Use the spinner control to define an **Offline Duration** timeout (from 5 - 43,200 minutes) to detect whether an adopted device is offline. The default setting is 10 minutes.

9 Use the spinner control to define a **Controller VLAN**. Select to enable this field and select the VLAN on which the adopting controllers can be found by the Access Point.

10 Enter **Controller Hostnames** as needed to define or override resources for Access Point adoption.

11 Select **+ Add Row** as needed to populate the table with IP Addresses or Hostnames used as Access Point adoption resources into the managed network.

Host	Use the drop-down menu to specify whether the adoption resource is defined as a (non DNS) *IP Address* or a *Hostname*. Once defined, provide the numerical IP or Hostname. A Hostname cannot exceed 64 characters and cannot include an underscore character.
Pool	Use the spinner control to set a pool of either 1 or 2. This is the pool the target controller or service platform belongs to.
Routing Level	Define a routing level (either 1 or 2) for the link between adopting devices. The default setting is 1.
IPSec Secure	Enable this option to provide IPSec secure peer authentication on the connection (link) between the adopting devices. This option is disabled by default.
IPSec GW	Select the numerical IP address or administrator defined hostname of the adopting controller resource.
Force	Enable this setting to create a forced link between an Access Point and adopting controller, even when not necessarily needed. This setting is disabled by default.
Remote VPN Client	Displays whether a secure controller link has been established using a remote VPN client.

12 Select **OK** to save the changes and overrides made to the Access Point profile adoption configuration. Select **Reset** to revert to the last saved configuration.

5.2.6.4 Adoption Overrides (Controllers Only)

Profile Overrides

Adoption is the process an Access Point uses to discover available controllers, pick the most desirable controller, establish a controller association and optionally obtain an image upgrade and configuration. Adoption is configurable and supported within a device profile and applied to other Access Points supported by the profile. Individual attributes of an Access Point's auto provisioning policy can be overridden as specific parameters require modification.

At adoption, an Access Point solicits and receives multiple adoption responses from controllers and service platforms available on the network. These adoption responses contain loading policy information the Access Point uses to select the optimum controller or service platform for adoption. By default, an auto provisioning policy generally distributes AP adoption evenly amongst available controllers and service platforms. Modify existing adoption policies or create a new one as needed to meet the adoption requirements of a device and their assigned profile.

NOTE: A device configuration does not need to be present for an auto provisioning policy to take effect. Once adopted, and the device's configuration is defined and applied by the controller or service platform, the auto provisioning policy mapping does not have impact on subsequent adoptions by the same device.

To define a controller or service platform's adoption configuration:

1 Select the **Devices** from the Web UI.

2 Select **Profiles.**

3 Select **Profile Overrides** to expand its sub-menu items.

4 Select **Adoption.**

A screen displays where a controller or service platform's adoption configuration can be set or overridden for a profile.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

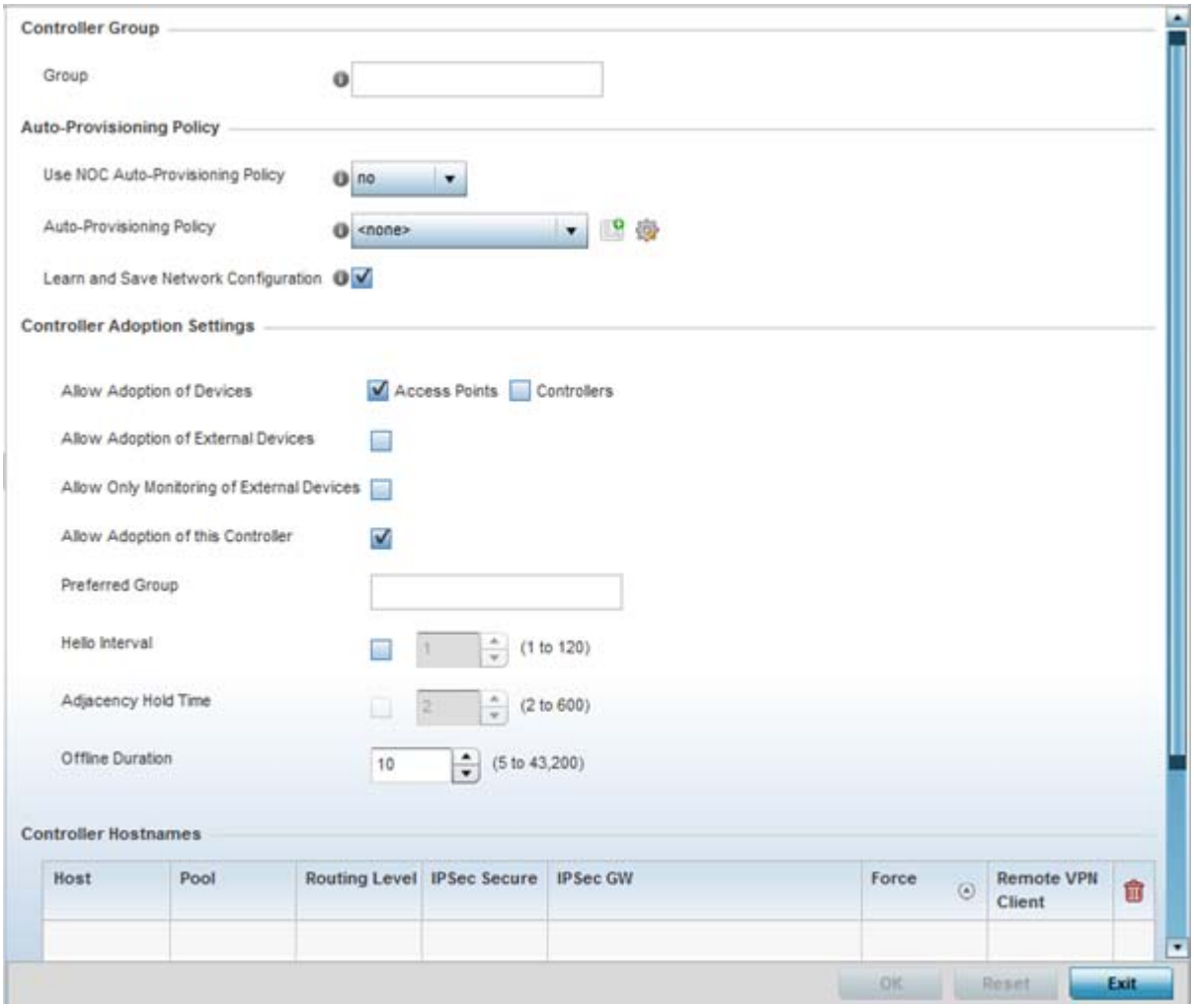


Figure 5-29 *Controller Adoption Override screen*

5 Within the **Controller Group** field, use the **Group** item to set provide the controller group this controller or service platform belongs to. A preferred group can also be selected for the adoption of this controller or service platform. The name of the preferred group cannot exceed 64 characters.

6 Set the following **Auto Provisioning Policy** parameters:

Use NOC Auto-Provisioning Policy	Select this option to use the NOC's auto provisioning policy instead of the policy local to the controller or service platform. The NOC is an elected controller or service platform capable of provisioning all of its peer controllers, service platforms and adopted devices. This setting is disabled by default.
Auto-Provisioning Policy	Select an auto provisioning policy from the drop-down menu. To create a new auto provisioning policy, select the *Create* icon or modify an existing one by selecting the *Edit* icon.

Learn and Save Network Configuration	Select this option to enable allow the controller tor service platform to maintain a local configuration records of devices requesting adoption and provisioning. This feature is enabled by default.
Rerun Policy Rules Every Time AP Adopted	Enabling this feature applies adoption rules on Access Points each time they're subsequently adopted, not just the first time. This setting is disabled by default.

7 Set the following **Controller Adoption Settings** settings:

Allow Adoption of Devices	Select either *Access Points* or *Controllers* (or both) to refine whether this controller or service platform can adopt just networked Access Points or peer controller devices as well.
Allow Adoption of External Devices	Select this option to enable this controller or service platform to adopt T5 model devices or EX3500 model switches.
Allow Monitoring of External Devices	Select this option to enable monitoring only of T5 model devices or EX3500 model switches by this controller or service platform. When enabled, WiNG does not configure EX3500 switches or a T5, it only monitors those devices for statistics and events.
Allow Adoption of this Controller	Select this option to enable this controller or service platform to be capable of adoption by other controllers or service platforms. This setting is disabled by default, and must be selected to allow peer adoptions and enable the four settings directly below it.
Preferred Group	If *Allow Adoption of this Controller* is selected, provide the controller group preferred as the adopting entity for this controller or service platform. If utilizing this feature, ensure the appropriate group is provided within the Controller Group field.
Hello Interval	Select this option to define the hello packet exchange interval (from 1 - 120 seconds) between the controller or service platform and an adoption requesting Access Point.
Adjacency Hold Time	Select this option to set a hold time interval (from 2 - 600 seconds) for the transmission of hello packets.
Offline Duration	Use the spinner control to define a timeout (from 5 - 43,200 minutes) to detect whether an adopted device is offline. The default setting is 10 minutes.

8 Enter **Controller Hostnames** as needed to define resources for adoption.

9 Select **+ Add Row** as needed to populate the table with IP Addresses or Hostnames used as Access Point adoption resources into the managed network.

Host	Use the drop-down menu to specify whether the adoption resource is defined as a (non DNS) *IP Address* or a *Hostname*. Once defined, provide the numerical IP or Hostname. A Hostname cannot exceed 64 characters or contain an underscore.
Pool	Use the spinner control to set a pool of either 1 or 2. This is the pool the target controller or service platform belongs to.
Routing Level	Define a routing level (either 1 or 2) for the link between adopting devices. The default setting is 1.
IPSec Secure	Enable this option to provide IPSec secure peer authentication on the connection (link) between the adopting devices. This option is disabled by default.

IPSec GW	Select the numerical IP address or administrator defined hostname of the adopting controller resource.
Force	Enable this setting to create a forced link between an Access Point and adopting controller, even when not necessarily needed. This setting is disabled by default.
Remote VPN Client	Displays whether a secure controller link has been established using a remote VPN client.

10 Select **OK** to save the changes and overrides made to the profile's adoption configuration. Select **Reset** to revert to the last saved configuration.

5.2.7 Profile Interface Override Configuration

Profile Overrides

A profile's interface configuration can be defined to support separate physical Ethernet configurations both unique and specific to RFS4000, RFS6000 controllers and NX4500, NX5500, NX6500, NX7500 and NX9000 series service platforms. Ports vary depending on platform, but controller or service platform models do have some of the same physical interfaces.

A controller or service platform requires its Virtual Interface be configured for layer 3 (IP) access or layer 3 service on a VLAN. A Virtual Interface defines which IP address is associated with each VLAN ID the controller or service platform is connected to.

If the profile is configured to support an Access Point radio, an additional Radios option is available, unique to the Access Point's radio configuration.

Each profile interface configuration can have overrides applied to customize the configuration to a unique controller or service platform deployment. However, once an override is applied to this configuration it becomes independent from the profile that may be shared by a group of devices in a specific deployment and my need careful administration until a profile can be re-applied to the target controller or service platform. For more information, refer to the following:

- *Ethernet Port Override Configuration*
- *Virtual Interface Override Configuration*
- *Port Channel Override Configuration*
- *VM Interface Override Configuration*
- *Radio Override Configuration*
- *WAN Backhaul Override Configuration*
- *PPPoE Override Configuration*
- *Bluetooth Configuration*

5.2.7.1 Ethernet Port Override Configuration

Profile Interface Override Configuration

The ports available on controllers vary depending RFS controller model. The following ports are available to controllers:

- RFS4000 - ge1, ge2, ge3, ge4, ge5, up1
- RFS6000 - ge1, ge2, ge3, ge4, ge5, ge6, ge7, ge8, me1, up1
- RFS7000 - ge1, ge2, ge3, ge4, me1

GE ports on RFS4000 and RFS6000 models are RJ-45 ports supporting 10/100/1000Mbps. The GE ports on a RFS7000 can be RJ-45 or fiber ports supporting 10/100/1000Mbps.

ME ports are available on RFS6000 and RFS7000 platforms. ME ports are out-of-band management ports used to manage the controller via CLI or Web UI, even when the other ports on the controller are unreachable.

The following ports are available to NX series service platform models:

- *NX4500* - up1, up2
- *NX4524* - ge1-ge24, up1, up2
- *NX5500* - ge1, ge2
- *NX6500* - up1, up2
- *NX6524* - ge1-ge24, up1, up2
- *NX7500* - ge1-ge10, xge1-xge2
- *NX9000* series - ge1, ge2

NOTE: For a NX7500 model service platform, there are options for either a 2 port or 4 port network management card. Either card can be managed using WiNG. If the 4 port card is used, ports ge7-ge10 are available. If the 2 port card is used, ports xge1-xge2 are available.

UP ports are available on RFS4000 and RFS6000 controllers and NX4500 and NX6500 series service platforms. An UP port is used to connect to the backbone network. An UP port supports either RJ-45 or fiber. The UP port is the preferred means to connect to the backbone as it has a non-blocking 1gbps connection unlike the GE ports.

T5 controllers have the following Ethernet port designations:

- *T5*- ge1-ge2 (T5 controller managed CPE devices have ports fe1 - fe2)

To set a profile's Ethernet port configuration and potentially apply overrides to the profile's configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

3 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

4 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

5 Select **Interface** to expand its sub menu options.

6 Select **Ethernet Ports**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

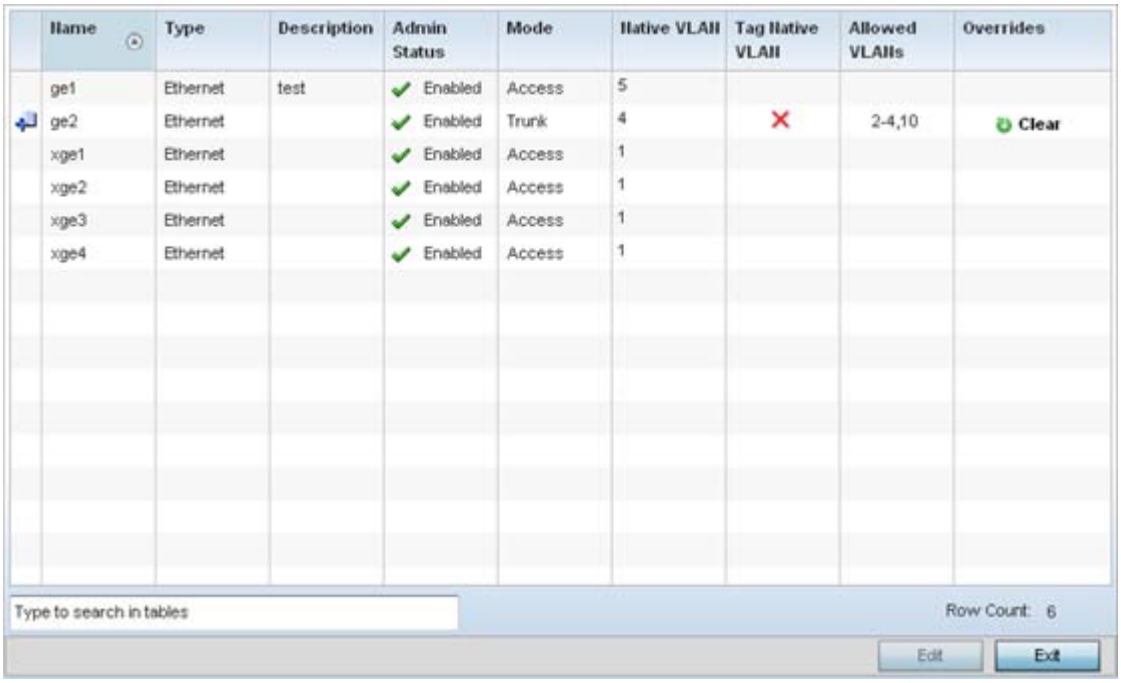


Figure 5-30 *Profiles Overrides - Ethernet Ports screen*

7 Refer to the following to assess port status and performance:

Name	Displays the physical port name reporting runtime data and statistics. Supported ports vary depending on controller or service platform model. RFS4000 - ge1, ge2, ge3, ge4, ge5, up1 RFS6000 - ge1, ge2, ge3, ge4, ge5, ge6, ge7, ge8, me1, up1 RFS7000 - ge1, ge2, ge3, ge4, me1 *NX4500* - up1, up2 *NX4524* - ge1-ge24, up1, up2 *NX5500* - ge1, ge2 *NX6500* - up1, up2 *NX6524* - ge1-ge24, up1, up2 *NX7500* - ge1-ge10, xge1-xge2 *NX9000* series- ge1, ge2, xge1-xge4
Type	Displays the physical controller or service platform port type. *Cooper* is used on RJ45 Ethernet ports and *Optical* materials are used on fiber optic gigabit Ethernet ports.
Description	Displays an administrator defined description for each listed controller or service platform port.
Admin Status	A green check mark defines the port as active and currently enabled with the profile. A red "X" defines the port as currently shut down and not available for use. The interface status can be modified with the port configuration as needed.

Mode	Displays the profile's switching mode as either *Access* or *Trunk* (as defined within the Ethernet Port Basic Configuration screen). If Access is selected, the listed port accepts packets only from the native VLAN. Frames are forwarded untagged with no 802.1Q header. All frames received on the port are expected as untagged and mapped to the native VLAN. If set to Trunk, the port allows packets from a list of VLANs added to the trunk. A port configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged.
Native VLAN	Lists the numerical VLAN ID (1 - 4094) set for the native VLAN. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.
Tag Native VLAN	A green check mark defines the native VLAN as tagged. A red "X" defines the native VLAN as untagged. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.
Allowed VLANs	Displays those VLANs allowed to send packets over the listed controller or service platform port. Allowed VLANs are only listed when the mode has been set to Trunk.
Overrides	A Clear option appears for each Ethernet port configuration that has an override applied to the profile's configuration. Select Clear to revert this specific interface configuration to the profile configuration originally defined by the administrator for this interface.

8 To edit or override the configuration of an existing controller or service platform port, select it from amongst those displayed and select the **Edit** button. The Ethernet Port **Basic Configuration** screen displays by default.

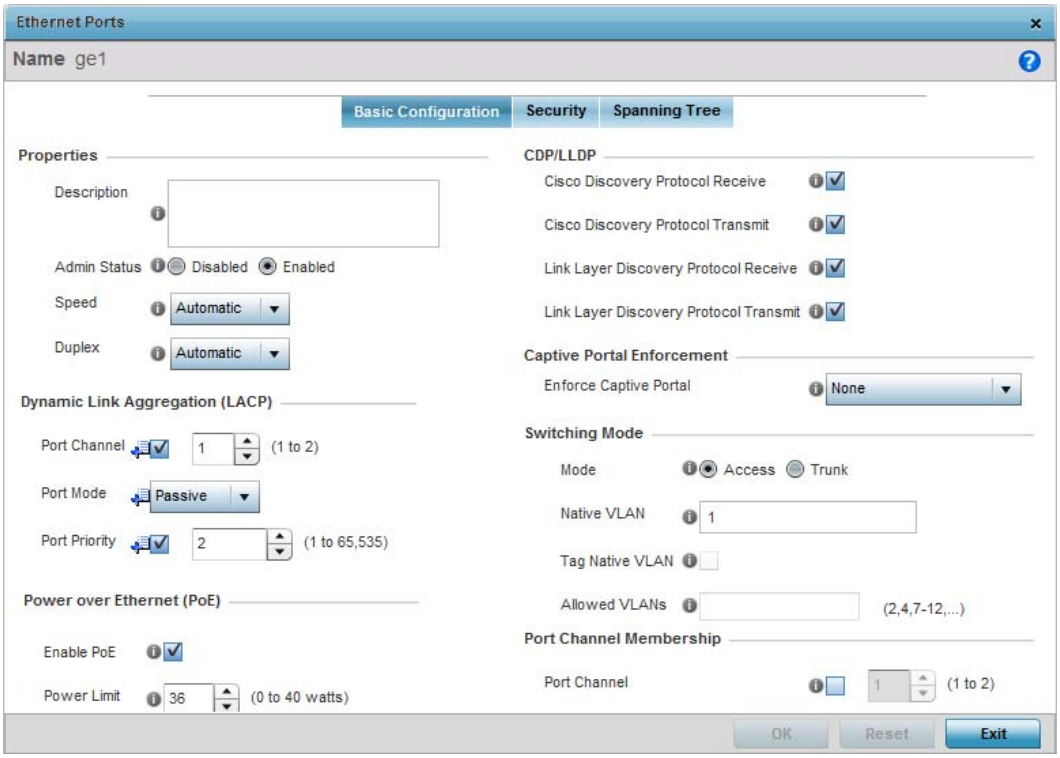


Figure 5-31 *Profile Overrides - Ethernet Ports Basic Configuration screen*

9 Set or override the following Ethernet port **Properties**:

Description	Enter a brief description for the controller or service platform port (64 characters maximum). The description should reflect the port's intended function to differentiate it from others with similar configurations, or perhaps just the name of the physical port.
Admin Status	Select the *Enabled* radio button to define this port as active to the profile it supports. Select the *Disabled* radio button to disable this physical port in the profile. It can be activated at any future time when needed. Admin status is enabled by default.
Speed	Select the speed at which the port can receive and transmit the data. Select either *10 Mbps*, *100 Mbps* or *1000 Mbps*. Select either of these options to establish a 10, 100 or 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission over the port. These options are not available if Auto is selected. Select *Automatic* to enable the port to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis. Automatic is the default setting.
Duplex	Select either *Half*, *Full* or *Automatic* as the duplex option. Select Half duplex to send data over the port, then immediately receive data from the same direction in which the data was transmitted. Like a Full-duplex transmission, a Half-duplex transmission can carry data in both directions, just not at the same time. Select Full duplex to transmit data to and from the port at the same time. Using Full duplex, the port can send data while receiving data as well. Select Automatic to enable to the controller or service platform to dynamically duplex as port performance needs dictate. Automatic is the default setting.

10 Enable or disable the following **CDP/LLDP** parameters used to configure *Cisco Discovery Protocol* (CDP) and *Link Layer Discovery Protocol* (LLDP) for this profile's Ethernet port configuration:

Cisco Discovery Protocol Receive	Select this option to allow the CDP to be received on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default.
Cisco Discovery Protocol Transmit	Select this option to allow the CDP to be transmitted on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors.
Link Layer Discovery Protocol Receive	Select this option to allow the LLDP to be received on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default.
Link Layer Discovery Protocol Transmit	Select this option to allow the LLDP to be transmitted on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors.

11 If supported and applicable, set or override the following **Power Over Ethernet (PoE)** parameters used with this profile's Ethernet port configuration:

Enable POE	Select this option to configure the selected controller or service platform port to use Power over Ethernet. To disable PoE on a port, uncheck this option. PoE is supported on RFS4000 and RFS6000 model controllers and NX4524 and NX6524 model service platforms. Each of a NX4524 or NX6524's 24 GE ports supports 3af (15.4W) on each of its 24 ports simultaneously. NX4524 and NX6524 models support up to 30W per port, with a maximum of 360W. NX4500 and NX6500 models do not support PoE over their UP1 and UP2 ports. When enabled, the controller or service platform supports 802.3af PoE on each of its ge ports. The PoE allows users to monitor port power consumption and configure power usage limits and priorities for each ge port.
Power Limit	Use the spinner control to set the total watts available for PoE on the ge port. Set a value from 0 - 40 watts.
Power Priority	Set the power priority for the listed port to either to either *Critical, High* or *Low*. This is the priority assigned to this port versus the power requirements of the other supports available on the controller or service platform.

12 Select **Enforce Captive Portal** to automatically apply captive portal access permission rules to data transmitted over this specific Ethernet port. This setting is disabled by default.

A captive portal is an access policy for providing temporary and restrictive access using a standard Web browser. Captive portals provides authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Once logged into the captive portal, additional *Terms and Agreement*, *Welcome*, *Fail* and *No Service* pages provide the administrator with a number of options on captive portal screen flow and user appearance.

Captive portal enforcement allows wired network users to pass traffic through the captive portal without being redirected to an authentication page. Authentication instead takes place when the RADIUS server is queried against the wired user's MAC address. If the MAC address is in the RADIUS server's user database, the user can pass traffic on the captive portal. If **None** is selected, captive portal policies are not enforced on the wired interface. If **Authentication Failure** is selected, captive portal policies are enforced only when RADIUS

authentication of the client's MAC address is not successful. If Always is selected, captive portal policies are enforced regardless of whether the client's MAC address is in the RADIUS server's user database. For information on configuring a captive portal policy, see Configuring Captive Portal Policies on page 11-1.

13 Define or override the following **Switching Mode** parameters applied to the Ethernet port configuration:

Mode	Select either the *Access* or *Trunk* radio button to set the VLAN switching mode over the port. If Access is selected, the port accepts packets only form the native VLANs. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are untagged and are mapped to the native VLAN. If the mode is set to Trunk, the port allows packets from a list of VLANs you add to the trunk. A port configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. Access is the default mode.
Native VLAN	Use the spinner control to define a numerical **Native VLAN ID** from 1 - 4094. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN which untagged traffic will be directed over when using a port in trunk mode. The default VLAN is 1.
Tag Native VLAN	Select this option to tag the native VLAN. Controller and service platforms support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is disabled by default.
Allowed VLANs	Selecting *Trunk* as the mode enables the *Allowed VLANs* parameter. Add VLANs that exclusively send packets over the listed port.

14 Optionally select the **Port Channel** check box from the **Port Channel Membership** area and define or override a setting from 1 - 8 using the spinner control. This sets the channel group for the port.

15 Select **OK** to save the changes and overrides made to the profile's Ethernet Port Basic Configuration. Select **Reset** to revert to the last saved configuration.

16 Select the **Security** tab.

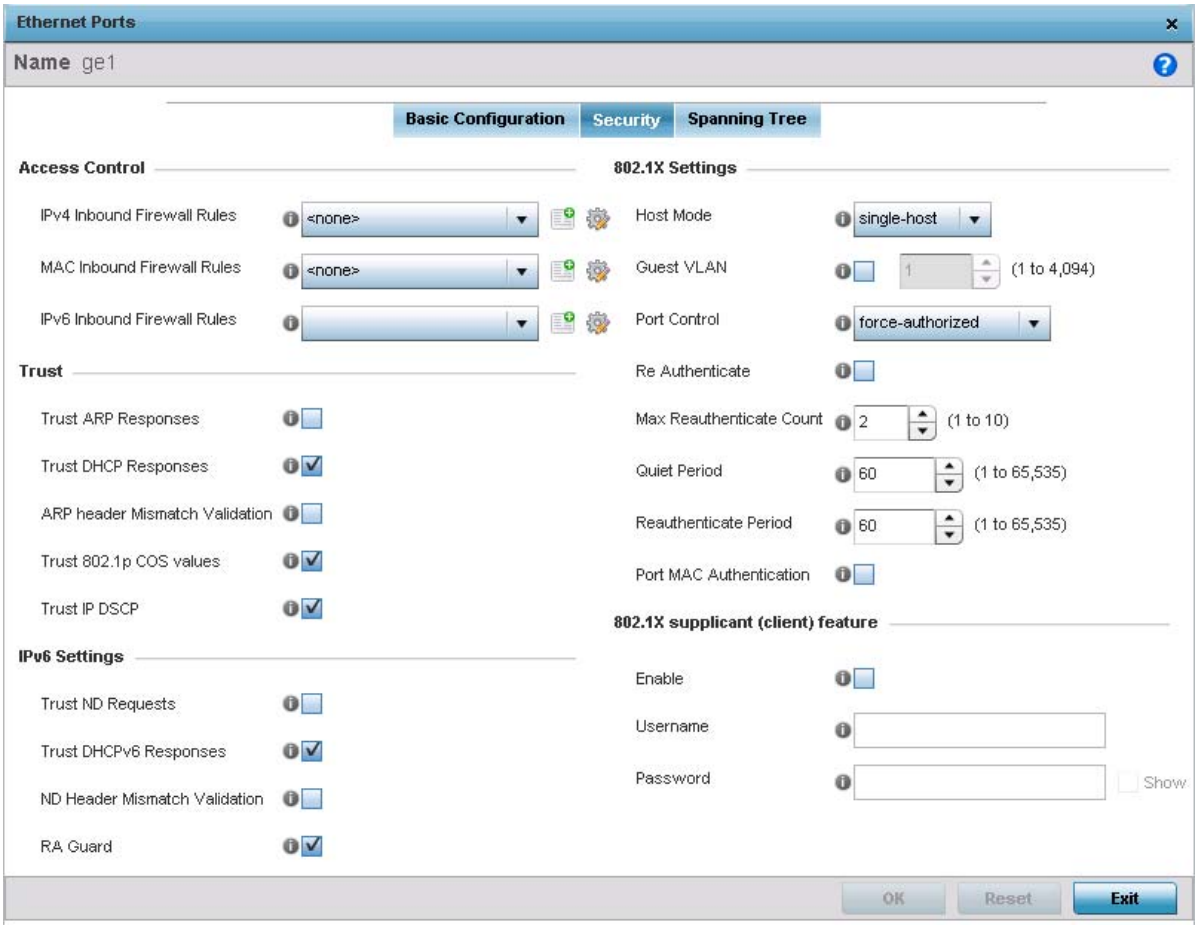


Figure 5-32 *Profile Overrides - Ethernet Ports Security screen*

17 Refer to the **Access Control** field. As part of the Ethernet port's security configuration, Inbound IP and MAC address firewall rules are required.

18 Use the **MAC Inbound Firewall Rules** drop-down menus to select the firewall rules to apply to this profile's Ethernet port configuration. The firewall inspects MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

Use the **IPv4 Inbound Firewall Rules** drop down menu to select the IPv4 specific firewall rules to apply to this profile's Ethernet port configuration. IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity.

19 Use the **IPv6 Inbound Firewall Rules** drop down menu to select the IPv6 specific firewall rules to apply to this profile's Ethernet port configuration. IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

20 If a firewall rule does not exist suiting the data protection needs of the target port configuration, select the **Create** icon to define a new rule configuration or the **Edit** icon to update or override an existing configuration. For more information, see Configuring IP Firewall Rules on page 10-20 or Wireless Firewall on page 10-1.

21 Refer to the **Trust** field to define or override the following:

Trust ARP Responses	Select this option to enable ARP trust on this port. ARP packets received on this port are considered trusted, and the information from these packets is used to identify rogue devices within the network. The default value is disabled.
Trust DHCP Responses	Select this option to enable DHCP trust on this port. If enabled, only DHCP responses are trusted and forwarded on this port, and a DHCP server can be connected only to a DHCP trusted port. The default value is enabled.
ARP header Mismatch Validation	Select this option to enable a mismatch check for the source MAC in both the ARP and Ethernet header. The default value is enabled.
Trust 802.1p COS values	Select this option to enable 802.1p COS values on this port. The default value is enabled.
Trust IP DSCP	Select this option to enable IP DSCP values on this port. The default value is enabled.

NOTE: Some vendor solutions with VRRP enabled send ARP packets with Ethernet SMAC as a physical MAC and inner ARP SMAC as VRRP MAC. If this configuration is enabled, a packet is allowed, despite a conflict existing.

22 Set the following **IPv6 Settings**:

Trust ND Requests	Select this option to enable the trust of neighbor discovery requests required on an IPv6 network on this Ethernet port. This setting is disabled by default.
Trust DHCPv6 Responses	Select this option to enable the trust all DHCPv6 responses on this Ethernet port. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is enabled by default.
ND Header Mismatch Validation	Select this option to enable a mismatch check for the source MAC within the ND header and Link Layer Option. This setting is disabled by default.
RA Guard	Select this option to enable router advertisements or ICMPv6 redirects from this Ethernet port. This setting is disabled by default.

23 Set the following **802.1X Settings**:

Host Mode	Use the drop-down menu to select the host mode configuration to apply to this port. Options include *single-host* or *multi-host*. The default setting is single-host.
Guest VLAN	Specify a guest VLAN for this port from 1 - 4094. This is the VLAN traffic is bridged on if this port is unauthorized and the guest VLAN is globally enabled.
Port Control	Use the drop-down menu to set the port control state to apply to this port. Options include *force-authorized*, *force-unauthorized* and *automatic*. The default setting is port-authorized.
Re Authenticate	Select this setting to force clients to reauthenticate on this port. The default setting is disabled, thus clients do not need to reauthenticate for connection over this port until this setting is enabled.
Max Reauthenticate Count	Set the maximum reauthentication attempts (1 - 10) before this port is moved to unauthorized. The default setting is 2.

Quiet Period	Set the quiet period for this port from 1 - 65,535 seconds.This is the maximum wait time 802.1x waits upon a failed authentication attempt. The default setting is 60 seconds.
Reauthenticate Period	Use the spinner control to set the reauthentication period for this port from 1 - 65,535 seconds. The default setting is 60 seconds.
Port MAC Authentication	When enabled, a port's MAC address is authenticated, as only one MAC address is supported per wired port. When successfully authenticated, packets from the source are processed. Packets from all other sources are dropped. Port MAC authentication is supported on RFS4000, RFS6000 model controllers and NX4500, NX6500 and NX9000 series service platforms. Port MAC authentication may be enabled on ports in conjunction with Wired 802.1x settings for a MAC Authentication AAA policy.

24 Select **Enable** within the 802.1x supplicant (client) feature field to enable a *username* and *password* pair used when authenticating users on this port. This setting is disabled by default. The password cannot exceed 32 characters.

25 Select **OK** to save the changes and overrides made to the Ethernet port's security configuration. Select **Reset** to revert to the last saved configuration.

26 Select the **Spanning Tree** tab.

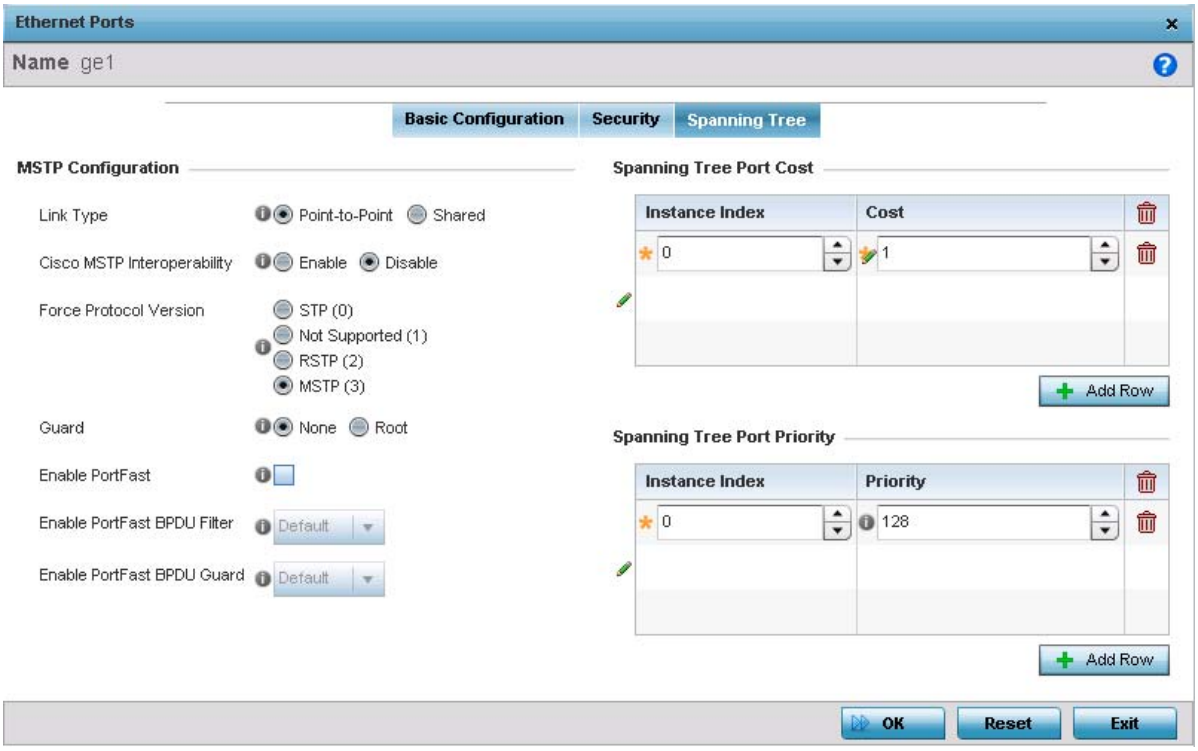


Figure 5-33 *Profile Overrides - Ethernet Ports Spanning Tree screen*

27 Set or override the following parameters for the port's **MSTP Configuration**:

Enable as Edge Port	Select this option to define this port as an edge port. Using an edge (private) port, you can isolate devices to prevent connectivity over this port.
Link Type	Select either the *Point-to-Point* or *Shared* radio button. Selecting Point-to-Point indicates the port should be treated as connected to a point-to-point link. Selecting Shared indicates this port should be treated as having a shared connection. A port connected to a hub is on a shared link, while one connected to a controller or service platform is a point-to-point link.
Cisco MSTP Interoperability	Select either the *Enable* or *Disable* radio buttons. This enables interoperability with Cisco's version of MSTP over the port, which is incompatible with standard MSTP.
Force Protocol Version	Sets the protocol version to either *STP(0)*, *Not Supported(1)*, *RSTP(2)* or *MSTP(3)*. MSTP is the default setting.
Guard	Determines whether the port enforces root bridge placement. Setting the guard to *Root* ensures the port is a designated port. Typically, each guard root port is a designated port, unless two or more ports (within the root bridge) are connected together. If the bridge receives superior BPDUs on a guard root-enabled port, the guard root moves the port to a root-inconsistent STP state. This state is equivalent to a listening state. No data is forwarded across the port. Thus, the guard root enforces the root bridge position.
Enable PortFast	Select this option to enable drop-down menus for both the Enable Portfast BPDU Filter and Enable Portfast BPDU guard options for the port.
Enable PortFast BPDU Filter	Enable PortFast to invoke a BPDU filter for this portfast enabled port. Enabling the BPDU filter feature ensures this PortFast enabled port does not transmit or receive BPDUs.
Enable PortFast BPDU Guard	Enable PortFast to invoke a BPDU guard for this portfast enabled port. Enabling the BPDU Guard feature means this portfast-enabled port will shutdown on receiving a BPDU.

28 Refer to the **Spanning Tree Port Cost** table.

Define or override an **Instance Index** using the spinner control and set the **Cost**. The default path cost depends on the user defined speed of the port.The cost helps determine the role of the port in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, the higher the cost.

Speed	Default Path Cost
<=100000 bits/sec	200000000
<=1000000 bits/sec	20000000
<=10000000 bits/sec	2000000
<=100000000 bits/sec	200000
<=1000000000 bits/sec	20000
<=10000000000 bits/sec	2000

<=100000000000 bits/sec	200
<=1000000000000 bits/sec	20
>1000000000000 bits/sec	2

29 Select **+ Add Row** as needed to include additional indexes.

30 Refer to the **Spanning Tree Port Priority** table.

Define or override an **Instance Index** using the spinner control and then set the **Priority**. The lower the priority, the greater likelihood of the port becoming a designated port. Applying a higher override value impacts the port's likelihood of becoming a designated port.

31 Select **+ Add Row** needed to include additional indexes.

32 Select **OK** to save the changes and overrides made to the Ethernet Port Spanning Tree configuration. Select **Reset** to revert to the last saved configuration.

5.2.7.2 Virtual Interface Override Configuration

Profile Interface Override Configuration

A virtual interface is required for layer 3 (IP) access to the controller or service platform or to provide layer 3 service on a VLAN. The virtual interface defines which IP address is associated with each VLAN ID the controller is connected to. A virtual interface is created for the default VLAN (VLAN 1) to enable remote controller administration. A virtual interface is also used to map VLANs to IP address ranges. This mapping determines the destination for controller or service platform routing.

To review existing virtual interface configurations and create a new virtual interface configuration, modify (override) an existing configuration or delete an existing configuration:

1 Select the Configuration tab from the Web UI.

2 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

3 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

4 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

5 Select **Interface** to expand its sub menu options.

6 Select **Virtual Interfaces**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

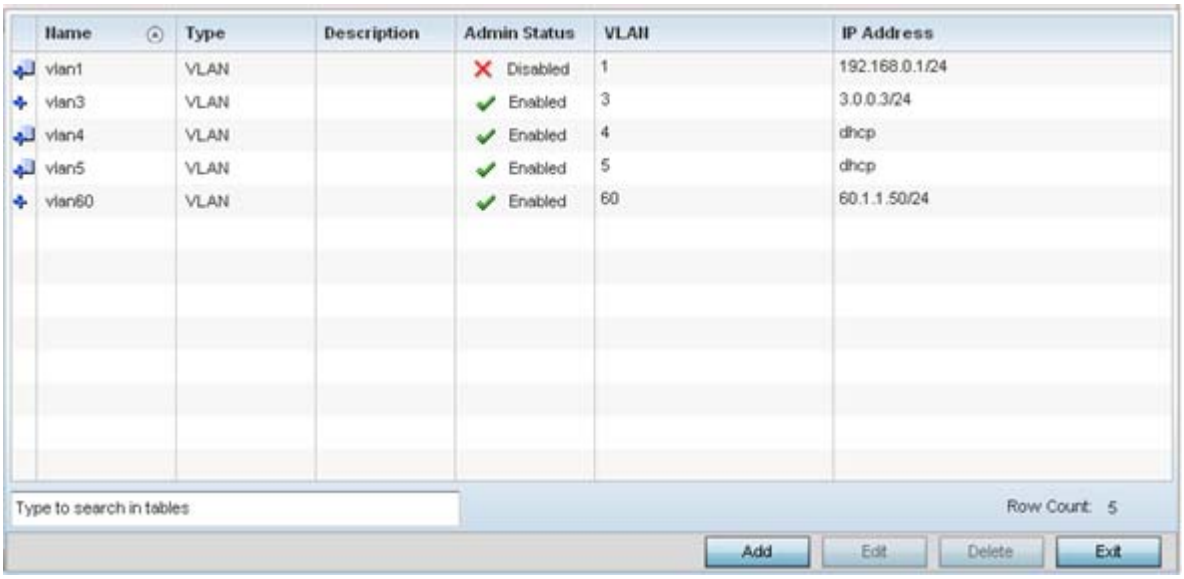


Figure 5-34 *Profile Overrides - Virtual Interfaces screen*

7 Review the following parameters unique to each virtual interface configuration to determine whether a parameter override is warranted:

Name	Displays the numeric ID of each listed virtual interface assigned when it was created. The name is between 1 - 4094, and cannot be modified as part of a virtual interface edit.
Type	Displays the type of virtual interface for each listed interface.
Description	Displays the description defined for the virtual interface when it was either initially created or edited.
Admin Status	A green check mark defines the listed virtual interface configuration as active and enabled with its supported profile. A red “X” defines the virtual interface as currently shut down. The interface status can be modified when a new virtual interface is created or an existing one modified.
VLAN	Displays the numerical VLAN ID associated with each listed interface.
IP Address	Defines whether DHCP was used to obtain the primary IP address used by the virtual interface configuration.

Once the configurations of existing virtual interfaces have been reviewed, determine whether a new interface requires creation, or an existing virtual interface requires edit (override) or deletion.

8 Select **Add** to define a new virtual interface configuration, Edit to modify or override the configuration of an existing virtual interface or **Delete** to permanently remove a selected virtual interface.

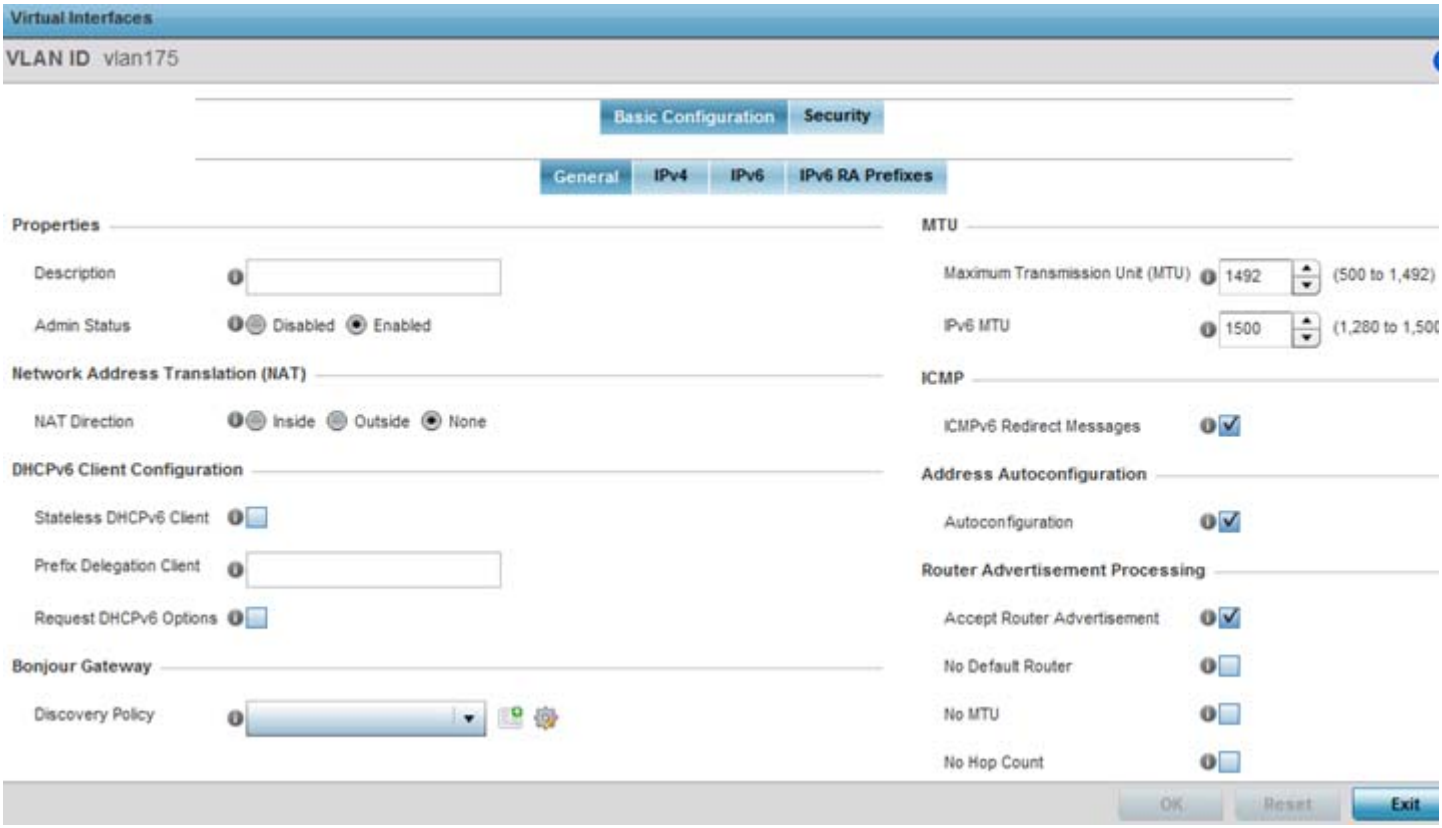


Figure 5-35 *Profile Overrides - Virtual Interfaces Basic Configuration screen*

The **Basic Configuration** screen displays by default regardless of a whether a new virtual interface is being created or an existing one is being modified. Select the **General** tab if not selected by default.

9 If creating a new virtual interface, use the VLAN ID spinner control to define a numeric VLAN ID from 1 - 4094.

10 Define or override the following parameters from within the **Properties** field:

Description	Provide or edit a description (up to 64 characters) for the virtual interface that helps differentiate it from others with similar configurations.
Admin Status	Either select the *Disabled* or *Enabled* radio button to define this interface's current status within the managed network. When set to Enabled, the virtual interface is operational and available to the controller or service platform. The default value is enabled.

11 Define or override the **Network Address Translation (NAT)** direction.

Select either the **Inside**, **Outside** or **None** radio buttons.

- *Inside* - The inside network is transmitting data over the network its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address.
- *Outside* - Packets passing through the NAT on the way back to the managed LAN are searched against to the records kept by the NAT engine. There the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the switch managed network.
- *None* - No NAT activity takes place. This is the default setting.

NOTE: Refer to Setting the Profile's NAT Configuration on page 8-186 for instructions on creating a profile's NAT configuration.

12 Set the following **DHCPv6 Client Configuration**. The *Dynamic Host Configuration Protocol for IPv6* (DHCPv6) provides a framework for passing configuration information.

Stateless DHCPv6 Client	Select this option to request information from the DHCPv6 server using stateless DHCPv6. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is disabled by default.
Prefix Delegation Client	Specify a 32 character maximum request prefix for prefix delegation from a DHCPv6 server over this virtual interface. Devices use prefixes to distinguish destinations that reside on-link from those reachable using a router.
Request DHCPv6 Options	Select this option to request DHCPv6 options on this virtual interface. DHCPv6 options provide configuration information for a node that must be booted using the network rather than locally. This setting is disabled by default.

13 Set the **Bonjour Gateway** settings for the virtual interface.Bonjour is Apple's implementation of zero-configuration networking (Zeroconf). Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates devices such as printers, other computers and services that these computers offer over a local network. Bonjour provides a general method to discover services on a *local area network* (LAN). It allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with special DNS configuration, it can be extended to find services across broadcast domains.

14 Select the Bonjour Gateway discover policy from the drop-down menu. Select the **Create** icon to define a new Bonjour Gateway policy configuration or select the **Edit** icon to modify an existing Bonjour Gateway policy configuration.

15 Set the following MTU settings for the virtual interface:

Maximum Transmission Unit (MTU)	Set the PPPoE client *maximum transmission unit* (MTU) from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492.
IPv6 MTU	Set an IPv6 MTU for this virtual interface from 1,280 - 1,500. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. The default is 1,500.

16 Within the **ICMP** field, define whether ICMPv6 redirect messages are sent. Redirect requests data packets be sent on an alternative route. This setting is enabled by default.

17 Within the **Address Autoconfiguration** field, define whether to configure IPv6 addresses on this virtual interface based on the prefixes received in router advertisement messages. Router advertisements contain prefixes used for link determination, address configuration and maximum hop limits. This setting is enabled by default.

18 Set the following **Router Advertisement Processing** settings for the virtual interface. Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

Accept RA	Enable this option to allow router advertisements over this virtual interface. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet layer configuration parameters.This setting is enabled by default.
No Default Router	Select this option to consider routers unavailable on this interface for default router selection. This setting is disabled by default.
No MTU	Select this option to not use the existing MTU setting for router advertisements on this virtual interface. If the value is set to zero no MTU options are sent. This setting is disabled by default.
No Hop Count	Select this option to not use the hop count advertisement setting for router advertisements on this virtual interface. This setting is disabled by default.

19 Select **OK** to save the changes. Select Reset to revert to the last saved configuration.

20 Select the **IPv4** tab to set IPv4 settings for this virtual interface.

IPv4 is a connectionless protocol. It operates on a best effort delivery model that does not guarantee delivery or assures proper sequencing or avoidance of duplicate delivery (unlike TCP).

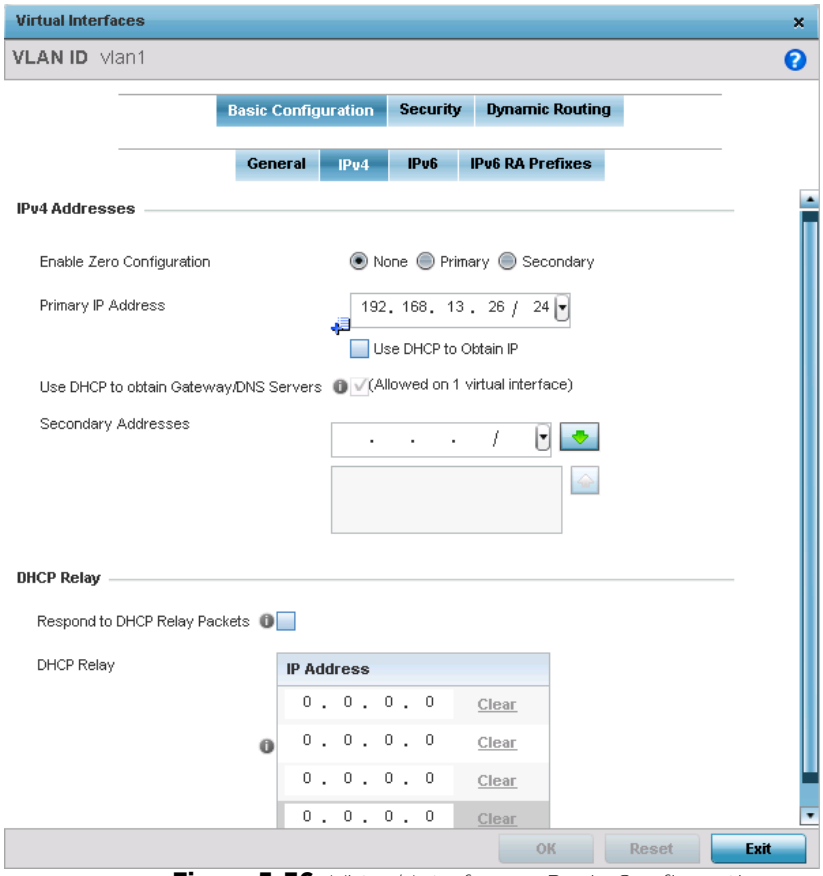


Figure 5-36 *Virtual Interfaces - Basic Configuration screen - IPv4 tab*

21 Set the following network information from within the **IPv4 Addresses** field:

Enable Zero Configuration	Zero configuration can be a means of providing a primary or secondary IP addresses for the virtual interface. Zero configuration (or zero config) is a wireless connection utility included with Microsoft Windows XP and later as a service dynamically selecting a network to connect based on a user's preferences and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device. This value is set to None by default.
Primary IP Address	Define the IP address for the VLAN associated Virtual Interface.
Use DHCP to Obtain IP	Select this option to allow DHCP to provide the IP address for the Virtual Interface. Selecting this option disables the Primary IP address field.
Use DHCP to obtain Gateway/DNS Servers	Select this option to allow DHCP to obtain a default gateway address and DNS resource for *one* virtual interface. This setting is disabled by default and only available when the *Use DHCP to Obtain IP* option is selected.
Secondary Addresses	Use the *Secondary Addresses* parameter to define additional IP addresses to associate with VLAN IDs. The address provided in this field is used if the primary IP address is unreachable.

22 Refer to the **DHCP Relay** field to set the DHCP relay server configuration used with the Virtual Interface.

Respond to DHCP Relay Packets	Select this option to allow the onboard DHCP server to respond to relayed DHCP packets on this interface. This setting is disabled by default.
DHCP Relay	Provide IP addresses for DHCP server relay resources. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When A DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.

23 Select **OK** to save the changes to the IPv4 configuration. Select **Reset** to revert to the last saved configuration.

24 Select the **IPv6** tab to set IPv6 settings for this virtual interface.

IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet layer configuration parameters.

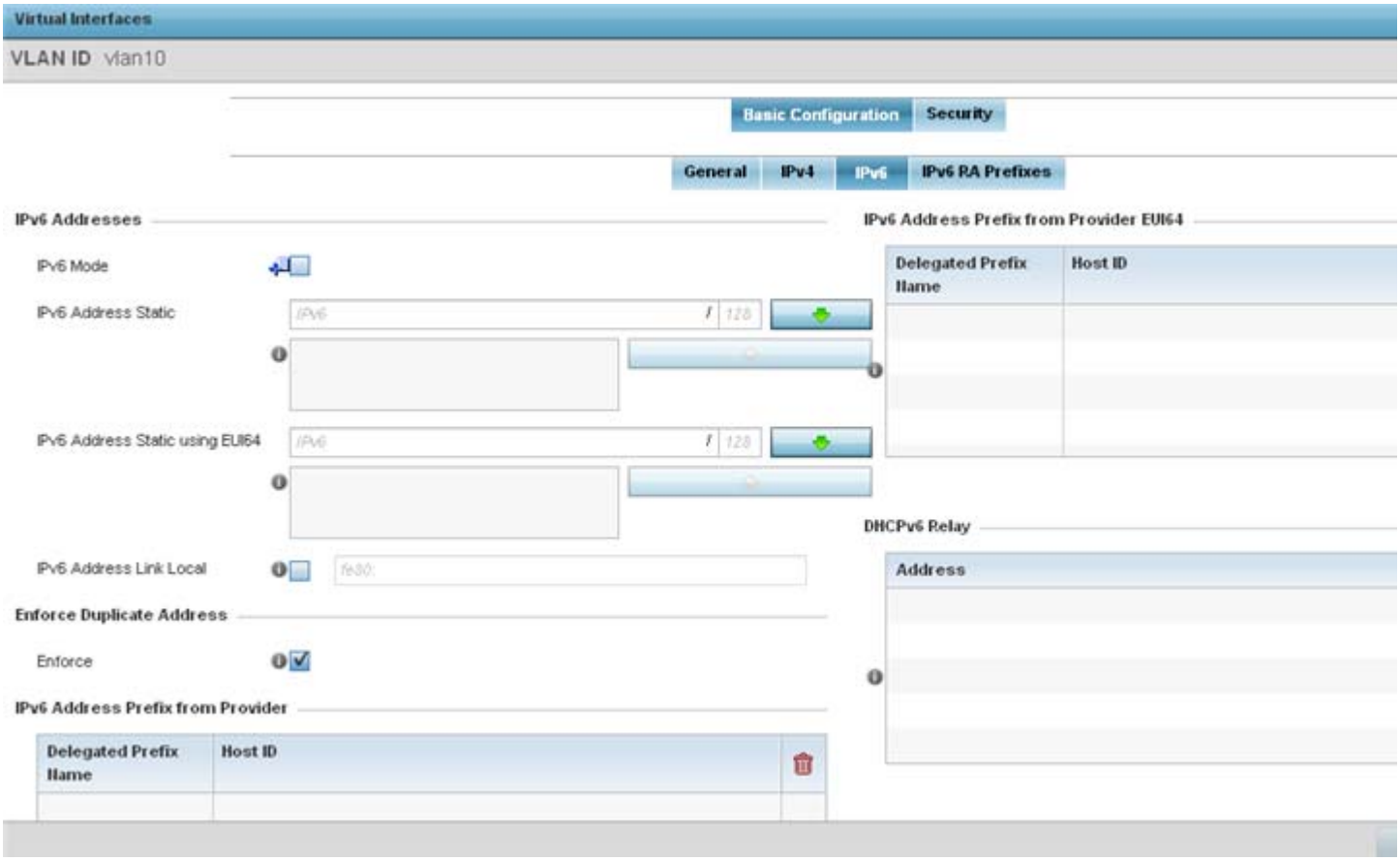


Figure 5-37 *Virtual Interfaces - Basic Configuration screen - IPv6 tab*

25 Refer to the **IPv6 Addresses** field to define how IP6 addresses are created and utilized.

IPv6 Mode	Select this option to enable IPv6 support on this virtual interface. IPv6 is disabled by default.
IPv6 Address Static	Define up to 15 global IPv6 IP addresses that can created statically. IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons.
IPv6 Address Static using EUI64	Optionally set up to 15 global IPv6 IP addresses (in the EUI-64 format) that can created statically. The IPv6 EUI-64 format address is obtained through a 48-bit MAC address. The MAC is initially separated into two 24-bits, with one being an OUI (*Organizationally Unique Identifier*) and the other being client specific. A 16-bit 0xFFFE is then inserted between the two 24-bits for the 64-bit EUI address. IEEE has chosen FFFE as a reserved value which can only appear in EUI-64 generated from the an EUI-48 MAC address.
IPv6 Address Link Local	Provide the IPv6 local link address. IPv6 requires a link local address assigned to every interface the IPv6 protocol is enabled, even when one or more routable addresses are assigned.

26 Enable the **Enforce Duplicate Address** option to enforce duplicate address protection when any wired port is connected and in a forwarding state. This option is enabled by default.

27 Refer to the **IPv6 Address Prefix from Provider** table to create IPv6 format prefix shortcuts as supplied by an ISP.

28 Select **+ Add Row** to launch a sub screen wherein a new delegated prefix name and host ID can be defined.

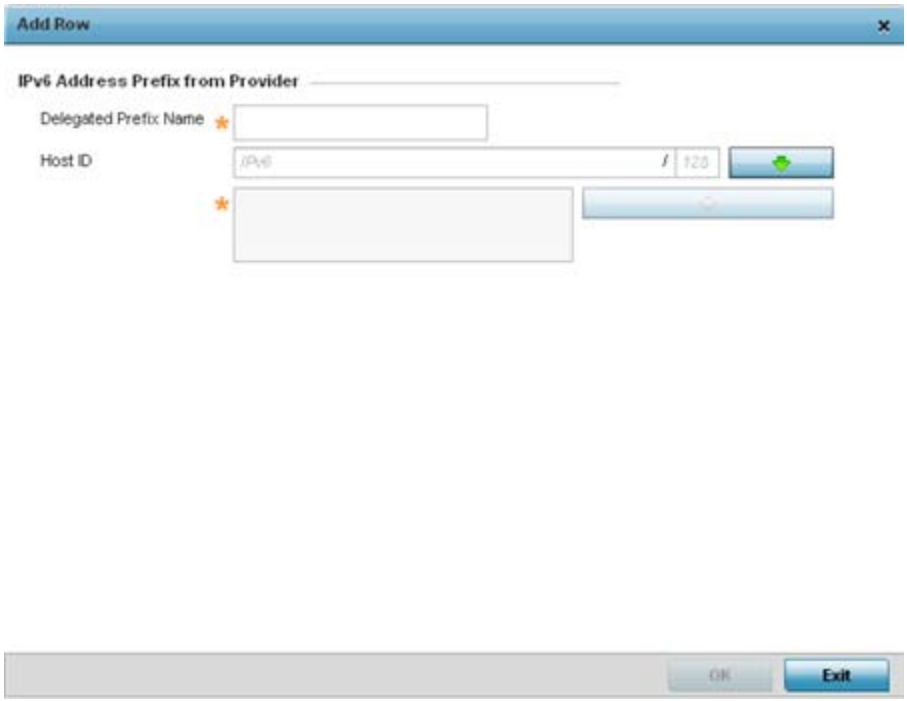


Figure 5-38 *Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider*

Delegated Prefix Name	Enter a 32 character maximum name for the IPv6 address prefix from provider.
Host ID	Define the subnet ID, host ID and prefix length.

29 Select **OK** to save the changes to the new IPv6 prefix from provider. Select **Exit** to close the screen without saving the updates.

30 Refer to the **IPv6 Address Prefix from Provider EUI64** table to set an (abbreviated) IP address prefix in EUI64 format.

31 Select **+ Add Row** to launch a sub screen wherein a new delegated prefix name and host ID can be defined in EUI64 format.

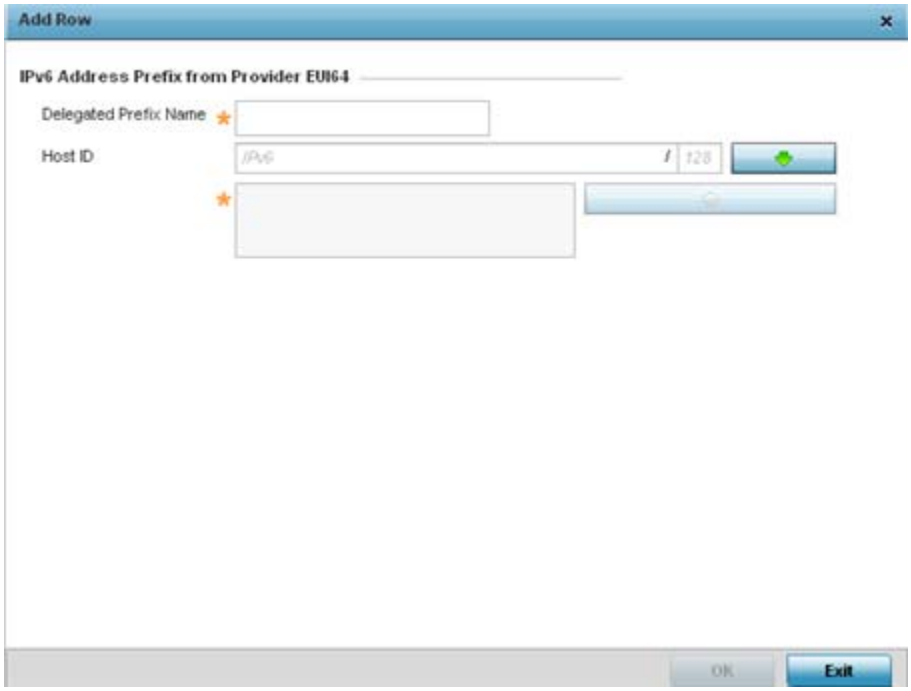


Figure 5-39 *Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider EUI64*

Delegated Prefix Name	Enter a 32 character maximum name for the IPv6 prefix from provider in EUI format. Using EUI64, a host can automatically assign itself a unique 64-bit IPv6 interface identifier without manual configuration or DHCP.
Host ID	Define the subnet ID and prefix length.

32 Select **OK** to save the changes to the new IPv6 prefix from provider in EUI64 format. Select **Exit** to close the screen without saving the updates.

33 Refer to the **DHCPv6 Relay** table to set the address and interface of the DHCPv6 relay.

The DHCPv6 relay enhances an extended DHCP relay agent by providing support in IPv6. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When A DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.

34 Select **+ Add Row** to launch a sub screen wherein a new DHCPv6 relay address and interface VLAN ID can be set.

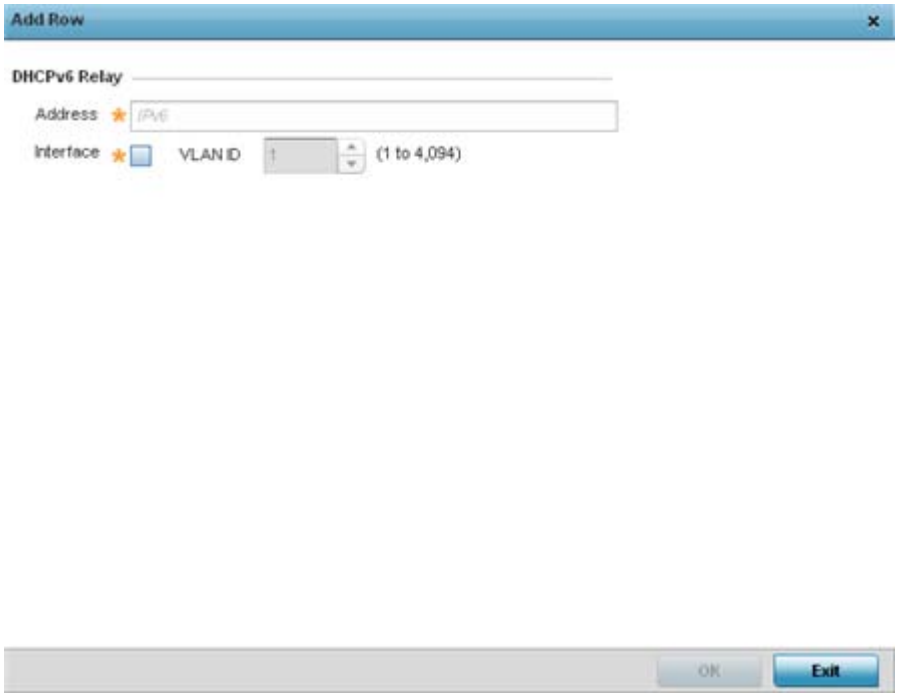


Figure 5-40 *Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add DHCPv6 Relay*

Address	Enter an address for the DHCPv6 relay. These DHCPv6 relay receive messages from DHCPv6 clients and forward them to DHCPv6 servers. The DHCPv6 server sends responses back to the relay, and the relay then sends these responses to the client on the local network.
Interface	Select this option to enable a spinner control to define a VLAN ID from 1 - 4,094 used as the virtual interface for the DHCPv6 relay. The interface designation is only required for link local and multicast addresses. A local link address is a locally derived address designed for addressing on a single link for automatic address configuration, neighbor discovery or when no routing resources are available.

35 Select **OK** to save the changes to the DHCPv6 relay configuration. Select **Exit** to close the screen without saving the updates.

36 Select the **IPv6 RA Prefixes** tab.

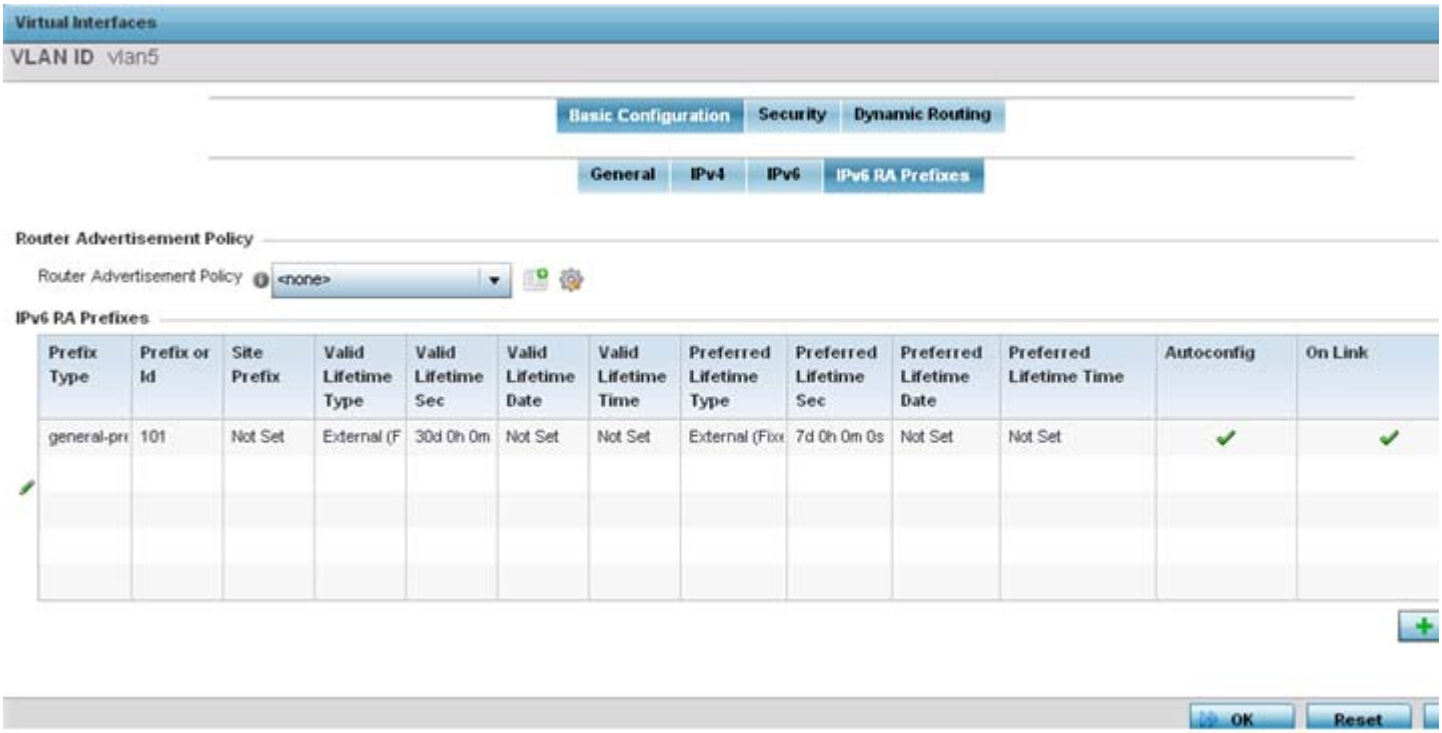


Figure 5-41 *Virtual Interfaces - Basic Configuration screen - IPv6 RA Prefixes tab*

37 Use the **Router Advertisement Policy** drop-down menu to select and apply a policy to the virtual interface.

Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

38 Review the configurations of existing IPv6 advertisement policies. If needed select **+ Add Row** to define the configuration of an additional IPv6 RA prefix.

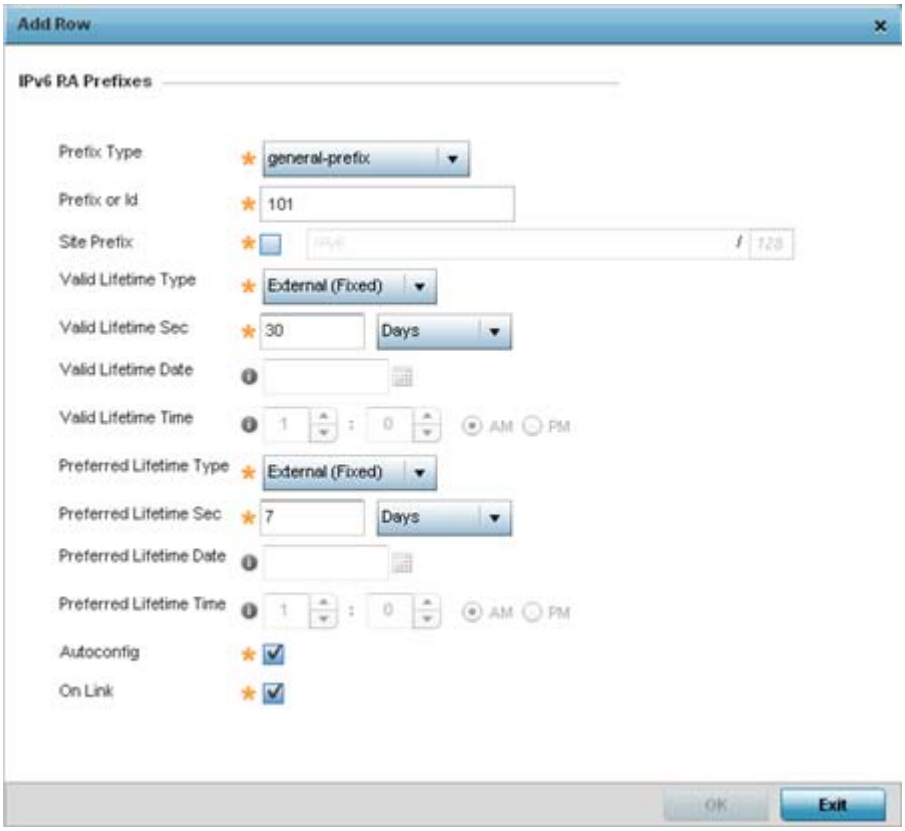


Figure 5-42 *Virtual Interfaces - Basic Configuration screen - Add IPv6 RA Prefix*

39 Set the following **IPv6 RA Prefix** settings:

Prefix Type	Set the prefix delegation type used with this configuration. Options include, *Prefix*, and *prefix-from-provider*. The default setting is Prefix. A prefix allows an administrator to associate a user defined name to an IPv6 prefix. A provider assigned prefix is made available from an *Internet Service Provider* (ISP) to automate the process of providing and informing the prefixes used.
Prefix or ID	Set the actual prefix or ID used with the IPv6 router advertisement.
Site Prefix	The site prefix is added into a router advertisement prefix. The site address prefix signifies the address is only on the local link.
Valid Lifetime Type	Set the lifetime for the prefix's validity. Options include *External (fixed), decrementing* and *infinite*. If set to External (fixed), just the *Valid Lifetime Sec* setting is enabled to define the exact time interval for prefix validity. If set to decrementing, use the lifetime date and time settings to refine the prefix expiry period. If the value is set for infinite, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is External (fixed).
Valid Lifetime Sec	If the lifetime type is set to *External (fixed),* set the *Seconds, Minutes, Hours* or *Days* value used to measurement criteria for the prefix's expiration. 30 days, 0 hours, 0 minutes and 0 seconds is the default lifetime.
Valid Lifetime Date	If the lifetime type is set to *External (fixed)*, set the date in MM/DD/YYYY format for the expiration of the prefix.

Valid Lifetime Time	If the lifetime type is set to *decrementing*, set the time for the prefix's validity.
Preferred Lifetime Type	Set the administrator preferred lifetime for the prefix's validity. Options include *External (fixed), decrementing* and *infinite*. If set to External (fixed), just the *Valid Lifetime Sec* setting is enabled to define the exact time interval for prefix validity. If set to decrementing, use the lifetime date and time settings to refine the prefix expiry period. If the value is set for infinite, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is External (fixed).
Preferred Lifetime Sec	If the administrator preferred lifetime type is set to *External (fixed)*, set the *Seconds, Minutes, Hours* or *Days* value used to measurement criteria for the prefix's expiration. 30 days, 0 hours, 0 minutes and 0 seconds is the default lifetime.
Preferred Lifetime Date	If the administrator preferred lifetime type is set to *External (fixed),* set the date in MM/DD/YYYY format for the expiration of the prefix.
Preferred Lifetime Time	If the preferred lifetime type is set to *decrementing,* set the time for the prefix's validity.
Autoconfig	Autoconfiguration includes generating a link-local address, global addresses via stateless address autoconfiguration and duplicate address detection to verify the uniqueness of the addresses on a link. This setting is enabled by default.
On Link	Select this option to keep the IPv6 RA prefix on the local link. The default setting is enabled.

40 Select **OK** to save the changes to the IPv6 RA prefix configuration. Select **Exit** to close the screen without saving the updates.

41 Select **OK** to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

42 Select the **Security** tab.

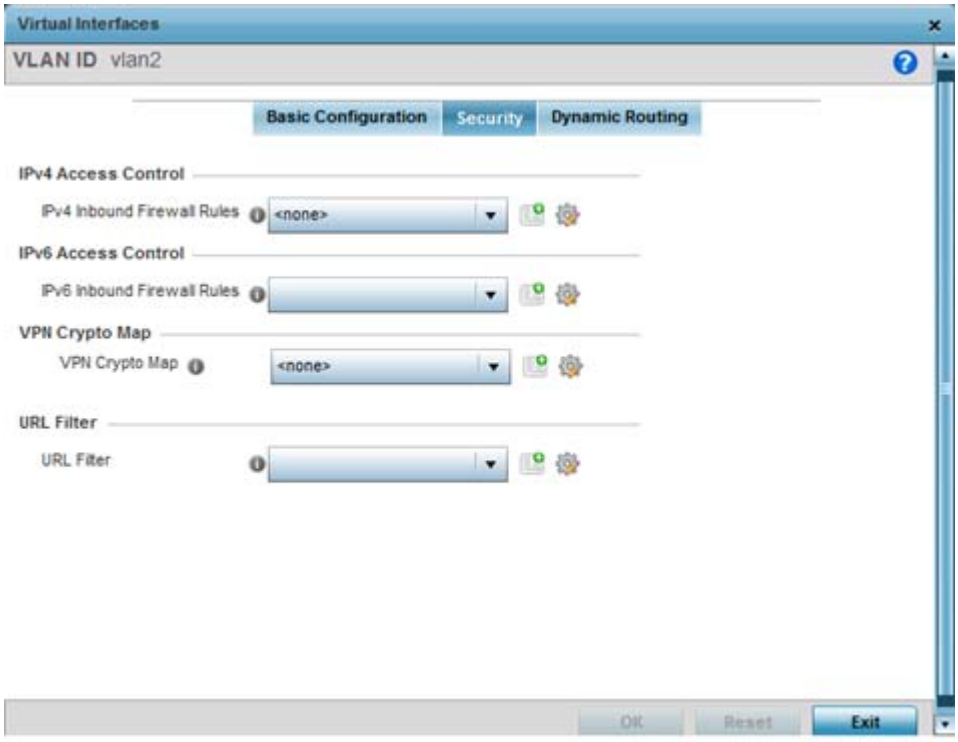


Figure 5-43 *Profile Overrides - Virtual Interfaces Security screen*

43 Use the **IPv4 Inbound Firewall Rules** drop down menu to select the IPv4 specific inbound firewall rules to apply to this profile's virtual interface configuration. Select the **Create** icon to define a new IPv4 firewall rule configuration or select the **Edit** icon to modify an existing configuration.

IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, since it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP).

IPv4 and IPv6 are different enough to warrant separate protocols. IPv6 devices can alternatively use stateless address autoconfiguration. IPv4 hosts can use link local addressing to provide local connectivity.

44 Use the **IPv6 Inbound Firewall Rules** drop down menu to select the IPv6 specific inbound firewall rules to apply to this profile's virtual interface configuration. Select the **Create** icon to define a new IPv6 firewall rule configuration or select the **Edit** icon to modify an existing configuration.

IPv6 is the latest revision of the *Internet Protocol* (IP) replacing IPv4. IPV6 provides enhanced identification and location information for systems routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

45 Use the **VPN Crypto Map** drop-down menu to select or override the **Crypto Map** configuration applied to this virtual interface.

Crypto Map entries are sets of configuration parameters for encrypting packets that pass through the VPN Tunnel. If a Crypto Map configuration does not exist suiting the needs of this virtual interface, select the **Create** icon to define a new Crypto Map configuration or the **Edit** icon to modify an existing configuration. For more information, see Overriding a Profile's VPN Configuration on page 5-207.

46 Use the **URL Filter** drop-down menu to select or override the **URL Filter** configuration applied to this virtual interface. URL filtering is used to restrict access to undesirable resources on the Internet.

47 Select the **Dynamic Routing** tab (if available with your controller or service platform).

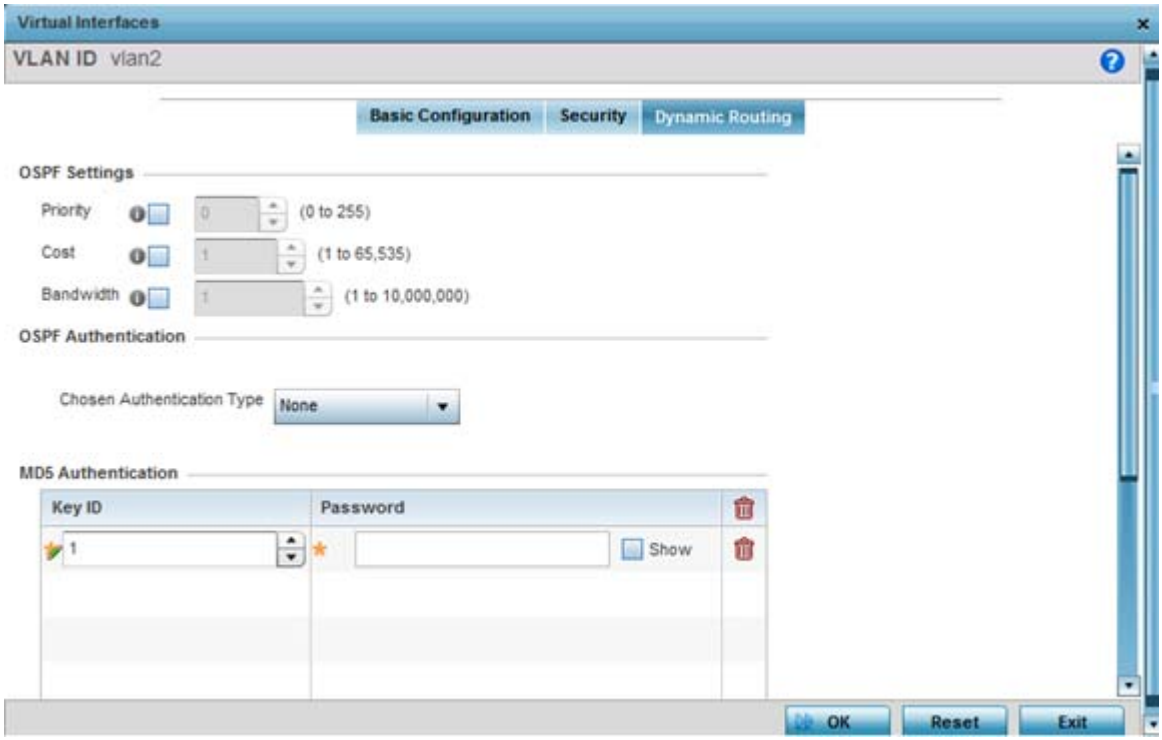


Figure 5-44 *Profile Overrides - Virtual Interfaces Security screen*

48 Define or override the following parameters from within the **OSPF Settings** field:

Priority	Select this option to set the OSPF priority used to select the network designated route. Use the spinner control to set the value from 0 - 255.
Cost	Select this option to set the cost of the OSPF interface. Use the spinner control to set the value from 1 - 65,535.
Bandwidth	Set the OSPF interface bandwidth (in Kbps) from 1 - 10,000,000.

49 Select the authentication type from the **Chosen Authentication Type** drop-down used to validate credentials within the OSPF dynamic route. Options include *simple-password*, *message-digest*, *null* and *None*. The default value is None.

50 Select the **+ Add Row** button at the bottom of the **MD5 Authentication** table to add the Key ID and Password used for an MD5 validation of authenticator credentials. Use the spinner control to set the OSPF message digest authentication key ID. The available range is from 1 - 255. The password is the OSPF key either displayed as series or asterisks or in plain text (by selecting **Show**).

51 Select the **OK** button located at the bottom right of the screen to save the changes and overrides to the Dynamic Routing screen. Select **Reset** to revert to the last saved configuration.

5.2.7.3 Port Channel Override Configuration

Profile Interface Override Configuration

Profiles can utilize customized port channel configurations as part of their interface settings. Existing port channel profile configurations can be overridden as the become obsolete for specific device deployments.

To define or override a port channel configuration on a profile:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

3 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the *Device Browser* in the lower, left-hand, side of the UI.

4 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

5 Select **Interface** to expand its sub menu options.

6 Select **Port Channels**.

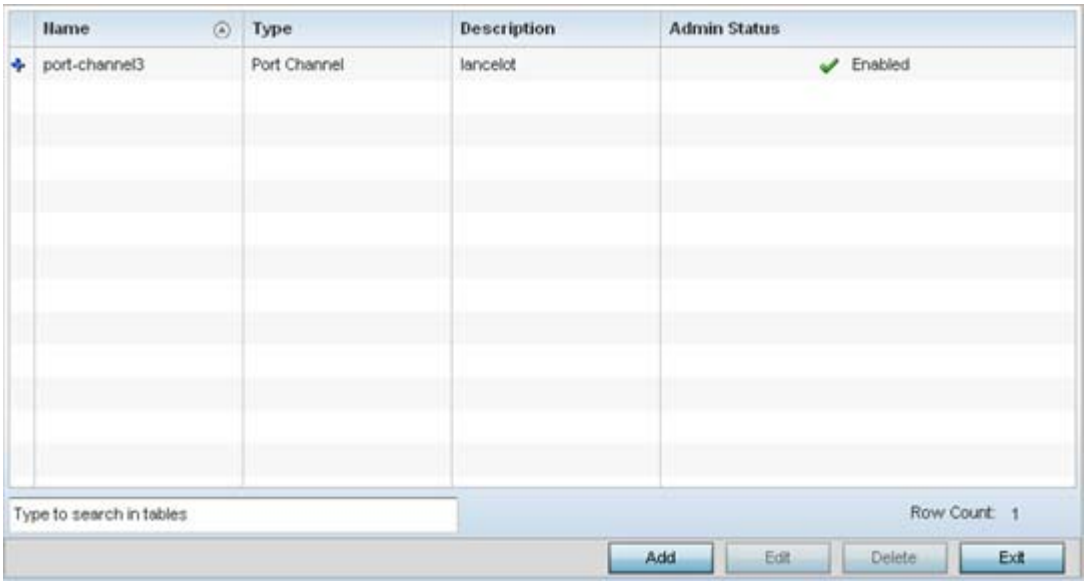


Figure 5-45 *Profile Overrides - Port Channels screen*

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

7 Refer to the following to review existing port channel configurations and status to determine whether a parameter requires an override:

Name	Displays the port channel's numerical identifier assigned when it was created. The numerical name cannot be modified as part of the edit process.
Type	Displays whether the type is port channel.

Description	Lists a a short description (64 characters maximum) describing the port channel or differentiating it from others with similar configurations.
Admin Status	A green check mark defines the listed port channel as active and currently enabled with the profile. A red “X” defines the port channel as currently disabled and not available for use. The interface status can be modified with the port channel configuration as required.

8 To edit or override the configuration of an existing port channel, select it from amongst those displayed and select the **Edit** button. The port channel Basic Configuration screen displays by default.

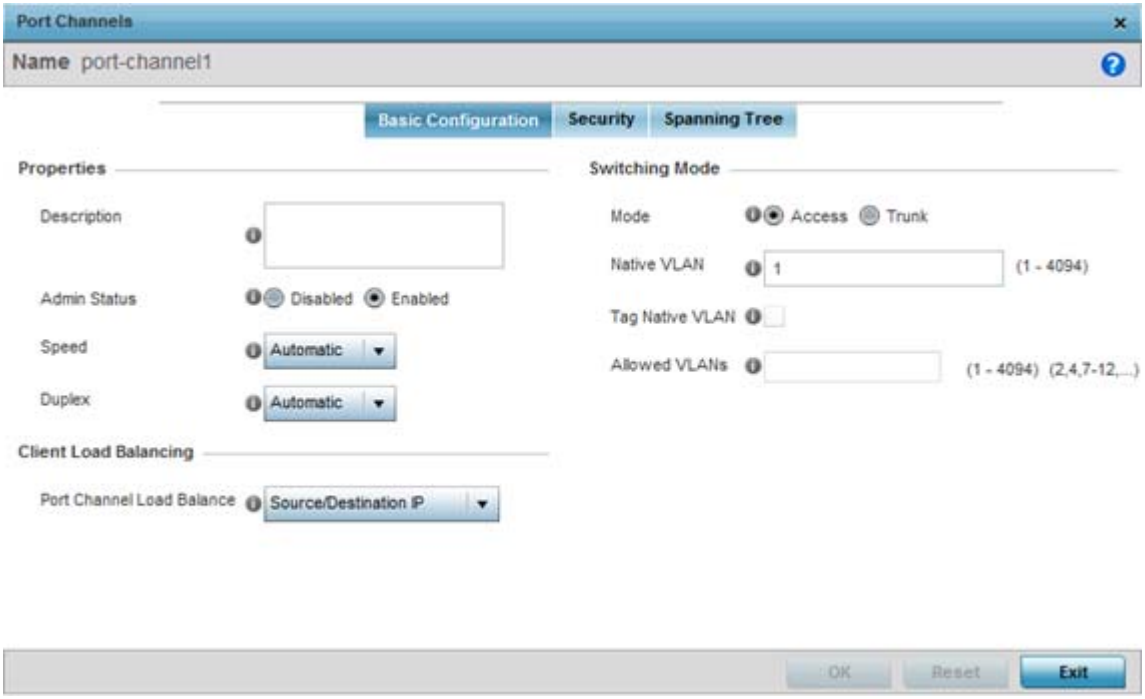


Figure 5-46 *Profile Overrides - Port Channels Basic Configuration screen*

9 Set or override the following port channel **Properties**:

Description	Enter a description for the controller or service platform port channel (64 characters maximum).
Admin Status	Select the *Enabled* radio button to define this port channel as active to the profile it supports. Select the *Disabled* radio button to disable this port channel configuration in the profile. It can be activated at any future time when needed. The default setting is enabled.

Speed	Select the speed at which the port channel can receive and transmit data. Select either 10 Mbps, 100 Mbps or 1000 Mbps to establish a 10, 100 or 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission. These options are not available if Auto is selected. Select Automatic to allow the port channel to automatically exchange information about data transmission speeds and duplex capabilities. Auto negotiation is helpful in an environment where different devices are connected and disconnected on a regular basis. Automatic is the default setting.
Duplex	Select either half, full or automatic as the duplex option. Select **Half** duplex to send data over the port channel, then immediately receive data from the same direction in which the data was transmitted. Like a full-duplex transmission, a half-duplex transmission can carry data in both directions, just not at the same time. Select **Full** duplex to transmit data to and from the port channel at the same time. Using full duplex, the port channel can send data while receiving data as well. Select **Automatic** to enable to the controller or service platform to dynamically duplex as port channel performance needs dictate. Automatic is the default setting.

10 Use the **Port Channel Load Balance** drop-down menu from the **Client Load Balancing** section to define whether port channel load balancing is conducted using a *Source/Destination IP* or a *Source/Destination MAC*. Source/Destination IP is the default setting.

11 Define or override the following **Switching Mode** parameters to apply to the port channel configuration:

Mode	Select either the *Access* or *Trunk* radio button to set the VLAN switching mode over the port channel. If Access is selected, the port channel accepts packets only from the native VLAN. Frames are forwarded untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. If the mode is set to Trunk, the port channel allows packets from a list of VLANs you add to the trunk. A port channel configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. Access is the default setting.
Native VLAN	Use the spinner control to define a numerical *Native VLAN ID* from 1 - 4094. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic will be directed over when using trunk mode. The default value is 1.

Tag the Native VLAN	Select this option to tag the native VLAN. Controllers and service platforms support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, a 12 bit frame VLAN ID is added to the 802.1Q header, so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This setting is disabled by default.
Allowed VLANs	Selecting *Trunk* as the mode enables the *Allowed VLANs* parameter. Add VLANs that exclusively send packets over the port channel.

12 Select **OK** to save the changes and overrides to the port channel Basic Configuration. Select **Reset** to revert to the last saved configuration.

13 Select the **Security** tab.

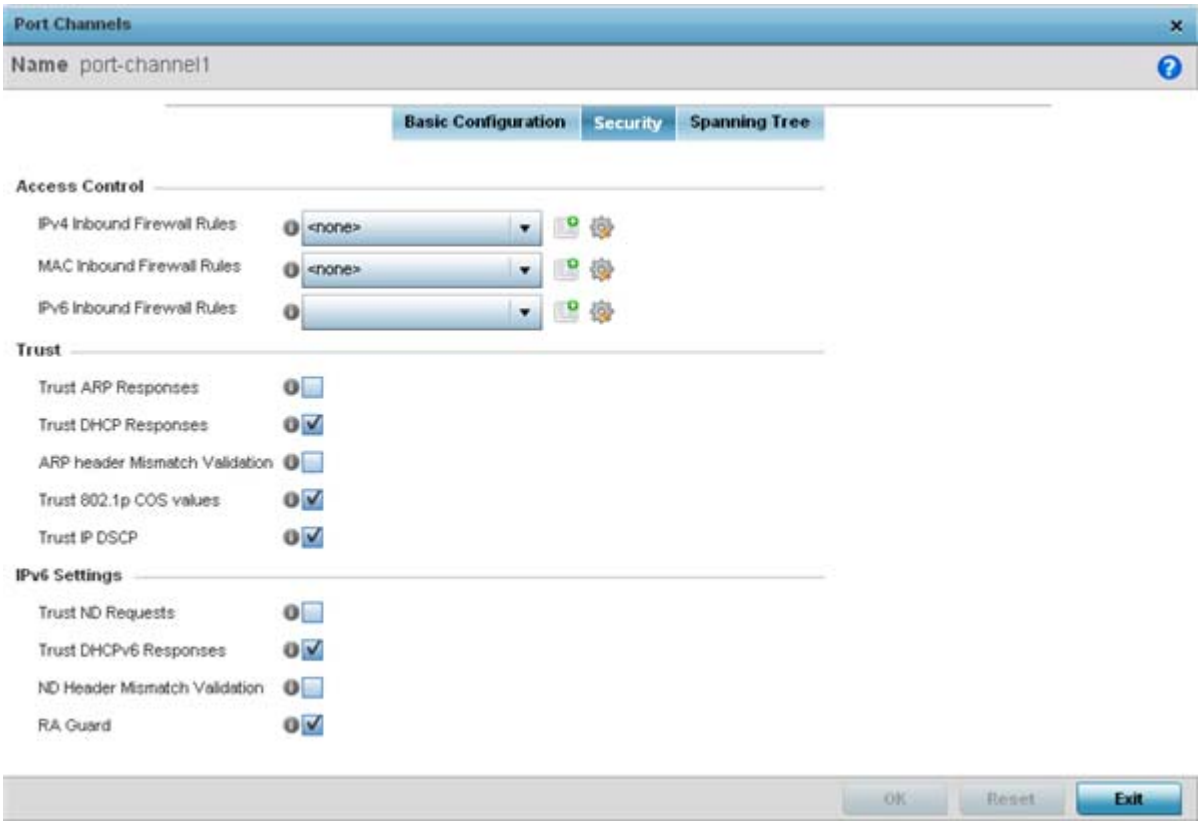


Figure 5-47 *Profile Overrides - Port Channels Security screen*

14 Refer to the **Access Control** section. As part of the port channel's security configuration, Inbound IPv4 IP, IPv6 IP and MAC address firewall rules are required.

15 Use the drop-down menus to select the firewall rules to apply to this profile's Ethernet port configuration. The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances

16 Use the **IPv4 Inbound Firewall Rules** drop down menu to select the IPv4 specific firewall rules to apply to this profile's port channel configuration. IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity.

17 Use the **IPv6 Inbound Firewall Rules** drop down menu to select the IPv6 specific firewall rules to apply to this profile's port channel configuration. IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

18 If a firewall rule does not exist suiting the data protection needs of the target port channel configuration, select the **Create** icon to define a new rule configuration or the **Edit** icon to modify an existing firewall rule configuration.

19 Refer to the **Trust** section to define or override the following:

Trust ARP Responses	Select this option to enable ARP trust on this port channel. ARP packets received on this port are considered trusted, and information from these packets is used to identify rogue devices. The default value is disabled.
Trust DHCP Responses	Select this option to enable DHCP trust. If enabled, only DHCP responses are trusted and forwarded on this port channel, and a DHCP server can be connected only to a DHCP trusted port. The default value is enabled.
ARP header Mismatch Validation	Select this option to enable a source MAC mismatch check in both the ARP and Ethernet header. The default value is enabled.
Trust 802.1p COS values	Select this option to enable 802.1p COS values on this port channel. The default value is enabled.
Trust IP DSCP	Select this option to enable IP DSCP values on this port channel. The default value is disabled.

20 Refer to the **IPv6 Settings** field to define the following:

Trust ND Requests	Select the check box to enable *neighbor discovery* (ND) request trust on this port channel (neighbor discovery requests received on this port are considered trusted). Neighbor discovery allows the discovery of an adjacent device's MAC addresses, similar to *Address Resolution Protocol* (ARP) on Ethernet in IPv4. The default value is disabled.
Trust DHCPv6 Responses	Select the check box to enable DHCPv6 trust. If enabled, only DHCPv6 responses are trusted and forwarded on this port channel, and a DHCPv6 server can be connected only to a trusted port. The default value is enabled.

ND header Mismatch Validation	Select the check box to enable a mismatch check for the source MAC in both the ND header and link layer option. The default value is disabled.
RA Guard	Select this option to allow router advertisements or IPv6 redirects from this port. Router advertisements are periodically sent to hosts or sends in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.This setting is enabled by default.

21 Select **OK** to save the changes and overrides to the security configuration. Select **Reset** to revert to the last saved configuration.

22 Select the **Spanning Tree** tab.

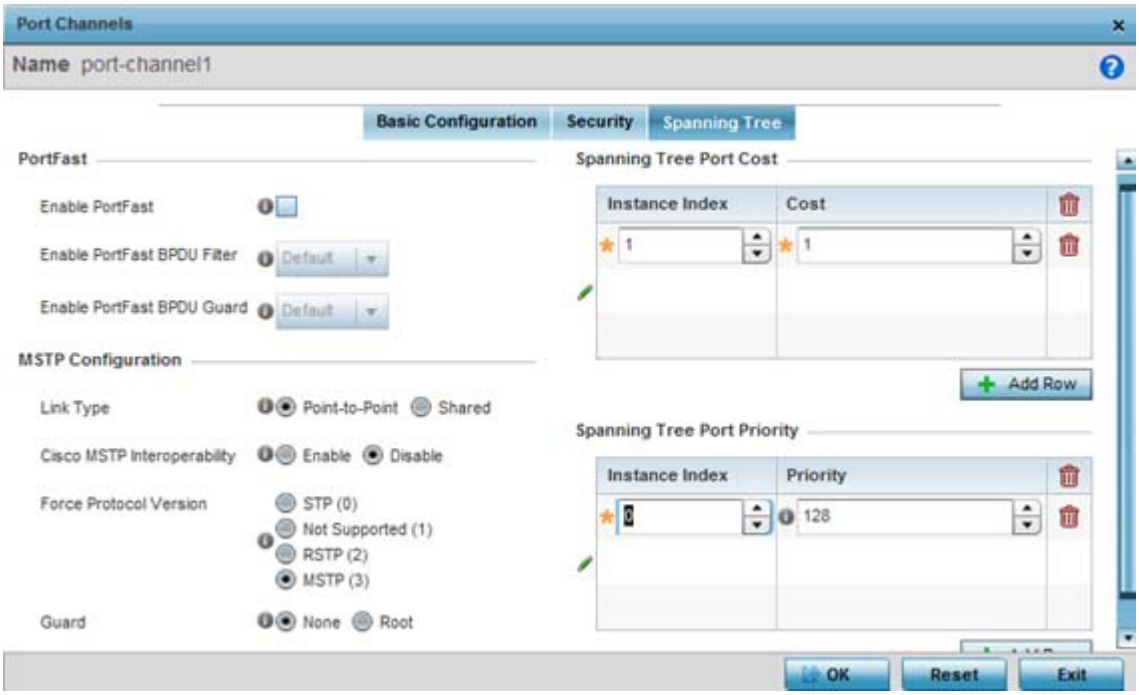


Figure 5-48 *Profile Overrides - Port Channels Spanning Tree screen*

23 Define or override the following **PortFast** parameters for the port channel's MSTP configuration:

Enable PortFast	Select this option to enable drop-down menus for both the Enable Portfast BPDU Filter and Enable Portfast BPDU guard options for the port. This setting is disabled by default.
Enable PortFast BPDU Filter	Enable PortFast to invoke a BPDU filter for this portfast enabled port channel. Enabling the BPDU filter feature ensures this port channel does not transmit or receive any BPDUs.
Enable PortFast BPDU Guard	Enable PortFast to invoke a BPDU guard for this portfast enabled port channel. Enabling the BPDU Guard feature means this port will shutdown on receiving a BPDU. Hence no BPDUs are processed.

24 Set or override the following **MSTP Configuration** parameters for the port channel:

Enable as Edge Port	Select this option to define this port as an edge port. Using an edge (private) port, you can isolate devices to prevent connectivity over this port channel. This setting is disabled by default.
Link Type	Select either the *Point-to-Point* or *Shared* radio button. Selecting Point-to-Point indicates the port should be treated as connected to a point-to-point link. Selecting Shared indicates this port should be treated as having a shared connection. A port connected to a hub is on a shared link, while one connected to a controller or service platform is a point-to-point link. Point-to-Point is the default setting.
Cisco MSTP Interoperability	Select either the *Enable* or *Disable* radio buttons. This enables interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default.
Force Protocol Version	Sets the protocol version to either *STP(0), Not Supported(1), RSTP(2)* or *MSTP(3).* MSTP is the default setting.
Guard	Determines whether the port channel enforces root bridge placement. Setting the guard to *Root* ensures the port is a designated port. Typically, each guard root port is a designated port, unless two or more ports (within the root bridge) are connected together. If the bridge receives superior (BPDUs) on a guard root-enabled port, the guard root moves the port to a root-inconsistent STP state. This state is equivalent to a listening state. No data is forwarded across the port. Thus, the guard root enforces the root bridge position.

25 Refer to the **Spanning Tree Port Cost** table.

26 Define or override an **Instance Index** using the spinner control and then set the **Cost**. The default path cost depends on the user defined port speed. The cost helps determine the role of the port channel in the MSTP network.

The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, the higher the cost.

Speed	Default Path Cost
<=100000 bits/sec	200000000
<=1000000 bits/sec	20000000
<=10000000 bits/sec	2000000
<=100000000 bits/sec	200000
<=1000000000 bits/sec	20000
<=10000000000 bits/sec	2000
<=100000000000 bits/sec	200
<=1000000000000 bits/sec	20
>1000000000000 bits/sec	2

27 Refer to the **Spanning Tree Port Priority** table.

Define or override an **Instance Index** using the spinner control, then set the **Priority**. The lower the priority, the greater likelihood of the port becoming a designated port.

28 Select **+ Add Row** as needed to include additional indexes.

29 Select **OK** to save the changes and overrides made to the Ethernet Port Spanning Tree configuration. Select **Reset** to revert to the last saved configuration.

5.2.7.4 VM Interface Override Configuration

Profile Interface Override Configuration

WiNG provides a dataplane bridge for external network connectivity for *Virtual Machines* (VMs). VM Interfaces define which IP address is associated with each VLAN ID the service platform is connected to and enables remote service platform administration. Each custom VM can have up to a maximum of two VM interfaces. Each VM interface can be mapped to one of sixteen VMIF ports on the dataplane bridge. This mapping determines the destination for service platform routing.

By default, VM interfaces are internally connected to the dataplane bridge via VMIF1. VMIF1 is an untagged port providing access to VLAN 1 to support the capability to connect the VM interfaces to any of the VMIF ports. This provides the flexibility to move a VM interface onto different VLANs as well as configure specific firewall and QOS rules.

NOTE: VM interfaces are only supported for NX4500 and NX6500 series service platforms.

To define or override a VM interfaces configuration on a profile:

1 Select the **Configuration** tab from the Web UI.

2 Select **Devices** from the Configuration tab.

The *Device Configuration* screen displays a list of managed devices or peer controllers, service platforms or Access Points.

3 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the *Device Browser* in the lower, left-hand, side of the UI.

4 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

5 Select **Interface** to expand its sub menu options.

6 Select **VM Interfaces**.

The VM Interfaces screen displays.

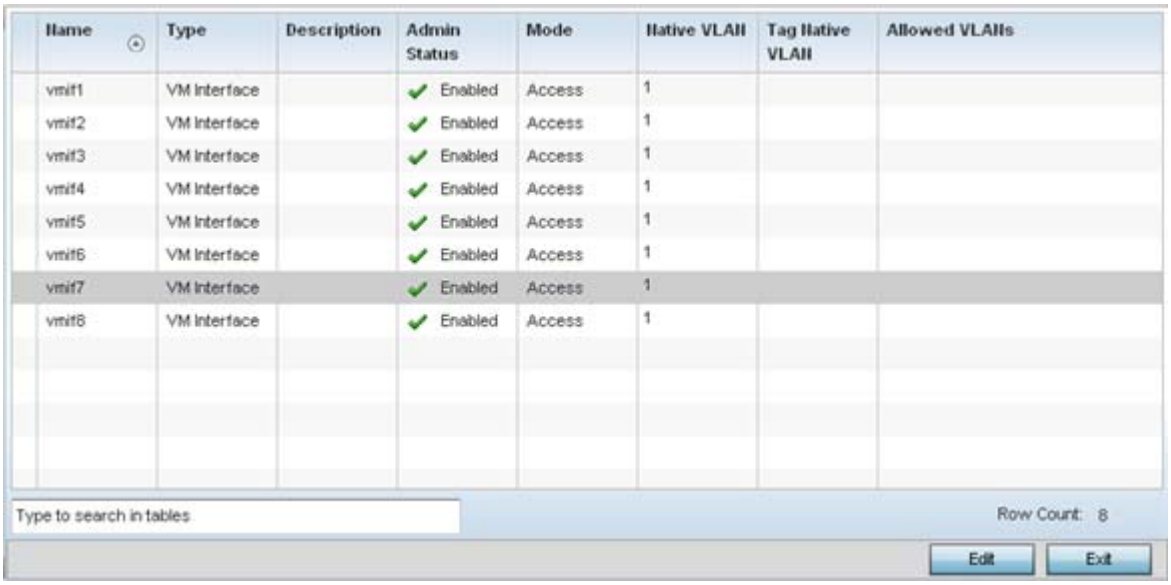


Figure 5-49 *Profile Overrides - VM Interfaces screen*

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

7 Refer to the following to review existing port channel configurations and status to determine whether a parameter requires an override:

Name	Displays the VM interface numerical identifier assigned when it was created. The numerical name cannot be modified as part of the edit process.
Type	Displays whether the type is a VM interface.
Description	Lists a short description (64 characters maximum) describing the VM interface or differentiating it from others with similar configurations.
Admin Status	A green check mark defines the listed VM interface as active and currently enabled with the profile. A red "X" defines the VM interface as currently disabled and not available for use. The interface status can be modified with the VM interface Basic Configuration screen as required.
Mode	Displays the layer 3 mode of the VM interface as either *Access* or *Trunk* (as defined within the VM Interfaces Basic Configuration screen). If Access is selected, the listed VM interface accepts packets only from the native VLAN. Frames are forwarded untagged with no 802.1Q header. All frames received on the port are expected as untagged and mapped to the native VLAN. If set to Trunk, the port allows packets from a list of VLANs added to the trunk. A VM interface configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged.
Native VLAN	Lists the numerical VLAN ID (1 - 4094) set for the native VLAN. The native VLAN allows a VM interface to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a VM interface in trunk mode.

Tag Native VLAN	A green check mark defines the native VLAN as tagged. A red "X" defines the native VLAN as untagged. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream VM interface ports know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream VM interface classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows a VM interface to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.
Allowed VLANs	Displays those VLANs allowed to send packets over the listed VM interface. Allowed VLANs are only listed when the mode has been set to Trunk.

8 To edit or override the configuration of an existing VM interface, select it from amongst those displayed and select the **Edit** button. The VM Interfaces Basic Configuration screen displays by default.

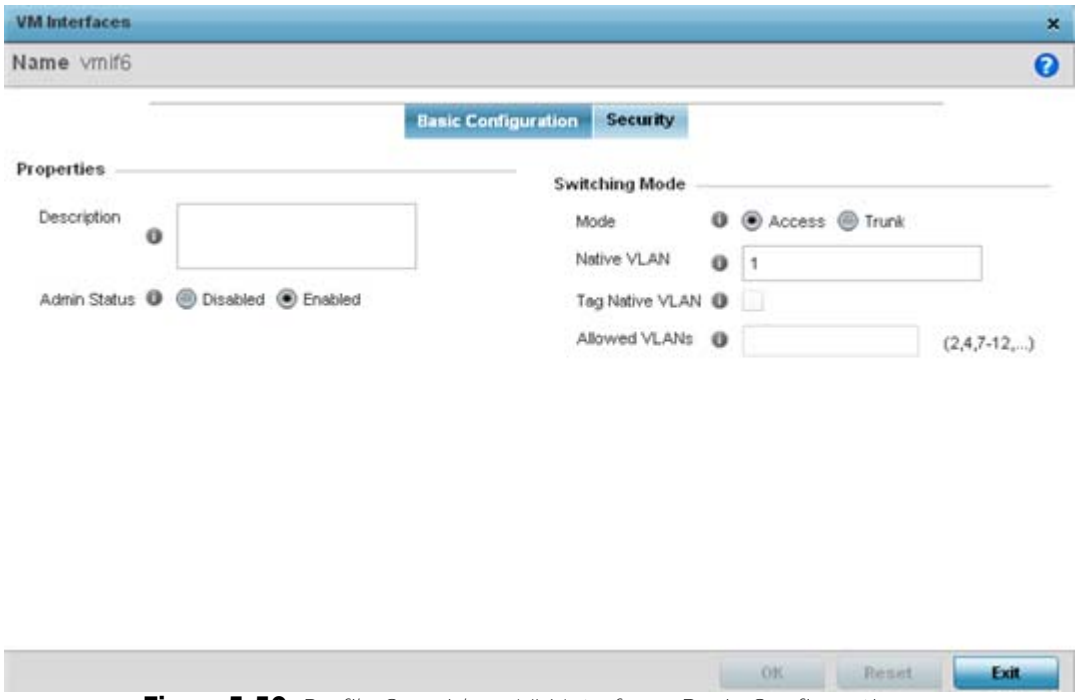


Figure 5-50 *Profile Overrides - VM Interfaces Basic Configuration screen*

9 Set or override the following VM Interface **Properties**:

Description	Enter a description for the controller or service platform VM interface (64 characters maximum).
Admin Status	Select the *Enabled* radio button to define this VM interface as active to the profile it supports. Select the *Disabled* radio button to disable this VM interface configuration in the profile. It can be activated at any future time when needed. The default setting is disabled.

10 Define or override the following **Switching Mode** parameters to apply to the VM Interface configuration:

Mode	Select either the *Access* or *Trunk* radio button to set the VLAN switching mode over the VM interface. If Access is selected, the VM interface accepts packets only from the native VLAN. Frames are forwarded untagged with no 802.1Q header. All frames received on the VMIF port are expected as untagged and are mapped to the native VLAN. If the mode is set to Trunk, the VM interface allows packets from a list of VLANs you add to the trunk. A VM interface configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. Access is the default setting.
Native VLAN	Use the spinner control to define a numerical *Native VLAN ID* from 1 - 4094. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic will be directed over when using trunk mode. The default value is 1.
Tag the Native VLAN	Select this option to tag the native VLAN. Service platforms support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream VMIF that the frame belongs. If the upstream VMIF does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between VM interface ports, both VM interfaces must support tagging and be configured to accept tagged VLANs. When a frame is tagged, a 12 bit frame VLAN ID is added to the 802.1Q header, so upstream VM interfaces know which VLAN ID the frame belongs to. The 12 bit VLAN ID is read and the frame is forwarded to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream VMIF classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows a VM interface to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This setting is disabled by default.
Allowed VLANs	Selecting *Trunk* as the mode enables the *Allowed VLANs* parameter. Add VLANs that exclusively send packets over the VM interface. The available range is from 1 - 4094. The maximum number of entries is 256.

11 Select **OK** to save the changes and overrides to the VM interface basic configuration. Select **Reset** to revert to the last saved configuration.

12 Select the **Security** tab.

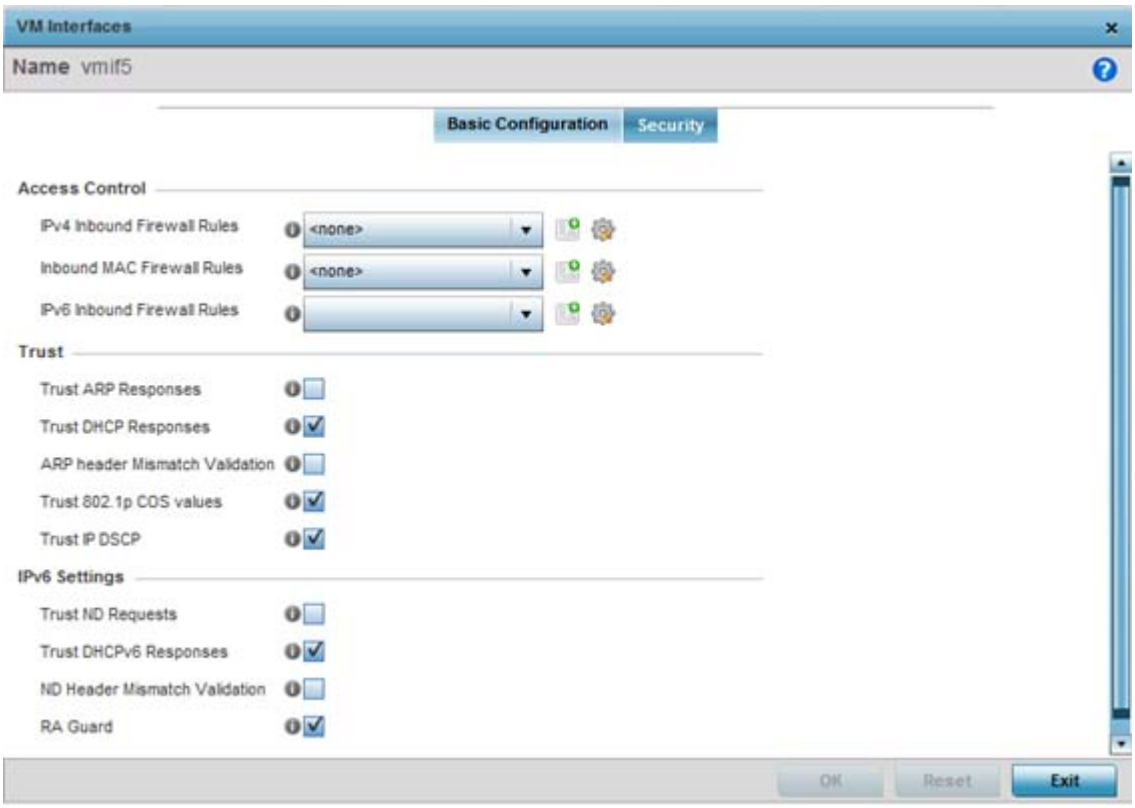


Figure 5-51 *Profile Overrides - VM Interfaces Security screen*

13 Refer to the **Access Control** field. As part of the VM interface's security configuration, IPv4 and IPv6 Inbound and MAC Inbound address firewall rules are required.

14 Use the drop-down menus to select the firewall rules to apply to this profile's VM interface configuration. The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

15 Use the **IPv4 Inbound Firewall Rules** drop down menu to select the IPv4 specific firewall rules to apply to this profile's VM interface configuration. IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity.

16 Use the **IPv6 Inbound Firewall Rules** drop down menu to select the IPv6 specific firewall rules to apply to this profile's VM interface configuration. IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

17 If a firewall rule does not exist suiting the data protection needs of the target VM interface configuration, select the **Create** icon to define a new rule configuration, or the **Edit** icon to modify an existing firewall rule configuration.

18 Refer to the **Trust** section to define or override the following:

Trust ARP Responses	Select this option to enable ARP trust on this VM interface. ARP packets received on this port are considered trusted, and information from these packets is used to identify rogue devices. The default value is disabled.
Trust DHCP Responses	Select this option to enable DHCP trust on this VM interface. If enabled, only DHCP responses are trusted and forwarded on this VM interface, and a DHCP server can be connected only to a DHCP trusted port. The default value is enabled.
ARP header Mismatch Validation	Select this option to enable a source MAC mismatch check in both the ARP and Ethernet header. The default value is enabled.
Trust 802.1p COS values	Select this option to enable 802.1p COS values on this VM interface. The default value is enabled.
Trust IP DSCP	Select this option to enable IP DSCP values on this VM interface. The default value is disabled.

19 Set the following **IPv6 Settings**:

Trust ND Requests	Select this option to enable the trust of neighbor discovery requests required on an IPv6 network on this VM interface. This setting is disabled by default.
Trust DHCPv6 Responses	Select this option to enable the trust all DHCPv6 responses on this VM interface. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. DHCPv6 relay agents receive messages from clients and forward them a DHCPv6 server. The server sends responses back to the relay agent, and the relay agent sends the responses to the client on the local link. This setting is enabled by default.
ND Header Mismatch Validation	Select this option to enable a mismatch check for the source MAC within the ND header and link layer option. This setting is disabled by default.
RA Guard	Select this option to enable router advertisements or ICMPv6 redirects from this VM interface. Router advertisements are periodically sent to hosts or sent in response to neighbor solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information. This setting is disabled by default.

20 Select **OK** to save the changes and overrides to the security configuration. Select **Reset** to revert to the last saved configuration.

5.2.7.5 Radio Override Configuration

Profile Interface Override Configuration

Access Points can have their radio profile configurations overridden once their radios have successfully associated to the network.

To define a radio configuration override from the Access Point's associated controller or service platform:

1 Select **Devices** from the Configuration tab.

The *Device Configuration* screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select an Access Point (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the *Device Browser* in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Interface** to expand its sub menu options.

5 Select **Radios**.

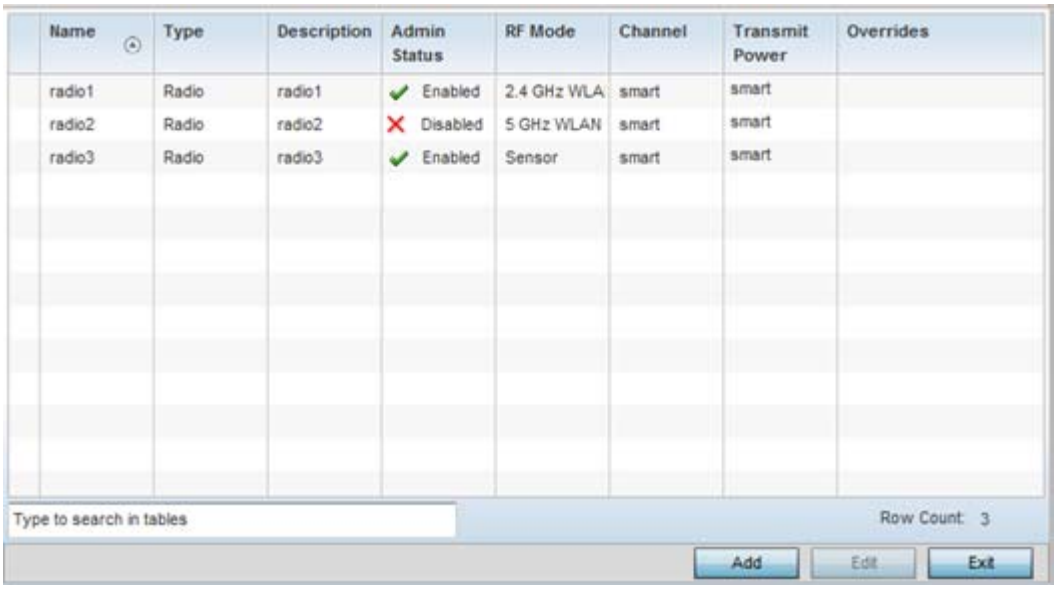


Figure 5-52 *Profile Overrides - Radios screen*

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

6 Review the following radio configuration data to determine whether a radio configuration requires modification or override to better support the managed network:

Name	Displays whether the reporting radio is the Access Point's radio1, radio2 or radio3.
Type	Displays the type of radio housed by each listed Access Point.
Description	Displays a brief description of the radio provided by the administrator when the radio's configuration was added or modified.
Admin Status	A green check mark defines the listed radio configuration as active and enabled with its supported profile. A red "X" defines the Virtual Interface as currently disabled. The interface status can be modified when a new Virtual Interface is created or an existing one modified.
RF Mode	Displays whether each listed radio is operating in the 802.11an or 802.11bgn radio band. If the radio is a dedicated sensor, it will be listed as a sensor to define the radio as not providing typical WLAN support. If the radio is a client-bridge, it provides a typical bridging function and does not provide WLAN support. The radio band is set from within the Radio Settings tab.

Channel	Lists the channel setting for the radio. Smart is the default setting. If set to smart, the Access Point scans non-overlapping channels listening for beacons from other Access Points. After the channels are scanned, it selects the channel with the fewest Access Points. In the case of multiple Access Points on the same channel, it will select the channel with the lowest average power level. The column displays smart if set for dynamic Smart RF support.
Transmit Power	Lists the transmit power for each radio displayed as a value in milliwatts. Selecting *smart* allows the radio to perform power adjustments to compensate for failed neighboring radios
Overrides	A Clear link appears for each radio configuration that has an override applied to the profile's configuration. Select *Clear* to revert this specific radio configuration to the profile configuration originally defined by the administrator for this radio.

7 If required, select a radio configuration and select **Edit** to modify or override portions of its configuration.

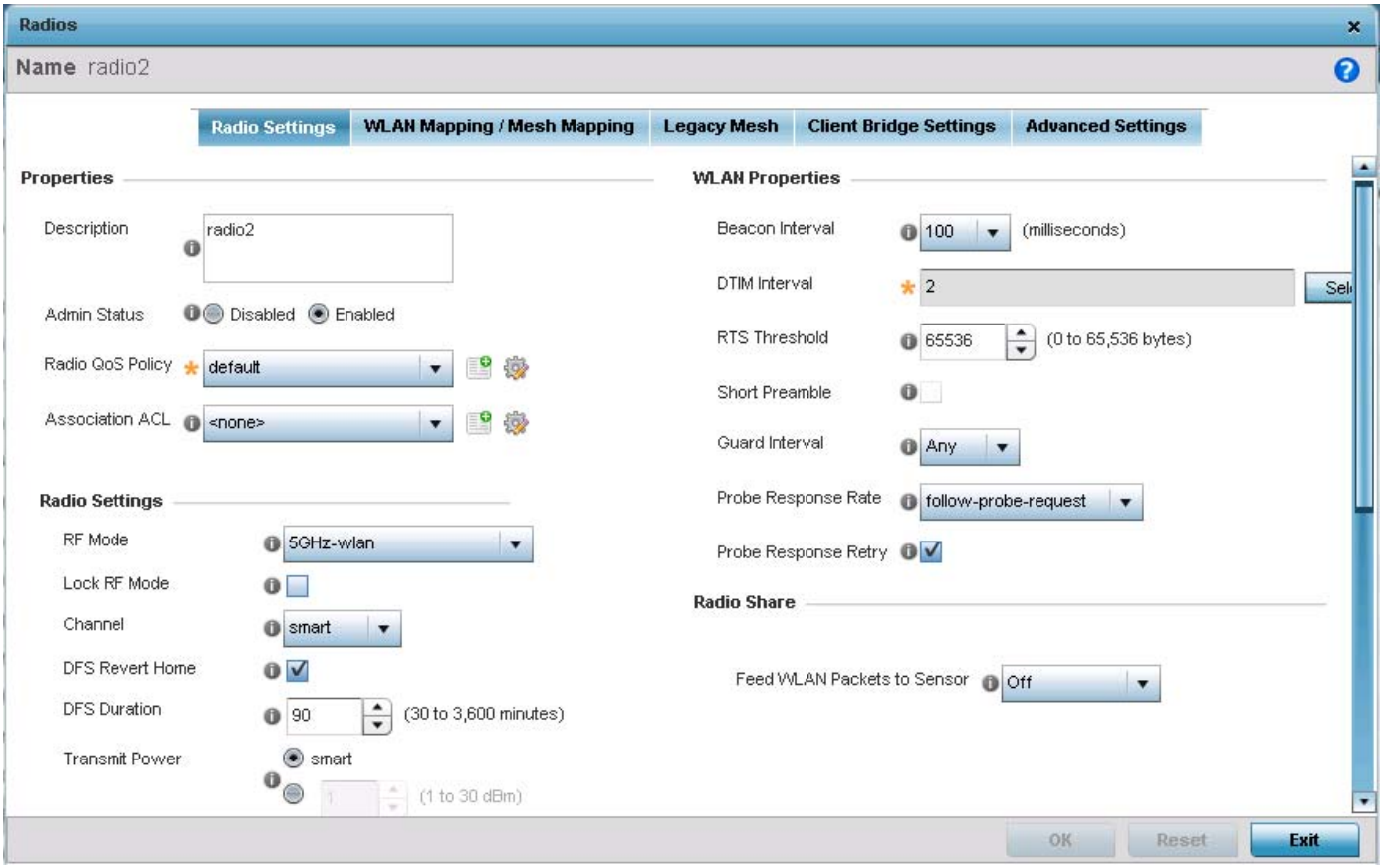


Figure 5-53 *Profile Overrides - Access Point Radio Settings tab*

The **Radio Settings** tab displays by default.

8 Define or override the following radio configuration parameters from within the **Properties** field:

Description	Provide or edit a description (1 - 64 characters in length) for the radio that helps differentiate it from others with similar configurations.
Admin Status	Either select the *Enabled* or *Disabled* radio button to define this radio's current status within the network. When enabled, the Access Point is operational and available for client support within the network. The radio is enabled by default and must be manually shutdown.
Radio QoS Policy	Use the drop-down menu to specify an existing QoS policy to apply to the Access Point radio in respect to its intended radio traffic. If there's no existing suiting the radio's intended operation, select the Create icon to define a new QoS policy that can be applied to this profile. For more information, see Radio QoS Policy on page 6-66.
Association ACL	Use the drop-down menu to specify an existing Association ACL policy to apply to the Access Point radio. An Association ACL is a policy-based *Access Control List* (ACL) that either prevents or allows wireless clients from connecting to a managed Access Point radio. An ACL is a sequential collection of permit and deny conditions that apply to controller or service platform packets. When a packet is received on an interface, the controller or service platform compares the fields in the packet against any applied ACLs to verify the packet has the required permissions to be forwarded, based on the criteria specified in the access lists. If a packet does not meet any of the criteria specified in the ACL, the packet is dropped. Select the *Create* icon to define a new Association ACL that can be applied to this profile.

9 Set or override the following profile **Radio Settings** for the selected Access Point radio.

RF Mode	Set the mode to either 2.4 GHz WLAN or 5 GHz WLAN depending on the radio's intended client support requirement. Set the mode to Sensor if using the radio for rogue device detection. To a radio as a detector, disable sensor support on the other Access Point radio. Set the mode to scan-ahead in DFS aware countries to allow a mesh points secondary radio to scan for an alternative channel for backhaul transmission in the event of a radar event on the principal radio. The secondary radio is continually monitoring the alternate channel, which means the principal radio can switch channels and transmit data immediately without waiting for the channel availability check.
Lock RF Mode	Select this option to lock Smart RF for this radio. The default setting is disabled.
Channel	Use the drop-down menu to select the channel of operation for the radio. Only a trained installation professional should define the radio channel. Select *Smart* for the radio to scan non-overlapping channels listening for beacons from other Access Points. After channels are scanned, the radio selects the channel with the fewest Access Points. In the case of multiple Access Points on the same channel, it selects the channel with the lowest average power level. The default value is Smart. Channels with a "w" appended to them are unique to the 40 MHz band. Channels with a "ww" appended to them are 802.11ac specific, only appear when using an AP8232, and are unique to the 80 MHz band.
DFS Revert Home	Select this option to revert to the home channel after a DFS evacuation period.

DFS Duration	Set the DFS duration between 30 to 3,600 minutes. This is the duration for which the radio stays in the in the new channel. The default value is 90 minutes.
Transmit Power	Set the transmit power of the selected Access Point radio. If using a dual or three radio model Access Point, each radio should be configured with a unique transmit power in respect to its intended client support function. Select the Smart RF option to let Smart RF determine the transmit power. A setting of 0 defines the radio as using Smart RF to determine its output power. 20 dBm is the default value.
Antenna Gain	Set the antenna between 0.00 - 15.00 dBm. The Access Point's *Power Management Antenna Configuration File* (PMACF) automatically configures the Access Point's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the Access Point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Only a professional installer should set the antenna gain. The default value is 0.00.
Antenna Mode	Set the number of transmit and receive antennas on the Access Point. 1x1 is used for transmissions over just the single "A" antenna, 1x3 is used for transmissions over the "A" antenna and all three antennas for receiving. 2x2 is used for transmissions and receipts over two antennas for dual antenna models. The default setting is dynamic based on the Access Point model deployed and its transmit power settings.
Enable Antenna Diversity	Select this option to enable antenna diversity on supported antennas. Antenna diversity uses two or more antennas to increase signal quality and strength. This option is disabled by default.
Adaptivity Recovery	Select this option to switch channels when an Access Point's radio is in adaptivity mode. In adaptivity mode, an Access Point monitors interference on its set channel and stops functioning when the radio's defined interference tolerance level is exceeded. When the defined adaptivity timeout is exceeded, the radio resumes functionality on a different channel. This option is enabled by default.
Adaptivity Timeout	Set the adaptivity timeout from 30 to 3,600 minutes. The default setting is 90 minutes.
Wireless Client Power	Select this option to specify the transmit power on supported wireless clients. If this is enabled set a client power level between 0 to 20 dBm. This option is disabled by default.
Dynamic Chain Selection	Select this option for the radio to dynamically change the number of transmit chains. This option is enabled by default.

Rate	Use the *Select* button to set rate options depending on the 802.11 protocols selected. If the radio band is set to Sensor or Detector, the Data Rates drop-down menu is not enabled, as the rates are fixed and not user configurable. If 2.4 GHz is selected as the radio band, select separate 802.11b, 802.11g and 802.11n rates and define how they are used in combination. If 5 GHz is selected as the radio band, select separate 802.11a and 802.11n rates then define how they are used together. When using 802.11n (in either the 2.4 or 5 GHz band), Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates). If dedicating an AP81XX model radio to either 2.4 or 5 Ghz support, a *Custom Rates* option is available to set a *modulation and coding scheme* (MCS) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates). If Basic is selected within the 802.11n Rates field, the MCS0-7 option is auto selected as a Supported rate and that option is greyed out. If Basic is not selected, any combination of MCS0-7, MCS8-15 and MCS16-23 can be supported, including a case where MCS0-7 and MCS16-23 are selected and not MCS8-15. The MCS0-7 and MCS8-15 options are available to each support Access Point. However, the MCS16-23 option is only available to AP81XX model Access Points and its ability to provide 3x3x3 MIMO support.
Radio Placement	Use the drop-down menu to specify whether the radio is located *Indoors* or *Outdoors*. The placement should depend on the country of operation selected and its regulatory domain requirements for radio emissions. The default setting is Indoors.
Max Clients	Use the spinner control to set a maximum permissible number of clients to connect with this radio. The available range is from 0 - 256 clients. The default is 256.
Rate Selection Methods	Specify a radio selection method for the radio. The selection methods are: *Standard* - Standard monotonic radio selection method will be used. *Opportunistic* - Sets opportunistic radio link adaptation as the radio selection method. This mode uses opportunistic data rate selection to provide the best throughput.

10 Set or override the following profile **WLAN Properties** for the selected Access Point radio:

Beacon Interval	Set the interval between radio beacons in milliseconds (either *50*, *100* or *200*). A beacon is a packet broadcast by adopted radios to keep the network synchronized. Included in a beacon is the WLAN service area, radio address, broadcast destination addresses, a time stamp, and indicators about traffic and delivery (such as a DTIM). Increase the DTIM/ beacon settings (lengthening the time) to let nodes sleep longer and preserve battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive. The default value is 100 milliseconds.
DTIM Interval	Set a DTIM Interval to specify a period for *Delivery Traffic Indication Messages* (DTIM). A DTIM is periodically included in a beacon frame transmitted from adopted radios. The DTIM indicates broadcast and multicast frames (buffered at the Access Point) are soon to arrive. These are simple data frames that require no acknowledgment, so nodes sometimes miss them. Increase the DTIM/ beacon settings (lengthening the time) to let nodes sleep longer and preserve their battery life. Decrease these settings (shortening the time) to support streaming multicast audio and video applications that are jitter-sensitive.
RTS Threshold	*Specify a Request To Send* (RTS) threshold (between 1 - 65,636 bytes) for use by the WLAN's adopted Access Point radios. RTS is a transmitting station's signal that requests a *Clear To Send* (CTS) response from a receiving client. This RTS/CTS procedure clears the air where clients are contending for transmission time. Benefits include fewer data collisions and better communication with nodes that are hard to find (or hidden) because of other active nodes in the transmission path. Control RTS/CTS by setting an RTS threshold. This setting initiates an RTS/CTS exchange for data frames larger than the threshold, and sends (without RTS/CTS) any data frames smaller than the threshold. Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's Access Point radios. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold. A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.
Short Preamble	If using an 802.11bg radio, select this option to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectraLink/Polycomm phones) require long preambles. The default value is disabled.

Guard Interval	Use the drop-down menu to specify a *Long* or *Any* guard interval. The guard interval is the space between characters being transmitted. The guard interval eliminates *inter-symbol interference* (ISI). ISI occurs when echoes or reflections from one character interfere with another character. Adding time between transmissions allows echo's and reflections to settle before the next character is transmitted. A shorter guard interval results in shorter character times which reduces overhead and increases data rates by up to 10%. The default value is Long.
Probe Response Rate	Use the drop-down menu to specify the data rate used for the transmission of probe responses. Options include, *highest-basic*, *lowest-basic* and *follow-probe-request* (default setting).
Probe Response Retry	Select this option to retry probe responses if they are not acknowledged by the target wireless client. The default value is enabled.

11 Select a mode from the **Feed WLAN Packets to Sensor** check box in the **Radio Share** section to enable this feature. Select either **Inline** or **Promiscuous** mode to allow the packets the radio is switching to also be used by the WIPS analysis module. This feature can be enabled in two modes: an inline mode where the WIPS sensor receives the packets from the radios with radio operating in normal mode. A promiscuous mode where the radio is configured to a mode where it receives all packets on the channel whether the destination address is the radio or not, and the WIPS module can analyze them.

12 Select the **WLAN Mapping/Mesh Mapping** tab.

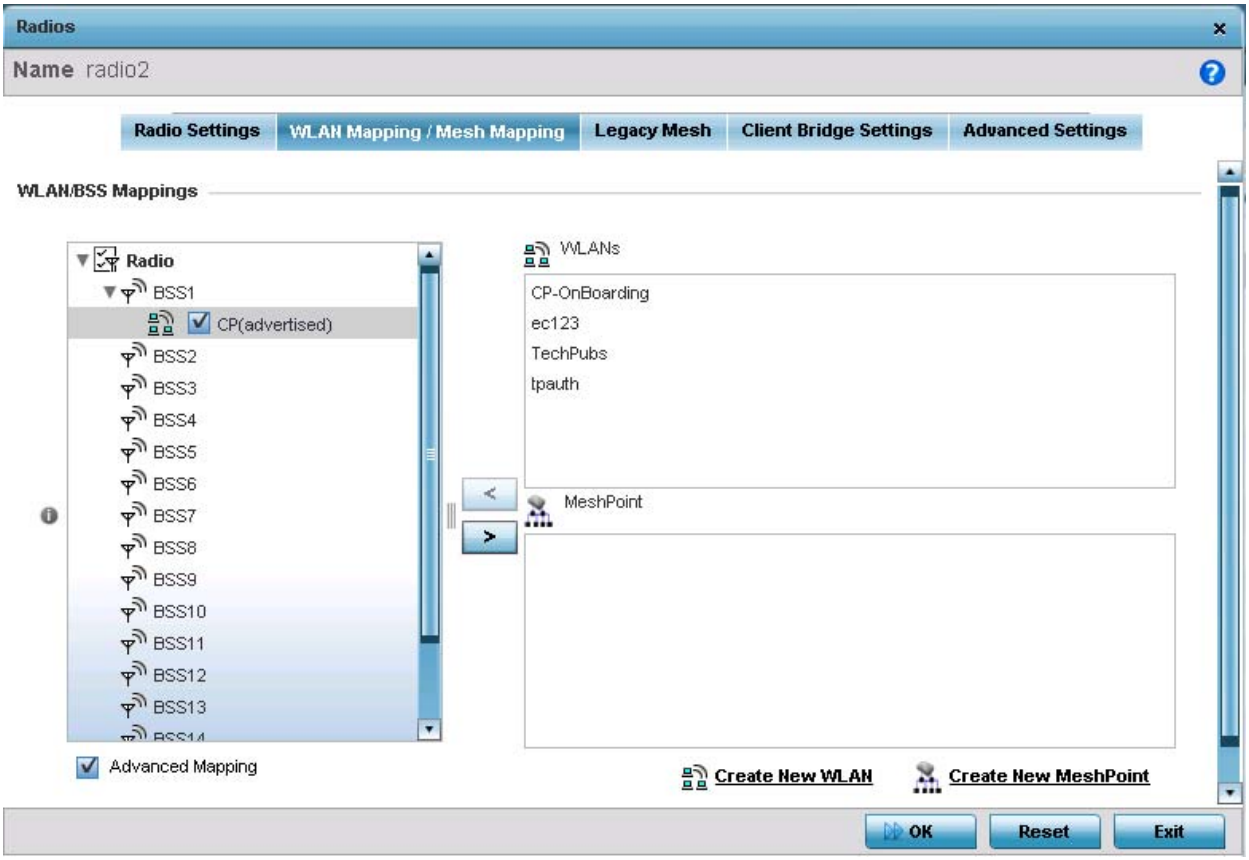


Figure 5-54 *Profile Overrides - Access Point Radio WLAN Mapping tab*

13 Refer to the **WLAN/BSS Mappings** field to set or override WLAN BSSID assignments for an existing Access Point deployment.

Administrators can assign each WLAN its own BSSID. If using a single-radio Access Point, there are 8 BSSIDs available. If using a dual-radio Access Point there are 8 BSSIDs for the 802.11b/g/n radio and 8 BSSIDs for the 802.11a/n radio.

14 Select **Advanced Mapping** to enable WLAN mapping to a specific BSS ID.

15 Select **OK** to save the changes and overrides to the WLAN Mapping. Select **Reset** to revert to the last saved configuration.

16 Select the **Legacy Mesh** tab.

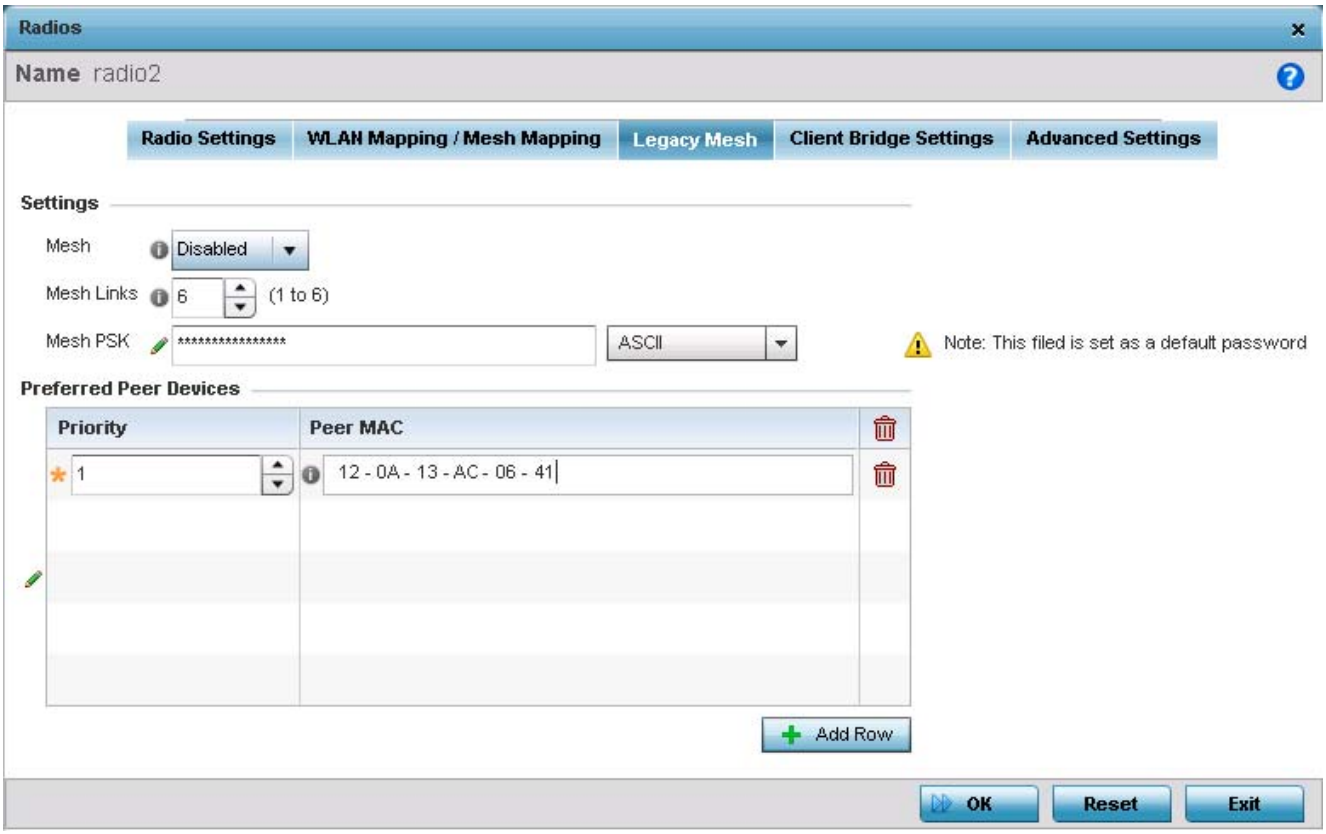


Figure 5-55 *Profile Overrides - Access Point Legacy Mesh tab*

17 Refer to the **Settings** field to define or override basic mesh settings for the Access Point radio.

Mesh	Use the drop-down to set the mesh mode for this radio. Available options include *Disabled*, *Portal* or *Client*. Setting the mesh mode to Disabled deactivates all mesh activity on this radio. Setting the mesh mode to Portal turns the radio into a mesh portal. This will start the radio beaconing immediately and will accept connections from other mesh nodes. Setting the mesh mode to client enables the radio to operate as a mesh client that scans and connects to mesh portals or nodes connected to portals.

Mesh Links	Specify the number of mesh links allowed by the radio. The radio can have from 1- 6 mesh links when the radio is configured as a Portal.
Mesh PSK	Provide the encryption key in either ASCII or Hex format. Administrators must ensure this key is configured on the Access Point when staged for mesh, added to the mesh client and to the portal Access Point's configuration on the controller or service platform. Select *Show* to expose the characters used in the PSK.

NOTE: Only single hop mesh links are supported at this time.

Refer to the **Preferred Peer Devices** table to add mesh peers. For each peer being added enter its MAC Address and a Priority from 1 - 6. The lower the priority number assigned, the higher the priority it's given when connecting to the mesh infrastructure.

18 Select the **+ Add Row** button to add preferred peer devices for the radio to connect to in mesh mode.

19 Select the **Client Bridge Settings** tab to configure the selected radio as a client-bridge. Note, before configuring the client-bridge parameters, set the radio's rf-mode to *bridge*.

An Access Point's radio can be configured to form a bridge between its wireless/wired clients and an infrastructure WLAN. The bridge radio authenticates and associates with an infrastructure WLAN Access Point. After successful association, the Access Point switches frames between its bridge radio and wired/wireless client(s) connected either to its GE port(s) or to the other radio, there by providing the clients access to the infrastructure WLAN resources. This feature is supported only on the AP6522, AP6562, AP7522, AP7532 and AP7562 model Access Points.

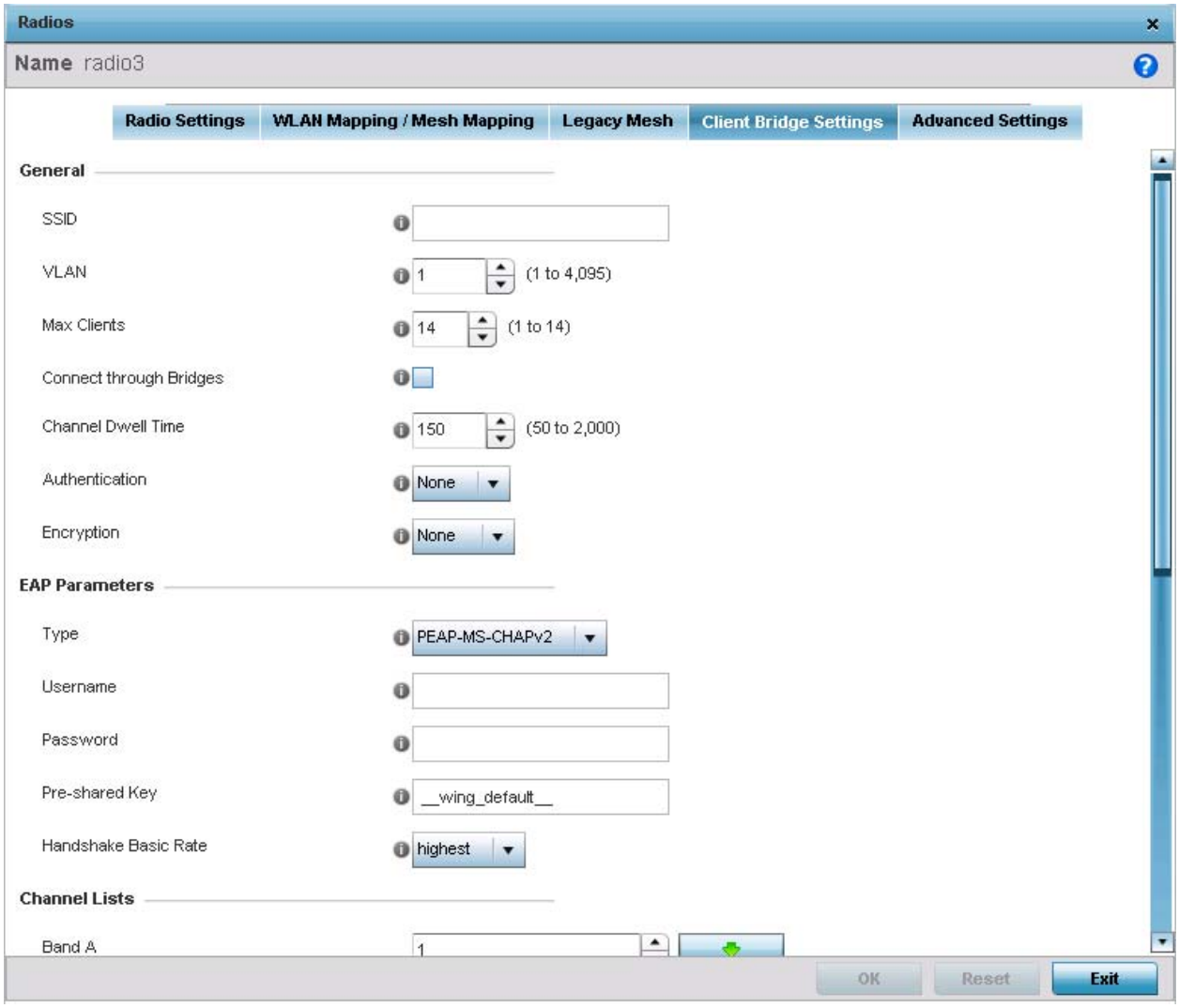


Figure 5-56 *Profile - Access Point Client Bridge Settings tab*

20 Refer to the **General** field and define the following configurations:

SSID	Set the infrastructure WLAN's SSID the client-bridge Access Point associates with.
VLAN	Set the VLAN to which the bridged clients' sessions are mapped after successful association with the infrastructure WLAN. Once mapped, the client bridge communicates with permitted hosts over the infrastructure WLAN. Specify the VLAN from 1 to 4095.
Max Clients	Set the maximum number of client-bridge Access Points that can associate with the infrastructure WLAN. Specify a value from 1 to 14. The default value is 14.
Connect through Bridges	Select this option to enable the client-bridge Access Point radio to associate with the infrastructure WLAN through another client-bridge radio thereby forming a chain. This is referred to as daisy chaining of client-bridge radios. This option is disabled by default.

Channel Dwell Time	Set the channel-dwell time from 50 to 2000 milliseconds. This is the time the client-bridge radio dwells on each channel (configured in the list of channels) when scanning for an infrastructure WLAN. The default is 150 milliseconds.
Authentication	Set the mode of authentication with the infrastructure WLAN. The authentication mode specified here should be the same as that configured on the infrastructure WLAN. The options are *None* and *EAP*. If selecting EAP, specify the EAP authentication parameters. The default setting in None. For information on WLAN authentication, see *Configuring WLAN Security*.
Encryption	Set the packet encryption mode. The encryption mode specified here should be the same as that configured on the infrastructure WLAN. The options are *None*, *CCMP* and *TKIP*. The default setting is None. For information on WLAN encryption, see *Configuring WLAN Security*.

21 Refer to the **EAP Parameters** field and define the following EAP authentication parameters:

Type	Use the drop-down menu to select the EAP authentication method used by the supplicant. The options are TLS and PEAP-MS-CHAPv2. The default EAP type is PEAP-MS-CHAPv2.
Username	Set the 32 character maximum user name for an EAP authentication credential exchange.
Password	Set the 32 character maximum password for the EAP user name specified above.
Pre-shared Key	Set the *pre-shared key* (PSK) used with EAP. Note, the authenticating algorithm and PSK configured should be same as that on the infrastructure WLAN.
Handshake Basic Rate	Set the basic rate of exchange of handshake packets between the client-bridge and infrastructure WLAN Access Points. The options are *highest* and *normal*. The default value is highest.

22 Refer to the **Channel Lists** field and define the list of channels the client-bridge radio scans when scanning for an infrastructure WLAN.

Band A	Define a list of channels for scanning across all the channels in the 5.0 GHz radio band.
Band BG	Define a list of channels for scanning across all the channels in the 2.4 GHz radio band.

23 Refer to the **Keepalive Parameters** field and define the following configurations:

Keepalive Type	Set the keepalive frame type exchanged between the client-bridge and infrastructure Access Points. This is the type of packets exchanged between the client-bridge and infrastructure Access Points, at specified intervals, to keep the client-bridge link up and active. The options are *null-data* and *WNMP* packets. The default value is null-data.

Keepalive Interval	Set the keepalive interval from 0 - 86,400 seconds. This is the interval between two successive keepalive frames exchanged between the client-bridge and infrastructure Access Points. The default value is 300 seconds.
Inactivity Timeout	Set the inactivity timeout for each bridge MAC address from 0 - 8,64,000 seconds. This is the time for which the client-bridge Access Point waits before deleting a wired/wireless client's MAC address from which a frame has not been received for more than the time specified here. For example, if the inactivity time is set at 120 seconds, and if no frames are received from a client (MAC address) for 120 seconds, it is deleted. The default value is 600 seconds.

24 Refer to the **Radio Link Behaviour** field and define the following configurations:

Shutdown Other Radio when Link Goes Down	Select this option to enable shutting down of the *non-client bridge* radio (this is the radio to which wireless-clients associate) when the link between the *client-bridge* and *infrastructure* Access Points is lost. When enabled, wireless clients associated with the non-client bridge radio are pushed to search for and associate with other Access Points having backhaul connectivity. This option is disabled by default. If enabling this option, specify the time for which the non-client bridge radio is shut down. Use the spinner to specify a time from 1 - 1,800 seconds.
Refresh VLAN Interface when Link Comes Up	Select this option to enable the SVI to refresh on re-establishing client bridge link to the infrastructure Access Point. And, if using a DHCP assigned IP address, it also causes a DHCP renew. This option is enabled by default.

25 Refer to the **Roam Criteria** field and define the following configuration:

Seconds for Missed Beacons	Set this interval from 0 to 60 seconds. This is the time for which the client-bridge Access Point waits, after missing a beacon from the associated infrastructure WLAN Access Point, before roaming to another infrastructure Access Point. For example, if the *Seconds for Missed Beacon* is set to 30 seconds, and if more than 30 seconds have passed since the last beacon received from the infrastructure Access Point, the client-bridge Access Point resumes scanning for another infrastructure Access Point. The default value s 20 seconds.
Minimum Signal Strength	Set the minimum signal-strength threshold for signals received from the infrastructure Access Point. Specify a value from -128 to -40 dBm. If the RSSI value of signals received from the infrastructure Access Point falls below the value specified here, the client-bridge Access Point resumes scanning for another infrastructure Access Point. The default is -75 dBm.

26 Select **OK** to save or override the changes to the Client Bridge Settings screen. Select **Reset** to revert to the last saved configuration.

27 Select the **Advanced Settings** tab.

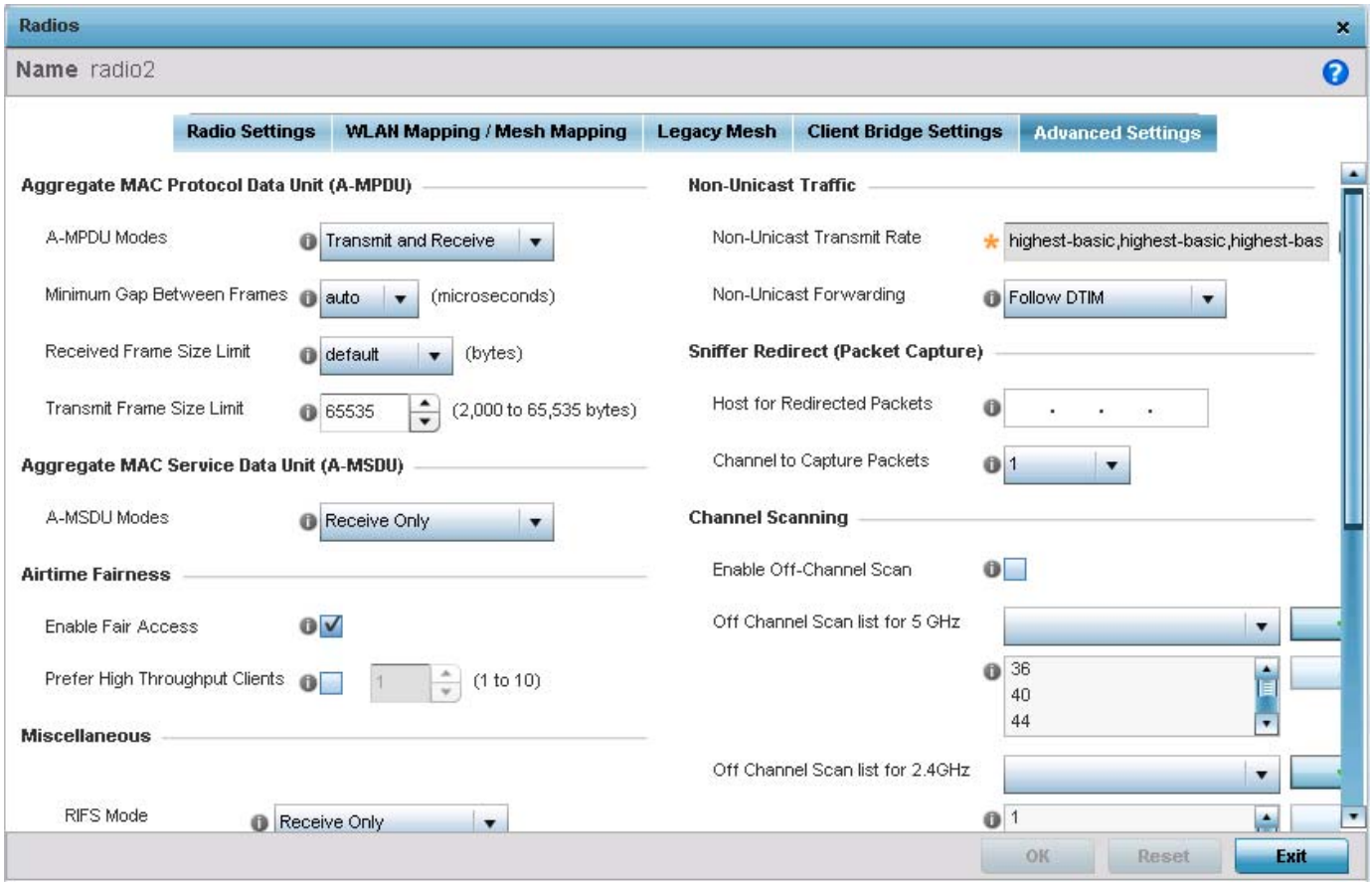


Figure 5-57 *Profile Overrides - Access Point Radio Advanced Settings tab*

28 Refer to the **Aggregate MAC Protocol Data Unit (A-MPDU)** field to define or override how MAC service frames are aggregated by the Access Point radio.

A-MPDU Modes	Use the drop-down menu to define the A-MPDU mode supported. Options include *Transmit Only*, *Receive Only*, *Transmit and Receive* and *None*. The default value is Transmit and Receive. Using the default value, long frames can be both sent and received (up to 64 KB). When enabled, define either a transmit or receive limit (or both).
Minimum Gap Between Frames	Use the drop-down menu to define the minimum gap between A-MPDU frames (in microseconds). The default value is 4 microseconds. A value of *auto* designates the gap is set by the system.
Received Frame Size Limit	If a support mode is enabled allowing A-MPDU frames to be received, define an advertised maximum limit for received A-MPDU aggregated frames. Options include 8191, 16383, 32767 or 65535 bytes. The default value is 65535 bytes.
Transmit Frame Size Limit	Use the spinner control to set a limit on transmitted A-MPDU aggregated frames. The available range is from 2,000 - 65,535 bytes. The default value is 65535 bytes.

29 Use the **A-MSDU Modes** drop-down menu in the **Aggregate MAC Service Data Unit (A-MSDU)** section to set or override the supported A-MSDU mode.

Available modes include *Receive Only* and *Transmit and Receive*. Transmit and Receive is the default value. Using Transmit and Receive, frames up to 4 KB can be sent and received. The buffer limit is not configurable.

30 Use the **Airtime Fairness** fields to optionally prioritize wireless access to devices.

Select **Enable Fair Access** to enable this feature and provide equal access client access to radio resources. Select **Prefer High Throughput Clients** to prioritize clients with higher throughput (802.11n clients) over clients with slower throughput (802.11 a/b/g) clients. Use the spinner control to set a weight for the higher throughput clients.

31 Set or override the following **Miscellaneous** advanced radio settings:

RIFS Mode	Define a RIFS mode to determine whether interframe spacing is applied to Access Point transmissions or received packets, both, or neither The default mode is *Transmit and Receive*. Interframe spacing is an interval between two consecutive Ethernet frames to enable a brief recovery between packets and allow target devices to prepare for the reception of the next packet. Consider setting this value to *None* for high priority traffic to reduce packet delay.
STBC Mode	Select a *space–time block coding* (STBC) option to transmit multiple data stream copies across Access Point antennas to improve signal reliability. An Access Point's transmitted signal traverses a problematic environment, with scattering, reflection and refraction all prevalent. The signal can be further corrupted by noise at the receiver. Consequently, some of the received data copies are less corrupt and better than others. This redundancy means there's a greater chance of using one, or more, of the received copies to successfully decode the signal. STBC effectively combines all the signal copies to extract as much information from each as possible.
Transmit Beamforming	Enable beamforming to steer signals to peers in a specific direction to enhance signal strength and improve throughput amongst meshed devices (not clients). Each Access Point radio support up to 16 beamforming capable mesh peers. When enabled, a *beamformer* steers its wireless signals to its peers. A *beamformee* device assists the beamformer with channel estimation by providing a *feedback* matrix. The feedback matrix is a set of values sent by the beamformee to assist the beamformer in computing a *steering* matrix. A steering matrix is an additional set of values used to steer wireless signals at the beamformer so constructive signals arrive at the beamformee for better SNR and throughput. Any beamforming capable mesh peer connecting to a radio whose capacity is exhausted cannot enable beamforming itself. Transmit beamforming is available on AP81XX (AP8122, AP8132 and AP8163) model Access Points only, and is disabled by default.

32 Set or override the following **Aeroscout Properties**:

Forward	Select enable to forward Aeroscout packets to a specified MAC address. Aeroscout tags associate with an Access Point, then communicate with a location engine. This setting is disabled by default.
MAC to be forwarded	Specify the MAC address to be forwarded.

33 Set or override the following **Ekahau Properties**:

Forward Host	Specify the Ekahau engine IP address. Using Ekahau small, battery powered Wi-Fi tags are attached to tracked assets or carried by people. Ekahau processes locations, rules, messages and environmental data and turns the information into locationing maps, alerts and reports.

Forwarding Port	Use the spinner control to set the Ekahau TZSP port used for processing information from locationing tags.
MAC to be forwarded	Specify the MAC address to be forwarded with location data requests.

34 Set or override the following **Non-Unicast Traffic** values for the profile's supported Access Point radio and its connected wireless clients:

Non-Unicast Transmit Rate	Use the *Select* drop-down menu to launch a sub screen to define the data rate for broadcast and multicast frame transmissions. Seven different rates are available if the not using the same rate for each BSSID, each with a separate menu.
Non-Unicast Forwarding	Define whether client broadcast and multicast packets should always follow DTIM, or only follow DTIM when using Power Save Aware mode. The default setting is Follow DTIM.

35 Refer to the **Sniffer Redirect (Packet Capture)** field to define or override the radio's captured packet configuration.

Host for Redirected Packets	If packets are re-directed from a controller or service platform's connected Access Point radio, define an IP address of a resource (additional host system) used to capture the re- directed packets. This address is the numerical (non DNS) address of the host used to capture the re-directed packets.
Channel to Capture Packets	Use the drop-down menu to specify the channel used to capture re-directed packets. The default value is channel 1.

36 Refer to the **Channel Scanning** field to define or override the radio's captured packet configuration.

Enable Off-Channel Scan	Enable this option to scan across all channels using this radio. Channel scans use Access Point resources and can be time consuming, so only enable when your sure the radio can afford the bandwidth be directed towards to the channel scan and does not negatively impact client support.
Off Channel Scan list for 5GHz	Define a list of channels for off channel scans using the 5GHz Access Point radio. Restricting off channel scans to specific channels frees bandwidth otherwise utilized for scanning across all the channels in the 5GHz radio band.
Off Channel Scan list for 2.4GHz	Define a list of channels for off channel scans using the 2.4GHz Access Point radio. Restricting off channel scans to specific channels frees bandwidth otherwise utilized for scanning across all the channels in the 2.4GHz radio band.
Max Multicast	Set the maximum number (from 0 - 100) of multicast/broadcast messages used to perform off channel scanning. The default setting is four.
Scan Interval	Set the interval (from 2 - 100 dtims) off channel scans occur. The default setting is 20dtims.
Sniffer Redirect	Specify the IP address of the host to which captured off channel scan packets are redirected.

37 If an AP7161 or AP7181 is deployed, refer to the following **AP7161/AP7181** specific values to set outdoor antenna characteristics:

Enable Antenna Downlift	Enable this settings (on AP7181 models only) to allow the Access Point to physically transmit in a downward orientation (ADEPT mode).
Extended Range	Set an extended range (from 1 - 25 kilometers) to allow AP7161 and AP7181 model Access Points to transmit and receive with their clients at greater distances without being timed out.

38 Select **OK** to save or override the changes to the Advanced Settings screen. Select **Reset** to revert to the last saved configuration.

5.2.7.6 WAN Backhaul Override Configuration

Profile Interface Override Configuration

A *Wireless Wide Area Network* (WWAN) card is a specialized network interface card that allows a device to connect, transmit and receive data over a Cellular Wide Area Network. The RFS4000 and RFS6000 each have a PCI Express card slot that supports 3G WWAN cards. The WWAN card uses *point to point protocol* (PPP) to connect to the *Internet Service Provider* (ISP) and gain access to the Internet. PPP is the protocol used for establishing internet links over dial-up modems, DSL connections, and many other types of point-to-point communications. PPP packages your system's TCP/IP packets and forwards them to the serial device where they can be put on the network. PPP is a full-duplex protocol that can be used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of *High Speed Data Link Control* (HDLC) for packet encapsulation.

NX4500 and NX6500 services platforms support an optional NX Expansion module for modular WAN and Telephony Gateway support. The NX Series Expansion Module kit (KT-NXMODC-01) allows for the installation and implementation of up to four Peripheral Component Interconnect Express (PCIe) cards. The Expansion Module kit can be installed in NX4500, NX4524, NX6500 or NX6524 model services platforms.

To define a WAN Backhaul configuration override:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target Access Point (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Interface** to expand its sub menu options.

5 Select **WAN Backhaul**.

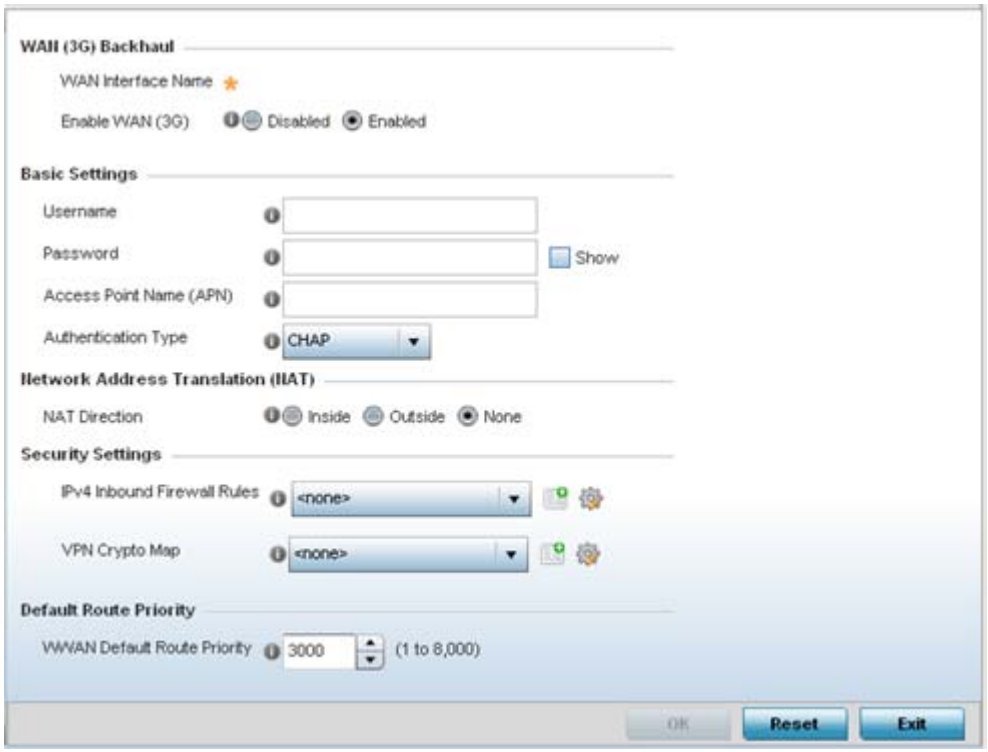


Figure 5-58 *Profile Overrides -WAN Backhaul screen*

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

6 Refer to the **WAN (3G) Backhaul** configuration to specify WAN card settings:

WAN Interface Name	Displays the WAN Interface name for the WAN 3G Backhaul card.
Reset WAN Card	If the WAN Card becomes unresponsive or is experiencing other errors click the *Reset WAN Card* button to power cycle and reboot the WAN card.
Enable WAN (3G)	Check this box to enable 3G WAN card support on the device. A supported 3G card must be connected to the device for this feature to work properly.

7 Define or override the following authentication parameters from within the **Basic Settings** field:

Username	Provide a username for authentication support by the cellular data carrier.
Password	Provide a password for authentication support by the cellular data carrier.
Access Point **Name (APN)**	Enter the name of the cellular data provider if necessary. This setting is needed in areas with multiple cellular data providers using the same protocols, such as Europe and Asia.
Authentication Type	Use the drop-down menu to specify the authentication type used by the cellular data provider. Supported authentication types are *None*, *PAP*, *CHAP*, *MSCHAP*, and *MSCHAP-v2*.

8 Define or override the following NAT parameters from within the **Network Address Translation (NAT)** field:

NAT Direction	Define the *Network Address Translation* (NAT) direction. Options include: *Inside* - The inside network is transmitting data over the network its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address. *Outside* - Packets passing through the NAT on the way back to the controller or service platform managed LAN are searched against to the records kept by the NAT engine. There, the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the network. *None* - No NAT activity takes place. This is the default setting.

9 Define or override the following security parameters from within the **Security Settings** field:

IPv4 Inbound Firewall Rules	Use the drop-down menu to select an inbound IPv4 ACL to associate with traffic on the WAN backhaul. This setting pertains to IPv4 inbound traffic only and not IPv6. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity. If an appropriate IP ACL does not exist, select the *Add* button to create a new one.
VPN Crypto Map	If necessary, specify a crypto map for the wireless WAN. A crypto map can be up to 256 characters long. If a suitable crypto map is not available, click the *Create* button to configure a new one.

Define or override the following route parameters from within the **Default Route Priority** field:

WWAN Default Route Priority	Use the spinner control to define a priority from 1 - 8,000 for the default route learned by the wireless WAN. The default value is 3000.

10 Select **OK** to save or override the changes to the Advanced Settings screen. Select **Reset** to revert to the last saved configuration.

5.2.7.7 PPPoE Override Configuration

Profile Interface Override Configuration

PPP over Ethernet (PPPoE) is a data-link protocol for dialup connections. PPPoE allows the Access Point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers support (or deploy) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables controllers, service platforms and Access Points to establish a point-to-point connection to an ISP over existing Ethernet interface.

To provide this point-to-point connection, each PPPoE session learns the Ethernet address of a remote PPPoE client, and establishes a session. PPPoE uses both a discover and session phase to identify a client and establish a point-to-point connection. By using such a connection, a Wireless WAN fail over is available to maintain seamless network access if the Access Point's Wired WAN were to fail.

NOTE: Devices with PPPoE enabled continue to support VPN, NAT, PBR and 3G fail over on the PPPoE interface. Multiple PPPoE sessions are supported using a single user account user account if RADIUS is configured to allow simultaneous access.

When PPPoE client operation is enabled, it discovers an available server and establishes a PPPoE link for traffic slow. When a wired WAN connection failure is detected, traffic flows through the WWAN interface in fail-over mode (if the WWAN network is configured and available). When the PPPoE link becomes accessible again, traffic is redirected back through the Access Point's wired WAN link.

When the Access Point initiates a PPPoE session, it first performs a discovery to identify the Ethernet MAC address of the PPPoE client and establish a PPPoE session ID. In discovery, the PPPoE client discovers a server to host the PPPoE connection.

To create a PPPoE point-to-point configuration:

1 Select **Devices** from the Configuration tab.

  The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target Access Point (by double-clicking it) from amongst those displayed within the Device Configuration screen.

  Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Interface** to expand its sub menu options.

5 Select **PPPoE**.

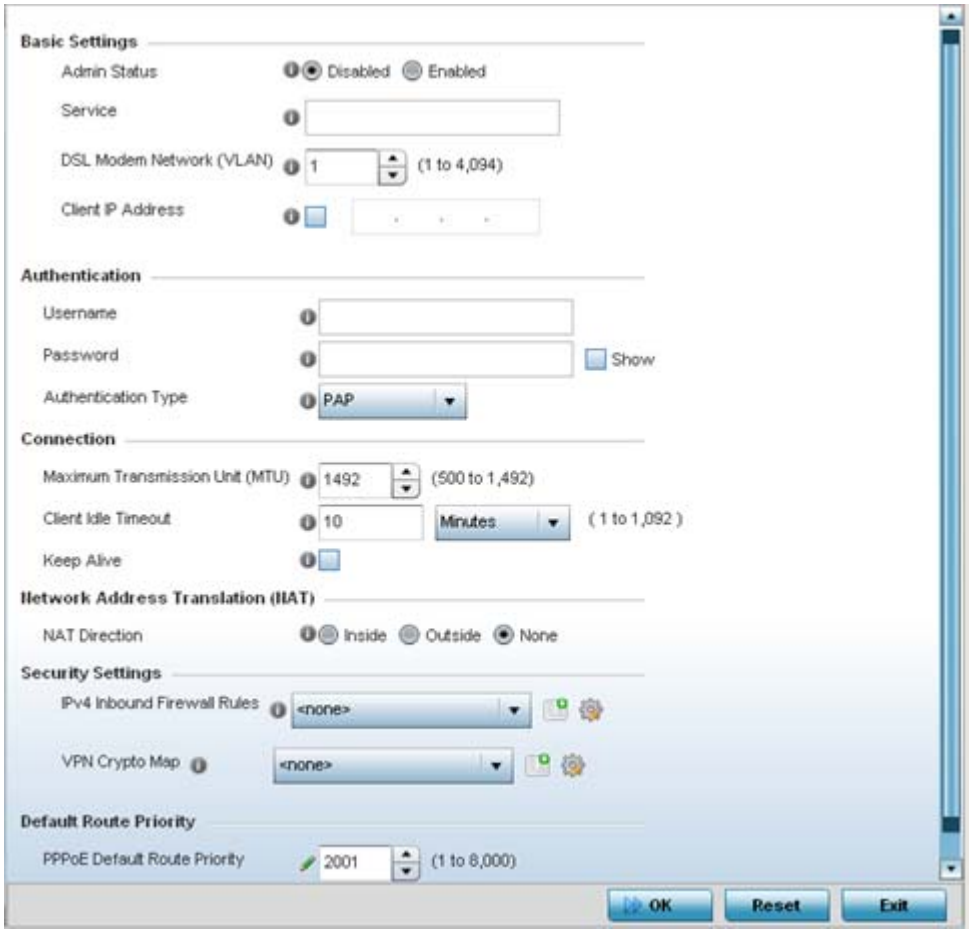


Figure 5-59 *Profile Overrides -PPPoE screen*

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

6 Use the **Basic Settings** field to enable PPPoE and define a PPPoE client

Admin Status	Select *Enable* to support a high speed client mode point-to-point connection using the PPPoE protocol. The default setting is disabled.
Service	Enter the 128 character maximum PPPoE client service name provided by the service provider.
DSL Modem Network (VLAN)	Use the spinner control to set the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to DSL modem. The available range is 1 - 4,094. The default VLAN is VLAN1.
Client IP Address	Provide the numerical (non hostname) IP address of the PPPoE client.

7 Define the following **Authentication** parameters for PPPoE client interoperation:

Username	Provide the 64 character maximum username used for authentication support by the PPPoE client.

Password	Provide the 64 character maximum password used for authentication by the PPPoE client.
Authentication Type	Use the drop-down menu to specify the authentication type used by the PPPoE client, and whose credentials must be shared by its peer Access Point. Supported authentication options include *None, PAP, CHAP, MSCHAP*, and *MSCHAP-v2*.

8 Define the following **Connection** settings for the PPPoE point-to-point connection with the PPPoE client:

Maximum Transmission Unit (MTU)	Set the PPPoE client *maximum transmission unit* (MTU) from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492.
Client Idle Timeout	Set a timeout in either *Seconds* (1 - 65,535), *Minutes* (1 - 1,092) or *Hours*. The Access Point uses the defined timeout so it does not sit idle waiting for input from the PPPoE client and server that may never come. The default setting is 10 minutes.
Keep Alive	Select this option to ensure the point-to-point connect to the PPPoE client is continuously maintained and not timed out. This setting is disabled by default.

9 Set the **Network Address Translation (NAT)** direction for the PPPoE configuration.

Network Address Translation (NAT) converts an IP address in one network to a different IP address or set of IP addresses in another network. The Access Point router maps its local (*Inside*) network addresses to WAN (*Outside*) IP addresses, and translates the WAN IP addresses on incoming packets to local IP addresses. NAT is useful because it allows the authentication of incoming and outgoing requests, and minimizes the number of WAN IP addresses needed when a range of local IP addresses is mapped to each WAN IP address. The default setting is None (neither inside or outside).

10 Define the following **Security Settings** for the PPPoE configuration:

IPV4 Inbound Firewall Rules	Use the drop-down menu to select a firewall (set of IPv4 formatted access connection rules) to apply to the PPPoE client connection. If a firewall rule does not exist suiting the data protection needs of the PPPoE client connection, select the Create icon to define a new rule configuration or the Edit icon to modify an existing rule. For more information, see Configuring IP Firewall Rules on page 10-20.
VPN Crypto Map	Use the drop-down menu to apply an existing crypt map configuration to this PPPoE interface.

11 Use the spinner control to set the **Default Route Priority** for the default route obtained using PPPoE.

Select from 1 - 8,000. The default setting is 2,000.

12 Select **OK** to save the changes to the PPPoE screen. Select **Reset** to revert to the last saved configuration. Saved configurations are persistent across reloads.

5.2.7.8 Bluetooth Configuration

Profile Interface Override Configuration

AP-8432 and AP-8533 model Access Points utilize a built in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network. AP-8432 and AP-8533 models support both Bluetooth *classic* and Bluetooth *low energy* technology. These platforms can use their Bluetooth classic enabled radio to sense other Bluetooth enabled devices and report device data (MAC address, RSSI and device calls) to an ADSP server for intrusion detection. If the device presence varies in an unexpected manner, ADSP can raise an alarm.

NOTE: AP-8132 model Access Points support an external USB Bluetooth radio providing ADSP Bluetooth classic sensing functionality only, not the Bluetooth low energy beaconing functionality available for AP-8432 and AP-8533 model Access Points described in this section.

AP-8432 and AP-8533 model Access Points support Bluetooth beaconing to emit either iBeacon or Eddystone-URL beacons. The Access Point's Bluetooth radio sends non-connectable, undirected *low-energy* (LE) advertisement packets on a periodic basis. These advertisement packets are short, and sent on Bluetooth advertising channels that conform to already-established iBeacon and Eddystone-URL standards. Portions of the advertising packet are still customizable however.

To define a Bluetooth radio interface configuration:

1 Select **Devices** from the Configuration tab.

2 The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

3 Select a target Access Point (by double-clicking it) from amongst those displayed within the Device Configuration screen.

4 Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

5 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

6 Select **Interface** to expand its sub menu options.

7 Select **Bluetooth**.

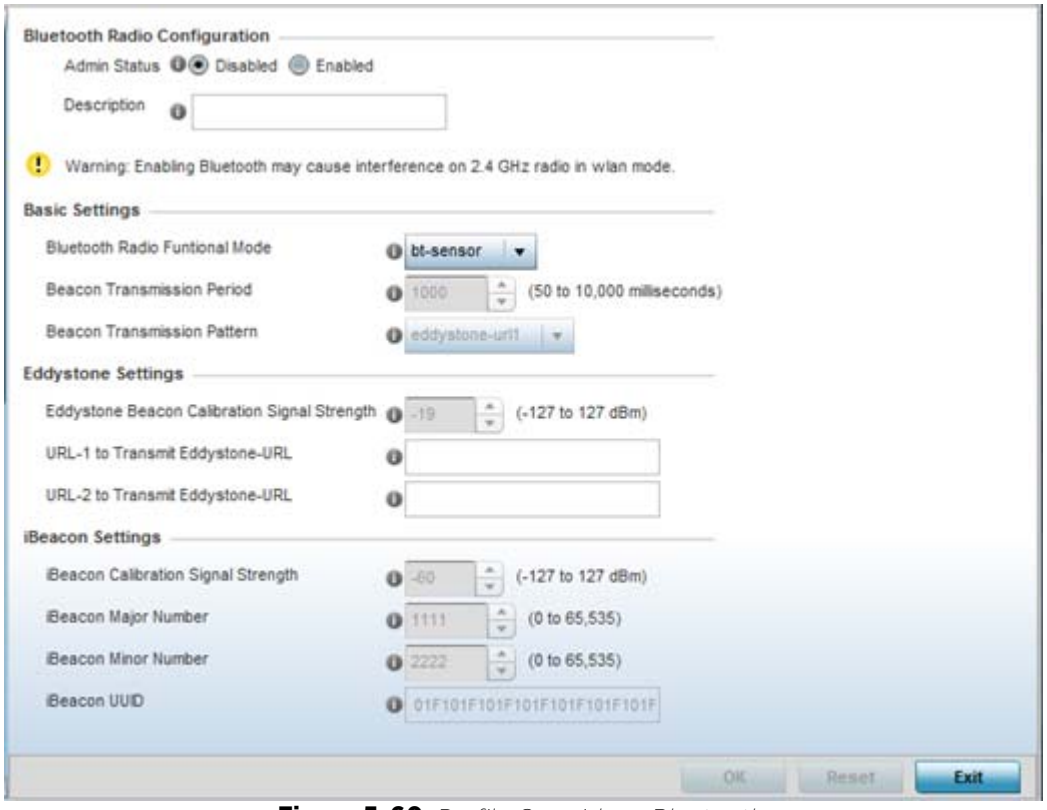


Figure 5-60 *Profile Overrides - Bluetooth screen*

8 Set the following **Bluetooth Radio Configuration** parameters:

Admin Status	*Enable* or *Disable* Bluetooth support capabilities for AP-8432 or AP-8533 model Access Point Bluetooth radio transmissions. The default value is disabled.
Description	Define a 64 character maximum description for the Access Point's Bluetooth radio to differentiate this radio interface from other Bluetooth supported radio's that may be members of the same RF Domain.

9 Set the following **Basic Settings**:

Bluetooth Radio Functional Mode	Set the Access Point's Bluetooth radio functional mode to either *bt-sensor* or *le-beacon*. Use bt-sensor mode for ADSP Bluetooth classic sensing. Use le-beacon mode to have the Access Point transmit both ibeacon and Eddystone-URL low energy beacons. le-beacon is the default setting.
Beacon Transmission Period	Set the Bluetooth radio's beacon transmission period from 100 - 10,000 milliseconds. The default setting is 1,000 milliseconds.

Beacon Transmission Pattern	When the Bluetooth radio's mode is set to le-beacon, use the enabled drop-down menu to set the beacon's emitted transmission pattern to either *eddystone_url1*, *eddystone_url2* or *ibeacon*. An eddystone-URL frame broadcasts a URL using a compressed encoding scheme to better fit within a limited advertisement packet. Once decoded, the URL can be used by a client for Internet access. iBeacon was created by Apple for use in iOS devices (beginning with iOS version 7.0). There are three data fields Apple has made available to iOS applications, a *UUID* for device identification, a *Major* value for device class and a *Minor* value for more refined information like product category.

10 Define the following Eddystone_Settings if the Beacon Transmission Pattern has been set to either eddystone_url_1 or eddystone_url_2:

Eddystone Beacon Calibration Signal Strength	Set the eddystone beacon measured calibration signal strength, from -127 to 127 dBm, at 0 meters. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 0 meters. The default setting is -19 dBm.
URL-1 to Transmit Eddystone-URL	Enter a 64 character maximum eddystone-URL1. The URL must be 18 characters or less once auto-encoding is applied. The encoding process is for getting the URL to fit within the beacon's payload.
URL-2 to Transmit Eddystone-URL	Enter a 64 character maximum eddystone-URL2. The URL must be 18 characters or less once auto-encoding is applied. The encoding process is for getting the URL to fit within the beacon's payload.

11 Define the following **iBeacon_Settings** if the Beacon Transmission Pattern has been set to iBeacon:

iBeacon Calibration Signal Strength	Set the ibeacon measured calibration signal strength, from -127 to 127 dBm, at 1 meter. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 1 meter. The default setting is -60 dBm.
iBeacon Major Number	Set the iBeacon Major value from 0 - 65,535. Major values identify and distinguish groups. For example, each beacon on a specific floor in a building could be assigned a unique major value. The default is 1,111.
iBeacon Minor Number	Set the iBeacon Minor value from 0 - 65,535. Minor values identify and distinguish individual beacons. Minor values help identify individual beacons within a group of beacons assigned a major value. The default setting is 2,222.
iBeacon UUID	Define a 32 hex character maximum UUID. The *Universally Unique IDentifier* (UUID) classification contains 32 hexadecimal digits. The UUID distinguishes iBeacons in the network from all other beacons in networks outside of your direct administration.

12 Select **OK** to save the changes to the Bluetooth configuration. Select **Reset** to revert to the last saved configuration. Saved configurations are persistent across reloads.

5.2.8 Overriding a Profile's Network Configuration

Profile Overrides

Setting a profile's network configuration is a large task comprised of numerous administration activities. Each of the activities described below can have an override applied to the original profile configuration. Applying an override removes the device from the profile configuration that may be shared by other devices and requires careful administration to ensure this one device still supports the deployment requirements within the managed network.

A profile's network configuration process consists of the following:

- *Overriding a Profile's DNS Configuration*
- *Overriding a Profile's ARP Configuration*
- *Overriding a Profile's L2TPV3 Configuration*
- *Overriding a Profile's GRE Configuration*
- *Overriding a Profile's IGMP Snooping Configuration*
- *Overriding a Profile's MLD Snooping Configuration*
- *Overriding a Profile's Quality of Service (QoS) Configuration*
- *Overriding a Profile's Spanning Tree Configuration*
- *Overriding a Profile's Routing Configuration*
- *Overriding a Profile's Dynamic Routing (OSPF) Configuration*
- *Overriding a Profile's Border Gateway Protocol (BGP) Configuration*
- *Overriding a Profile's Forwarding Database Configuration*
- *Overriding a Profile's Bridge VLAN Configuration*
- *Overriding a Profile's Cisco Discovery Protocol Configuration*
- *Overriding a Profile's Link Layer Discovery Protocol Configuration*
- *Overriding a Profile's Miscellaneous Network Configuration*
- *Overriding a Profile's Network Alias Configuration*
- *Overriding a Profile's IPv6 Neighbor Configuration*

5.2.8.1 Overriding a Profile's DNS Configuration

Overriding a Profile's Network Configuration

Domain Naming System (DNS) DNS is a hierarchical naming system for resources connected to the Internet or a private network. Primarily, the controller or service platform's DNS resources translate domain names into IP addresses. If a DNS server doesn't know how to translate a particular domain name, it asks another one until the correct IP address is returned. DNS enables access to resources using human friendly notations. DNS converts human friendly domain names into notations used by networking equipment for locating resources.

As a resource is accessed (using human-friendly hostnames), it's possible to access the resource even if the underlying machine friendly notation name changes. Without DNS you need to remember a series of numbers (123.123.123.123) instead of a domain name (*www.domainname.com*).

Controllers and service platforms maintain their own DNS facility that can assist in domain name translation. A DNS assignment can be overridden as needed, but removes the device configuration from the managed profile that may be shared with other similar device models.

To define the DNS configuration or apply overrides to an existing configuration:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **DNS**.

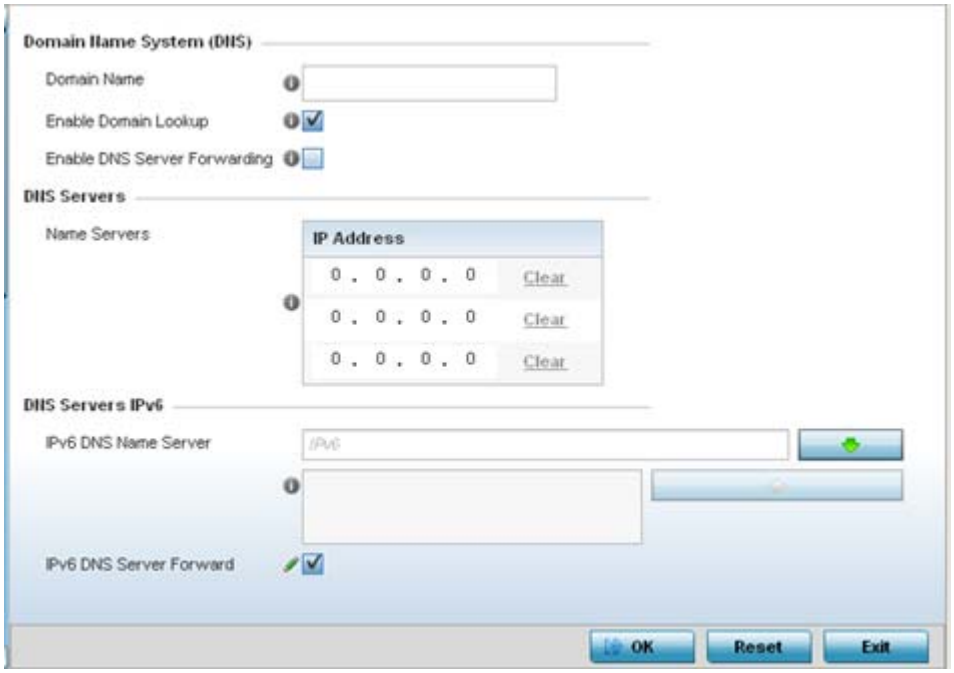


Figure 5-61 *Profile Overrides - Network DNS screen*

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

6 Set or override the following **Domain Name System (DNS)** configuration data:

Domain Name	Provide or override the default Domain Name used to resolve DNS names. The name cannot exceed 64 characters.
Enable Domain Lookup	Select this option to enable DNS on the controller or service platform. When enabled, the controller or service platform can convert human friendly domain names into numerical IP destination addresses. This option is selected by default.
Enable DNS Server Forwarding	Click to enable the forwarding of DNS queries to external DNS servers if a DNS query cannot be processed by the controller or service platform's own DNS resources. This feature is disabled by default.

7 Set or override the following **DNS Server** configuration data:

Name Servers	Provide a list of up to three DNS servers to forward DNS queries if the controller or service platform's DNS resources are unavailable. DNS name servers are used to resolve IP addresses. Use the *Clear* link next to each DNS server to clear the DNS name server's IP address from the list.

8 Set the following **DNS Servers IPv6** configuration data when using IPv6:

IPv6 DNS Name Server	Provide the default domain name used to resolve IPv6 DNS names. When an IPv6 host is configured with the address of a DNS server, the host sends DNS name queries to the server for resolution. A maximum of three entries are permitted.
IPv6 DNS Server Forward	Select the check box to enable IPv6 DNS domain names to be converted into numerical IP destination addresses. The setting is disabled by default.

9 Select **OK** to save the changes and overrides made to the DNS configuration. Select **Reset** to revert to the last saved configuration.

5.2.8.2 Overriding a Profile's ARP Configuration

Overriding a Profile's Network Configuration

Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a hardware MAC address recognized on the managed network. ARP provides rules for making this correlation and providing address conversion in both directions. ARP assignment s can be overridden as needed, but an override removes the device configuration from the managed profile that may be shared with other similar device models.

When an incoming packet destined for a host arrives at the controller or service platform, the gateway uses ARP to find a physical host or MAC address that matches the IP address. ARP looks in its ARP cache and, if it finds the address, provides it so the packet can be converted to the right packet length and format and sent to the destination. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

To define an ARP supported configuration on a controller or service platform:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **ARP.**

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

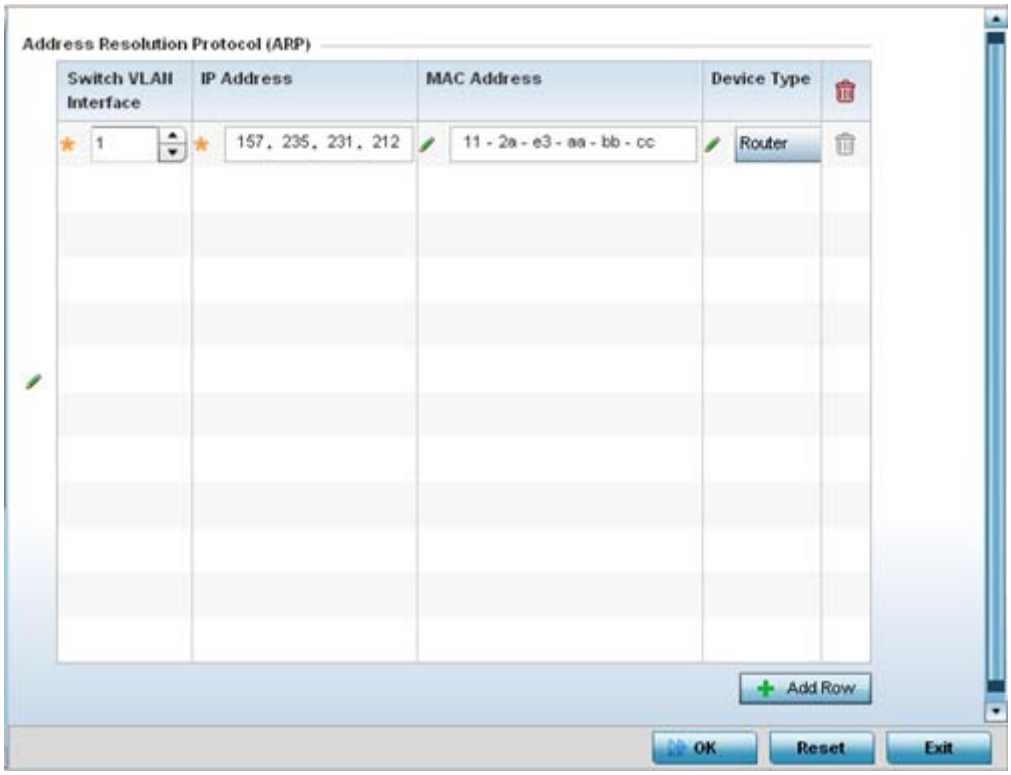


Figure 5-62 *Profile Overrides - Network ARP screen*

6 Set or override the following parameters to define the controller or service platform's ARP configuration:

Switch VLAN Interface	Use the spinner control to select a VLAN interface (1 - 4094) for an address requiring resolution.
IP Address	Define the IP address used to fetch a MAC address.
MAC Address	Displays the target MAC address that's subject to resolution. This is the MAC used for mapping an IP address to a MAC address that's recognized on the network.
Device Type	Specify the device type the ARP entry supports. Host is the default setting.

7 To add additional ARP overrides click on the **+ Add Row** button and enter the configuration information in the table above.

8 Select the **OK** button to save the changes and overrides to the ARP configuration. Select **Reset** to revert to the last saved configuration.

5.2.8.3 Overriding a Profile's L2TPV3 Configuration

Overriding a Profile's Network Configuration

L2TP V3 is a standard used for transporting different types of layer 2 frames in an IP network (and Access Point profile). L2TP V3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes.

Use L2TP V3 to create tunnels for transporting layer 2 frames. L2TP V3 enables controllers, service platforms and Access Points to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TP V3 tunnels can be defined between WING devices and other vendor devices supporting the L2TP V3 protocol.

Multiple pseudowires can be created within an L2TP V3 tunnel. WING supported Access Points support an Ethernet VLAN pseudowire type exclusively.

NOTE: A pseudowire is an emulation of a layer 2 point-to-point connection over a *packet-switching network* (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TP V3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TP V3 sessions. Each tunnel session corresponds to one pseudowire. An L2TP V3 control connection (a L2TP V3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TP V3 session originator and responder need to know the psuedowire type and identifier. These two parameters are communicated during L2TP V3 session establishment. An L2TP V3 session created within an L2TP V3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.

The working status of a pseudowire is reflected by the state of the L2TP V3 session. If a L2TP V3 session is down, the pseudowire associated with it must be shut down. The L2TP V3 control connection keep-alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.

NOTE: If connecting an Ethernet port to another Ethernet port, the pseudowire type must be *Ethernet port*, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be *Ethernet VLAN*.

To define an L2TPV3 configuration for an Access Point profile:

1 Select **Devices** from the Configuration tab.

  The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

  Devices can also be selected directly from the *Device Browser* in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Expand the **Network** menu and select **L2TPv3**.

5 The **General** tab displays by default with additional **L2RPv3 Tunnel** and **Manual Session** tabs available.

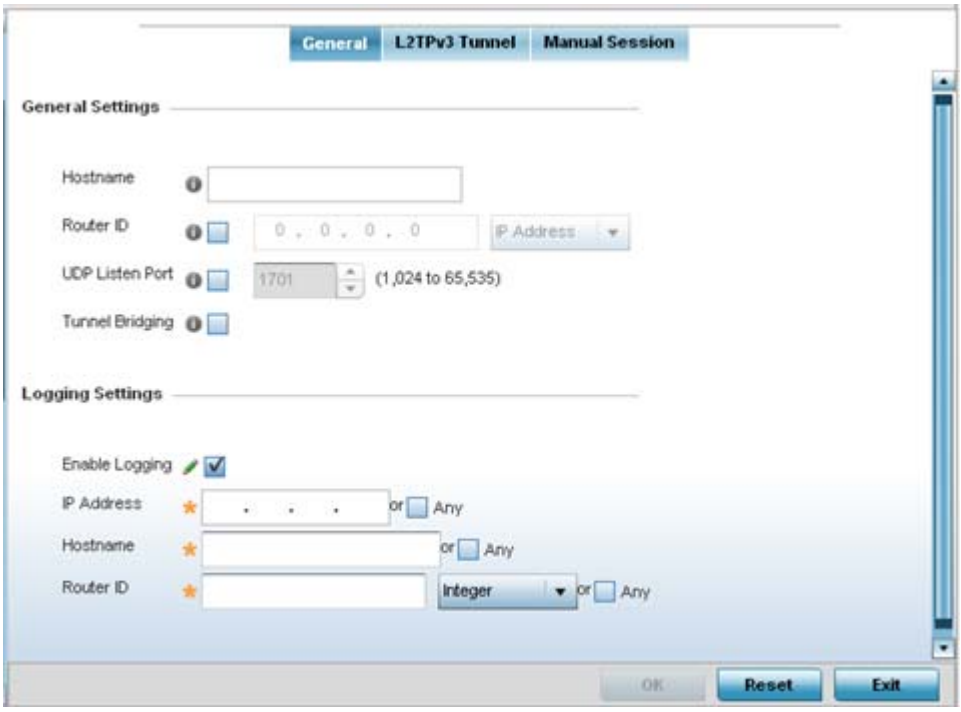


Figure 5-63 *Network - L2TPv3 screen, General tab*

6 Set the following **General Settings** for an L2TPv3 profile configuration:

Hostname	Define a 64 character maximum host name to specify the name of the host that's sent tunnel messages. Tunnel establishment involves exchanging 3 message types (SCCRQ, SCCRP and SCCN) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host.
Router ID	Set either the numeric IP address or the integer used as an identifier for tunnel AVP messages. AVP messages assist in the identification of a tunnelled peer.
UDP Listen Port	Select this option to set the port used for listening to incoming traffic. Select a port from 1,024 - 65,535.
Tunnel Bridging	Select this option to *enable* or *disable* bridge packets between two tunnel end points. This setting is disabled by default.

7 Set the following **Logging Settings** for a L2TPv3 profile configuration:

Enable Logging	Select this option to enable the logging of Ethernet frame events to and from bridge VLANs and physical ports on a defined IP address, host or router ID. This setting is disabled by default.
IP Address	Optionally use a peer tunnel ID address to capture and log L2TPv3 events. Use *Any* to log any IP address.
Hostname	If not using an IP address for event logging, optionally use a peer tunnel hostname to capture and log L2TPv3 events. Use *Any* to log any hostname. Hostnames cannot include an underscore character.

Router ID	If not using an IP address or a hostname for event logging, use a router ID to capture and log L2TPv3 events. Use *Any* to log any router ID.

8 Select the **L2TPV3 Tunnel** tab.

Figure 5-64 *Network - L2TPv3 screen, T2TP tunnel tab*

9 Review the following L2TPv3 tunnel configuration data:

Name	Displays the name of each listed L2TPv3 tunnel assigned upon creation.
Local IP Address	Lists the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address.
MTU	Displays the *maximum transmission unit* (MTU) size for each listed tunnel. The MTU is the size (in bytes) of the largest protocol data unit that the layer can pass between tunnel peers.
Use Tunnel Policy	Lists the L2TPv3 tunnel policy assigned to each listed tunnel.
Local Hostname	Lists the tunnel specific hostname used by each listed tunnel. This is the host name advertised in tunnel establishment messages.
Local Router ID	Specifies the router ID sent in tunnel establishment messages.
Establishment Criteria	Specifies the criteria required for a tunnel between two peers.

Critical Resource	Specifies the critical resource that should exist for a tunnel between two peers. Critical resources are device IP addresses or interface destinations interopreted as critical to the health of the network. Critical resources allow for the continuous monitoring of these defined addresses. A critical resource, if not available, can result in the network suffering performance degradation. A critical resource can be a gateway, AAA server, WAN interface or any hardware or service on which the stability of the network depends. Critical resources are pinged regularly. If there's a connectivity issue, an event is generated stating a critical resource is unavailable.
Peer IP Address	Specifies the IP address of the tunnel destination peer device.
Hostname	Specifies the administrator assigned hostname of the tunnel.

10 Either select **Add** to create a new L2TPv3 tunnel configuration, **Edit** to modify an existing tunnel configuration or **Delete** to remove a tunnel from those available to this profile.

11 If creating a new tunnel configuration, assign it a 31 character maximum **Name**.

12 Select **+ Add Row** to populate the table with configurable session parameters for this tunnel configuration.

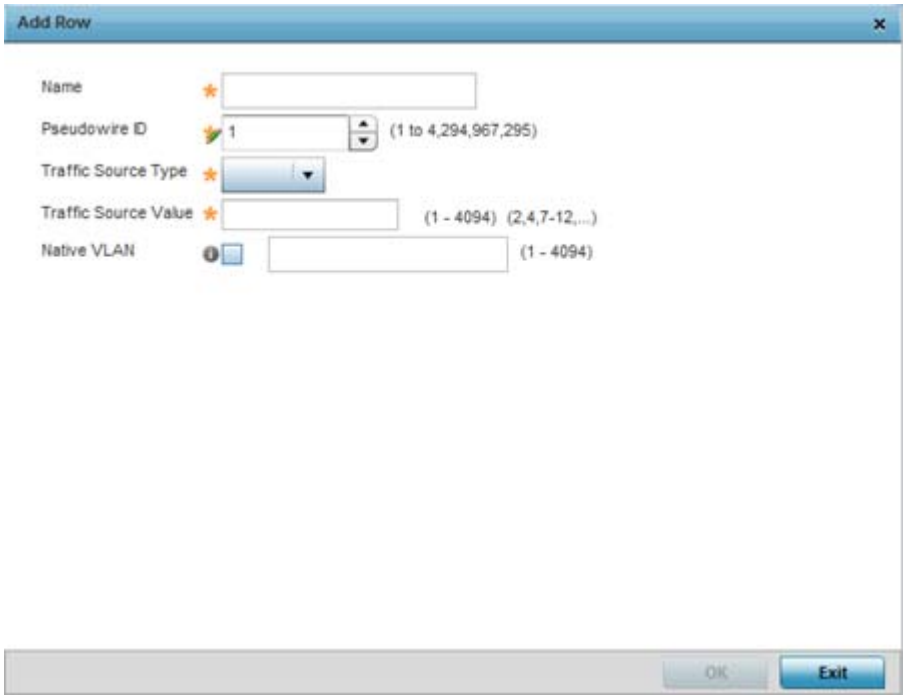


Figure 5-65 *Network - L2TPv3 screen, Add L2TPv3 Tunnel Configuration*

13 Define the following **Session** parameters required for the L2TPv3 tunnel configuration:

Name	Enter a 31 character maximum session name. There is no idle timeout for a tunnel. A tunnel is not usable without a session and a subsequent session name.The tunnel is closed when the last session tunnel session is closed.
Pseudowire ID	Define a psuedowire ID for this session. A pseudowire is an emulation of a layer 2 point-to-point connection over a *packet-switching network* (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.
Traffic Source Type	Lists the type of traffic tunnelled in this session (VLAN etc).

Traffic Source Value	Define a VLAN range to include in the tunnel session.
Native VLAN	Select this option to provide a VLAN ID that will not be tagged in tunnel establishment and packet transfer. Available VLAN ranges are from 1 - 4,094.

14 Select **OK** to save the updates to **Exit** to revert to the last configuration.

15 Select the **Settings** tab.

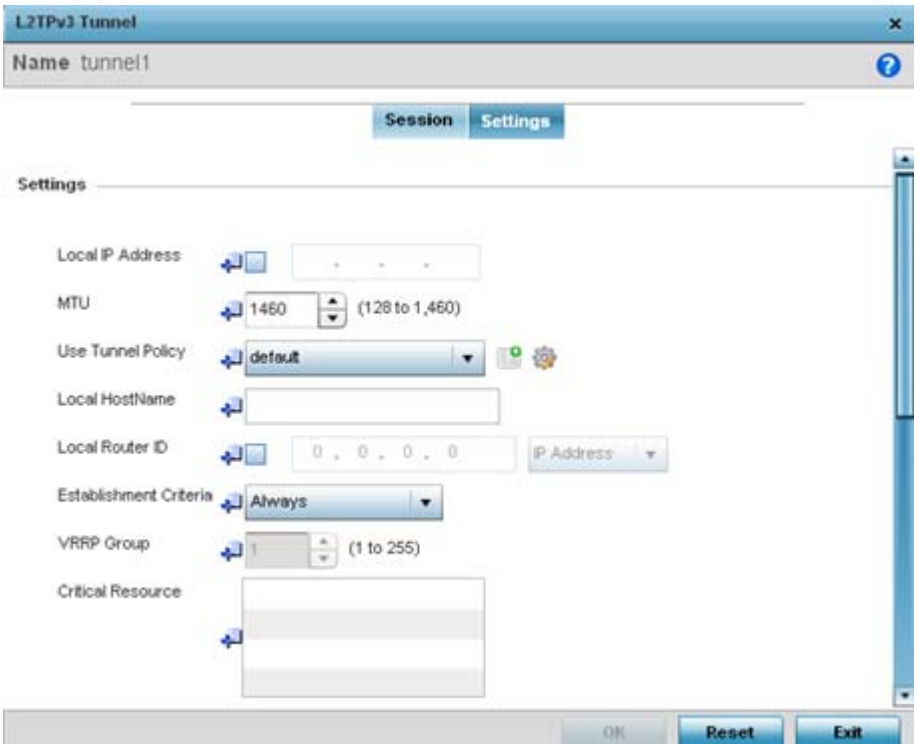


Figure 5-66 *Network - L2TPv3 screen, Settings*

16 Define the following **Settings** required for the L2TPv3 tunnel configuration:

Local IP Address	Enter the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address. This parameter is applicable when establishing the tunnel and responding to incoming tunnel create requests.
MTU	Set the *maximum transmission unit* (MTU). The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers. Define a MTU from 128 - 1,460 bytes. The default setting is 1,460. A larger MTU means processing fewer packets for the same amount of data.
Use Tunnel Policy	Select the L2TPv3 tunnel policy. The policy consists of user defined values for protocol specific parameters which can be used with different tunnels. If none is available, a new policy can be created or an existing one can be modified.
Local Hostname	Provide the tunnel specific hostname used by this tunnel. This is the host name advertised in tunnel establishment messages. Hostnames cannot include an underscore character.

Local Router ID	Specify the router ID sent in tunnel establishment messages with a target peer device.
Establishment Criteria	Specify the establishment criteria for creating a tunnel. The tunnel is only created if this device is one of the following: *vrrp-master* *cluster-master* *rf-domain-manager* The tunnel is always created if *Always* is selected. This indicates the device need not be any one of the above three (3) to establish a tunnel.
VRRP Group	Set the VRRP group ID. VRRP groups is only enabled when the Establishment Criteria is set to vrrp-master.
Critical Resource	The Critical Resources table lists important resources defined for this system. The tunnel is created and maintained only if these critical resources are available. The tunnel is removed if any one of the defined resources goes down or is unreachable.

17 Define the following **Rate Limit** settings for the L2TP tunnel configuration. Rate limiting manages the maximum rate sent to or received from L2TPv3 tunnel members.

Session Name	Use the drop-down menu to select the tunnel session that will have the direction, burst size and traffic rate settings applied.
Direction	Select the direction for L2TPv3 tunnel traffic rate limiting. *Egress* traffic is outbound L2TPv3 tunnel data coming to the controller, service platform or Access Point. *Ingress* traffic is inbound L2TPv3 tunnel data coming to the controller, service platform or Access Point.
Maximum Burst Size	Set the maximum burst size for egress or ingress traffic rate limiting (depending on which direction is selected) on a L2TPv3 tunnel. Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the upstream packet transmission will result in congestion for L2TPv3 tunnel traffic. The default setting is 320 bytes.
Rate	Set the data rate (from 50 - 1,000,000 kbps) for egress or ingress traffic rate limiting (depending on which direction is selected) for an L2TPv3 tunnel. The default setting is 5000 kbps.

18 Refer to the **Peer** table to review the configurations of the peers destinations for tunnel connection.

19 Select **+ Add Row** to populate the table with a maximum of two peer configurations.

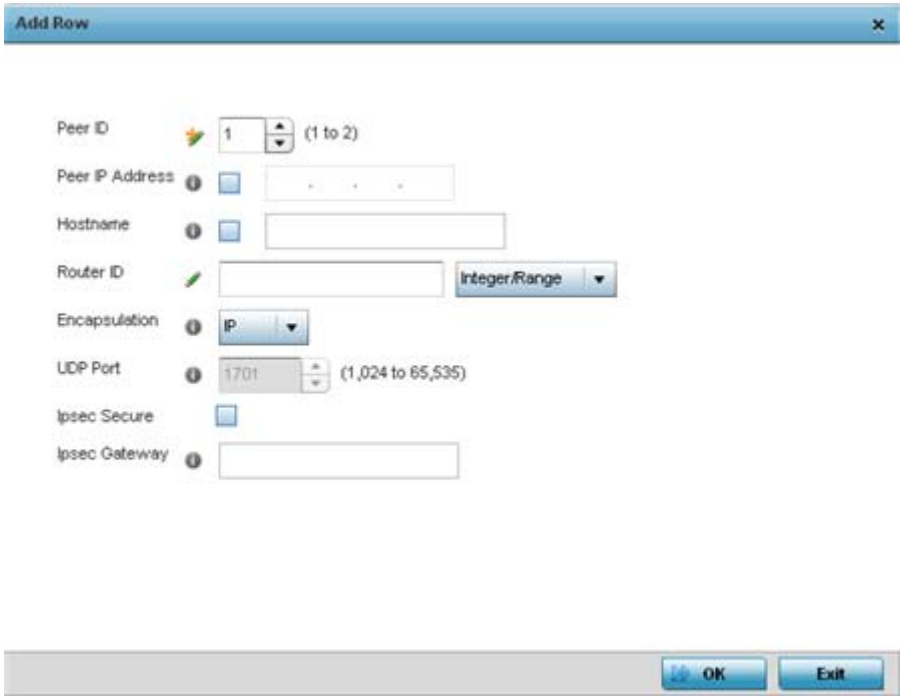


Figure 5-67 *Network - L2TPv3 screen, Add Peer Configuration*

20 Define the following **Peer** parameters:

Peer ID	Define the primary peer ID used to set the primary and secondary peer for tunnel fail over. If the peer is not specified, tunnel establishment does not occur. However, if a peer tries to establish a tunnel with this Access Point, it creates the tunnel if the hostname and/or Router ID matches.
Peer IP Address	Select this option to enter the numeric IP address used as the destination peer address for tunnel establishment.
Hostname	Assign the peer a hostname that can be used as matching criteria in the tunnel establishment process. Hostnames cannot include an underscore character.
Router ID	Specify the router ID sent in tunnel establishment messages with this specific peer.
Encapsulation	Select either *IP* or *UDP* as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes.
IPSec Secure	Enable this option to enable security on the connection between the Access Point and Virtual Controller.
IPSec Gateway	Specify the IP Address of the IPSec Secure Gateway.
UDP Port	If UDP encapsulation is selected, use the spinner control to define the UDP encapsulation port.

21 From back at the **Settings** tab, set the following **Fast Failover** parameters.

Enable	When enabled, the device starts sending tunnel requests on both peers, and in turn, establishes the tunnel on both peers. If disabled, tunnel establishment only occurs on one peer, with failover and other functionality the same as legacy behavior. If fast failover is enabled after establishing a single tunnel the establishment is restarted with two peers. One tunnels defined as active and the other standby. Both tunnels perform connection health checkups with individual hello intervals. This setting is disabled by default.
Enable Aggressive Mode	When enabled, tunnel initiation hello requests are set to zero. For failure detections, hello attempts are not retried, regardless of defined retry attempts. This setting is disabled by default.

22 Select **OK** to save the peer configuration.

23 Select **OK** to save the changes within the T2TP Tunnel screen. Select **Reset** to revert the screen to its last saved configuration.

24 Select the **Manual Session** tab.

Individual sessions can be created after a successful tunnel connection and establishment. Each session is a single data stream. After successful session establishment, data corresponding to that session (pseudowire) can be transferred. If a session is down, the pseudowire associated with it is shut down as well.

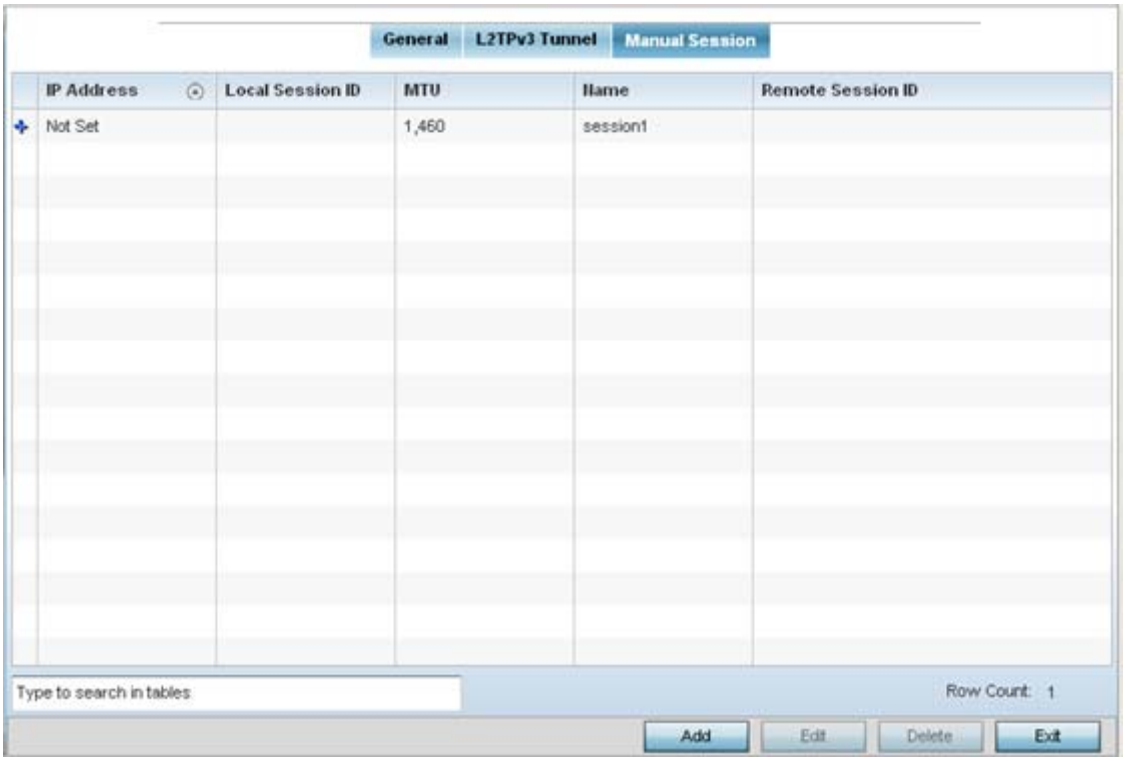


Figure 5-68 *Network - L2TPv3 screen, Manual Session tab*

25 Refer to the following manual session configurations to determine whether one should be created or modified:

IP Address	Lists the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address. This parameter is applicable when establishing the session and responding to incoming requests.
Local Session ID	Displays the numeric identifier assigned to each listed tunnel session. This is the pseudowire ID for the session. This pseudowire ID is sent in a session establishment message to the L2TP peer.
MTU	Displays each sessions's *maximum transmission unit* (MTU). The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data.
Name	Lists the name assigned to each listed manual session.
Remote Session ID	Lists the remote session ID passed in the establishment of the tunnel, used a a unique identifier for this tunnel session.

26 Select **Add** to create a new manual session, **Edit** to modify an existing session configuration or **Delete** to remove a selected manual session.

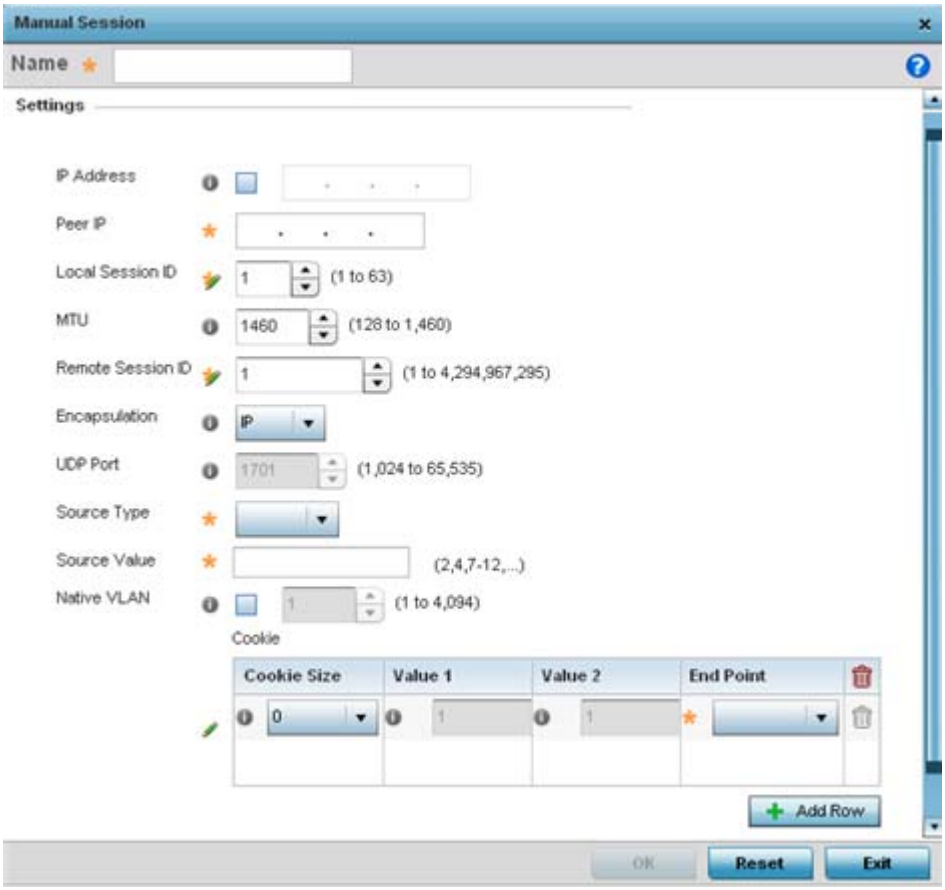


Figure 5-69 *Network - L2TPv3 screen, Add T2TP Peer Configuration*

27 Set the following session parameters:

Name	Define a 31 character maximum name of this tunnel session. After a successful tunnel connection and establishment, the session is created. Each session name represents a single data stream.
IP Address	Specify the IP address used to be as tunnel source IP address. If not specified, the tunnel source IP address is selected automatically based on the tunnel peer IP address. This address is applicable only for initiating the tunnel. When responding to incoming tunnel create requests, it would use the IP address on which it had received the tunnel create request.
Peer IP	Set the IP address of an L2TP tunnel destination peer. This is the peer allowed to establish the tunnel.
Local Session ID	Set the numeric identifier for the tunnel session. This is the pseudowire ID for the session. This pseudowire ID is sent in a session establishment message to the L2TP peer.
MTU	Define the session's *maximum transmission unit* (MTU) as the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data.
Remote Session ID	Use the spinner control to set the remote session ID passed in the establishment of the tunnel and sed a a unique identifier for this tunnel session. Assign an ID from 1 - 4,294,967,295.
Encapsulation	Select either *IP* or *UDP* as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes.
UDP Port	If UDP encapsulation is selected, use the spinner control to define the UDP encapsulation port. This is the port where the L2TP service is running.
Source Type	Select a VLAN as the virtual interface source type.
Source Value	Define the *Source Value* range (1 - 4,094) to include in the tunnel. Tunnel session data includes VLAN tagged frames.
Native VLAN	Select this option to define the native VLAN that's not tagged.

28 Select the **+ Add Row** button to set the following:

Cookie Size	Set the size of the cookie field within each L2TP data packet. Options include *0*, *4* and *8*. The default setting is 0.
Value 1	Set the cookie value first word.
Value 2	Set the cookie value second word.
End Point	Define whether the tunnel end point is *local* or *remote*.

29 Select **OK** to save the changes to the session configuration. Select **Reset** to revert to the last saved configuration.

5.2.8.4 Overriding a Profile's GRE Configuration

Overriding a Profile's Network Configuration

Generic routing encapsulation (GRE) tunneling can be configured to bridge Ethernet packets between WLANs and a remote WLAN gateway over a GRE tunnel. The tunneling of 802.3 packets using GRE is an alternative to MiNT or L2TPv3. Related features like ACLs for extended VLANs are still available using layer 2 tunneling over GRE.

Using GRE, Access Points map one or more VLANs to a tunnel. The remote endpoint is a user-configured WLAN gateway IP address, with an optional secondary IP address should connectivity to the primary GRE peer be lost. VLAN traffic is expected in both directions in the GRE tunnel. A WLAN mapped to these VLANs can be either open or secure. Secure WLANs require authentication to a remote RADIUS server available within your deployment using standard RADIUS protocols. Access Points can reach both the GRE peer as well as the RADIUS.

Previous releases supported only IPv4 tunnel end points, now support for both IPv4 or IPv6 tunnel endpoints is available. However, a tunnel needs to contain either IPv4 or IPv6 formatted device addresses and cannot be mixed. With the new IPv6 tunnel implementation, all outbound packets are encapsulated with the GRE header, then the IPv6 header. The header source IP address is the local address of the IPv6 address of tunnel interface, and the destination address peer address of the tunnel. All inbound packets are de-capsulated by removing the IPv6 and GRE header before sending it over to the IP stack.

To define a profile's GRE settings:

1 Select **Devices** from the Configuration tab.

  The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

  Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **GRE.**

  The screen displays existing GRE configurations.

6 Select the **Add** button to create a new GRE tunnel configuration or select an existing tunnel and select **Edit** to modify its current configuration. To remove an existing GRE tunnel, select it from amongst those displayed and select the **Delete** button.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

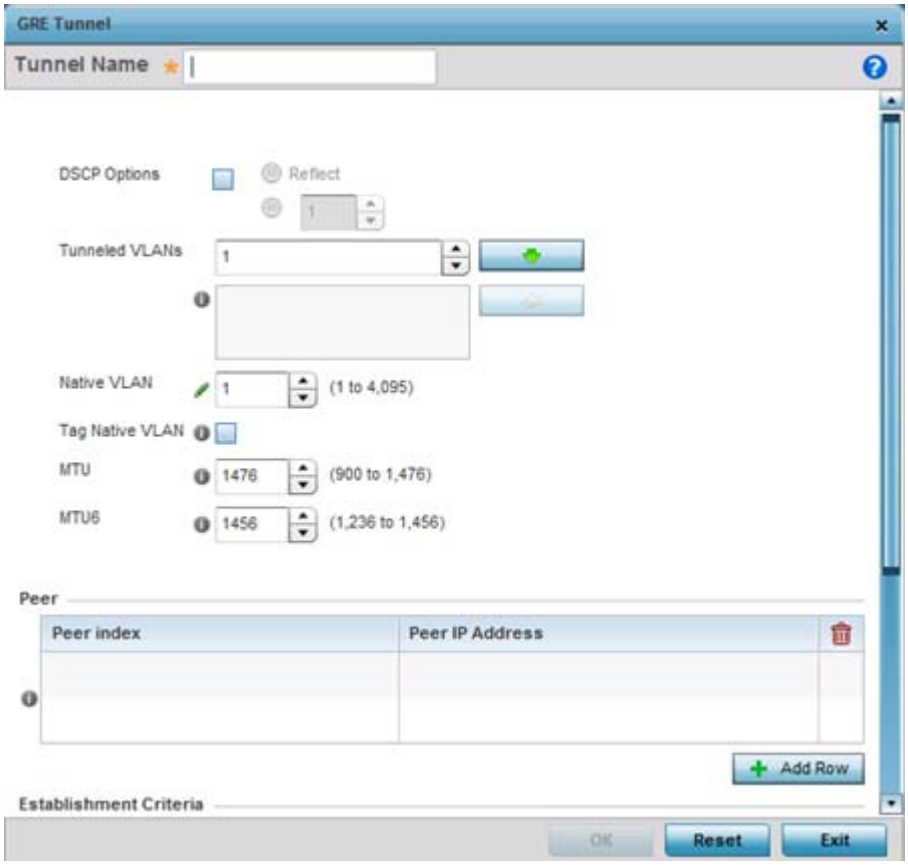


Figure 5-70 *Profile Overrides - Network GRE screen*

7 If creating a new GRE configuration, assign it a 32 character maximum name to distinguish its configuration.

8 Define the following settings for the GRE configuration:

DSCP Options	Use the spinner control to set the tunnel DSCP / 802.1q priority value from encapsulated packets to the outer packet IPv4 header.
Tunneled VLANs	Define the VLAN connected clients use to route GRE tunneled traffic within their respective WLANs.
Native VLAN	Set a numerical VLAN ID (1 - 4094) for the native VLAN. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.

Tag Native VLAN	Select this option to tag the native VLAN. The IEEE 802.1Q specification is supported for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is disabled by default.
MTU	Set an IPv4 tunnel's *maximum transmission unit* (MTU) from 128 - 1,476. The MTU is the largest physical packet size (in bytes) transmittable within the tunnel. Any messages larger than the MTU are divided into smaller packets before being sent. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. For IPv4, the overhead is 24 bytes (20 bytes IPv4 header + 4 bytes GRE Header), thus the default setting for an IPv4 MTU is 1,476.
MTU6	Set an IPv6 tunnel's MTU from 128 - 1,456. The MTU is the largest physical packet size (in bytes) transmit able within the tunnel. Any messages larger than the MTU are divided into smaller packets before being sent. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. For IPv6, the overhead is 44 bytes (40 bytes IPv6 header + 4 bytes GRE header), thus the default setting for an IPv6 MTU is 1,456.

9 The **Peer** table lists the credentials of the GRE tunnel end points. Add new table rows as needed to add additional GRE tunnel peers.

Select **+ Add Row** to populate the table with a maximum of two peer configurations.

10 Define the following **Peer** parameters:

Peer Index	Assign a numeric index to each peer to help differentiate tunnel end points.

Peer IP Address	Define the IP address of the added GRE peer to serve as a network address identifier. Designate whether the IP is formatted as an IPv4 or IPv6 address. *IPv4* is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike TCP). IPv4 hosts can use link local addressing to provide local connectivity. *IPv6* is the latest revision of the Internet Protocol (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are eight groups of four hexadecimal digits separated by colons.

11 Set the following **Establishment Criteria** for the GRE tunnel configuration:

Criteria	Specify the establishment criteria for creating a GRE tunnel. In a multi-controller within a RF domain, it's always the master node with which the tunnel is established. The tunnel is only created if the tunnel device is designated one of the following: vrrp-master cluster-master rf-domain-manager The tunnel is automatically created if *Always* (default setting) is selected. This indicates the device need not be any one of the above three (3) to establish a tunnel.
VRRP Group	Set the VRRP group ID only enabled when the *Establishment Criteria* is set to *vrrp-master*. A *virtual router redundancy group* (VRRP) enables the creation of a group of routers as a default gateway for redundancy. Clients can point to the IP address of the VRRP virtual router as their default gateway and utilize a different group member if a master becomes unavailable.

12 Define or override the following **Failover** parameters to apply to the GRE tunnel configuration:

Enable Failover	Select this option to periodically ping the primary gateway to assess its availability. If the primary gateway is unreachable.
Ping Interval	Set the duration between two successive pings to the gateway. Define this value in seconds from 1 - 21,600.
Number of Retries	Set the number of ping retries (from 1 - 63) when no response is received before the session is terminated.

13 Select the **OK** button to save the changes and overrides to the GRE configuration. Select **Reset** to revert to the last saved configuration.

5.2.8.5 Overriding a Profile's IGMP Snooping Configuration

Overriding a Profile's Network Configuration

The *Internet Group Management Protocol* (IGMP) is used for managing IP multicast group members. The controller or service platform listens to IGMP network traffic and forwards the IGMP multicast packets to radios on which the

interested hosts are connected. On the wired side of the network, the controller or service platform floods all the wired interfaces. This feature reduces unnecessary flooding of multicast traffic in the network.

To define a Profile's IGMP settings:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the *Device Browser* in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **IGMP Snooping**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override, go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

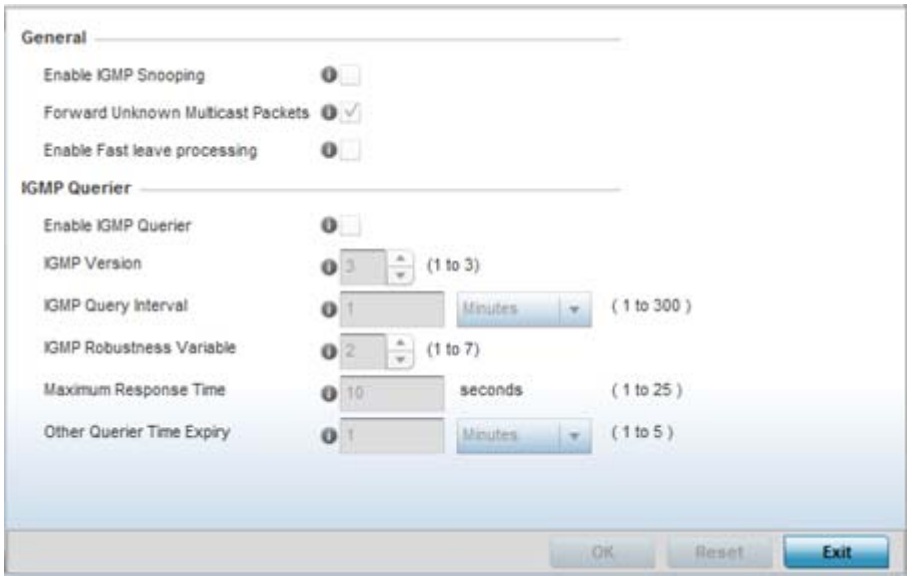


Figure 5-71 *Profile Overrides - Network IGMP Snooping*

6 Define or override the following **General IGMP Snooping** parameters for the bridge VLAN configuration:

Enable IGMP Snooping	Select this option to enable IGMP snooping. If disabled, snooping on a per VLAN basis is also disabled. This feature is enabled by default. If disabled, the settings under the bridge configuration are overridden. For example, if IGMP snooping is disabled, but the bridge VLAN is enabled, the effective setting is disabled.

Forward Unknown Multicast Packets	Select this option to enable the forwarding of multicast packets from unregistered multicast groups. If disabled (the default setting), the unknown multicast forward feature is also disabled for individual VLANs.
Enable Fast leave processing	Select this option to remove a Layer 2 LAN interface from the IGMP snooping forwarding table entry without initially sending IGMP group-specific queries to the interface. When receiving a group-specific IGMPv2 leave message, IGMP snooping removes the interface from the Layer 2 forwarding table entry for that multicast group, unless a multicast router was learned on the port. Fast-leave processing enhances bandwidth management for all hosts on the network.

7 Set or override the following **IGMP Querier** parameters for the profile's bridge VLAN configuration:

Enable IGMP Querier	Select this option to enable IGMP querier. IGMP snoop querier is used to keep host memberships alive. It's primarily used in a network where there's a multicast streaming server and hosts subscribed to the server and no IGMP querier present. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then it is forwarded on that port.
IGMP Version	Use the spinner control to set the IGMP version compatibility to either version 1, 2 or 3. IGMPv1 is defined by RFC 1112, IGMPv2 is defined by RFC 2236 and IGMPv3 defined by RFC 4604 which defines both IGMPv3 and MLDv2. IGMPv2 improves over IGMPv1 by adding the ability for a host to signal desire to leave a multicast group. IGMPv3 improves over IGMPv2 by adding the ability to listen to multicast traffic originating from a set of source IP addresses exclusively. The default setting is 3.
IGMP Query Interval	Set the interval IGMP queries are made. Options include *Seconds* (1 - 18,000), *Minutes* (1 - 300) and *Hours* (1 - 5). The default setting is one minute.
IGMP Robustness Variable	IGMP utilizes a robustness value used by the sender of a query. Update the robustness variable to match the most recently received query unless the value is zero.
Maximum Response Time	Specify the maximum interval (from 1 - 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the snooping table. The controller or service platform only forwards multicast packets to radios present in the snooping table. For IGMP reports from wired ports, the controller or service platform forwards these reports to the multicast router ports. The default setting is 10 seconds.
Other Querier Timer Expiry	Specify an interval in either *Seconds* (60 - 300) or *Minutes* (1 - 5) used as a timeout interval for other querier resource connections. The default setting is 1 minute.

8 Select the **OK** button to save the changes and overrides to the IGMP Snooping tab. Select **Reset** to revert to the last saved configuration.

5.2.8.6 Overriding a Profile's MLD Snooping Configuration

Overriding a Profile's Network Configuration

Multicast Listener Discovery (MLD) snooping enables a controller, service platform or Access Point to examine MLD packets and make forwarding decisions based on content. MLD is used by IPv6 devices to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups.

MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or Access Point VLANs. When enabled, MLD messages are examined between hosts and multicast routers and to discern which hosts are receiving multicast group traffic. The controller, service platform or Access Point then forwards multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces.

To set an IPv6 MLD snooping configuration for the profile:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **MLD Snooping**.

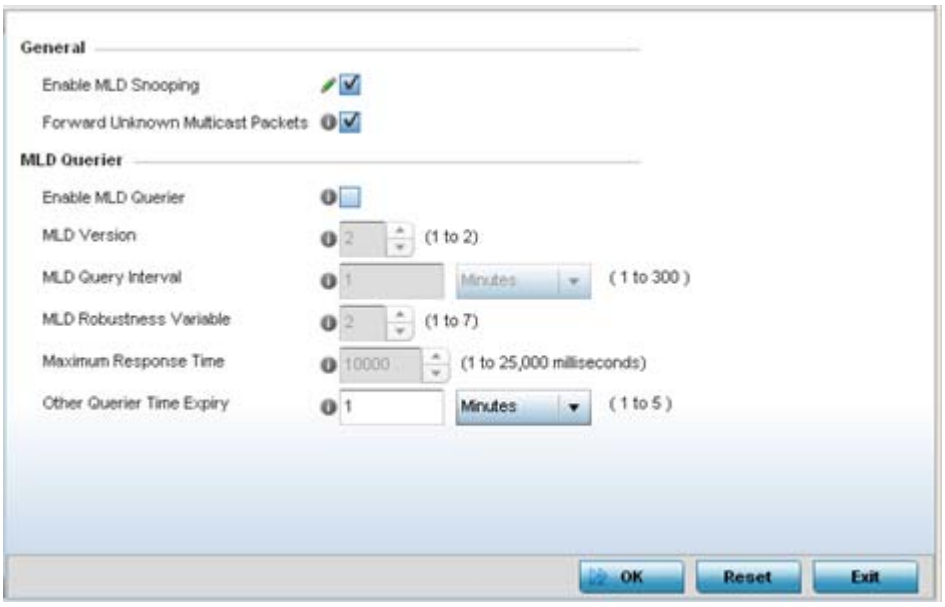


Figure 5-72 *Profile - Network MLD Snooping screen*

4 Define the following **General** MLD snooping settings:

Enable MLD Snooping	Enable MLD snooping to examine MLD packets and make content forwarding for this profile. Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability, just like IPv6 unicast. MLD snooping is disabled by default.
Forward Unknown Multicast Packets	Use this option to either enable or disable IPv6 unknown multicast forwarding. This setting is enabled by default.

5 Define the following **MLD Querier** settings for the MLD snooping configuration:

Enable MLD Querier	Select the option to enable MLD querier on the controller, service platform or Access Point. When enabled, the device sends query messages to discover which network devices are members of a given multicast group. This setting is disabled by default.
MLD Version	Define whether MLD version *1* or *2* is utilized as the MLD querier. MLD version 1 is based on IGMP version 2 for IPv4. MLD version 2 is based on IGMP version 3 for IPv4 and is fully backward compatible. IPv6 multicast uses MLD version 2. The default MLD version is 2.
MLD Query Interval	Set the interval in which query messages are sent to discover device multicast group memberships. Set an interval in either *Seconds* (1 - 18,000), *Minutes* (1 - 300) or *Hours* (1 - 5). The default interval is 1 minute.
MLD Robustness Variable	Set a MLD IGMP robustness value (1 - 7) used by the sender of a query. The MLD robustness variable enables refinements to account for expected packet loss on a subnet. Increasing the robust count allows for more packet loss, but increases the leave latency of the subnetwork unless the value is zero. The default variable is 2.
Maximum Response Time	Specify the maximum response time (from 1 - 25,000 milliseconds) before sending a responding report. Queriers use MLD reports to join and leave multicast groups and receive group traffic. The default setting is 10 milliseconds.
Other Querier time Expiry	Specify an interval in either *Seconds* (60 - 300) or *Minutes* (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute.

6 Select the **OK** button located to save the changes. Select **Reset** to revert to the last saved configuration.

5.2.8.7 Overriding a Profile's Quality of Service (QoS) Configuration

Overriding a Profile's Network Configuration

The controller or service platform use different *Quality of Service (QoS)* screens to define WLAN and device radio QoS and traffic shaping configurations for profiles.

Traffic shaping regulates network data transfers to ensure a specific performance level. Traffic shaping delays the flow of packets defined as less important than prioritized traffic streams. Traffic shaping enables traffic control out an interface to match its flow to the speed of a remote target's interface and ensure traffic conforms applied policies. Traffic can be shaped to meet downstream requirements and eliminate network congestion when data rates are in conflict.

QoS values are required to provide priority of service to some packets over others. For example, VoIP packets get higher priority than data packets to provide a better quality of service for high priority voice traffic.

The profile QoS screen maps the 6-bit *Differentiated Service Code Point* (DSCP) code points to the older 3-bit IP Precedent field located in the Type of Service byte of an IP header. DSCP is a protocol for specifying and controlling network traffic by class so that certain traffic types get precedence. DSCP specifies a specific per-hop behavior that is applied to a packet. This QoS assignment can be overridden as needed, but removes the device configuration from the profile that may be shared with other similar device models.

To define an QoS configuration:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the *Device Browser* in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **Quality of Service**.

The **Traffic Shaping** screen displays with the **Basic Configuration** tab displayed by default.

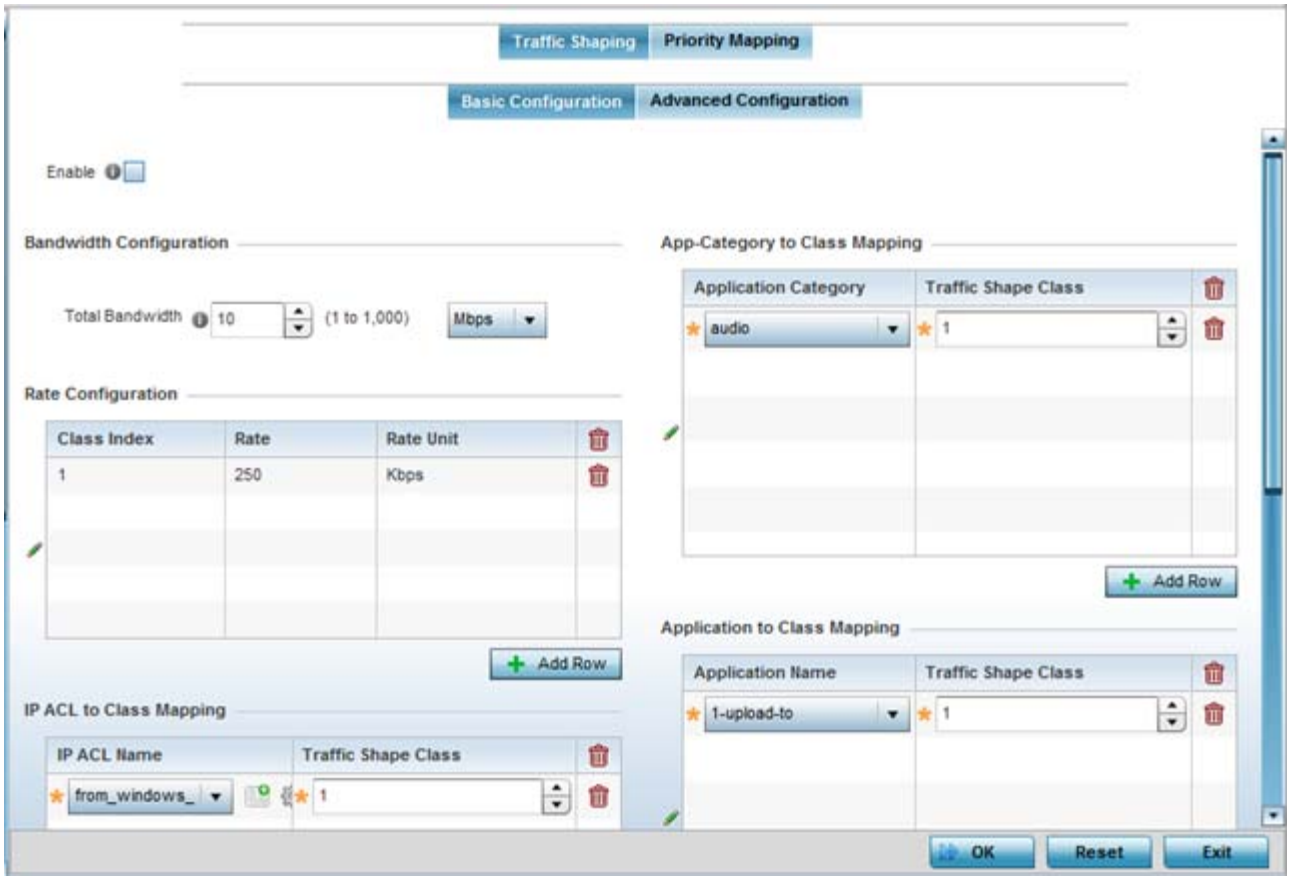


Figure 5-73 *Profile Overrides - Network QoS Traffic Shaping Basic Configuration screen*

Apply traffic shaping to specific applications to apply application categories. When application and ACL rules are conflicting, applications have priority, followed by application categories, then ACLs.

6 Select **Enable** to provide traffic shaping using the defined bandwidth, rate and class mappings.

7 Set the **Total Bandwidth** configurable for the traffic shaper. Set the value from either 1 - 1,000 Mbps, or from 250 - 1,000,000 Kbps.

8 Select **+ Add Row** within the **Rate Configuration** table to set the **Class Index** and **Rate** (in either Kbps, Mbps or percentage) for the traffic shaper class. Use the rate configuration to control the maximum traffic rate sent or received on the device. Consider this form of rate limiting on interfaces at the edge of a network to limit traffic

into or out of the network. Traffic within the set limit is sent and traffic exceeding the set limit is dropped or sent with a different priority.

9 Refer to the **IP ACL Class Mapping** table and select **+ Add Row** to apply an IPv4 formatted ACL to the shaper class mapping. Select **+ Add Row** to add mappings. For more information on creating IP based firewall rules, refer to Configuring IP Firewall Rules on page 10-20 and Setting an IPv4 or IPv6 Firewall Policy on page 10-21.

10 Refer to the **IPv6 ACL Class Mapping** table and select **+ Add Row** to apply an IPv6 formatted ACL to the shaper class mapping. Select **+ Add Row** to add mappings. For more information on creating IP based firewall rules, refer to Configuring IP Firewall Rules on page 10-20 and Setting an IPv4 or IPv6 Firewall Policy on page 10-21.

11 Refer to the **App-Category to Class Mapping** table and select **+ Add Row** to apply an application category to shaper class mapping. Select **+ Add Row** to add mappings by selecting the application category and its traffic shaper class. For more information on creating an application category, refer to Application on page 7-58.

12 Refer to the **Application to Class Mapping** table and select **+ Add Row** to apply an application to shaper class mapping. Select **+ Add Row** to add mappings by selecting the application and its traffic shaper class. For more information on creating an application, refer to Application on page 7-58.

13 Select the **OK** button located to save the changes to the traffic shaping basic configuration. Select **Reset** to revert to the last saved configuration.

14 Select the **Advanced Configuration** tab.

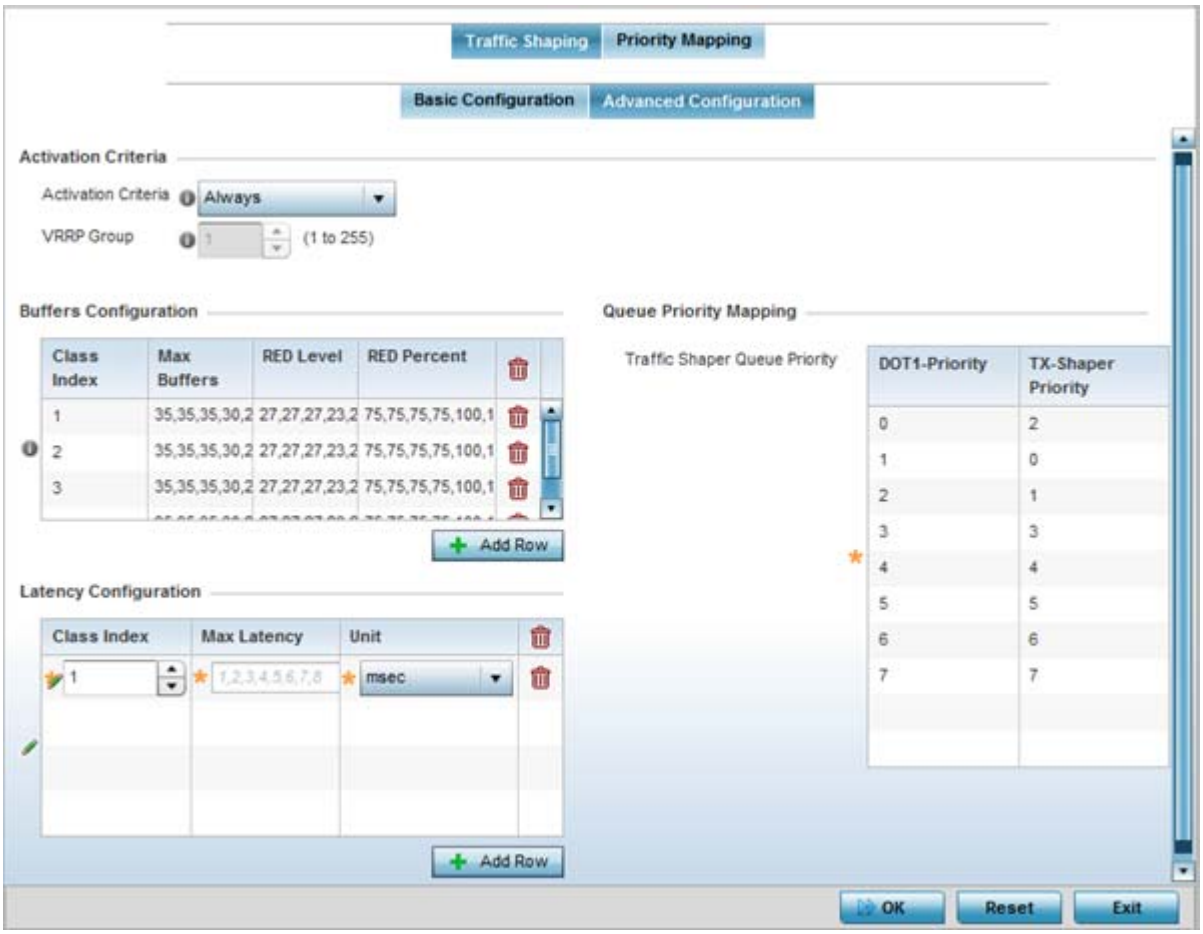


Figure 5-74 *Profile Overrides - Network QoS Traffic Shaping Advanced Configuration screen*

15 Set the following **Activation Criteria** for traffic shaper activation:

Activation Criteria	Use the drop-down menu to determine when the traffic shaper is invoked. Options include *vrrp-master, cluster-master*, *rf-domain-manager* and *Always*. A *VRRP master* responds to ARP requests, forwards packets with a destination link MAC layer address equal to the virtual router MAC layer address, rejects packets addressed to the IP associated with the virtual router and accepts packets addressed to the IP associated with the virtual router. The solitary *cluster master* is the cluster member elected, using a priority assignment scheme, to provide management configuration and Smart RF data to other cluster members. Cluster requests go through the elected master before dissemination to other cluster members. The RF Domain manager is the elected member capable of storing and provisioning configuration and firmware images for other members of the RF Domain.
VRRP Group	Set the VRRP group ID from 1 - 255. VRRP groups is only enabled when the Establishment Criteria is set to vrrp-master.

16 Select **+ Add Row** within the **Buffers Configuration** table to set the following:

Class Index	Set a class index from 1 - 4.
Max Buffers	Se the *Max Buffers* to specify the queue length limit after which the queue starts to drop packets. Set the maximum queue lengths for packets. The upper length is 400 for Access Points.
RED Level	Set the packet queue length for RED. The upper limit is 400 for Access Points. The rate limiter uses the *random early detection* (RED) algorithm for rate limiting traffic. RED is a queueing technique for congestion avoidance. RED monitors the average queue size and drops or marks packets. If the buffer is near empty, all incoming packets are accepted. When the queue grows, the probability for dropping an incoming packet also grows. When the buffer is full, the probability has reached 1 and all incoming packets are dropped.
RED Percent	Set a percentage (1 - 100) for RED rate limiting at a percentage of maximum buffers.

17 Select **+ Add Row** within the **Latency Configuration** table to set the **Class Index** (1 - 4), **Max Latency** and latency measurement **Unit**. Max latency specifies the time limit after which packets start dropping (maximum packet delay in the queue). The maximum number of entries is 8. Select whether *msec* (default) or *usec* is unit for latency measurement.

When a new packet arrives it knows how much time to wait in the queue. If a packet takes longer than the latency value it's dropped. By default latency is not set, so packets remain in queue for long time.

18 Refer to the **Que Priority Mapping** table to set the traffic shaper queue priority and specify a particular queue inside a class. There are 8 queues (0 - 7), and traffic is queued in each based on incoming packets mark 802.1p markings.

19 Select the **OK** button located to save the changes to the traffic shaping advanced configuration. Select **Reset** to revert to the last saved configuration.

20 Select the **Priority Mapping** tab.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

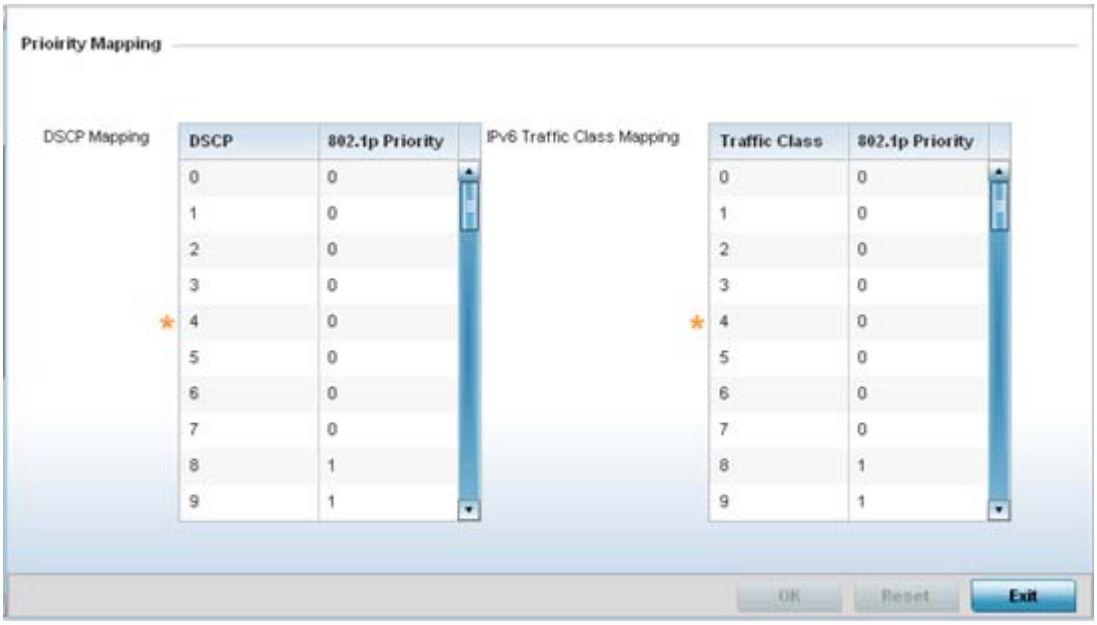


Figure 5-75 *Profile Overrides - Network QoS screen*

21 Set or override the following parameters for IP **DSCP Mappings** for untagged frames:

DSCP	Lists the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification.
802.1p Priority	Assign a 802.1p priority as a 3-bit IP precedence value in the Type of Service field of the IP header used to set the priority. The valid values for this field are 0-7. Up to 64 entries are permitted. The priority values are: 0 – *Best Effort* 1 – *Background* 2 – *Spare* 3 – *Excellent Effort* 4 – *Controlled Load* 5 – *Video* 6 – *Voice* 7 – *Network Control*

22 Set or override the following parameters for **IPv6 Traffic Class Mapping** for untagged frames:

Traffic Class	Devices that originate a packet must identify different classes or priorities for IPv6 packets. Devices use the traffic class field in the IPv6 header to set this priority.
802.1p Priority	Assign a 802.1p priority as a 3-bit IPv6 precedence value in the Type of Service field of the IPv6 header used to set the priority. The valid values for this field are 0-7. Up to 64 entries are permitted. The priority values are: 0 – *Best Effort* 1 – *Background* 2 – *Spare* 3 – *Excellent Effort* 4 – *Controlled Load* 5 – *Video* 6 – *Voice* 7 – *Network Control*

23 Use the spinner controls within the **802.1p Priority** field for each DSCP row to change or override the assigned priority value.

24 Select the **OK** button located to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

5.2.8.8 Overriding a Profile's Spanning Tree Configuration

- *Overriding a Profile's Network Configuration*

The *Multiple Spanning Tree Protocol* (MSTP) provides an extension to RSTP to optimize the usefulness of VLANs. MSTP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.

If there's just one VLAN in the Access Point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it's possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

A MSTP supported deployment uses multiple MST regions with *multiple MST instances* (MSTI). Multiple regions and other STP bridges are interconnected using one single *common spanning tree* (CST).

MSTP includes all of its spanning tree information in a single *Bridge Protocol Data Unit* (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. MSTP encodes additional region information after the standard RSTP BPDU as well as a number of MSTI messages. Each MSTI messages conveys spanning tree information for each instance. Each instance can be assigned a number of configured VLANs. The frames assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, the Access Point encodes an MD5 digest of their VLAN to an instance table in the MSTP BPDU. This digest is used by other MSTP supported devices to determine if the neighboring device is in the same MST region as itself.

To create or override a profile's spanning tree configuration:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **Spanning Tree**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

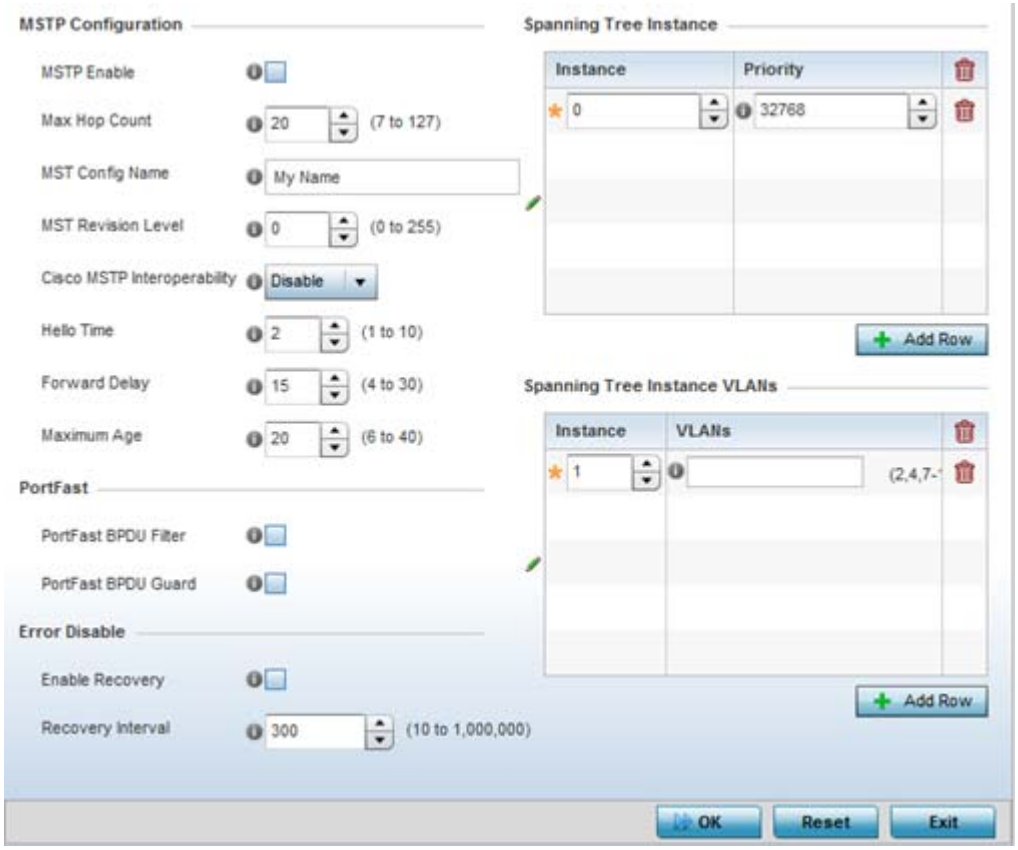


Figure 5-76 *Spanning Tree screen*

6 Set the following **MSTP Configuration** parameters:

MSTP Enable	Select this option to enable MSTP for this profile. MSTP is disabled by default, so if requiring different (groups) of VLANs with the profile supported network segment.

Max Hop Count	Define the maximum number of hops the BPDU will consider valid in the spanning tree topology. The available range is from 7 -127. The default setting is 20.
MST Config Name	Define a 64 character maximum name for the MST region as an identifier.
MST Revision Level	Set a numeric revision value ID for MST configuration information. Set a value from 0 - 255. The default setting is 0.
Cisco MSTP Interoperability	Select either the *Enable* or *Disable* radio buttons to enable/disable interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default.
Hello Time	Set a BPDU hello interval from 1 - 10 seconds. BPDUs are exchanged regularly (every 2 seconds by default) and enable supported devices to keep track of network changes and star/stop port forwarding as required.
Forward Delay	Set the forward delay time from 4 - 30 seconds. When a device is first attached to a port, it does not immediately forward data. It first processes BPDUs and determines the network topology. When a host is attached the port always goes into the forwarding state, after a delay of while it goes through the listening and learning states. The time spent in listening and learning states is set by the forward delay (15 seconds by default).
Maximum Age	Use the spinner control to set the maximum time (in seconds) to listen for the root bridge. The root bridge is the spanning tree bridge with the smallest (lowest) bridge ID. Each bridge has a unique ID and a configurable priority number, the bridge ID contains both. The available range is from 6 - 40 seconds. The default setting is 20 seconds.

7 Set the following **PortFast** parameters for the profile configuration:

PortFast BPDU Filter	Select Enable to invoke a BPDU filter for this portfast enabled port. Enabling the BPDU filter feature ensures this port channel does not transmit or receive any BPDUs. BPDUs are exchanged regularly and enable the Access Point to keep track of network changes and to start and stop port forwarding as required. The default setting is Disabled.
PortFast BPDU Guard	Select Enable to invoke a BPDU guard for the portfast enabled port. Enabling the BPDU Guard feature means this port will shutdown on receiving a BPDU. Thus, no BPDUs are processed. BPDUs are exchanged regularly and enable the Access Point to keep track of network changes and to start and stop port forwarding as required. The default is Disabled.

8 Set the following **Error Disable** parameters for the profile configuration:

Enable Recovery	Select this option to enable a error disable timeout resulting from a BPDU guard. This setting is disabled by default.
Recovery Interval	Define the recovery interval used to enable disabled ports. The available range is from 10 - 1,000,000 seconds with a default setting of 300.

9 Use the **Spanning Tree Instance** table to add indexes to the spanning tree topology.

10 Add up to 16 indexes and use the Priority setting to define the bridge priority used to determine the root bridge. The lower the setting defined, the greater the likelihood of becoming the root bridge in the spanning tree topology.

11 Use the **Spanning Tree Instance VLANs** table to add up to 15 VLAN instance indexes (by numeric ID) and VLANs to the spanning tree topology as virtual route resources.

12 Select the **OK** button located at the bottom right of the screen to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

5.2.8.9 Overriding a Profile's Routing Configuration

Overriding a Profile's Network Configuration

Routing is the process of selecting IP paths within the wireless network to route traffic. Use the *Routing* screen to set *Destination IP* and *Gateway* addresses enabling the assignment of static IP addresses for requesting clients without creating numerous host pools with manual bindings. This eliminates the need for a long configuration file and reduces the resource space required to maintain address pools.

Both IPv4 and IPv6 routes are separately configurable using their appropriate tabs. For IPv6 networks, routing is the part of IPv6 that provides forwarding between hosts located on separate segments within a larger IPv6 network where IPv6 routers provide packet forwarding for other IPv6 hosts.

To create or override a profile's static routes:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the *Device Browser* in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **Routing**. The **IPv4 Routing** tab displays by default.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

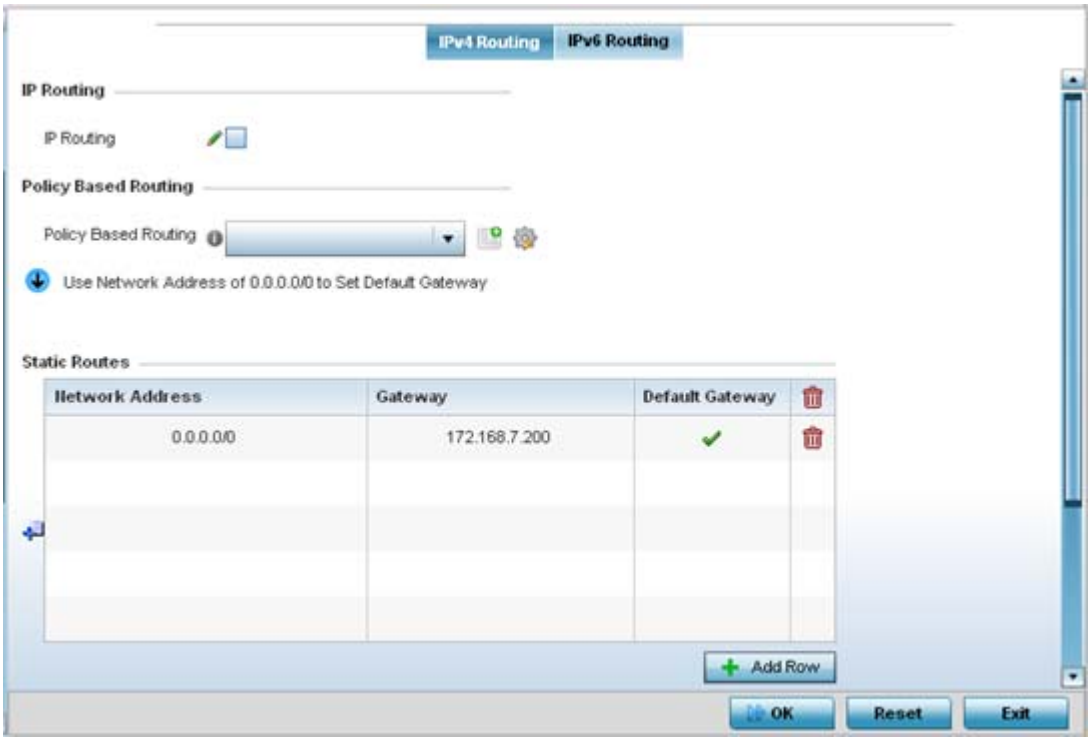


Figure 5-77 *IPv4 Static Routes screen*

6 Select **IP Routing** to enable static routes using IP addresses. This sets Destination IP and Gateway addresses enabling the assignment of static IP addresses for requesting clients. This option is enabled by default.

7 Use the drop-down menu to select a **Policy Based Routing** policy. If a suitable policy is not available, select the Create icon or modify an existing policy-based routing policy by selecting the Edit icon.

Policy-based routing (PBR) is a means of expressing and forwarding (routing) data packets based on policies defined by administrators. PBR provides a flexible mechanism for routing packets through routers, complementing existing routing protocols. PBR is applied to incoming packets. Packets received on an interface with PBR enabled are considered are passed through enhanced packet filters (route maps). Based on the route maps, packets are forwarded/routed to their next hop.

Refer to the **Static Routes** table to set Destination IP and Gateway addresses enabling the assignment of static IP addresses to requesting clients (without creating numerous host pools with manual bindings).

- Add IP addresses and network masks in the **Network Address** column.
- Provide the **Gateway** address used to route traffic.
- Provide an IP address for the **Default Gateway** used to route traffic.

Note, when routing packets, the controller, by default, obtains Default Gateway and Name Servers IP addresses from the DHCP server policy. If manually configuring the Default Gateway for static routing, also configure the Name Server's IP address in the controller's device/profile config contexts. For more information on using the GUI to configure Name Servers, see *Overriding a Profile's DNS Configuration*. If using the CLI, in the device/profile context, execute the following command: ip name-server <NAME-SERVER-IP-ADDRESS>.

8 Refer to the **Default Route Priority** field and set the following parameters:

Static Default Route Priority	Use the spinner control to set the priority value (1 - 8,000) for the default static route. This is weight (priority) assigned to this route versus others that have been defined. The default setting is 100.

DHCP Client Default Route Priority	Use the spinner control to set the priority value (1 - 8,000) for the default route learnt from the DHCP client. The default setting is 1000.
Enable Routing Failure	When selected, all default gateways are monitored for activity. The system will failover to a live gateway if the current gateway becomes unusable. This feature is enabled by default.

9 Select the **OK** button located at the bottom right of the screen to save the changes to IPv4 routing configuration. Select **Reset** to revert to the last saved configuration.

10 Select the **IPv6 Routing** tab. IPv6 networks are connected by IPv6 routers. IPv6 routers pass IPv6 packets from one network segment to another.

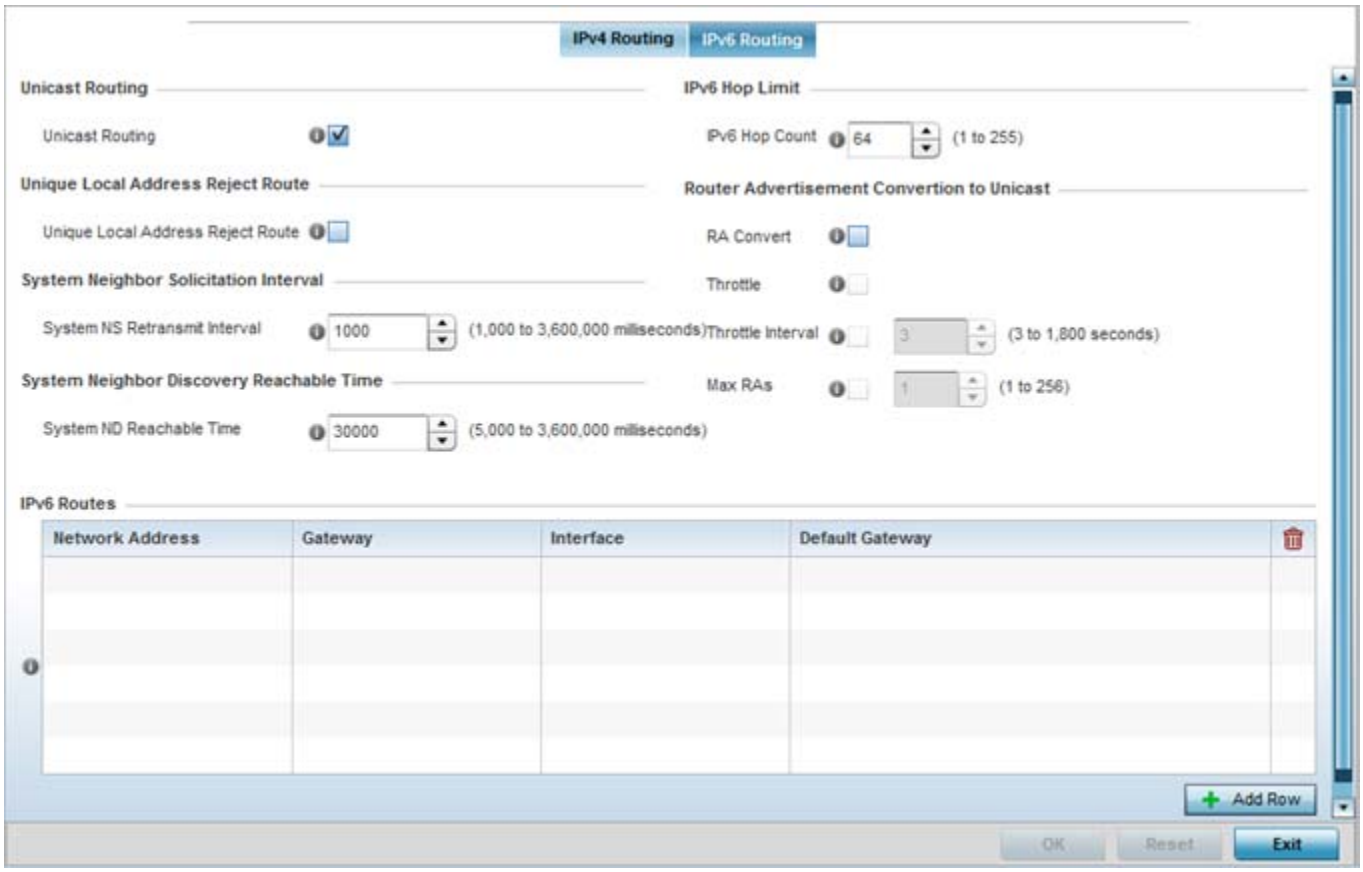


Figure 5-78 *Static Routes screen, IPv6 Routing tab*

11 Select **Unicast Routing** to enable IPv6 unicast routing for this profile. Keeping unicast enabled allows the profile's neighbor advertisements and solicitations in unicast (as well as multicast) to provide better neighbor discovery. This setting is enabled by default.

12 Select **Unique Local Address Reject Route** to reject *Unique Local Address* (ULA). ULA is an IPv6 address block (fc00::/7) that is an approximate IPv6 counterpart to IPv4 private addresses. When selected, a reject entry is added to the IPv6 routing table to reject packets with Unique Local Address.

13 Set a **System NS Retransmit Interval** (from 1,000 to 3,600,000 milliseconds) as the interval between *neighbor solicitation* (NS) messages. NS messages are sent by a node to determine the link layer address of a neighbor, or verify a neighbor is still reachable via a cached link-layer address. The default is 1,000 milliseconds.

14 Set a **System ND Reachable Time** (from 5,000 to 3,600,000 milliseconds) as the time a neighbor is assumed to be reachable after receiving a receiving a *neighbor discovery* (ND) confirmation for their reachability. The default is 30,000 milliseconds.

15 Set an **IPv6 Hop Count** (from 1 - 255) as the maximum number of hops considered valid when sending IP packets. The default setting is 64.

16 Set the **Router Advertisement Conversion to Unicast** settings:

RA Convert	Select this option to convert multicast *router advertisements* (RA) to unicast router advertisements at the dot11 layer. Unicast addresses identify a single network interface, whereas a multicast address is used by multiple hosts. This setting is disabled by default.
Throttle	Select this option to throttle RAs before converting to unicast. Once enabled, set the throttle interval and maximum number of RAs. This setting is disabled by default.
Throttle Interval	Enable this setting to define the throttle interval (3 - 1,800 seconds). The default setting is 3 seconds.
Max RAs	Enable this setting to define the maximum number of router advertisements per router (1 - 256) during the throttle interval. The default setting is 1.

17 Select **+ Add Row** as needed within the **IPv6 Routes** table to add an additional 256 IPv6 route resources.

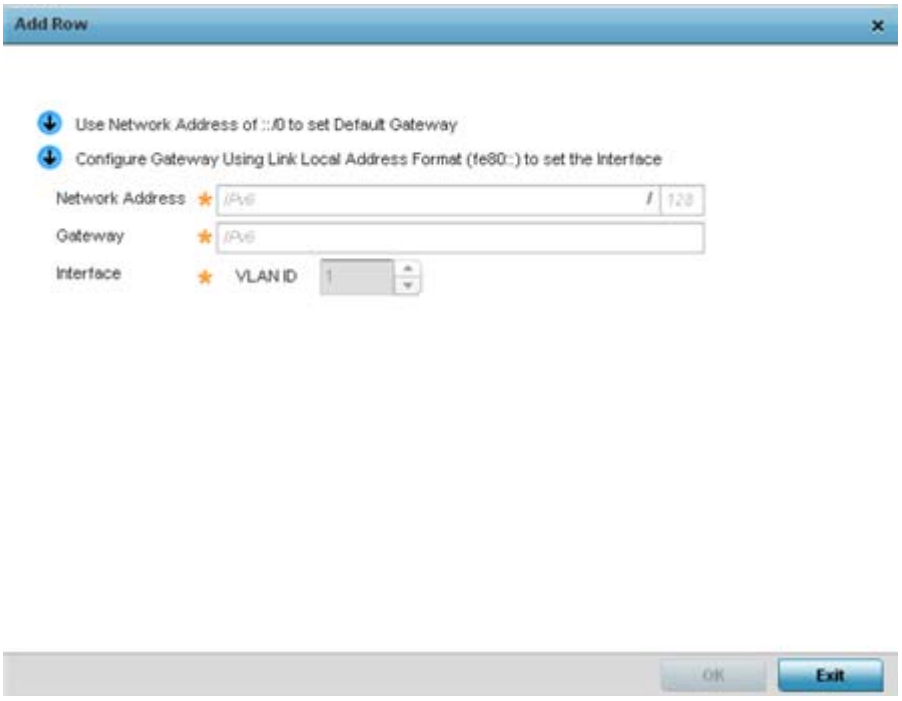


Figure 5-79 *Static Routes screen, Add IPv6 Route*

Network Address	Set the IPv6 network address. Other than the length and slightly different look versus an IPv4 address, the IPv6 address concept is same as IPv4.

Gateway	Set the IPv6 route gateway. A network gateway in IPv6 is the same as in IPv4. A gateway address designates how traffic is routed out of the current subnet.
Interface	If using a link local address, set the VLAN (1 - 4,094) used a virtual routing interface for the local address.

18 Select the **OK** button located at the bottom right of the screen to save the changes to the IPv6 routing configuration. Select **Reset** to revert to the last saved configuration.

5.2.8.10 Overriding a Profile's Dynamic Routing (OSPF) Configuration

Overriding a Profile's Network Configuration

Open Shortest Path First (OSPF) is a link-state *interior gateway protocol* (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

OSPF detects changes in the topology, like a link failure, and plots a new loop-free routing structure. It computes the shortest path for each route using a shortest path first algorithm. Link state data is maintained on each router and is periodically updated on all OSPF member routers.

OSPF uses a route table managed by the link *cost* (external metrics) defined for each routing interface. The cost could be the distance of a router (round-trip time), link throughput or link availability. Setting a cost value provides a dynamic way to load balancing traffic between routes of equal cost.

An OSPF network can be subdivided into routing areas to simplify administration and optimize traffic utilization. Areas are logical groupings of hosts and networks, including routers having interfaces connected to an included network. Each area maintains a separate link state database whose information may be summarized towards the rest of the network by the connecting router. Areas are identified by 32-bit IDs, expressed either in decimal, or octet-based dot-decimal notation. Areas can defined as:

stub area - A stub area is an area which does not receive route advertisements external to the autonomous system (AS) and routing from within the area is based entirely on a default route.

totally-stub - A totally stubby area does not allow summary routes and external routes. A default route is the only way to route traffic outside of the area. When there's only one route out of the area, fewer routing decisions are needed, lowering system resource utilization.

non-stub - A non-stub area imports autonomous system external routes and send them to other areas. However. it still cannot receive external routes from other areas.

nssa - NSSA is an extension of a stub that allows the injection of limited external routes into a stub area. If selecting NSSA, no external routes, except a default route, enter the area.

totally nssa - Totally nssa is an NSSA using 3 and 4 summary routes are not flooded into this type of area. It is also possible to declare an area both totally stubby and not-so-stubby, which means that the area will receive only the default route from area 0.0.0.0, but can also contain an autonomous system boundary router (ASBR) that accepts external routing information and injects it into the local area, and from the local area into area 0.0.0.0.

A router running OSPF sends hello packets to discover neighbors and elect a designated router. The hello packet includes link state information and list of neighbors. OSPF is savvy with layer 2 topologies. If on a *point-to-point*

link, OSPF knows it is sufficient, and the link stays *up*. If on a *broadcast* link, the router waits for election before determining if the link is functional.

To define a dynamic routing configuration:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the *Device Browser* in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Expand the **Network** menu and select **OSPF**.

The **OSPF Settings** tab displays by default, with additional **Area Settings** and **Interface Settings** tabs available.

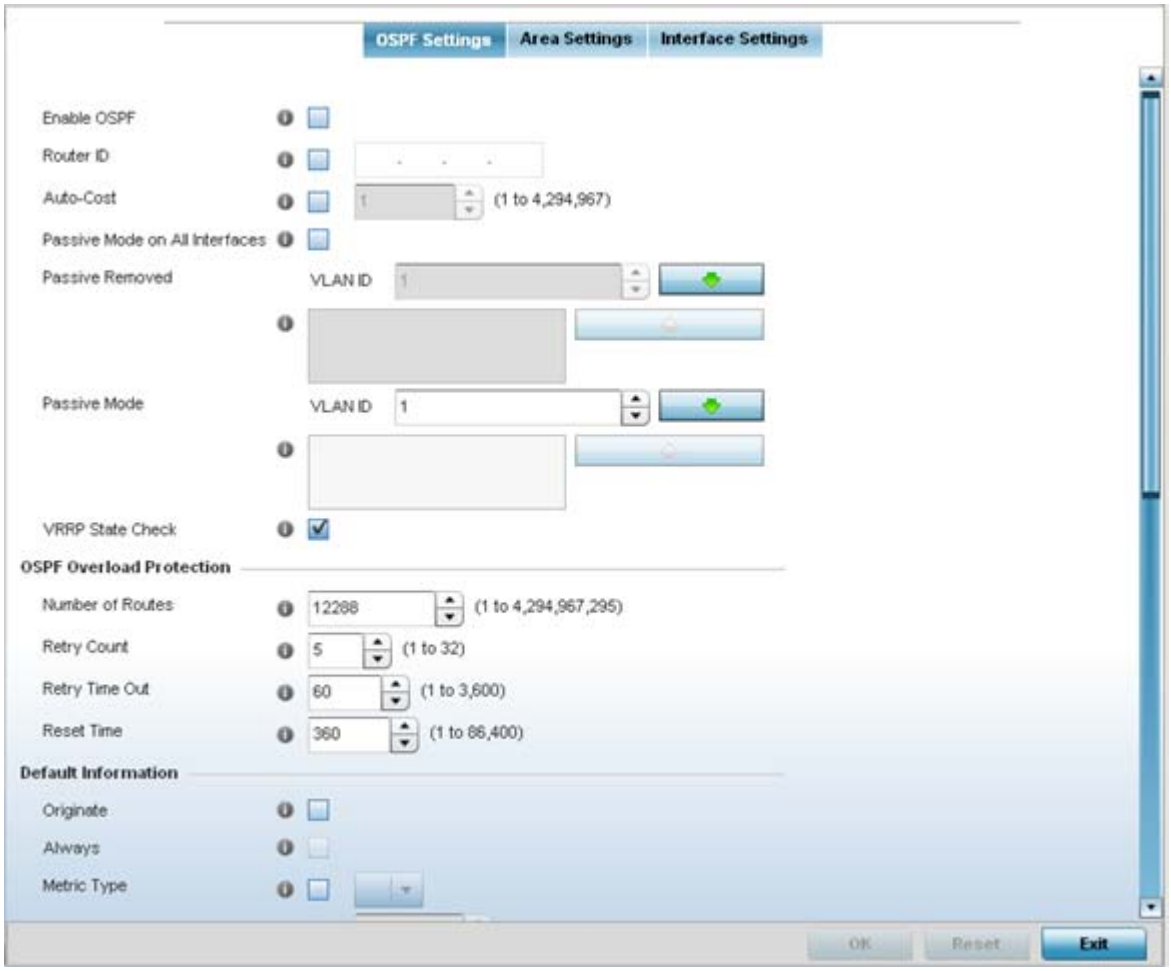


Figure 5-80 *OSPF Settings screen*

5 Enable/disable OSPF and provide the following dynamic routing settings:

Enable OSPF	Select this option to enable OSPF. OSPF is disabled by default.

Router ID	Select this option to define a router ID (numeric IP address) for this OSPF configuration. This ID must be established in every OSPF instance. If not explicitly configured, the highest logical IP address is duplicated as the router identifier. However, since the router identifier is not an IP address, it does not have to be a part of any routable subnet in the network.
Auto-Cost	Select this option to specify the reference bandwidth (in Mbps) used to calculate the OSPF interface cost if OSPF is either STUB or NSSA. The default setting is 1.
Passive Mode on All Interfaces	When selected, all layer 3 interfaces are set as an OSPF passive interface. This setting is disabled by default.
Passive Removed	If *enabling* Passive Mode on All Interfaces, use the spinner control to select VLANs (by numeric ID) as OSPF *non* passive interfaces. Multiple VLANs can be added to the list.
Passive Mode	If *disabling* Passive Mode on All Interfaces, use the spinner control to select VLANs (by numeric ID) as OSPF passive interfaces. Multiple VLANs can be added to the list.
VRRP State Check	Select this option to use OSPF only if the VRRP interface is not in a backup state. The *Virtual Router Redundancy Protocol* (VRRP) provides automatic assignments of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork. This setting is enabled by default.

6 Set the following **OSPF Overload Protection** settings:

Number of Routes	Use the spinner control to set the maximum number of OSPN routes permitted. The available range is from 1 - 4,294,967,295.
Retry Count	Set the maximum number of retries (OSPF resets) permitted before the OSPF process is shut down. The available range is from 1 - 32. The default setting is 5.
Retry Time Out	Set the duration (in seconds) the OSPF process remains off before initiating its next retry. The available range is from 1 - 3,600 seconds. The default is 60 seconds.
Reset Time	Set the reset time (in seconds) that, when exceeded, changes the retry count is zero. The available range is from 1 - 86,400. The default is 360 seconds.

7 Set the following **Default Information**:

Originate	Select this option to make the default route a distributed route. This setting is disabled by default.
Always	Enabling this settings continuously maintains a default route, even when no routes appear in the routing table. This setting is disabled by default.
Metric Type	Select this option to define the exterior metric type (1 or 2) used with the default route.
Route Metric	Select this option to define route metric used with the default route. OSPF uses path cost as its routing metric. It's defined by the speed (bandwidth) of the interface supporting given route.

Refer to the **Route Redistribution** table to set the types of routes that can be used by OSPF.

Select the **+ Add Row** button to populate the table. Set the **Route Type** used to define the redistributed route. Options include *connected*, *kernal* and static.

8 Select the **Metric Type** option to define the exterior metric type (1 or 2) used with the route redistribution. Select the **Metric** option to define route metric used with the redistributed route.

9 Use the **OSPF Network** table to define networks (IP addresses) to connect using dynamic routes.

10 Select the **+ Add Row** button to populate the table. Add the IP address and mask of the **Network(s)** participating in OSPF. Additionally, define the OSPF area (IP address) to which the network belongs.

11 Set an **OSPF Default Route Priority** (1 - 8,000) as the priority of the default route learnt from OSPF. The default setting is 7,000.

12 Select the **Area Settings** tab.

An OSPF *Area* contains a set of routers exchanging *Link State Advertisements* (LSAs) with others in the same area. Areas limit LSAs and encourage aggregate routes.

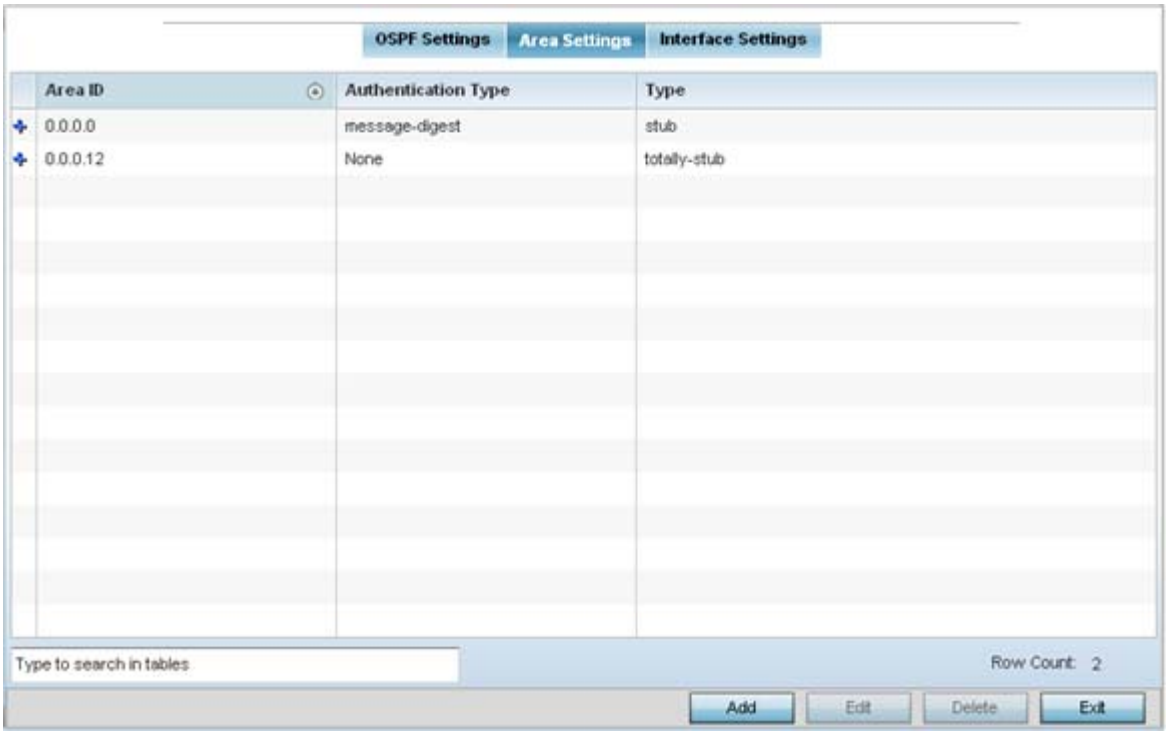


Figure 5-81 *OSPF Area Settings screen*

13 Review existing **Area Settings** configurations:

Area ID	Displays either the IP address or integer representing the OSPF area.
Authentication Type	Lists the authentication schemes used to validate the credentials of each dynamic route connection.
Type	Lists the OSPF area type for each listed configuration.

14 Select **Add** to create a new OSPF configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.

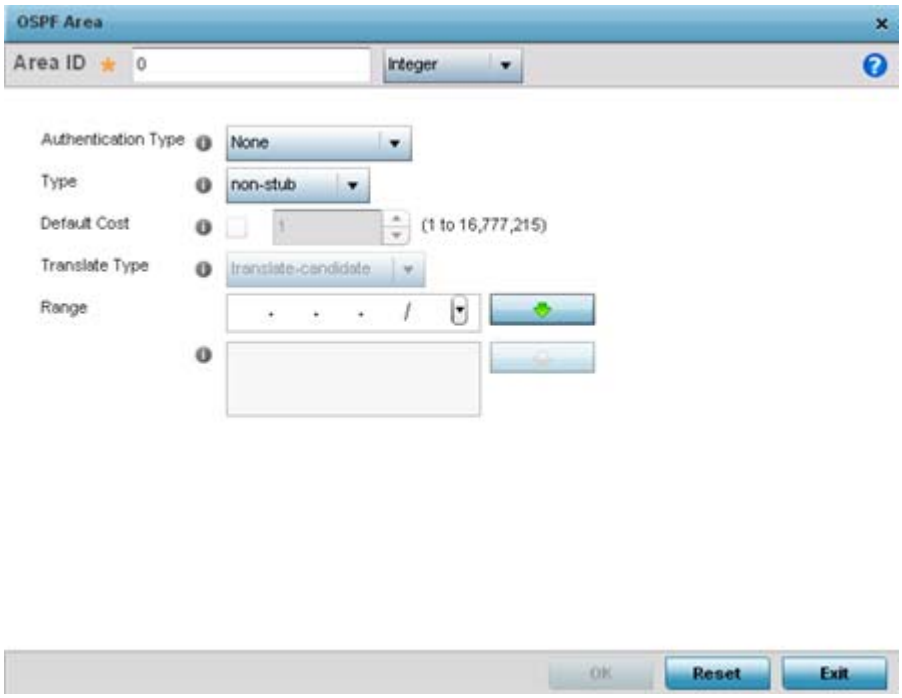


Figure 5-82 *OSPF Area Configuration screen*

15 Set the **OSPF Area** configuration.

Area ID	Use the drop down menu and specify either an IP address or integer for the OSPF area.
Authentication Type	Select either *None*, *simple-password* or *message-digest* as credential validation scheme used with the OSPF dynamic route. The default setting is None.
Type	Set the OSPF area type as either *stub*, *totally-stub*, *nssa*, *totally-nssa* or *non-stub*.
Default Cost	Select this option to set the default summary cost advertised if creating a stub. Set a value from 1 - 16, 777,215.
Translate Type	Define how messages are translated. Options include *translate-candidate*, *translate always* and *translate-never.* The default setting is translate-candidate.
Range	Specify a range of addresses for routes matching address/mask for OSPF summarization.

16 Select the **OK** button to save the changes to the area configuration. Select **Reset** to revert to the last saved configuration.

17 Select the **Interface Settings** tab.

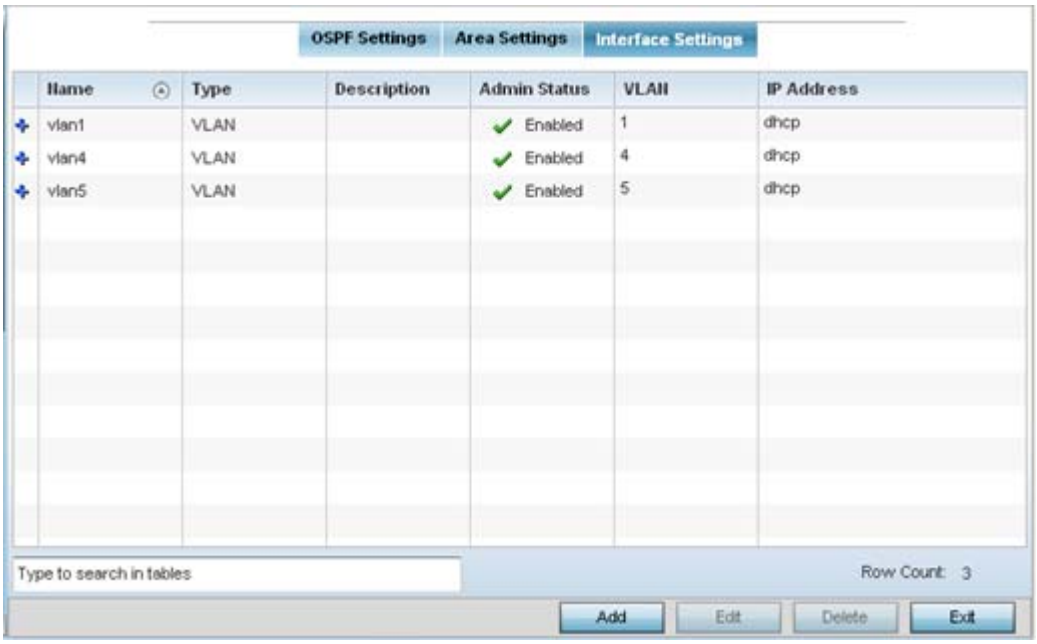


Figure 5-83 *OSPF Interface Settings screen*

18 Review the following **Interface Settings**:

Name	Displays the name defined for the interface configuration.
Type	Displays the type of interface.
Description	Lists each interface's 32 character maximum description.
Admin Status	Displays whether admin status privileges have been *enabled* or *disabled* for the OSPF route's virtual interface connection.
VLAN	Lists the VLAN IDs set for each listed OSPF route virtual interface.
IP Address	Displays the IP addresses defined as virtual interfaces for dynamic OSPF routes. Zero config and DHCP can be used to generate route addresses, or a primary and secondary address can be manually provided.

19 Select the **Add** button to define a new set of virtual interface basic settings, or **Edit** to update the settings of an existing virtual interface configuration.

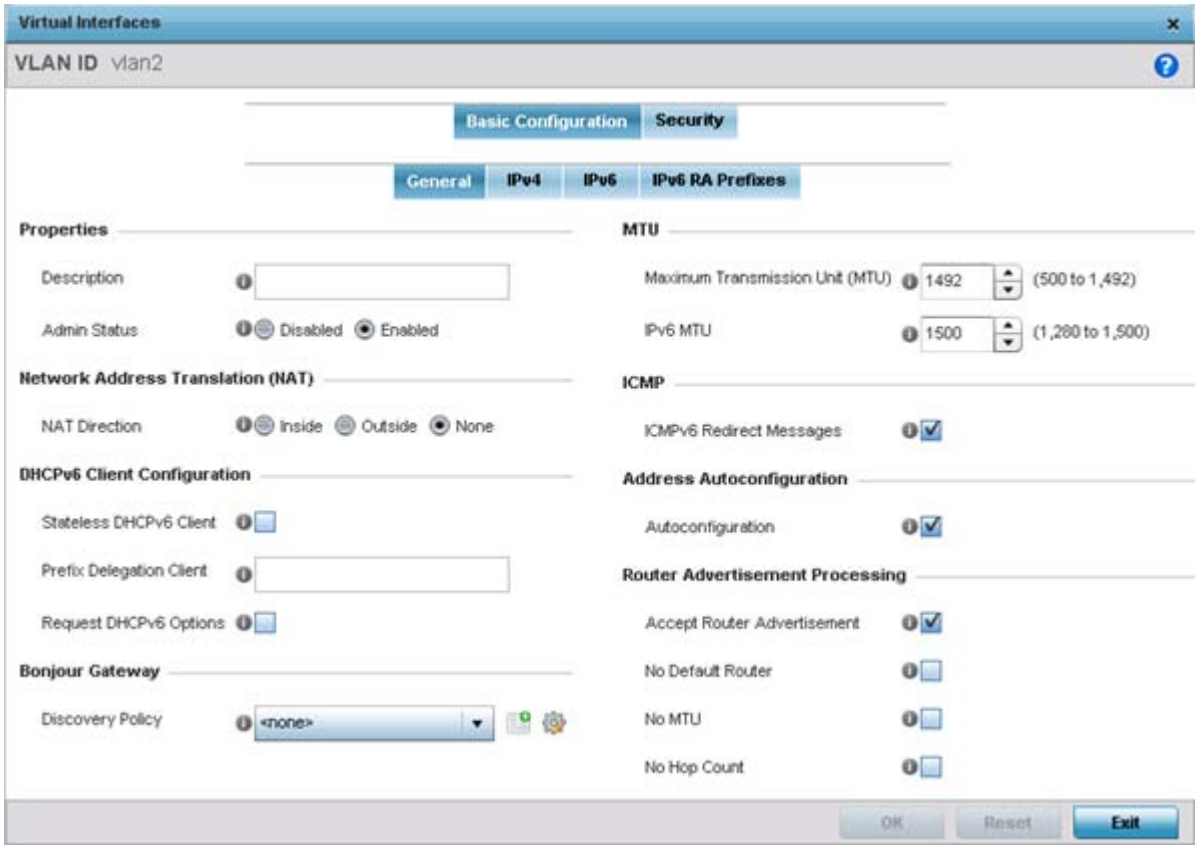


Figure 5-84 *OSPF Virtual Interface - Basic Configuration screen - General tab*

20 Within the **Properties** field, enter a 32 character maximum **Description** to help differentiate the virtual interface configuration used with this OSPF route. Enable/disable **Admin Status** as needed. They're enabled by default.

21 Define the **NAT Direction** as either *Inside*, *Outside* or *None*. *Network Address Translation* (NAT), is an Internet standard enabling a *local area network* (LAN) to use IP addresses for internal traffic (inside) and a second set of addresses for external (outside) traffic.

22 Set the following **DHCPv6 Client Configuration**. The *Dynamic Host Configuration Protocol for IPv6* (DHCPv6) provides a framework for passing configuration information.

Stateless DHCPv6 Client	Select this option to request information from the DHCPv6 server using stateless DHCPv6. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is disabled by default.
Prefix Delegation Client	Specify a 32 character maximum request prefix for prefix delegation from a DHCPv6 server over this virtual interface.
Request DHCPv6 Options	Select this option to request DHCPv6 options on this virtual interface. DHCPv6 options provide configuration information for a node that must be booted using the network rather than from locally. This setting is disabled by default.

23 Set the following **Bonjour Gateway** settings.Bonjour is Apple's implementation of zero-configuration networking (Zeroconf). Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates devices such as printers, other computers and services that these computers offer over a local network.

Bonjour provides a general method to discover services on a *local area network* (LAN). It allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with special DNS configuration, it can be extended to find services across broadcast domains.

From the drop-down, select the Bonjour Gateway discover policy. Select the **Create** icon to define a new Bonjour Gateway policy configuration or select the **Edit** icon to modify an existing Bonjour Gateway policy configuration.

24 Set the following MTU settings for the virtual interface:

Maximum Transmission Unit (MTU)	Set the PPPoE client *maximum transmission unit* (MTU) from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492.
IPv6 MTU	Set an IPv6 MTU for this virtual interface from 1,280 - 1,500. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. The default is 1,500.

25 Within the **ICMP** field, define whether ICMPv6 redirect messages are sent. Redirect requests data packets be sent on an alternative route. This setting is enabled by default.

26 Within the **Address Autoconfiguration** field, define whether to configure IPv6 addresses on this virtual interface based on the prefixes received in router advertisement messages. This setting is enabled by default.

27 Set the following **Router Advertisement Processing** settings for the virtual interface. Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

Accept RA	Enable this option to allow router advertisements over this virtual interface. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6)router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters.This setting is enabled by default.
No Default Router	Select this option to not consider routers present on this interface for default router selection. This setting is disabled by default.
No MTU	Select this option to not use the set MTU value for router advertisements on this virtual interface. This setting is disabled by default.
No Hop Count	Select this option to not use the hop count advertisement setting for router advertisements on this virtual interface. This setting is disabled by default.

28 Select **OK** to save the changes. Select Reset to revert to the last saved configuration.

29 Select the **IPv4** tab to set IPv4 settings for this virtual interface.

IPv4 is a connectionless protocol. It operates on a best effort delivery model that does not guarantee delivery or assures proper sequencing or avoidance of duplicate delivery (unlike TCP).

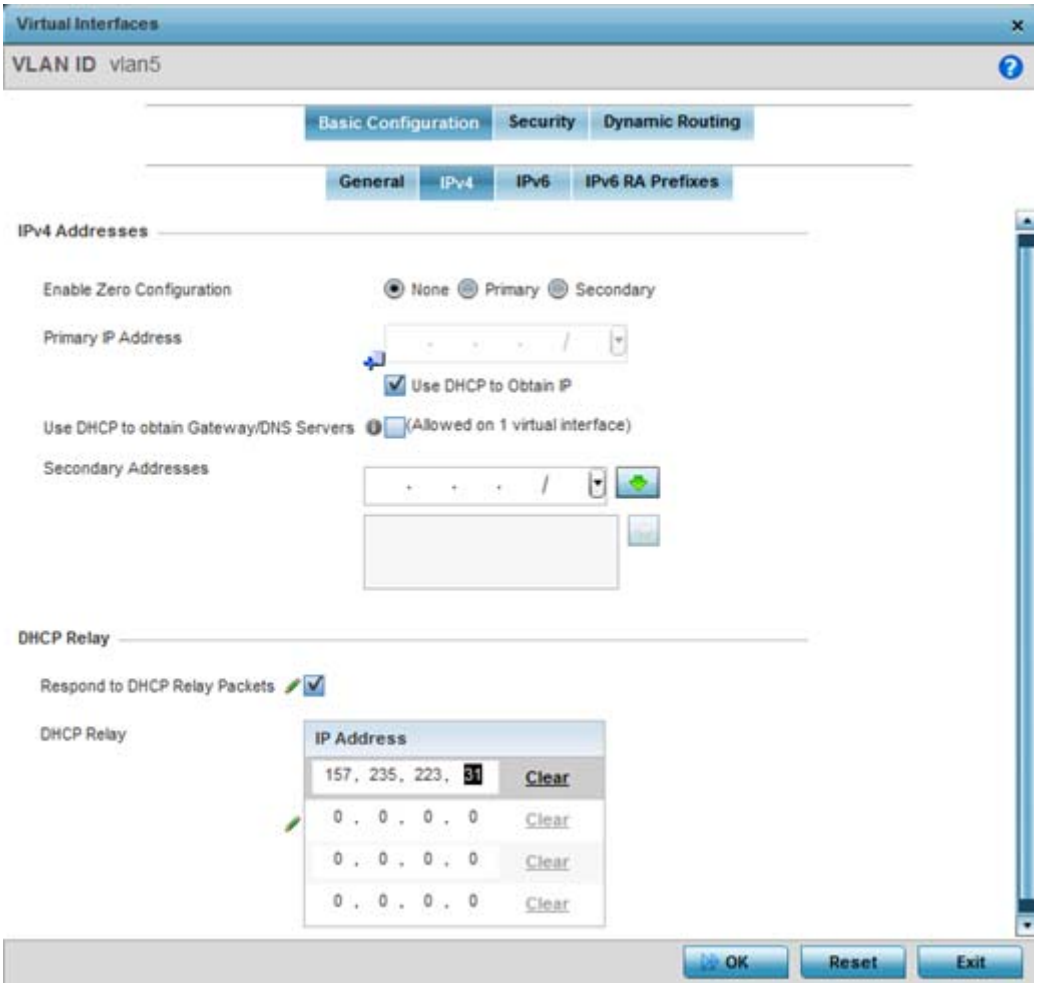


Figure 5-85 *Virtual Interfaces - Basic Configuration screen - IPv4 tab*

30 Set the following network information from within the **IPv4 Addresses** field:

Enable Zero Configuration	Zero Configuration can be a means of providing a primary or secondary IP addresses for the virtual interface. Zero configuration (or zero config) is a wireless connection utility included with Microsoft Windows XP and later as a service dynamically selecting a network to connect based on a user's preferences and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device. This value is set to None by default.
Primary IP Address	Define the IP address for the VLAN associated Virtual Interface.
Use DHCP to Obtain IP	Select this option to allow DHCP to provide the IP address for the Virtual Interface. Selecting this option disables the Primary IP address field.
Use DHCP to obtain Gateway/DNS Servers	Select this option to allow DHCP to obtain a default gateway address, and DNS resource for *one* virtual interface. This setting is disabled by default and only available when the Use DHCP to Obtain IP option is selected.
Secondary Addresses	Use the Secondary Addresses parameter to define additional IP addresses to associate with VLAN IDs. The address provided in this field is used if the primary IP address is unreachable.

31 Refer to the **DHCP Relay** field to set the DHCP relay server configuration used with the Virtual Interface.

Respond to DHCP Relay Packets	Select this option to allow the onboard DHCP server to respond to relayed DHCP packets on this interface. This setting is disabled by default.
DHCP Relays	Provide IP addresses for DHCP server relay resources. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When a DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.

32 Select **OK** to save the changes to the IPv4 configuration. Select **Reset** to revert to the last saved configuration.

33 Select the **IPv6** tab to set IPv6 settings for this virtual interface.

IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters.

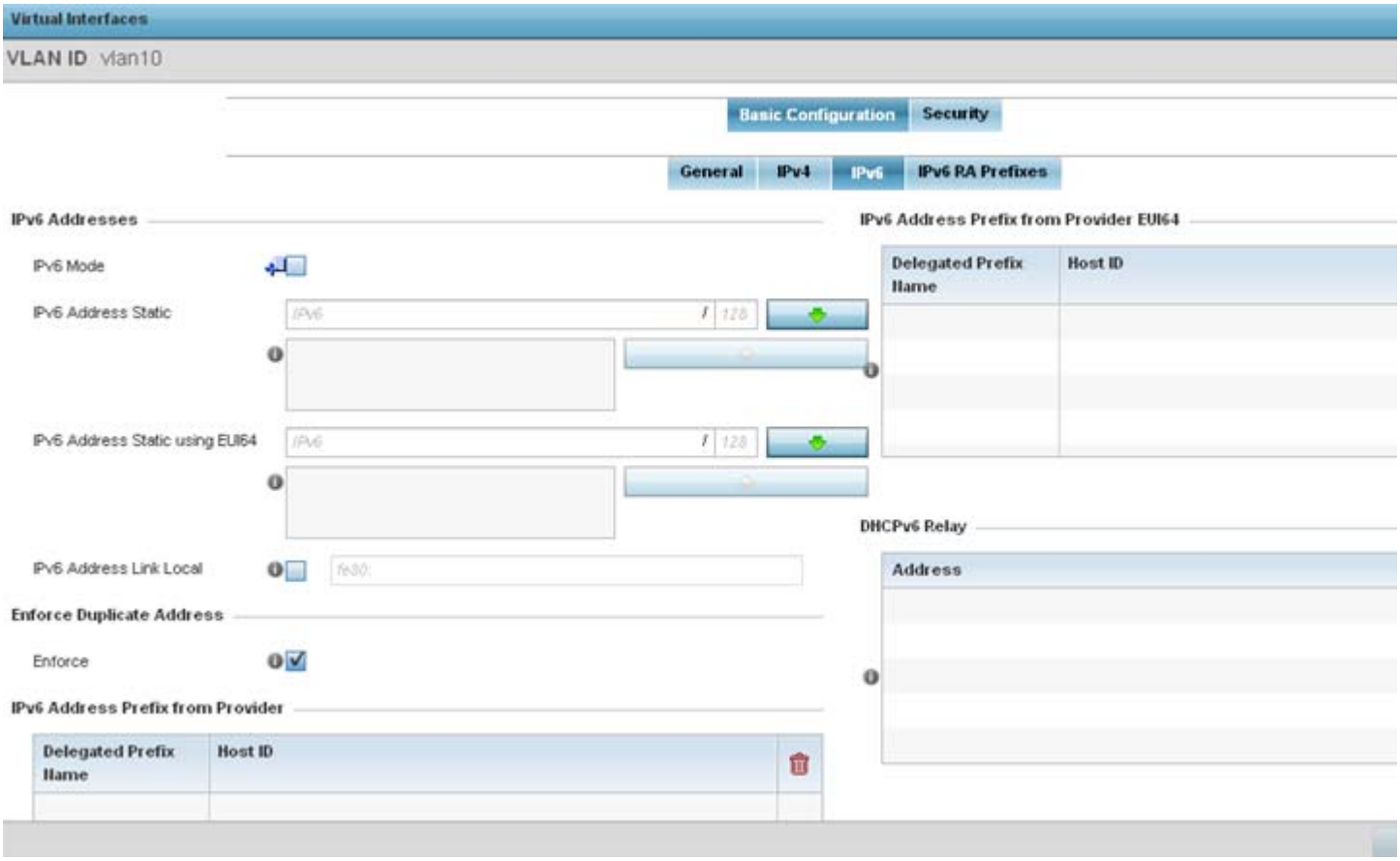


Figure 5-86 *Virtual Interfaces - Basic Configuration screen - IPv6 tab*

34 Refer to the **IPv6 Addresses** field to define how IP6 addresses are created and utilized.

IPv6 Mode	Select this option to enable IPv6 support on this virtual interface.
IPv6 Address Static	Define up to 15 global IPv6 IP addresses that can created statically. IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons.
IPv6 Address Static using EU164	Optionally set up to 15 global IPv6 IP addresses (in the EUI-64 format) that can created statically. The IPv6 EUI-64 format address is obtained through a 48-bit MAC address. The MAC is initially separated into two 24-bits, with one being an OUI (*Organizationally Unique Identifier*) and the other being client specific. A 16-bit 0xFFFE is then inserted between the two 24-bits for the 64-bit EUI address. IEEE has chosen FFFE as a reserved value which can only appear in EUI-64 generated from the an EUI-48 MAC address.
IPv6 Address Link Local	Provide the IPv6 local link address. IPv6 requires a link local address assigned to every interface the IPv6 protocol is enabled, even when one or more routable addresses are assigned.

35 Enable the **Enforce Duplicate Address** option to enforce duplicate address protection when any wired port is connected and in a forwarding state. This option is enabled by default.

36 Refer to the **IPv6 Address Prefix from Provider** table use prefix abbreviations (in EUI64 format) as shortcuts of the entire character set comprising an IPv6 formatted IP address.

37 Select **+ Add Row** to launch a sub screen wherein a new delegated prefix name and host ID can be defined.

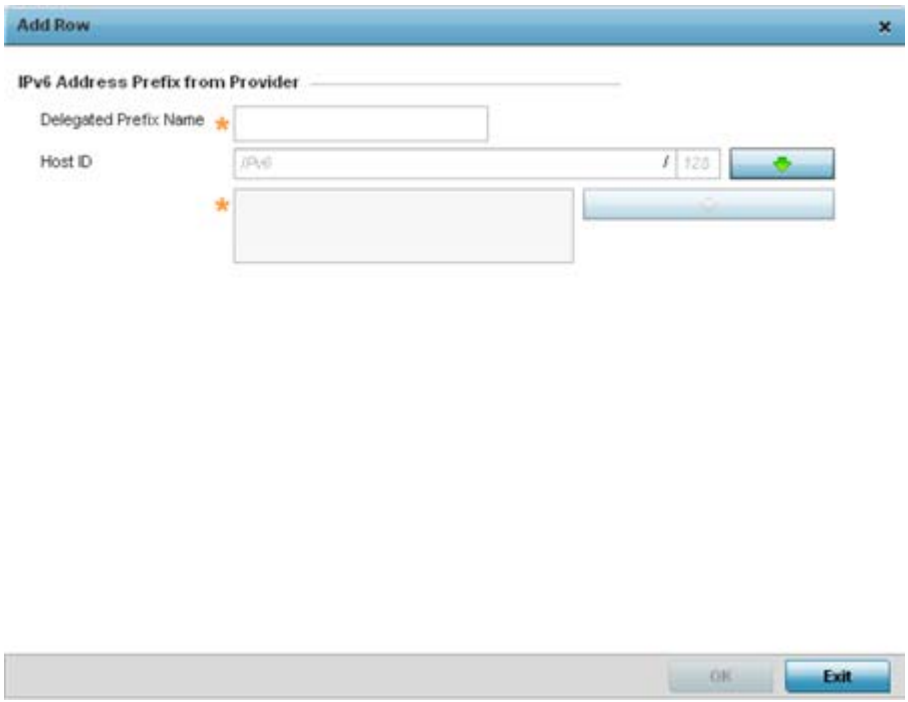


Figure 5-87 *Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider*

Delegated Prefix Name	Enter a 32 character maximum name for the IPv6 address prefix from provider.
Host ID	Define the subnet ID, host ID and prefix length.

38 Select **OK** to save the changes to the new IPv6 prefix from provider. Select **Exit** to close the screen without saving the updates.

39 Refer to the **IPv6 Address Prefix from Provider EUI64** table to review ISP provided prefix abbreviations.

40 Select **+ Add Row** to launch a sub screen wherein a new delegated prefix name and host ID can be defined in EUI64 format.

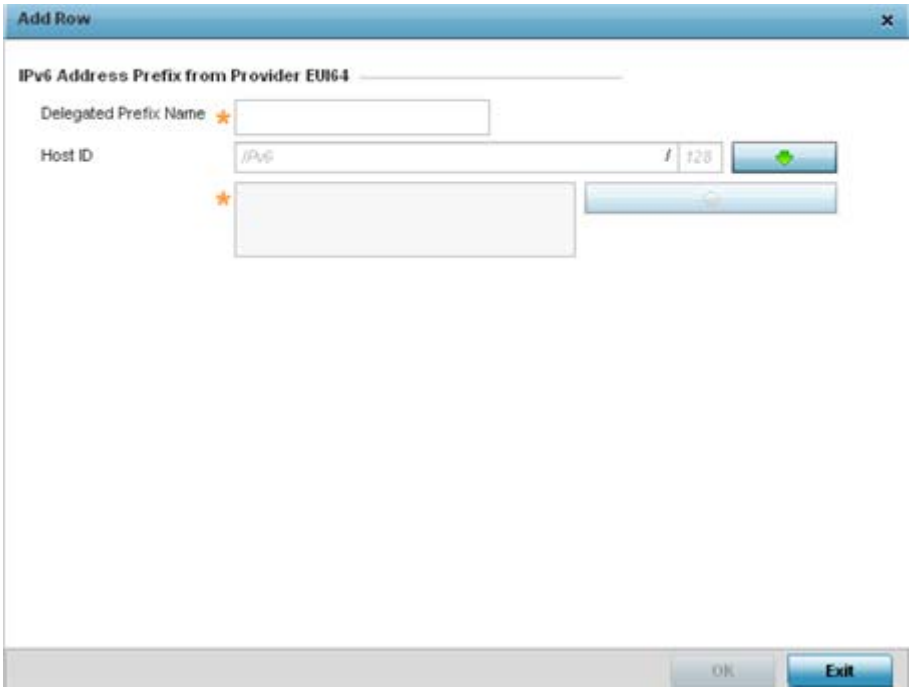


Figure 5-88 *Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider EUI64*

Delegated Prefix Name	Enter a 32 character maximum name for the IPv6 address prefix from provider in EUI format.
Host ID	Define the subnet ID and prefix length.

41 Select **OK** to save the changes to the new IPv6 prefix from provider in EUI64 format. Select **Exit** to close the screen without saving the updates.

42 Refer to the **DHCPv6 Relay** table to set the address and interface of the DHCPv6 relay.

The DHCPv6 relay enhances an extended DHCP relay agent by providing support in IPv6. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When A DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.

43 Select **+ Add Row** to launch a sub screen wherein a new DHCPv6 relay address and interface VLAN ID can be set.

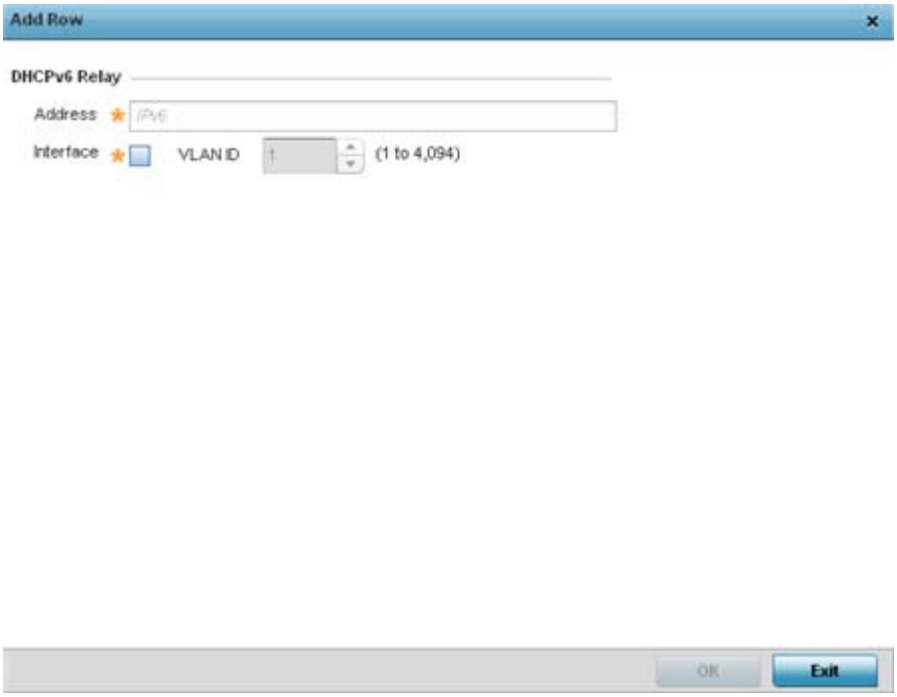


Figure 5-89 *Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add DHCPv6 Relay*

Address	Enter an address for the DHCPv6 relay. These DHCPv6 relay receive messages from DHCPv6 clients and forward them to DHCPv6 servers. The DHCPv6 server sends responses back to the relay, and the relay then sends these responses to the client on the local network link.
Interface	Select this option to enable a spinner control to define a VLAN ID from 1 - 4,094 used as the virtual interface for the DHCPv6 relay. The interface designation is only required for link local and multicast addresses. A local link address is a locally derived address designed for addressing on a single link for automatic address configuration, neighbor discovery or when no routing resources are available.

44 Select **OK** to save the changes to the DHCPv6 relay configuration. Select **Exit** to close the screen without saving the updates.

45 Select the **IPv6 RA Prefixes** tab.

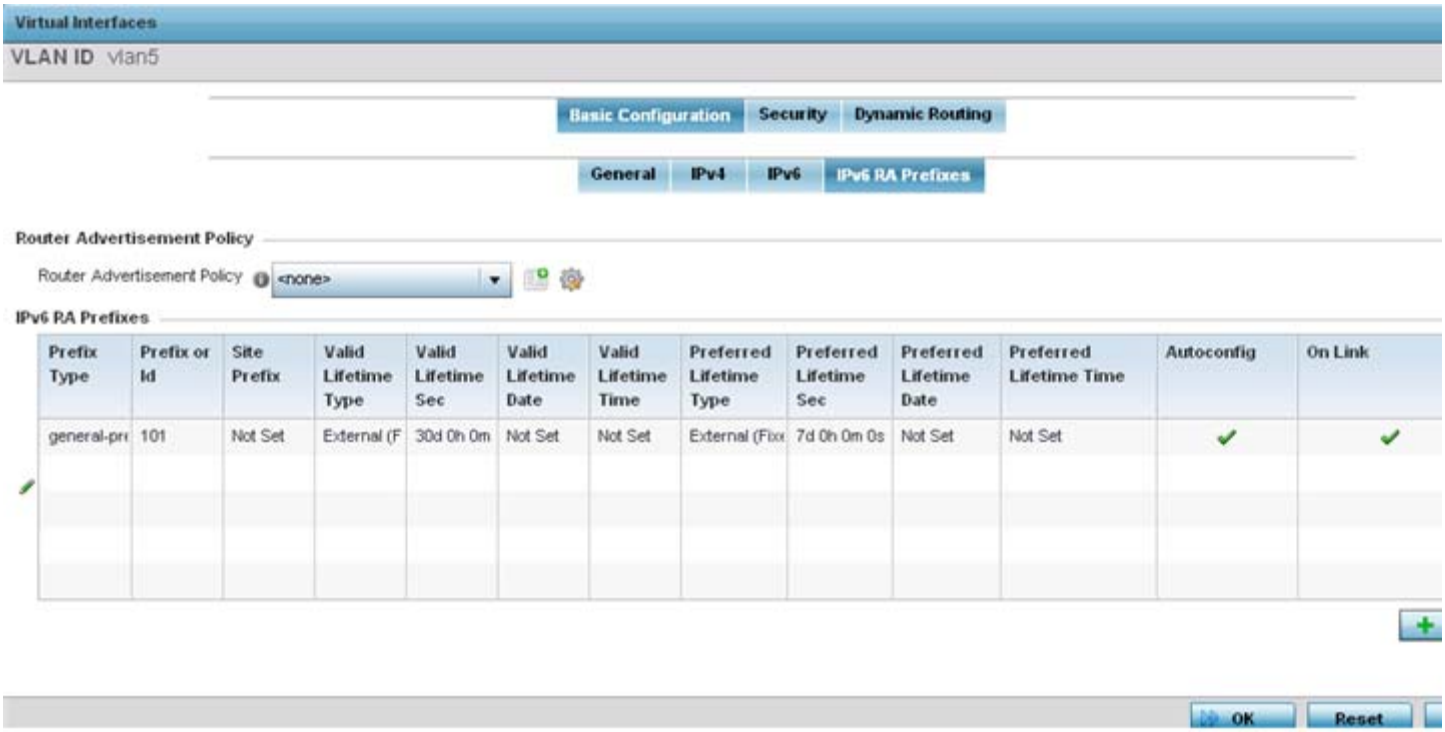


Figure 5-90 *Virtual Interfaces - Basic Configuration screen - IPv6 RA Prefixes tab*

46 Use the **Router Advertisement Policy** drop-down menu to select and apply a policy to the virtual interface.

Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

Review the configurations of existing IPv6 advertisement policies. If needed select **+ Add Row** to define the configuration of an additional IPv6 RA prefix.

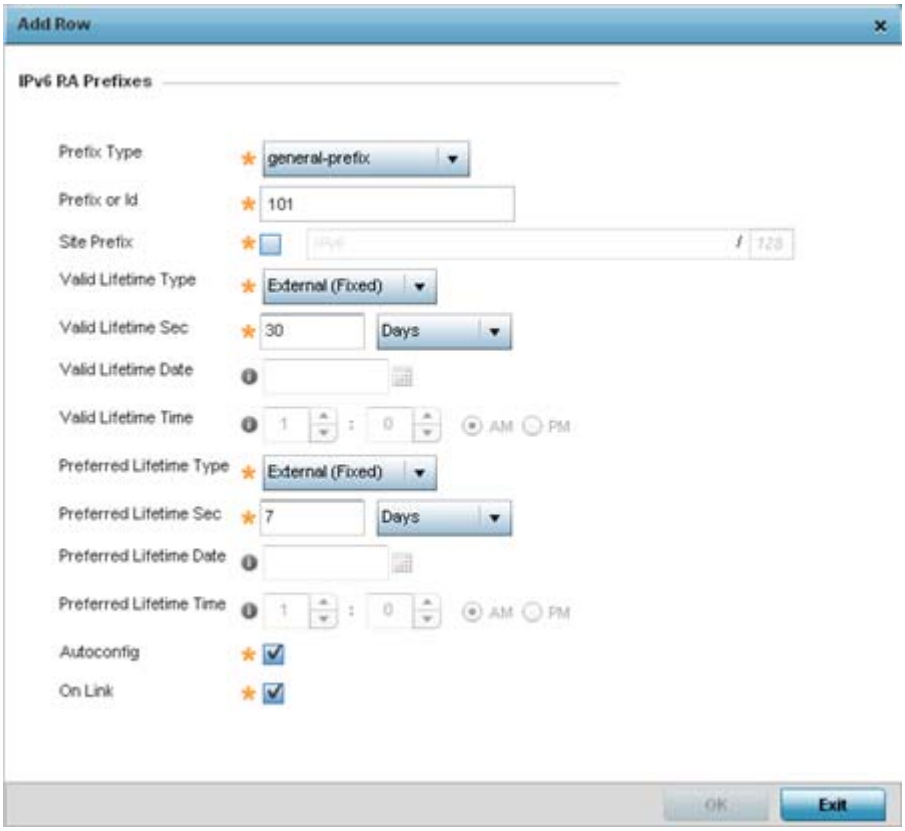


Figure 5-91 *Virtual Interfaces - Basic Configuration screen - Add IPv6 RA Prefix*

47 Set the following **IPv6 RA Prefix** settings:

Prefix Type	Set the prefix delegation type used with this configuration. Options include, *Prefix,* and *prefix-from-provider.* The default setting is Prefix. A prefix allows an administrator to associate a user defined name to an IPv6 prefix. A provider assigned prefix is made available from an *Internet Service Provider* (ISP) to automate the process of providing and informing the prefixes used.
Prefix or ID	Set the actual prefix or ID used with the IPv6 router advertisement.
Site Prefix	The site prefix is added into a router advertisement prefix. The site address prefix signifies the address is only on the local link.
Valid Lifetime Type	Set the lifetime for the prefix's validity. Options include *External (fixed), decrementing* and *infinite*. If set to External (fixed), just the *Valid Lifetime Sec* setting is enabled to define the exact time interval for prefix validity. If set to decrementing, use the lifetime date and time settings to refine the prefix expiry period. If the value is set for infinite, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is External (fixed).
Valid Lifetime Sec	If the lifetime type is set to *External (fixed),* set the *Seconds, Minutes, Hours* or *Days* value used to measurement criteria for the prefix's expiration. 30 days, 0 hours, 0 minutes and 0 seconds is the default lifetime.
Valid Lifetime Date	If the lifetime type is set to *External (fixed)*, set the date in MM/DD/YYYY format for the expiration of the prefix.

Valid Lifetime Time	If the lifetime type is set to *decrementing*, set the time for the prefix's validity.
Preferred Lifetime Type	Set the administrator preferred lifetime for the prefix's validity. Options include *External (fixed), decrementing* and *infinite*. If set to External (fixed), just the *Valid Lifetime Sec* setting is enabled to define the exact time interval for prefix validity. If set to decrementing, use the lifetime date and time settings to refine the prefix expiry period. If the value is set for infinite, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is External (fixed).
Preferred Lifetime Sec	If the administrator preferred lifetime type is set to *External (fixed)*, set the *Seconds, Minutes, Hours* or *Days* value used to measurement criteria for the prefix's expiration. 30 days, 0 hours, 0 minutes and 0 seconds is the default lifetime.
Preferred Lifetime Date	If the administrator preferred lifetime type is set to *External (fixed),* set the date in MM/DD/YYYY format for the expiration of the prefix.
Preferred Lifetime Time	If the preferred lifetime type is set to *decrementing,* set the time for the prefix's validity.
Autoconfig	Autoconfiguration entails generating a link-local address, global addresses via stateless address autoconfiguration and duplicate address detection to verify the uniqueness of the addresses on a link. This setting is enabled by default.
On Link	Select this option to keep the IPv6 RA prefix on the local link. The default setting is enabled.

48 Select **OK** to save the changes to the IPv6 RA prefix configuration. Select **Exit** to close the screen without saving the updates.

49 Select the **Security** tab.

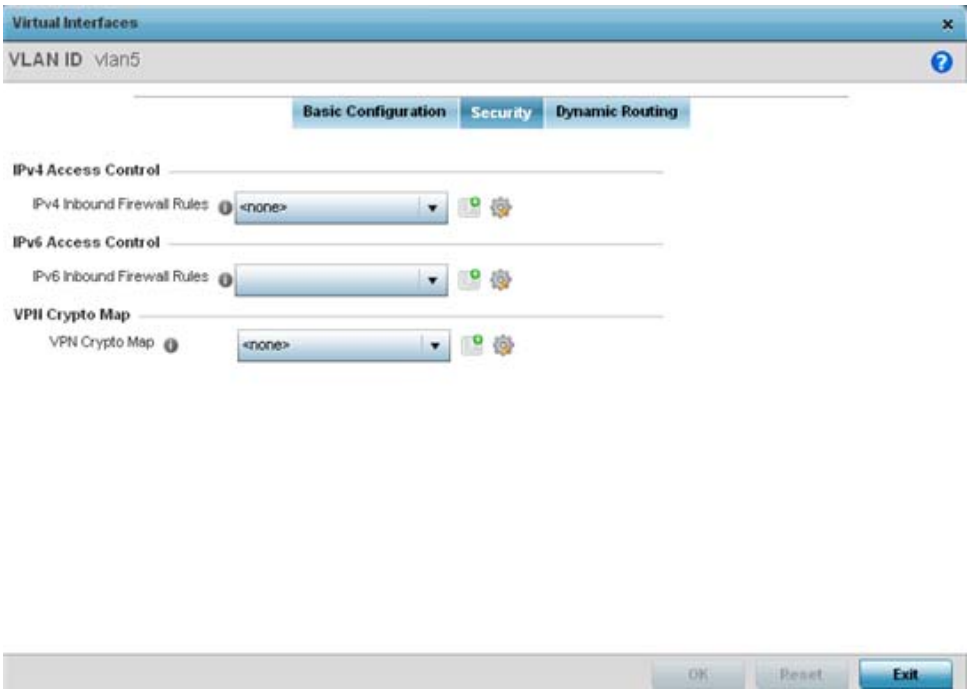


Figure 5-92 *OSPF Virtual Interface - Security screen*

50 Use the **IPv4 Inbound Firewall Rules** drop down menu to select the IPv4 specific inbound firewall rules to apply to this profile's virtual interface configuration. Select the **Create** icon to define a new IPv4 firewall rule configuration or select the **Edit** icon to modify an existing configuration.

IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, since it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP).

IPv4 and IPv6 are different enough to warrant separate protocols. IPv6 devices can alternatively use stateless address autoconfiguration. IPv4 hosts can use link local addressing to provide local connectivity.

51 Use the **IPv6 Inbound Firewall Rules** drop down menu to select the IPv6 specific inbound firewall rules to apply to this profile's virtual interface configuration. Select the **Create** icon to define a new IPv6 firewall rule configuration or select the **Edit** icon to modify an existing configuration.

IPv6 is the latest revision of the *Internet Protocol* (IP) replacing IPv4. IPV6 provides enhanced identification and location information for systems routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

52 Refer to the **VPN Crypto Map** drop down menu to attach an existing crypto map to this virtual interface. New crypto map configuration can be added by selecting the **Create** icon, or existing configurations can be modified by selecting the **Edit** icon.

Crypto Map entries are sets of configuration parameters for encrypting packets that pass through the VPN Tunnel. If a Crypto Map configuration does not exist suiting the needs of this virtual interface, select the **Create** icon to define a new Crypto Map configuration or the **Edit** icon to modify an existing configuration. For more information, see Overriding a Profile's VPN Configuration on page 5-207.

53 Use the **Web Filter** drop-down menu to select or override the **URL Filter** configuration applied to this virtual interface. Web filtering is used to restrict access to resources on the Internet.

54 Select **OK** to save the changes to the configuration. Select **Reset** to revert to the last saved configuration.

55 Select the **Dynamic Routing** tab.

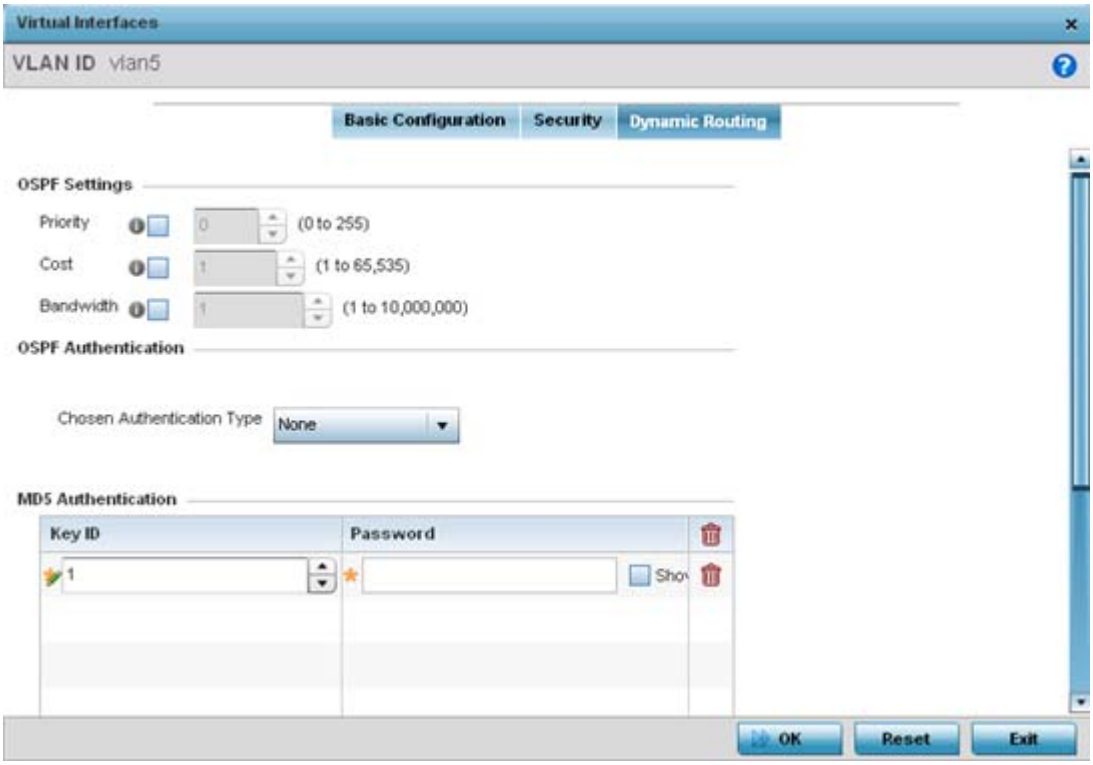


Figure 5-93 *OSPF Virtual Interface - Dynamic Routing screen*

56 Define or override the following parameters from within the **OSPF Settings** field

Priority	Select this option to set the OSPF priority used to select the network designated route. Use the spinner control to set the value from 0 - 255.
Cost	Select this option to set the cost of the OSPF interface. Use the spinner control to set the value from 1 - 65,535.
Bandwidth	Set the OSPF interface bandwidth (in Kbps) from 1 - 10,000,000.

57 Select the authentication type from the **Chosen Authentication Type** drop-down used to validate credentials within the OSPF dynamic route. Options include *simple-password*, *message-digest*, *null* and *None*. The default is None.

58 Select the **+ Add Row** button at the bottom of the **MD5 Authentication** table to add the Key ID and Password used for an MD5 validation of authenticator credentials. Use the spinner control to set the OSPF message digest authentication key ID. The available range is from 1 - 255. The password is the OSPF key either displayed as series or asterisks or in plain text (by selecting *Show*).

MD5 is a message digest algorithm using a cryptographic hash producing a 128-bit (16-byte) hash value, usually expressed in text as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

59 Select **OK** to save the changes to the configuration. Select **Reset** to revert to the last saved configuration.

5.2.8.11 Overriding a Profile's Border Gateway Protocol (BGP) Configuration

Overriding a Profile's Network Configuration

Border Gateway Protocol (BGP) is an inter-ISP routing protocol which establishes routing between ISPs. ISPs use BGP to exchange routing and reachability information between *Autonomous Systems* (AS) on the Internet. BGP makes routing decisions based on paths, network policies and/or rules configured by network administrators. The primary role of a BGP system is to exchange network reachability information with other BGP peers. This information includes information on AS that the reachability information traverses. This information is sufficient to create a graph of AS connectivity from which routing decisions can be created and rules enforced.

An *Autonomous System* (AS) is a set of routers under the same administration that use *Interior Gateway Protocol* (IGP) and common metrics to define how to route packets within the AS. AS uses inter-AS routing to route packets to other ASs. For an external AS, an AS appears to have a single coherent interior routing plan and presents a consistent picture of the destinations reachable through it.

Routing information exchanged through BGP supports only destination based forwarding (it assumes a router forwards packets based on the destination address carried in the IP header of the packet).

BGP uses TCP as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgement, and sequencing. BGP listens on TCP port 179. The error notification mechanism used in BGP assumes that TCP supports a *graceful* close (all outstanding data is delivered before the connection is closed).

To define or override a profile's BGP configuration:

1 Select **Devices** from the Configuration tab.

  The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

  Devices can also be selected directly from the *Device Browser* in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **BGP**.

NOTE: BGP is only supported on RFS4000, RFS6000, NX4500, NX6500, NX9000 and NX9500 model controllers and service platforms.

  The **General** tab displays by default.

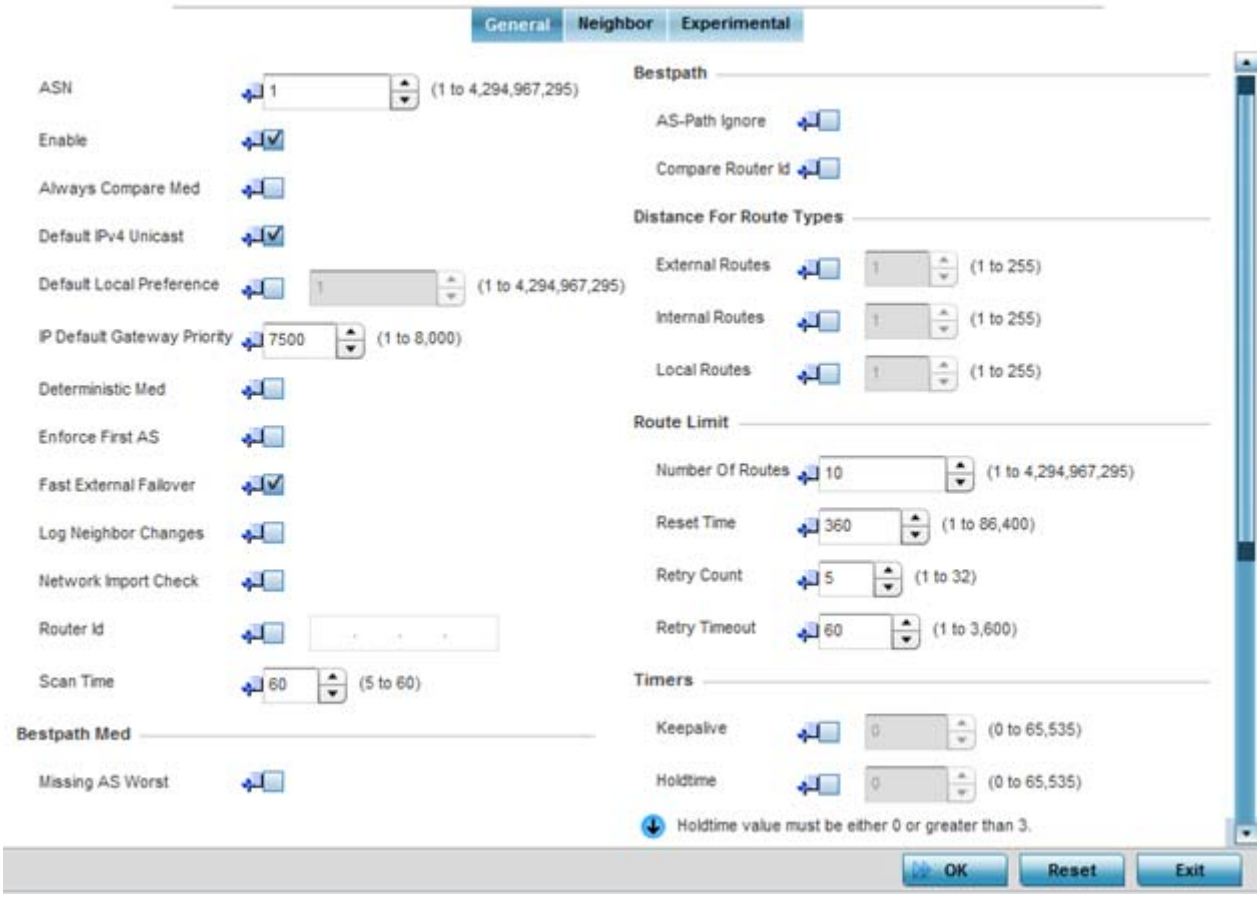


Figure 5-94 *Border Gateway Protocol - General tab*

6 Review the following BGP general configuration parameters to determine whether an override is warranted:

ASN	Define the *Autonomous System Number* (ASN). ASN is a set of routers under the same administration that use *Interior Gateway Protocol* (IGP) and common metrics to define how to route packets. Select a value from 1 - 4,294,967,295.
Enable	Enable to start BGP on this controller or service platform. BGP is only supported on RFS4000, RFS6000, NX4500, NX6500, NX9000 and NX9500 model controllers and service platforms. The default is disabled.
Always Compare Med	*Multi-exit Discriminator* (MED) is a value used by BGP peers to select the best route among multiple routes. When enabled, the MED value encoded in the route is always compared when selecting the best route to the host network. A route with a lower MED value is always selected over a route with a higher MED value. BGP does not discriminate between iBGP and eBGP when using MED for route selection. This option is mutually exclusive to the *Deterministic MED* option.
Default IPv4 Unicast	Select this option to enable IPv4 unicast traffic for neighbors. This option is disabled by default.
Default Local Preference	Select this option to enable a local preference for the neighbor. When enabled, set the local preference value (1 - 4,294,967,295).
IP Default Gateway Priority	Set the default priority value for the IP Default Gateway. Set a value from 1 - 8000. The default is 7500.

Deterministic Med	*Multi-exit Discriminator* (MED) is used by BGP peers to select the best route among multiple routes. When enabled, MED route values (from the same AS) are compared to select the best route. This best route is then compared with other routes in the BGP route table to select the best overall route. This option is mutually exclusive to the *Always Compare MED* option.
Enforce First AS	Select this option to deny any updates received from an external neighbor that does not have the neighbor's configured AS at the beginning of the received AS path parameter. This enhances security by not allowing traffic from an unauthorized AS. This setting is disabled by default.
Fast External Failover	Select this option to immediately reset the BGP session on the interface once the BGP connection goes down. Normally, when a BGP connection goes down, the device waits for the expiry of the duration specified in *Holdtime* parameter before bringing down the interface. This setting is enabled by default.
Log Neighbor Changes	Select this option to enable logging of changes in routes to neighbor BGP peers. This enables the logging of only the changes in neighbor routes. All other events must be explicitly turned on using debug commands. This setting is disabled by default.
Network Import Check	Select this option to enable a network import check to ensure consistency in advertisements. This setting is disabled by default.
Router ID	Select this option to manually configure the router ID for this BGP supported controller or service platform. The router ID identifies the device uniquely. When no router ID is specified, the IP address of the interface is considered the router ID. This setting is disabled by default.
Scan Time	Select this option to set the scanning interval for updating BGP routes. This interval is the period between two consecutive scans the BGP device checks for the validity of routes in its routing table. To disable this setting, set the value to Zero (0). The default setting is 60 seconds.

7 Optionally select the **Missing AS Worst** option to treat any path that does not contain a MED value as the least preferable route. This setting is disabled by default.

8 Review the following **Bestpath** parameters:

AS-Path Ignore	Select this option to prevent an AS path from being considered as a criteria for selecting a preferred route. The route selection algorithm uses the AS path as one of the criteria when selecting the best route. When this option is enabled, the AS path is ignored.
Compare Router Id	Select this option to use the router ID as a selection criteria when determining a preferred route. The route selection algorithm uses various criteria when selecting the best route. When this option is enabled, the router ID is used to select the best path between two identical BGP routes. The route with the lower route ID is selected over a route with a higher route id.

9 Set or override the following **Distance for Route Types**. The distance parameter is a rating of route trustworthiness. The greater the distance, the lower the trust rating. The distance can be set for each type of route indicating its trust rating.

External Routes	External routes are those routes learned from a neighbor of this BGP device. Set a value from 1 - 255.

Internal Routes	Internal routes are those routes learned from another router within the same AS. Set a value from 1 - 255.
Local Routes	Local routes are those routes being redistributed from other processes within this BGP router. Set a value from 1 - 255.

10 Set or override the following **Route Limit** parameters:

Number of Routes	Configures the number of routes that can be stored on this BGP router. Set this value based on the available memory on this BGP router. Configure a value from 1 - 4,294,967,295. The default value is 9,216 routes.
Reset Time	Configures the reset time. This is the time limit after which the *Retry Count* value is set to Zero (0). Set a value from 1- 86,400 seconds.
Retry Count	Configures the number of time the BGP process is reset before it is shut down. Once shut down, the BGP process has to be started manually. The BGP process is reset if it is flooded with route entries that exceed its number of routes. Set a value from 1 - 32.
Retry Timeout	Configures the time duration in seconds the BGP process is shutdown temporarily before a reset of the process is attempted. Set a value from 1 - 3,600 seconds.

11 Set or override the following **Timers**:

Keepalive	Set the duration, in seconds, for the keep alive timer used to maintain connections between BGP neighbors. Set a value from 0 - 65,535 seconds.
Holdtime	Set the time duration, in seconds, for the hold (delay) of packet transmissions.

12 Set the following **Aggregate Address** parameters:

Aggregate addresses are used to minimize the size of the routing tables. Aggregation combines the attributes of several different routes and advertises a single route. This creates an aggregation entry in the BGP routing table if more specific BGP routes are available in the specified address range.

IP Prefix	Enter an IP address and mask used as the aggregate address.
Summary Only	Select this option to advertise the IP Prefix route to the BGP neighbor while suppressing the detailed and more specific routes.
As Set	Generates AS set path information. Select to enable. When selected, it creates an aggregate entry advertising the path for this route, consisting of all elements contained in all the paths being summarized. Use this parameter to reduce the size of path information by listing the AS number only once, even if it was included in the multiple paths that were aggregated.

13 Set the following **Distance for IP Source Prefix** fields:

IP Source Prefix	Enter an IP address and mask used as the prefix source address.
Admin Distance	Use the spinner control to set the BGP route's admin distance from 1 - 255.
IP Access List	Provide the IP address used to define the prefix list rule.

14 Configure the following **Network** values.

Network	Configure an IP address to broadcast to neighboring BGP peers. This network can be a single IP address or a range of IP addresses in *A.B.C.D/M* format.
Pathlimit	Configure the maximum path limit for this AS. Set a value from 1 - 255 AS hops.
Backdoor	Select this option to indicate to border devices this network is reachable using a backdoor route. A backdoor network is treated the same as a local network, except it is not advertised. This setting is disabled by default.
Route Map	Select an existing route map as a method of controlling and modifying routing information. The control of route information occurs using route redistribution keys.

15 Configure the following **Route Redistribute** values.

Route Type	Use the drop-down menu to define the route type as either *connected*, *kernal*, *ospf* or *static*.
Metric	Select this option to set a numeric route metric used for route matching and permit designations.
Route Map	Select an existing route map as a method of controlling and modifying routing information. The control of route information occurs using route redistribution keys.

16 Select **OK** to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

17 Select the **Neighbor** tab.

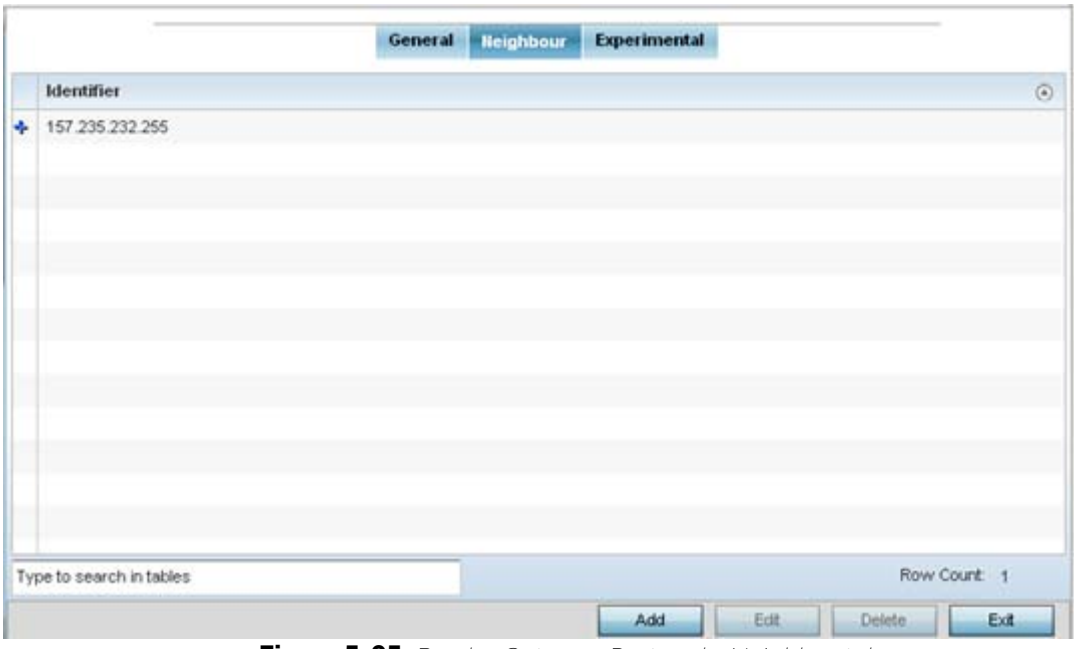


Figure 5-95 *Border Gateway Protocol - Neighbor tab*

The **Neighbor** tab displays a list of configured BGP neighbor devices identified by their IP address.

18 Select **Add** to add a new BGP neighbor configuration or select an existing Identifier and select Edit to modify it. The following screen displays with the General tab displayed by default.

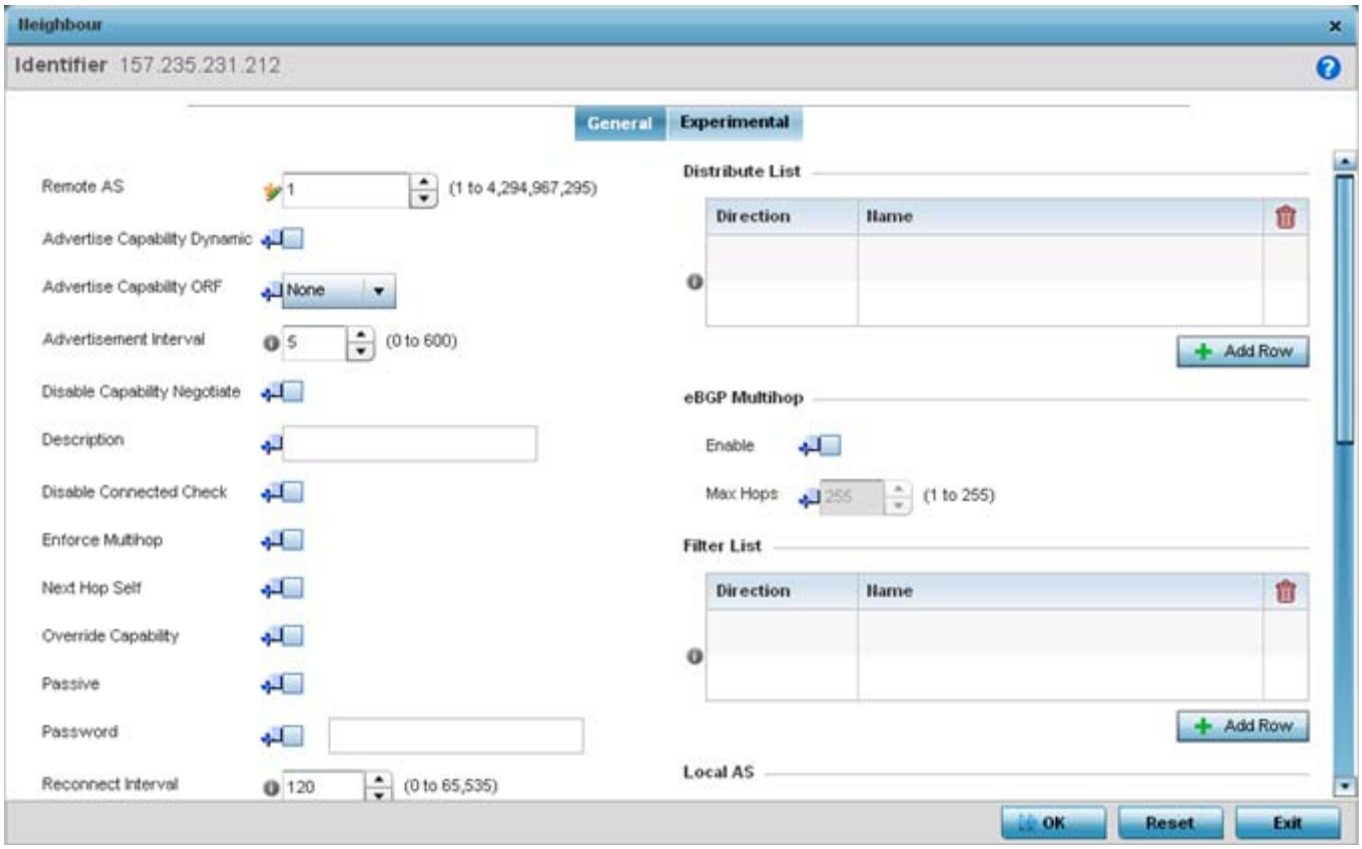


Figure 5-96 *Border Gateway Protocol - Neighbor tab - Add/Edit screen*

The **General** tab displays the different configuration parameters for the neighbor BGP device.

19 Configure the following common parameters:

Remote AS	Define the *Autonomous System Number* (ASN) for the neighbor BGP device. ASN is a set of routers under the same administration that use *Interior Gateway Protocol* (IGP) and common metrics to define how to route packets within the AS. Set a value from 1 - 4,294,967,295.
Advertise Capability Dynamic	Select this option to show a neighbor device's capability to advertise or withdraw and address capability to other peers in a non-disruptive manner. This setting is disabled by default.
Advertise Capability ORF	Select this option to enable *Outbound Router Filtering* (ORF) and advertise this capability to peer devices. ORFs send and receive capabilities to lessen the number of updates exchanged between BGP peers. By filtering updates, ORF minimizes update generation and exchange overhead. The local BGP device advertises ORF in the *send* mode. The peer BGP device receives the ORF capability in *receive* mode. The two devices exchange updates to maintain the ORF for each router. Only a peer group or an individual BGP router can be configured to be in *receive* or *send* mode. A member of a peer group cannot be configured.

Advertisement Interval	Use the *Advertisement Interval* to set the minimum interval between sending BGP router updates. Sending too many router updates creates flapping of routes leading to possible disruptions. Set a minimum interval so that the BGP routing updates are sent after the set interval in seconds. The default is 5 seconds.
Disable Capability Negotiate	Select to disable capability negotiation with BGP neighbors. This is to allow compatibility with older BGP versions that have no capability parameters used in the *open* messages between peers. This setting id disabled by default.
Description	Provide a 80 character maximum description for this BGP neighbor device.
Disable Connected Check	If utilizing loopback interfaces to connect single-hop BGP peers, enable the neighbor disable connected check before establishing a the BGP peering session.This setting is disabled by default.
Enforce Multihop	A *multihop* route is a route to external peers on indirectly connected networks. Select to enforce neighbors to perform multi-hop check. This setting is disabled by default.
Next Hop Self	Select to enable *Next Hop Self*. Use this to configure this device as the next hop for a BGP speaking neighbor or peer group. This allows the BGP device to change the next hop information that is sent to iBGP peers. The next hop address is set to the IP address of the interface used to communicate with the eBGP neighbor. This setting is disabled by default.
Override Capability	Select this to enable the ability to override capability negotiation result. This setting is disabled by default.
Passive	Select this option to set this BGP neighbor as passive. When a neighbor is set as passive, the local device should not attempt to *open* a connection to this device. This setting is disabled by default
Reconnect Interval	Set a reconnection interval for peer BGP devices from 0 - 65,535 seconds. The default setting is 120 seconds.
Send Community	Select this option to ensure the community attribute is sent to the BGP neighbor. The community attribute groups destinations in a certain community and applies routing decisions based on the community. On receiving community attribute, the BGP router announces it to the neighbor.
Shutdown	Select this option to administratively shutdown this BGP neighbor. This setting is disabled by default.
Soft Reconfiguration Inbound	Select this option to store updates for inbound soft reconfiguration. Soft-reconfiguration can be used in lieu of BGP route refresh capability. Selecting this option enables local storage of all received routes and their attributes. This requires additional memory on the BGP device. When a soft reset (inbound) is performed on the neighbor device, the locally stored routes are reprocessed according to the inbound policy. The BGP neighbor connection is not affected.

Update Source	Select this option to allow internal BGP sessions to use any operational interface for TCP connections. Use *Update Source* in conjunction with any specified interface on the router. The loopback interface is the interface that is most commonly used with this command. The use of loopback interface eliminates a dependency and BGP does not have to rely on the availability of a particular interface for making TCP connections. This setting is disabled by default.
Unsuppress Map	Enable *Unsuppress Map* to selectively advertise more precise routing information to this neighbor. Use this in conjunction with the *Route Aggregate* command. The route aggregate command creates a route map with a IP/mask address that consolidates the subnets under it. This enables a reduction in number of route maps on the BGP device to one entry that encompasses all the different subnets. Use Unsuppress Map to selectively allow/deny a subnet or a set of subnets. Use the *Create* icon to create a new route map. Use the *Edit* icon to edit an existing route map list after selecting it.
Weight	Select to set the weight of all routes learned from this BGP neighbor. Weight is used to decide the preferred route when the same route is learned from multiple neighbors. The highest weight is always chosen.

20 Configure or set the following **Default Originate** parameters. Default originate is used by the local BGP router to send the default route 0.0.0.0 to its neighbor for use as a default route.

Enable	Select to enable *Default* Originate on this BGP neighbor. This setting is disabled by default.
Route Map	Use the drop-down menu to select a route map (enhanced packet filter) to use as the *Default Originate* route.

21 Configure or set the following **Route Map** parameters. This configures how route maps are applied for this BGP neighbor.

Direction	Use the drop-down menu to configure the direction on which the selected route map is applied. Select one from *in*, *out*, *export* or *import.*
Route Map	Use the drop-down menu to select the route map to use with this BGP neighbor. Use the *Create* icon to create a new route map. Use the *Edit* icon to edit an existing route map after selecting it.

22 Configure or set the following **Distribute List** parameters. Up to 2 distribute list entries can be created.

Direction	Use the drop-down menu to configure the direction on which the selected IP access list is applied. Select either *in* or *out.*
Name	Use the drop-down menu to select the route map to use with this BGP neighbor. Use the *Create* icon to create a new IP Access list. Use the *Edit* icon to edit an existing IP Access list after selecting it.

23 Configure or set the following **eBGP Multihop** parameters. This configures the maximum number of hops that can be between eBGP neighbors not directly connected to each other.

Enable	Select to enable *eBGP Multihop* on this BGP neighbor.
Max Hops	Set the maximum number of hops between eBGP neighbors not connected directly. Select a value from 1 - 255.

24 Configure or set the following **Filter List** parameters. Up to 2 filter list entries can be created.

Direction	Use the drop-down menu to configure the direction on which the selected AS Path list is applied. Select either *in* or *out.*
Name	Use the drop-down menu to select the AS Path list to use with this BGP neighbor. Use the *Create* icon to create a new AS Path list. Use the *Edit* icon to edit an existing AS Path list after selecting it.

25 Configure or set the following **Local AS** parameters.

CAUTION: This is an experimental feature and its actual operation may be unpredictable.

AS Number	Specify the local *Autonomous System* (AS) number. Select from 1 - 4,294,967,295.
No Prepend	Select to enable. When enabled, the local AS number is not prepended to route updates from eBGP peers.

26 Configure or set the following **Maximum Prefix** value. This configures the maximum number of prefix that can be received from a BGP neighbor.

Prefix Limit	Sets the maximum number of prefix that can be received from a BGP neighbor. Select from 1 - 4,294,967,295. Once this threshold is reached, the BGP peer connection is reset.
Threshold Percent	Sets the threshold limit for generating a log message. When this percent of the *Prefix Limit* is reached, a log entry is generated. For example if the *Prefix Limit* is set to 100 and *Threshold Percent* is set to 65, then after receiving 65 prefixes, a log entry is created.
Restart Limit	Sets the number of times a reset BGP peer connection is restarted. Select a value from 1 - 65535.
Warning Only	Select to enable. When the number of prefixes specified in *Prefix Limit* field is exceeded, the connection is reset. However, when this option is enabled, the connection is not reset and an event is generated instead. This setting is disabled by default.

27 Configure or set the following **Prefix List** parameters. Up to 2 prefix list entries can be created.

Direction	Use the drop-down menu to configure the direction on which the selected IP prefix list is applied. Select either *in* or *out.*
Name	Use the drop-down menu to select the IP prefix list to use with this BGP neighbor. Use the *Create* icon to create a new IP prefix list or select the *Edit* icon to edit an existing IP prefix list after selecting it.

28 Set or override the following **Timers** for this BGP neighbor:

Keepalive	Set the time duration in seconds for keepalive. The keep alive timer is used to maintain connections between BGP neighbors. Set a value from 1 - 65,535 seconds.
Holdtime	Set the time duration in seconds for the hold time.

29 Select **OK** to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

30 Select the **Experimental** tab.

CAUTION: This is an experimental feature and its actual operation may be unpredictable.

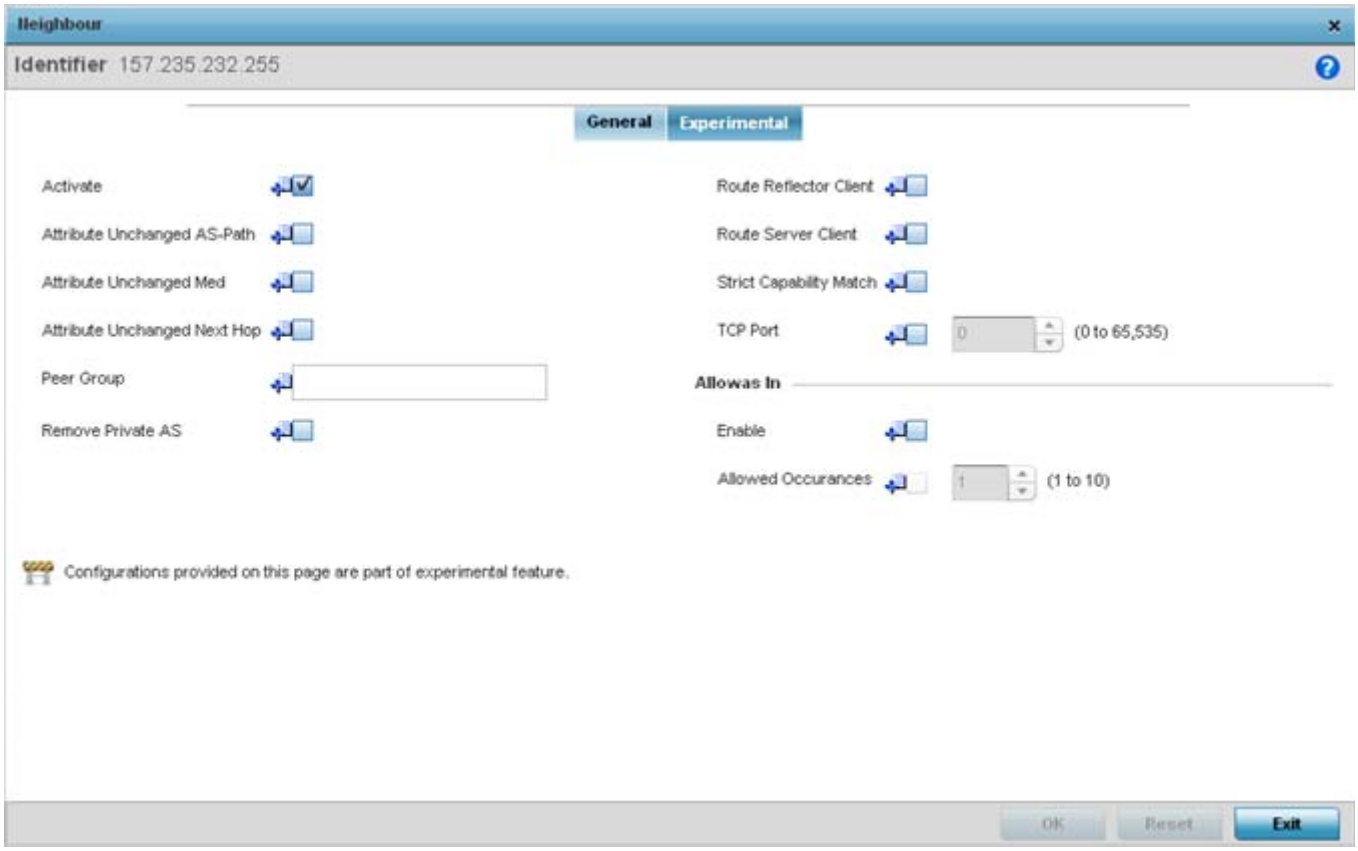


Figure 5-97 *Border Gateway Protocol - Neighbor tab - Experimental tab*

31 Set the following **Experimental** BGP parameters:

Activate	Enable an address family for this neighbor. This setting is enabled by default.
Attribute Unchanged AS-Path	Select to enable propagating AS path BGP attribute unchanged to this neighbor BGP device. This setting is enabled by default.
Attribute Unchanged Med	Select to enable propagating MED BGP attribute unchanged to this neighbor BGP device. This setting is enabled by default.
Attribute Unchanged Next Hop	Select to enable propagating the next hop BGP attribute value unchanged to this neighbor BGP device. This setting is enabled by default.
Peer Group	Set the peer group for this BGP neighbor device. Peer groups are a set of BGP neighbors with the same update policies. This facilitates the updates of various policies, such as, distribute lists and filter lists. The peer group can be configured as a single entity. Any changes made to the peer group is propagated to all members.

Remove Private AS	Select this option to remove the private *Autonomous System* (AS) number from outbound updates. Private AS numbers are not advertised to the Internet. This option is used with external BGP (eBGP) peers only. The router removes the AS numbers only if the update includes private AS numbers. If the update includes both private and public AS numbers, the system treats it as an error.
Route Reflector Client	Select this option to enable this BGP neighbor as a route reflector client for the local router. Route reflectors control large numbers of iBGP peering.Using route reflection, the number of iBGP peers is reduced. This option configures the local BGP device as a route reflector and the neighbor as its route reflector client. This setting is disabled by default.
Route Server Client	Select this option to enable this neighbor BGP device to act as a route server client. This setting is disabled by default.
Strict Capability Match	Select this option to enable a strict capability match before allowing a neighbor BGP peer to open a connection. When capabilities do not match, the BGP connection is closed. This setting is disabled by default.
TCP Port	Select to enable configuration of non-standard BGP port for this BGP neighbor. By default the BGP port number is 179. To configure a non standard port for this BGP neighbor, use the control to set the port number. Select a value from 1 - 65,535.

32 Configure or set the following **Allowas In** parameters.

This configures the Provider Edge (PE) routers to allow the re-advertisement of all prefixes containing duplicate Autonomous System Numbers (ASN). This creates a pair of VPN Routing/Forwarding (VRF) instances on each PE router to receive and re-advertise prefixes. The PE router receives prefixes with ASNs from all PE routers and advertises to its neighbor PE routers on one VRF. The other VRF receives prefixes with ASNs from the Customer Edge (CE) routers and re-advertises them to all PE routers in the configuration.

Enable	Select this option to enable re-advertisement of all prefixes containing duplicate ASNs.
Allowed Occurrences	Set the maximum number of times an ASN is advertised. Select a value in the rage 1 - 10.

33 Select **OK** to save the changes and overrides. Select **Reset** to revert to the last saved configuration. Select **Exit** to close this window and go back to the main screen.

34 Select the **Experimental** tab from the BGP main screen.

CAUTION: This is an experimental feature and its actual operation may be unpredictable.

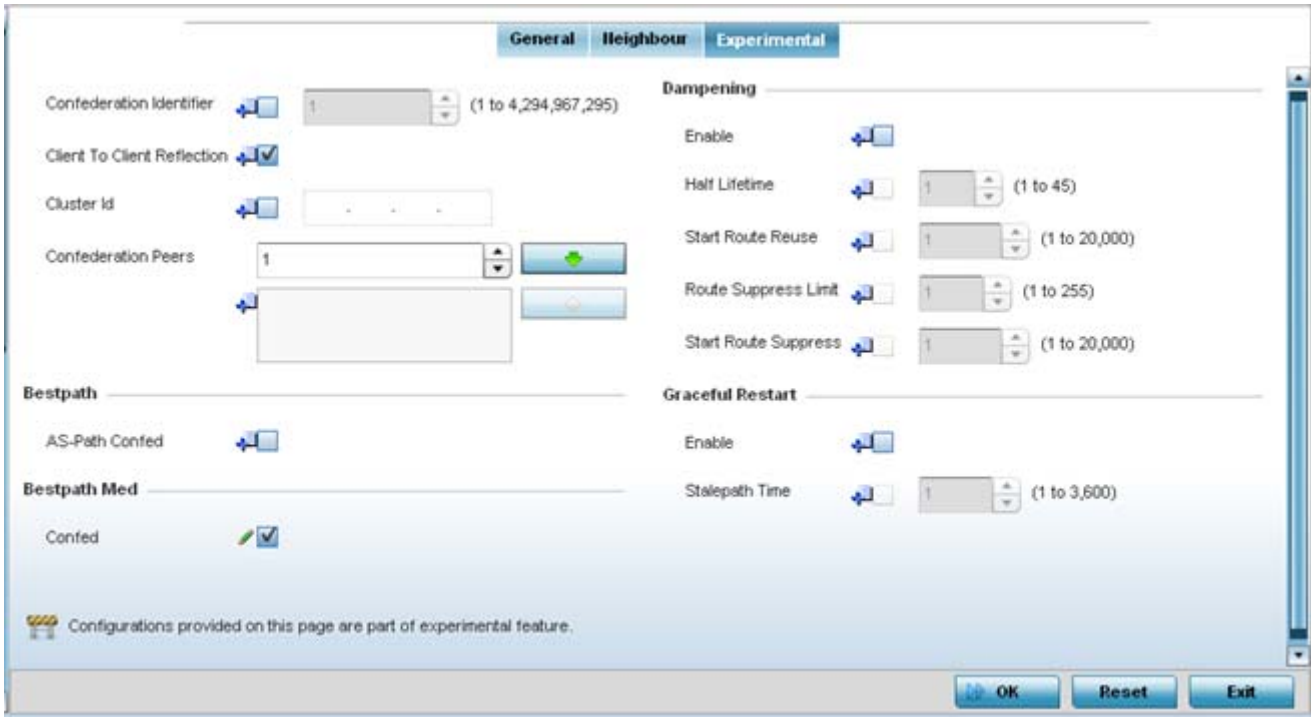


Figure 5-98 *Border Gateway Protocol - Experimental tab*

35 Set the following **Experimental** BGP features:

Confederation Identifier	Enable and set a *confederation identifier* to allow an AS to be divided into several ASs. This confederation is visible to external routers as a single AS. Select a value from 1 - 4,294,967,295.
Client to Client Reflection	Select to enable client-to-client route reflection. Route reflectors are used when all iBGP speakers are not fully meshed. If the clients are fully meshed, the route-reflectors are not required. The default is enabled.
Cluster ID	Select to enable and set a Cluster ID if the BGP cluster has more than one route-reflectors. A cluster generally consists of a single route-reflector and its clients. The cluster is usually identified by the router ID of this single route-reflector. Sometimes, to increase the redundancy, a cluster might have more than one route-reflectors configured. In this case, all route-reflectors in the cluster are identified by the Cluster ID. Select a value from 1 - 4,294,967,295.
Confederation Peers	Use this spinner to select the confederation members. Once selected, select the *Down Arrow* button next to this control to add the AS as a confederation member. Multiple AS configurations can be added to the list of confederation members. To remove an AS as a confederation member, select the AS from the list and select the *Up Arrow* button next to the list.

36 Configure or set the following **Bestpath** parameter:

AS-Path Confed	Select this option to allow the comparison of the confederation AS path length when selecting the best route. This indicates the AS confederation path length must be used, if available, in the BGP path when deciding the best path.

37 Configure or set the following **Bestpath Med** parameter:

Confed	Select to enable. Use this option to allow comparing MED when selecting the best route when learned from confederation peers. This indicates that MED must be used, when available, in the BGP best path when deciding the best path between routes from different confederation peers.

38 Configure or set the following **Dampening** parameters.

Dampening minimizes the instability caused by route flapping. A penalty is added for every flap in the flapping route. As soon as the total penalty reaches the Route Suppress Limit value, the advertisement of this route is suppressed. This penalty is delayed when the time specified in Half Lifetime occurs. Once the penalty becomes lower than the value specified in Start Route Reuse, the advertisement of the route is un-suppressed.

Enable	Select to enable dampening on advertised routes. When this option is selected, other configuration fields in this Dampening field are enabled. This setting is disabled by default.
Half Lifetime	Select to enable and configure the half lifetime value. A penalty is imposed on a route that flaps. This is the time for the penalty to decrease to half its current value. Set a value from 1 - 45 in minutes. The default is 1 second.
Start Route Reuse	Select to enable and configure the route reuse value. When the penalty for a suppressed route decays below the value specified in *Start Route Reuse* field, the route is un-suppressed. Set a value from 1 - 20000.
Route Suppress Limit	Select to enable and configure the maximum duration in minutes a suppressed route is suppressed. This is the maximum duration for which a route remains suppressed before it is reused. Set a value from 1 - 255 minutes.
Start Route Suppress	Select to enable and configure the route suppress value. When a route flaps, a penalty is added to the route. When the penalty reaches or exceeds the value specified in *Route Suppress Limit*, the route is suppressed. Set a value from 1 - 20000.

39 Configure or set the **Graceful Restart** parameters. This provides a graceful restart mechanism for a BGP session reset in which the BGP daemon is not restarted, so that any changes in network configuration that caused the BGP reset does not affect packet forwarding.

Enable	Select to enable a graceful restart on this BGP router. This section is disabled by default.
Stalepath Time	Configure the maximum time to retain stale paths from restarting neighbor. This is the time the paths from a restarting neighbor is preserved. All stale paths, unless reinstated by the neighbor after re-establishment, are deleted at the expiry of this timer value. Set a value from 1 - 3600 seconds.

40 Select **OK** to save the changes and overrides. Select **Reset** to revert to the last saved configuration. Select **Exit** to close this window and go back to the main screen.

5.2.8.12 Overriding a Profile's Forwarding Database Configuration

Overriding a Profile's Network Configuration

A *Forwarding Database* forwards or filter packets on behalf of the managing controller, service platform or Access Point. The bridge reads the packet's destination MAC address and decides to either forward the packet or drop

(filter) it. If it's determined the destination MAC is on a different network segment, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered). As nodes transmit packets through the bridge, the bridge updates its forwarding database with known MAC addresses and their locations on the network. This information is then used to decide to filter or forward the packet.

This forwarding database assignment can be overridden as needed, but removes the device configuration from the managed profile that may be shared with other similar device models.

To define or override a profile's forwarding database configuration:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **Forwarding Database**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

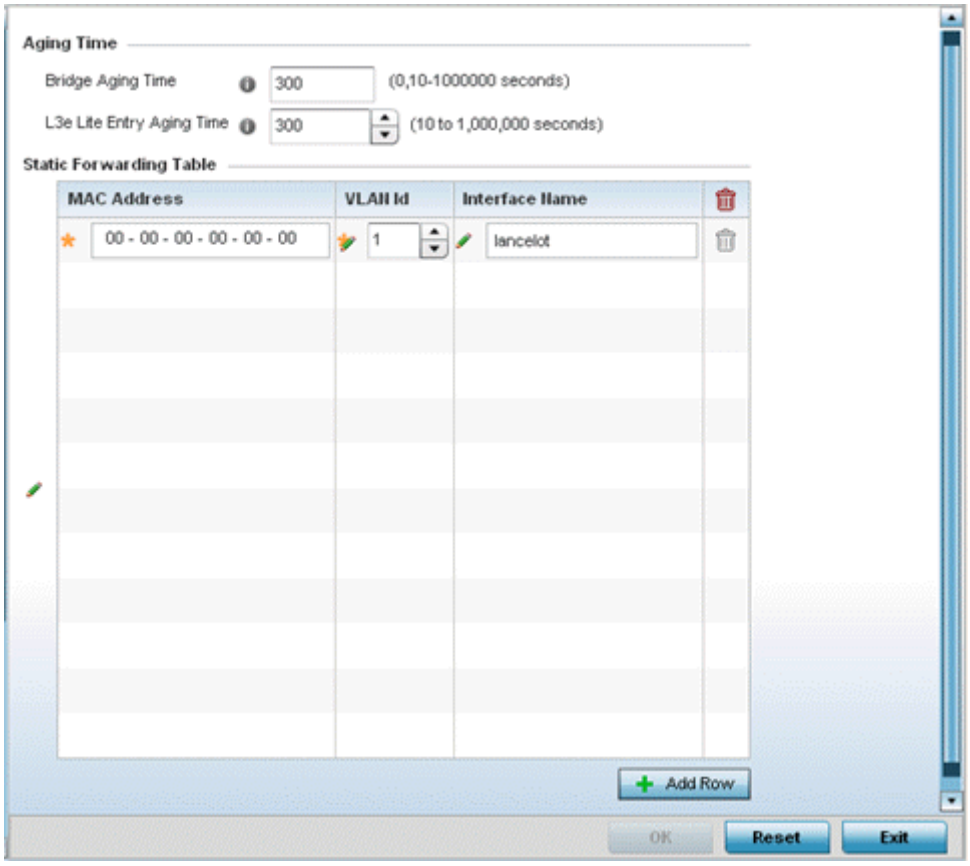


Figure 5-99 *Profile Overrides - Network Forwarding Database screen*

6 Define or override a **Bridge Aging Time** between 0, 10-1,000,000 seconds.

The aging time defines the interval an entry remains in the a bridge's forwarding table before being deleted due to lack of activity. If an entry replenishments a destination generating continuous traffic, this timeout value will never be invoked. However, if the destination becomes idle, the timeout value represents the length of time that must be exceeded before an entry is deleted from the forwarding table. The default setting is 300 seconds.

7 Define or override a **L3e Lite Entry Aging Time** between 10-1,000,000 seconds.

The default setting is 300 seconds. This setting is not available on all device platforms.

8 Use the **+ Add Row** button to create a new row within the **Static Forwarding Table**.

9 Set or override a destination **MAC Address**. The bridge reads the packet's destination MAC address and decides to forward the packet or drop (filter) it. If it's determined the destination MAC is on a different network, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered).

10 Define or override the target **VLAN ID** if the destination MAC is on a different network segment.

11 Provide an **Interface Name** used as the target destination interface for the target MAC address.

12 Select **OK** to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

5.2.8.13 Overriding a Profile's Bridge VLAN Configuration

Overriding a Profile's Network Configuration

A *Virtual LAN* (VLAN) is separately administrated virtual network within the same physical managed network. VLANs are broadcast domains defined within switches to allow control of broadcast, multicast, unicast, and unknown unicast within a Layer 2 device.

Administrators often need to route traffic to interoperate between different VLANs. Bridging VLANs are only for non-routable traffic, like tagged VLAN frames destined to some other device which will untag it. When a data frame is received on a port, the VLAN bridge determines the associated VLAN based on the port of reception. Using forwarding database information, the Bridge VLAN forwards the data frame on the appropriate port(s). VLAN's are useful to set separate networks to isolate some computers from others, without actually having to have separate cabling and Ethernet switches. Controllers and service platforms can do this on their own, without need for the computer or other gear to know itself what VLAN it's on (this is called port-based VLAN, since it's assigned by port of the switch). Another common use is to put specialized devices like VoIP Phones on a separate network for easier configuration, administration, security, or quality of service.

Two main VLAN bridging modes are available:

- *Tunnel Mode:* In tunnel mode, the traffic at the Access Point is always forwarded through the best path. The Access Point decides the best path to use and appropriately forwards packets. Setting the VLAN to tunnel mode ensures packets are Bridge packets between local Ethernet ports, any local radios, and tunnels to other APs and wireless controller.
- *Local Mode*: Local mode is typically configured in remote branch offices where traffic on remote private LAN segment needs to be bridged locally. Local mode implies that the wired and the wireless traffic are to be bridged locally.

To define a bridge VLAN configuration or override for a device profile:

1 Select **Devices** from the Configuration tab.

  The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

  Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **Bridge VLAN**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

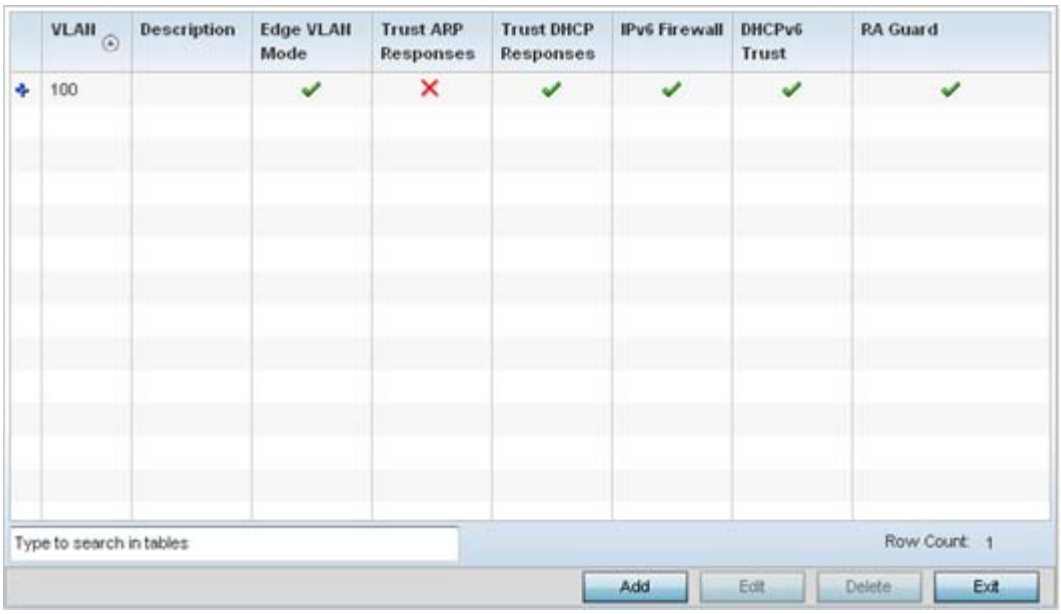


Figure 5-100 *Profile Overrides - Network Bridge VLAN screen*

6 Review the following VLAN configuration parameters to determine whether an override is warranted:

VLAN	Lists the numerical identifier defined for the Bridge VLAN when it was initially created. The available range is from 1 - 495. This value cannot be modified during the edit process.
Description	Lists a VLAN description assigned when the VLAN was created or modified. The description should be unique to the VLAN's specific configuration and help differentiate it from other VLANs with similar configurations.
Edge VLAN Mode	Defines whether the VLAN is currently in edge VLAN mode. A green check mark defines the VLAN as extended. An edge VLAN is the VLAN where hosts are connected. For example, if VLAN 10 is defined with wireless clients, and VLAN 20 is where the default gateway resides, VLAN 10 should be marked as an edge VLAN and VLAN 20 shouldn't be marked as an edge VLAN. When defining a VLAN as edge VLAN, the firewall enforces additional checks on hosts in that VLAN. For example, a host cannot move from an edge VLAN to another VLAN and still keep firewall flows active.
Trust ARP Responses	Trusted ARP packets are used to update the IP-MAC Table to prevent IP spoof and arp-cache poisoning attacks. When ARP trust is enabled, a green check mark displays. When disabled, a red "X" displays.
Trust DHCP Responses	When enabled, DHCP packets from a DHCP server are trusted and permissible. DHCP packets update the DHCP Snoop Table to prevent IP spoof attacks. When DHCP trust is enabled, a green check mark displays. When disabled, a red "X" displays.

IPv6 Firewall	Lists whether IPv6 is enabled on this bridge VLAN. A green checkmark defines this setting as enabled. A red X defines this setting as disabled. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters.
DHCPv6 Trust	Lists whether DHCPv6 responses are trusted on this bridge VLAN. A green checkmark defines this setting as enabled. A red X defines this setting as disabled. If enabled, only DHCPv6 responses are trusted and forwarded over the bridge VLAN.
RA Guard	Lists whether *router advertisements* (RA) are allowed on this bridge VLAN. A green checkmark defines this setting as enabled. A red X defines this setting as disabled. RAs are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

7 Select **Add** to define a new Bridge VLAN configuration, **Edit** to modify or override an existing Bridge VLAN configuration or **Delete** to remove a VLAN configuration.

Figure 5-101 *Profile Overrides - Network Bridge VLAN screen, General tab*

The **General** tab displays by default.

8 If adding a new Bridge VLAN configuration, use the spinner control to define or override a **VLAN** ID between 1 - 4094. This value must be defined and saved before the General tab can become enabled and the remainder of the settings defined. VLAN IDs 0 and 4095 are reserved and unavailable.

9 Set or override the following **General** bridge VLAN parameters:

Description	If creating a new Bridge VLAN, provide a description (up to 64 characters) unique to the VLAN's specific configuration to help differentiate it from other VLANs with similar configurations.
Per VLAN Firewall	Enable this setting to provide firewall allow and deny conditions over the bridge VLAN. This setting is enabled by default.

10 Set or override the following **URL Filter** parameters. URL filters are used to control access to specific resources on the Internet.

URL Filter	Use the drop-down menu to select a URL filter to use with this Bridge VLAN.

11 Use the drop-down to select the appropriate **Application Policy** to use with this Bridge VLAN configuration. An application policy defines the rules or actions executed on recognized HTTP (Facebook), enterprise (Webex) and peer-to-peer (gaming) applications or application-categories.

12 Set or override the following **Extended VLAN Tunnel** parameters:

Bridging Mode	Specify one of the following bridging mode for use on the VLAN. • *Automatic* - Select automatic mode to let the controller or service platform determine the best bridging mode for the VLAN. • *Local* - Select Local to use local bridging mode for bridging traffic on the VLAN. • *Tunnel* - Select Tunnel to use a shared tunnel for bridging traffic on the VLAN. • *Isolated Tunnel* - Select isolated-tunnel to use a dedicated tunnel for bridging traffic on the VLAN.
IP Outbound Tunnel ACL	Select an *IP Outbound Tunnel ACL* for outbound traffic from the drop-down menu. If an appropriate outbound IP ACL is not available, select the *Create* button.
IPv6 Outbound Tunnel ACL	Select an IPv6 Outbound Tunnel ACL for outbound IPv6 traffic from the drop-down menu. If an appropriate outbound IPv6 ACL is not available, select the Create button.
MAC Outbound Tunnel ACL	Select a *MAC Outbound Tunnel ACL* for outbound traffic from the drop-down menu. If an appropriate outbound MAC ACL is not available, select the *Create* button.
Tunnel Over Level 2	Select this option to allow VLAN traffic to be tunneled over level 2 links. This setting is disabled by default.

NOTE: Local and Automatic bridging modes do not work with ACLs. ACLs can only be used with tunnel or isolated-tunnel modes.

13 Select the **Level 2 Tunnel Broadcast Optimization** checkbox to enable broadcast optimization on this bridge VLAN. L2 Tunnel Broadcast Optimization prevents flooding of ARP packets over the virtual interface. Based on the learned information, ARP packets are filtered at the wireless controller level. This option is enabled by default.

14 If enabling L2 tunnel broadcast optimization, set the **Level 2 Forward Additional Packet Types** as *None* or *WNMP* to specify if additional packet types are forwarded or not across the L2 tunnel. By default, L2 tunnel broadcast optimization disables *Wireless Network Management Protocol* (WNMP) packet forwarding also across the L2 tunnel. Use this option to enable the forwarding of only WNMP packets. The default value is None.

15 Set the following **Tunnel Rate Limit** parameters:

Mint Link Level	Select the MINT link level being rate limited for layer 2 from the drop-down menu.
Rate	Define a transmit rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the bridge VLAN. Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5,000 kbps.
Maximum Burst Size	Set a maximum burst size between 0 - 1024 kbytes. The smaller the burst, the less likely the receive packet transmission will result in congestion. The default burst size is 320 kbytes.
Background	Set the random early detection threshold in % for low priority background traffic. Set a value from 1 - 100%. The default is 50%.
Best-Effort	Set the random early detection threshold in % for low priority best-effort traffic. Set a value from 1 - 100%. The default is 50%.
Video	Set the random early detection threshold in % for high priority video traffic. Set a value from 1 - 100%. The default is 25%.
Voice	Set the random early detection threshold in % for high priority voice traffic. Set a value from 1 - 100%. The default is 25%.

16 Set or override the following **Layer 2 Firewall** parameters:

Trust ARP Response	Select the check box to use trusted ARP packets to update the DHCP Snoop Table to prevent IP spoof and ARP-cache poisoning attacks. This feature is disabled by default.
Trust DHCP Responses	Select the check box to use DHCP packets from a DHCP server as trusted and permissible within the managed network. DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks. This feature is disabled by default.
Edge VLAN Mode	Select the check box to enable edge VLAN mode. When selected, the edge controller or service platform's IP address in the VLAN is not used for normal operations, as its now designated to isolate devices and prevent connectivity. This feature is enabled by default.

17 Set the following **IPv6 Settings**:

IPv6 Firewall	Select this option to enable IPv6 on this bridge VLAN. This setting is enabled by default.
DHCPv6 Trust	Select this option to enable the trust all DHCPv6 responses on this bridge VLAN. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is enabled by default.
RA Guard	Select this option to enable router advertisements or ICMPv6 redirects on this bridge VLAN. This setting is enabled by default.

18 Refer to the **Captive Portal** field to select an existing captive portal configuration to apply access restrictions to the bridge VLAN configuration.

A captive portal is an access policy for providing temporary and restrictive access using a standard Web browser. Captive portals provides authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the

network. Once logged into the captive portal, additional *Terms and Agreement*, *Welcome*, *Fail* and *No Service* pages provide the administrator with a number of options on captive portal screen flow and user appearance.

If an existing captive portal does not suite the bridge VLAN configuration, either select the **Edit** icon to modify an existing configuration or select the **Create** icon to define a new configuration that can be applied to the bridge VLAN. For information on configuring a captive portal policy, see Configuring Captive Portal Policies on page 11-1.

19 Refer to the **Captive Portal Snoop IPv6 Subnet** field to configure the subnet on which IPv6 snooping is enabled/disabled for wired captive portal support. Up to 16 excluded addresses are permitted.

20 Select the **IGMP Snooping** tab.

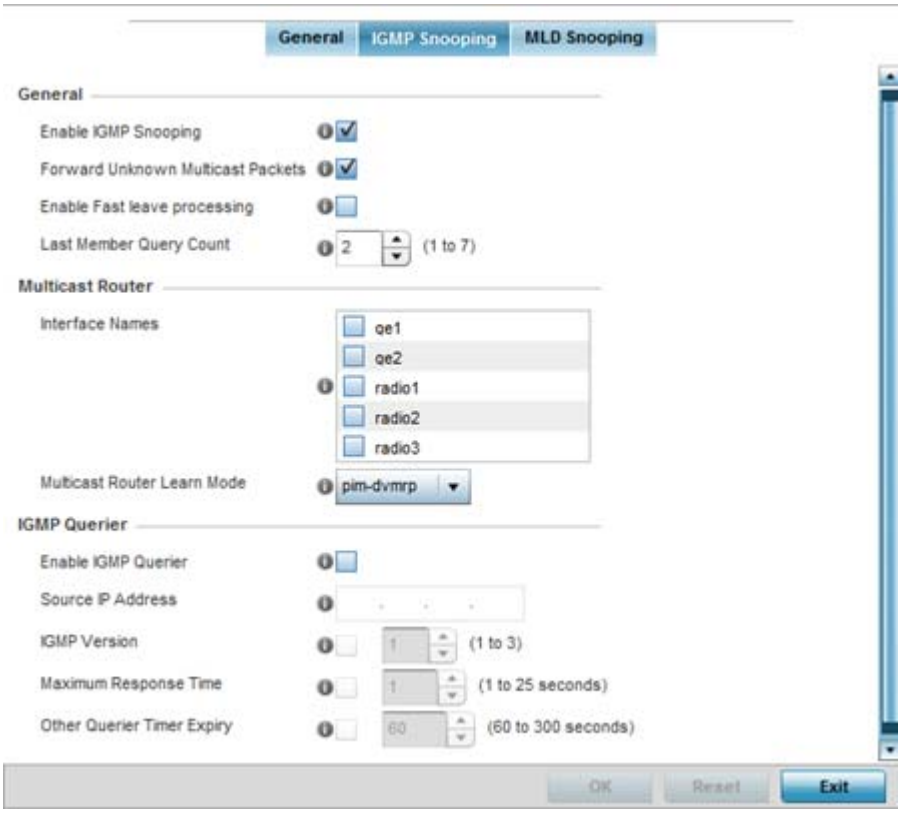


Figure 5-102 *Profile Overrides - Network Bridge VLAN screen, IGMP Snooping tab*

21 Define the following **General** settings:

Enable IGMP Snooping	Select this option to enable IGMP snooping. If disabled, snooping on a per VLAN basis is also disabled. This feature is enabled by default. If disabled, the settings under the bridge configuration are overridden. For example, if IGMP snooping is disabled, but the bridge VLAN is enabled, the setting is disabled.
Forward Unknown Multicast Packets	Select this option to enable the forwarding of multicast packets from unregistered multicast groups. If disabled (the default setting), the unknown multicast forward feature is also disabled for individual VLANs.

Enable Fast leave processing	Select this option to remove a Layer 2 LAN interface from the IGMP snooping forwarding table entry without initially sending IGMP group-specific queries to the interface. When receiving a group specific IGMPv2 leave message, IGMP snooping removes the interface from the Layer 2 forwarding table entry for that multicast group, unless a multicast router was learned on the port. Fast-leave processing enhances bandwidth management for all hosts on the network. This setting is disabled by default.
Last Member Query Count	Specify the number (1 - 7) of group specific queries sent before removing an IGMP snooping entry. The default settings is 2.

22 Define the following **Multicast Router** settings

Interface Names	Select the ge1 or radio interfaces used to IGMP snooping over a multicast router.
Multicast Router Learn Mode	Set the pim-dvmrp or static multicast routing learn mode. DVMRP builds a parent-child database using a constrained multicast model to build a forwarding tree rooted at the source of the multicast packets. Multicast packets are initially flooded down this source tree. If redundant paths are on the source tree, packets are not forwarded along those paths.

23 Define the following **IGMP Querier** settings:

Enable IGMP Querier	Select this option to enable IGMP querier. IGMP snoop querier is used to keep host memberships alive. It's primarily used in a network where there's a multicast streaming server and hosts subscribed to the server and no IGMP querier present. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then it is forwarded on that port.
Source IP Address	If enabling IGMP querier, set the source IP address used for IGMP snooping over a multicast router.
IGMP Version	Use the spinner control to set the IGMP version compatibility to either version 1, 2 or 3. IGMPv1 is defined by RFC 1112, IGMPv2 is defined by RFC 2236 and IGMPv3 defined by RFC 4604 which defines both IGMPv3 and MLDv2. IGMPv2 improves over IGMPv1 by adding the ability for a host to signal desire to leave a multicast group. IGMPv3 improves over IGMPv2 by adding the ability to listen to multicast traffic originating from a set of source IP addresses exclusively.
Maximum Response Time	Specify the maximum interval (from 1 - 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the snooping table. The controller or service platform only forwards multicast packets to radios present in the snooping table. For IGMP reports from wired ports, the controller or service platform forwards these reports to the multicast router ports. The default setting is 1 seconds.
Other Querier Timer Expiry	Specify an interval (from 60 - 300 seconds) used as a timeout interval for other querier resources.

24 Select the **OK** button located at the bottom right of the screen to save the changes to the IGMP Snooping tab. Select **Reset** to revert to the last saved configuration.

25 Select the **MLD Snooping** tab.

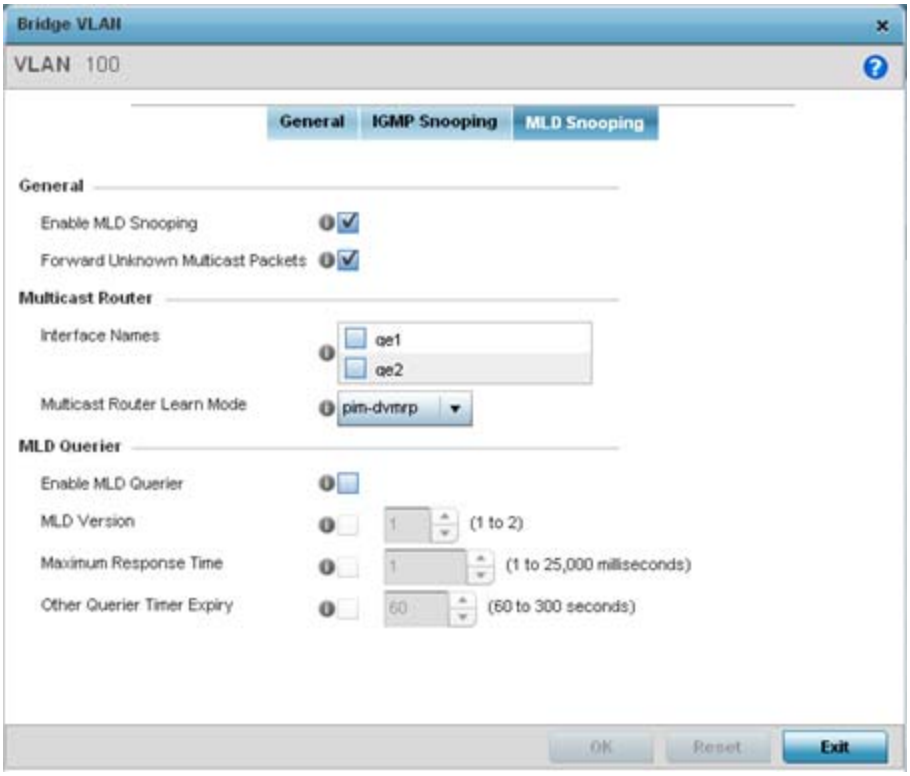


Figure 5-103 *Profile Overrides - Network Bridge VLAN screen, MLD Snooping tab*

26 Define the following **General** MLD snooping parameters for the bridge VLAN configuration:

Multicast Listener Discovery (MLD) snooping enables a controller, service platform or Access Point to examine MLD packets and make forwarding decisions based on content. MLD is used by IPv6 devices to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups.

MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or Access Point VLANs. When enabled, MLD messages are examined between hosts and multicast routers and to discern which hosts are receiving multicast group traffic. The controller, service platform or Access Point then forwards multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces.

Enable MLD Snooping	Enable MLD snooping to examine MLD packets and support content forwarding on this bridge VLAN. Packets delivered are identified by a single multicast group address. Multicast packets are delivered using best-effort reliability, just like IPv6 unicast. MLD snooping is enabled by default.
Forward Unknown Unicast Packets	Use this option to either enable or disable IPv6 unknown unicast forwarding. This setting is enabled by default.

27 Define the following **Multicast Router** settings

Interface Names	Select the ge or radio interfaces used for MLD snooping.
Multicast Router Learn Mode	Set the *pim-dvmrp* or *static* multicast routing learn mode. DVMRP builds a parent-child database using a constrained multicast model to build a forwarding tree rooted at the source of the multicast packets. Multicast packets are initially flooded down this source tree. If redundant paths are on the source tree, packets are not forwarded along those paths.

28 Set the following **MLD Querier** parameters for the profile's bridge VLAN configuration:

Enable MLD Querier	Select the option to enable MLD querier on the controller, service platform or Access Point. When enabled, the device sends query messages to discover which network devices are members of a given multicast group. This setting is enabled by default.
MLD Version	Define whether MLD version *1* or *2* is utilized with the MLD querier. MLD version 1 is based on IGMP version 2 for IPv4. MLD version 2 is based on IGMP version 3 for IPv4 and is fully backward compatible. IPv6 multicast uses MLD version 2. The default MLD version is 2.
Maximum Response Time	Specify the maximum response time (from 1 - 25,000 milliseconds) before sending a responding report. Queriers use MLD reports to join and leave multicast groups and receive group traffic. The default setting is 1 milliseconds.
Other Querier Timer Expiry	Specify an interval in either *Seconds (*60 - 300) or *Minutes* (1 - 5) used as a timeout interval for other querier resources. The default setting is 60 seconds

29 Select the **OK** button to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

5.2.8.14 Overriding a Profile's Cisco Discovery Protocol Configuration

Overriding a Profile's Network Configuration

The *Cisco Discovery Protocol* (CDP) is a proprietary data link layer network protocol implemented in Cisco networking equipment and used to share information about network devices.

To override a CDP configuration:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **Cisco Discovery Protocol**.

Figure 5-104 *Profile Overrides - Network Cisco Discovery Protocol screen*

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

6 Check the **Enable CDP** box to enable CDP on the device.

7 Refer to the **Hold Time** field and use the spinner control to define a hold time between 10 - 1800 seconds for transmitted CDP Packets. The default value is 180 seconds.

8 Refer to the **Timer** field and use the spinner control to define a interval between 5 - 900 seconds to transmit CDP Packets. The default value is 60 seconds.

9 Select the **OK** button to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

5.2.8.15 Overriding a Profile's Link Layer Discovery Protocol Configuration

Overriding a Profile's Network Configuration

The *Link Layer Discovery Protocol* (LLDP) or IEEE 802.1AB is a vendor-neutral data link layer protocol used by network devices for advertising (announcing) their identity, capabilities, and interconnections

on a IEEE 802 LAN network. The protocol is formally referred to by the IEEE as *Station and Media Access Control Connectivity Discovery*. Both LLDP snooping and ability to generate and transmit LLDP packets will be provided.

Information obtained via CDP and LLDP snooping is available in the UI. In addition, information obtained via CDP / LLDP snooping is provided by an AP during the adoption process, so the L2 switch device name detected by the AP can be used as a criteria in the auto provisioning policy.

To override a LLDP configuration:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **Link Layer Discovery Protocol**.

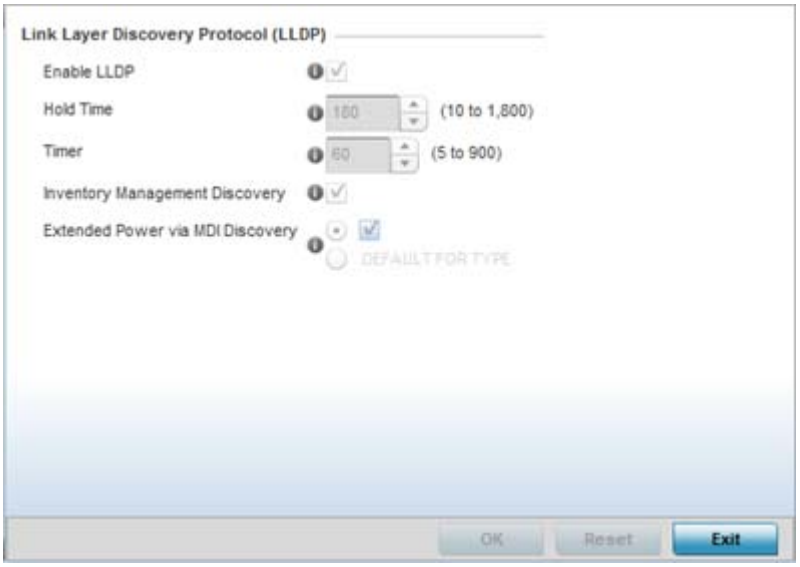


Figure 5-105 *Profile Overrides - Network Link Layer Discovery Protocol screen*

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

6 Check the **Enable LLDP** box to enable Link Layer Discovery Protocol on the device.

7 Refer to the **Hold Time** field and use the spinner control to define a hold time between 10 - 1800 seconds for transmitted LLDP Packets. The default value is 180 seconds.

8 Refer to the **Timer** field and use the spinner control to define the interval between 5 - 900 seconds to transmit LLDP packets. The default value is 60 seconds.

9 Check the **Inventory Management Discovery** box to enable this feature. Inventory Management Discovery is used to track and identify inventory attributes including manufacturer, model, or software version.

10 Extended Power via MDI Discovery provides detailed power information through end points and other connected devices. Select the **Extended Power via MDI Discovery** box to enable this feature. or select the **Default for Type** option to use a WiNG internal default value.

11 Select the **OK** button to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

5.2.8.16 Overriding a Profile's Miscellaneous Network Configuration

Overriding a Profile's Network Configuration

A profile can include a hostname within a DHCP lease for a requesting device. This helps an administrator track the leased DHCP IP address by hostname for the device profile. When numerous DHCP leases are assigned, an administrator can better track the leases when hostnames are used instead of devices.

To include a hostnames in DHCP request:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **Miscellaneous**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

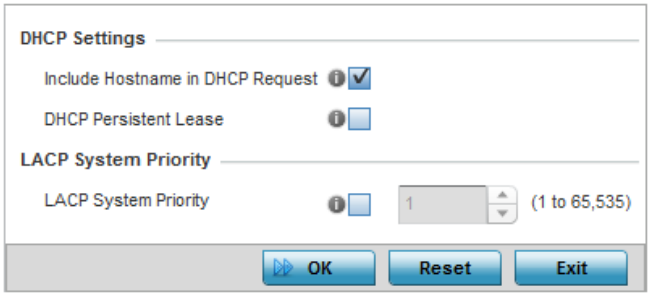


Figure 5-106 *Profile Overrides - Network Miscellaneous screen*

6 Refer to the DHCP Settings section to configure miscellaneous DHCP Settings.

Include Hostname in DHCP Request	Select the *Include Hostname in DHCP Request* option to include a hostname within a DHCP lease for a requesting device. This feature is enabled by default.
DHCP Persistent Lease	Check this option to enable a persistent DHCP lease for the device. A persistent DHCP lease assigns the same IP Address and other network information to the device each time it renews its DHCP lease.

7 Select the **LACP System Priority** value in the range of 1 - 65,535. The system with a lower number will have a higher priority when setting up a connection with a LACP peer. If a value is not set for this field, the default value of 32768 is used.

Link Aggregation Control Protocol (LACP) enables combining and managing multiple physical connections like Ethernet ports as a single logical channel as defined in the IEEE 802.1ax standard. LACP provides redundancy

and increase in throughput for connections between two peers. LACP provides automatic recovery in cases where one or more of the physical links - making up the aggregation - fail. Similarly, LACP also provides a theoretical boost in speed compared to an individual physical link.

NOTE: Disable or physically disconnect interfaces that do not use spanning tree to prevent loop formation until LACP is fully configured on both the local WiNG device and the remote device.

8 To enable critical resource monitoring for the device, select a **Critical Resource Policy** from the drop-down menu in the **Critical Resource Monitoring** section. If a new critical resource monitoring policy is needed click the **Create** button and specify the Ping Interval, IP Address, Ping Mode and VLAN for the devices being monitored.

9 Select the **OK** button to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

5.2.8.17 Overriding a Profile's Network Alias Configuration

Overriding a Profile's Network Configuration

With large deployments, the configuration of remote sites utilizes a set of shared attributes, of which a small set of attributes are unique for each location. For such deployments, maintaining separate configuration (WLANs, profiles, policies and ACLs) for each remote site is complex. Migrating any global change to a particular configuration item to all the remote sites is a complex and time consuming operation.

Also, this practice does not scale gracefully for quick growing deployments.

An alias enables an administrator to define a configuration item, such as a hostname, as an alias once and use the defined alias across different configuration items such as multiple ACLs.

Once a configuration item, such as an ACL, is utilized across remote locations, the Alias used in the configuration item (ACL) is modified to meet local deployment requirement. Any other ACL or other configuration items using the modified alias also get modified, simplifying maintenance at the remote deployment.

Aliases have scope depending on where the Alias is defined. Alias are defined with the following scopes:

- *Global aliases* are defined from the **Configuration** > **Network** > **Alias** screen. Global aliases are available for use globally across all devices, profiles and RF Domains in the system.
- *Profiles aliases* are defined from the **Configuration** > **Devices** > **System Profile** > **Network** > **Alias** screen. Profile aliases are available for use to a specific group of wireless controllers or Access Points. Alias values defined in a profile override the alias values defined within global aliases.
- *RF Domain aliases* are defined from the **Configuration** > **Devices** > **RF Domain** > **Alias** screen. RF Domain aliases are available for use for a site as a RF Domain is site specific. RF Domain alias values override alias values defined in a global alias or a profile alias configuration.
- *Device aliases* are defined from the **Configuration** > **Devices** > **Device Overrides** > **Network** > **Alias** screen. Device aliases are utilized by a singular device only. Device alias values override global, profile or RF Domain alias configurations.

Using an alias, configuration changes made at a remote location override any updates at the management center. For example, if an network alias defines a network range as 192.168.10.0/24 for the entire network, and at a remote deployment location, the local network range is 172.16.10.0/24, the network alias can be overridden at the deployment location to suit the local requirement. For the remote deployment location, the network alias work

with the 172.16.10.0/24 network. Existing ACLs using this network alias need not be modified and will work with the local network for the deployment location. This simplifies ACL definition and management while taking care of specific local deployment requirements.

For more information, refer to the following:

- *Basic Alias*
- *Network Group Alias*
- *Network Service Alias*

5.2.8.17.1 Basic Alias

A *basic alias* is a set of configurations consisting of *VLAN*, *Host*, *Network* and *Address Range* alias configurations. A VLAN alias is a configuration for optimal VLAN re-use and management for local and remote deployments. A host alias configuration is for a particular host device's IP address. A network alias configuration is utilized for an IP address on a particular network. An address range alias is a configuration for a range of IP addresses.

To set a network basic alias configuration:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **Alias.**

The Alias screen displays with the **Basic Alias** tab displayed by default.

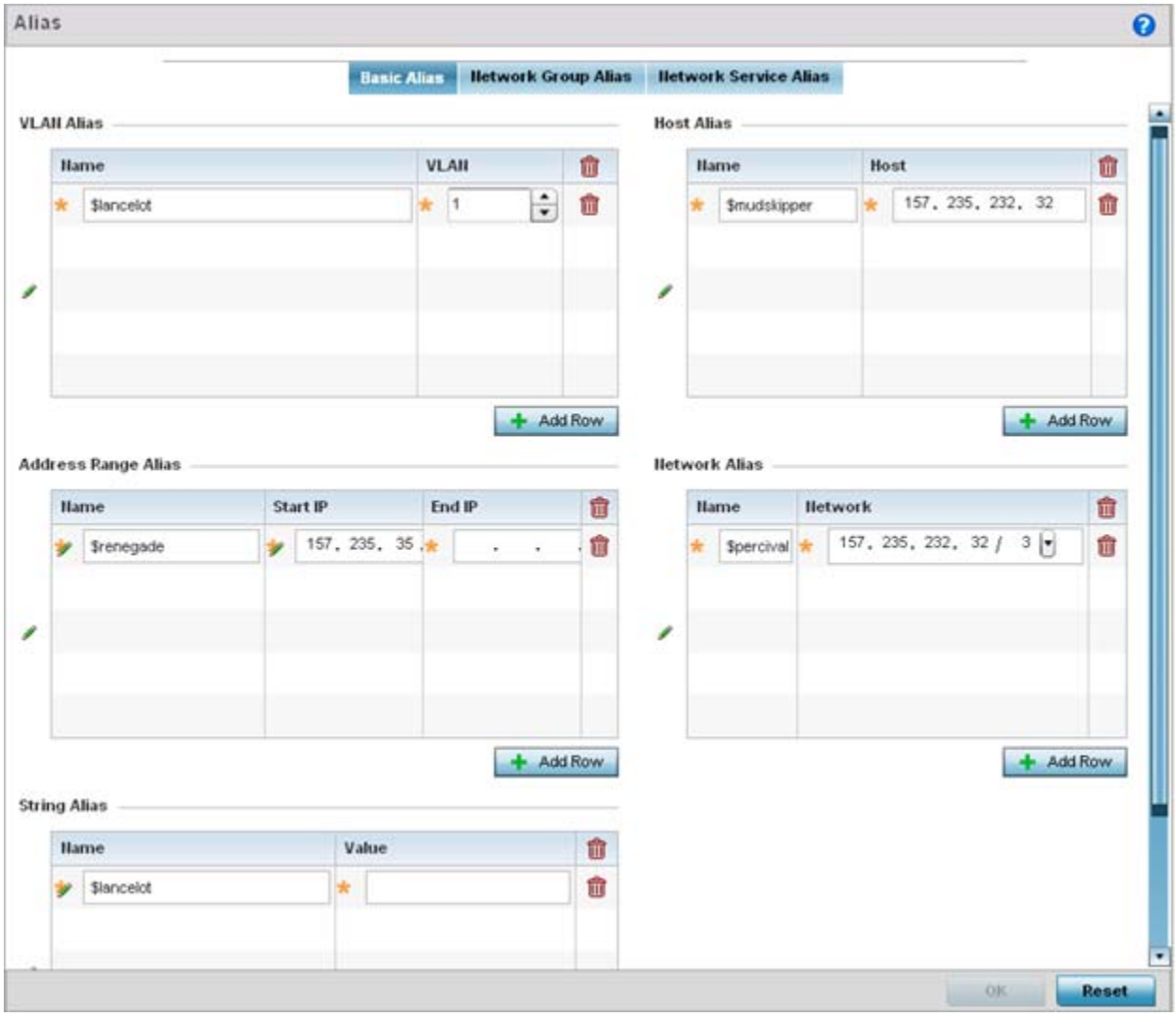


Figure 5-107 *Network Basic Alias screen*

6 Select **+ Add Row** to define **VLAN Alias** settings:

Use the *VLAN Alias* field to create unique aliases for VLANs that can be utilized at different deployments. For example, if a VLAN ID is set as 10 for the central network, and the VLAN is set as 26 at a remote location, the VLAN can be overridden at the remote location using an alias. At the remote location, the network is functional with an ID of 26, but utilizes the name defined at the central local network. A new VLAN need not be created specifically at the remote location.

Name	If adding a new *VLAN Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Vlan	Use the spinner control to set a numeric VLAN ID from 1 - 4094.

7 Select **+ Add Row** to define **Address Range Alias** settings:

Use the **Address Range Alias** field to create aliases for IP address ranges that can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110,

the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.

Name	If adding a new *Address Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Start IP	Set a starting IP address used with a range of addresses utilized with the address range alias.
End IP	Set an ending IP address used with a range of addresses utilized with the address range alias.

8 Select **+ Add Row** to define **String Alias** settings:

Use the **String Alias** field to create aliases for hosts that can be utilized at different deployments. For example, if the main domain at a remote location is called loc1.domain.com and at another deployment location it is called loc2.domain.com, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the loc1.domain.com domain and at the other with the loc2.domain.com domain.

Name	If adding a new *String Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Value	Provide a string value to use in the alias.

9 Select **+ Add Row** to define **Host Alias** settings:

Use the **Host Alias** field to create aliases for hosts that can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.

Name	If adding a new *Host Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Host	Set the IP address of the host machine.

10 Select **+ Add Row** to define **Network Alias** settings:

Use the **Network Alias** field to create aliases for IP networks that can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

Name	If adding a new *Network Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Network	Provide a network address in the form of *host/mask*.

11 Select **OK** when completed to update the set of basic alias rules. Select **Reset** to revert the screen back to its last saved configuration.

5.2.8.17.2 Network Group Alias

A *network group alias* is a set of configurations consisting of host and network configurations. Network configurations are complete networks in the form of 192.168.10.0/24 or an IP address range in the form of 192.168.10.10-192.168.10.20. Host configurations are in the form of a single IP address, 192.168.10.23.

A network group alias can contain multiple definitions for a host, network, and IP address range. A maximum of eight (8) Host entries, eight (8) network entries and eight (8) IP addresses range entries can be configured inside a network group alias. A maximum of 32 network group alias entries can be created.

To set a network group alias configuration:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **Alias.**

6 Select the **Network Group Alias** tab. The screen displays the attributes of existing network group alias configurations.

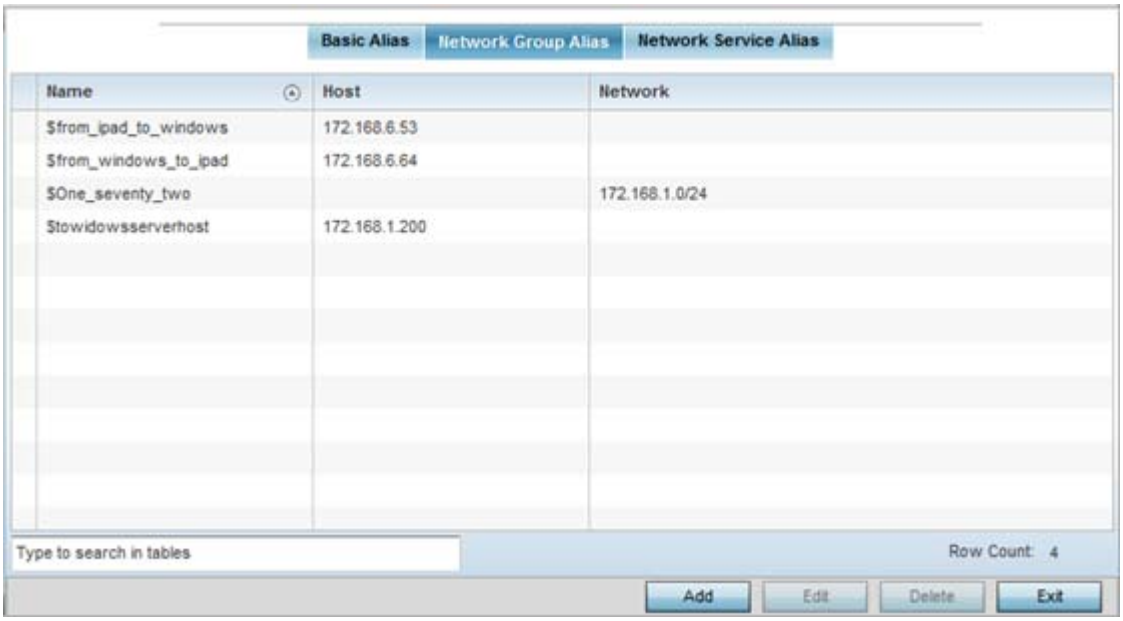


Figure 5-108 *Network Group Alias screen*

Name	Displays the administrator assigned name used with the network group alias.

Host	Displays all the host aliases configured in the listed network group alias. Displays a blank column if no host alias is defined.
Network	Displays all network aliases configured in the listed network group alias. Displays a blank column if no network alias is defined.

7 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies.

8 Select the added row to expand it into configurable parameters for defining the network alias rule.

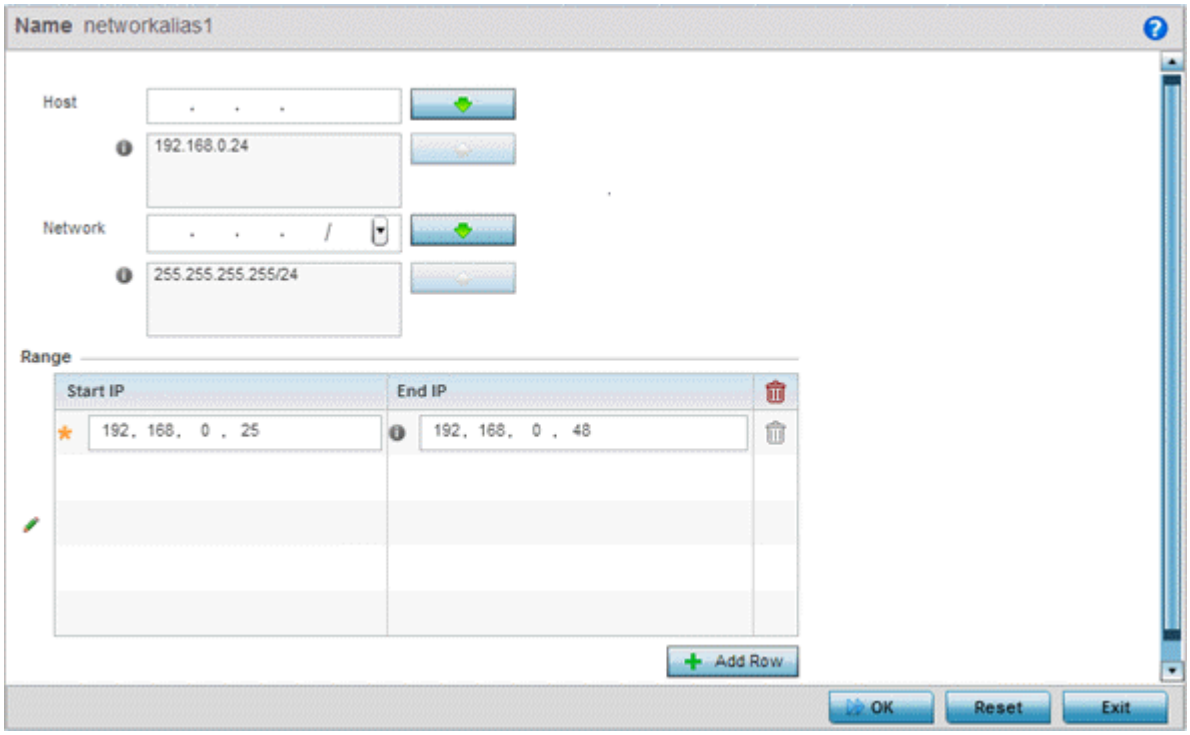


Figure 5-109 *Network Group Alias Add screen*

9 If adding a new **Network Alias Rule,** provide it a name up to 32 characters. The network group alias name always starts with a dollar sign ($).

10 Define the following network group alias parameters:

Host	Specify the Host IP address for up to eight IP addresses supporting network aliasing. Select the down arrow to add the IP address to the table.
Network	Specify the netmask for up to eight IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Select the down arrow to add the mask to the table.

11 Within the **Range** table, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the alias range or double-click on an existing an alias range entry to edit it.

12 Select **OK** when completed to update the network alias rules. Select **Reset** to revert the screen back to its last saved configuration.

5.2.8.17.3 Network Service Alias

A *network service alias* is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per network service alias.

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

To define a service alias configuration:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Network** to expand its sub menu options.

5 Select **Alias.**

6 Select the **Network Service Alias** tab. The screen displays existing network service alias configurations.

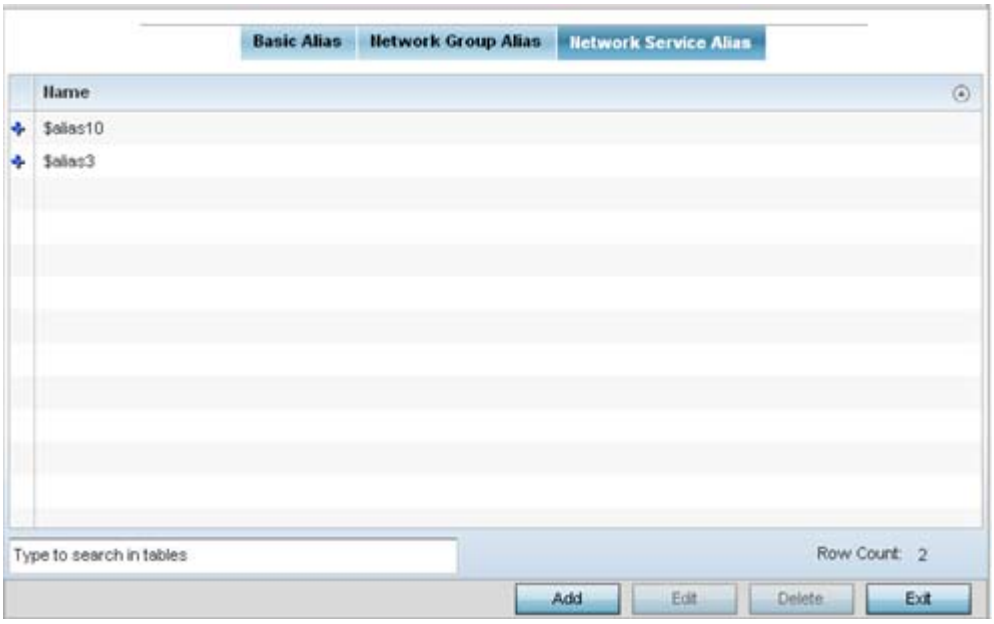


Figure 5-110 *Network Service Alias screen*

7 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies.

8 Select the added row to expand it into configurable parameters for defining the service alias rule.

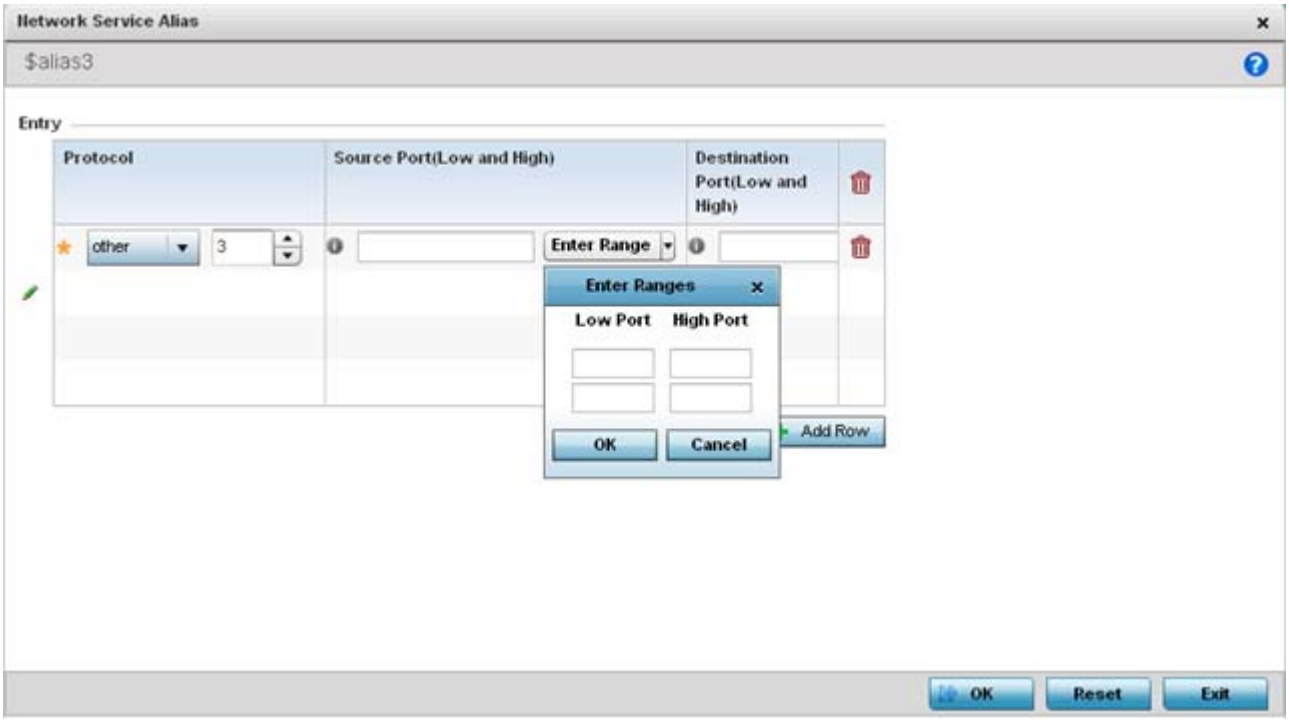


Figure 5-111 *Network Service Alias Add screen*

9 If adding a new **Network Service Alias Rule,** provide it a name up to 32 characters. Ensure a $ precedes the name.

10 Select **+ Add Row** and provide the following configuration parameters:

Protocol	Specify the protocol for which the alias has to be created. Use the drop down to select the protocol from *eigrp, gre, icmp, igmp, ip, vrrp, igp, ospf, tcp* and *udp.* Select *other* if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected.
Source Port (Low and High)	This field is only relevant if the protocol is either *tcp* or *udp.* Specify the source ports for this protocol entry. A range of ports can be specified. Select the *Enter Ranges* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.
Destination Port (Low and High)	This field is only relevant if the protocol is either *tcp* or *udp*. Specify the destination ports for this protocol entry. A range of ports can be specified. Select the *Enter Ranges* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

11 Within the **Range** field, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the service alias range or double-click on an existing service alias range entry to edit it.

12 Select **OK** when completed to update the service alias rules. Select **Reset** to revert the screen back to its last saved configuration.

5.2.8.18 Overriding a Profile's IPv6 Neighbor Configuration

Overriding a Profile's Network Configuration

IPv6 neighbor discovery uses ICMP messages and solicited multicast addresses to find the link layer address of a neighbor on the same local network, verify the neighbor's reachability and track neighboring devices.

Upon receiving a neighbor solicitation message, the destination replies with *neighbor advertisement* (NA). The source address in the NA is the IPv6 address of the device sending the NA message. The destination address in the neighbor advertisement message is the IPv6 address of the device sending the neighbor solicitation. The data portion of the NA includes the link layer address of the node sending the neighbor advertisement.

Neighbor solicitation messages also verify the availability of a neighbor once its the link layer address is identified. When a node wants to verify the reachability of a neighbor, the destination address in a neighbor solicitation message is the unicast address of the neighbor.

A neighbor is interpreted as reachable when an acknowledgment is returned indicating packets have been received and processed. If packets are reaching the device, they're also reaching the next hop neighbor, providing a confirmation the next hop is reachable.

To set an IPv6 neighbor discovery configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **IPv6 Neighbor**.

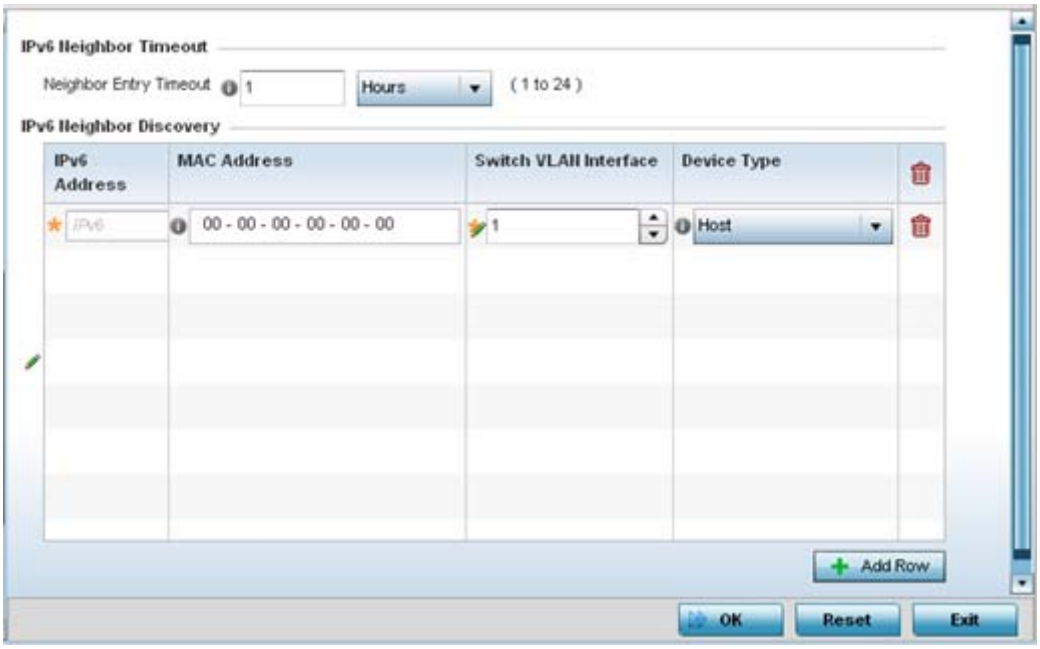


Figure 5-112 *IPv6 Neighbor screen*

4 Set an IPv6 **Neighbor Entry Timeout** in either *Seconds* (15 - 86,400), *Minutes* (1 - 1,440), *Hours* (1 - 24) or *Days* (1). The default setting is 1 hour.

5 Select **+ Add Row** to define the configuration of **IPv6 Neighbor Discovery** configurations. A maximum of 256 neighbor entries can be defined.

IPv6 Address	Provide a static IPv6 IP address for neighbor discovery. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the Neighbor Discovery Protocol via *Internet Control Message Protocol version 6* (ICMPv6) router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
MAC Address	Enter the hardware encoded MAC addresses of up to 256 IPv6 neighbor devices. A neighbor is interpreted as reachable when an acknowledgment is returned indicating packets have been received and processed. If packets are reaching the device, they're also reaching the next hop neighbor, providing a confirmation the next hop is reachable.
Switch VLAN Interface	Use the spinner control to set the virtual interface (from 1 - 4094) used for neighbor advertisements and solicitation messages.
Device Type	Specify the device type for this neighbor solicitation is for. Options include *Host*, *Router* and *DHCP Server.* The default setting is Host.

6 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

5.2.9 Overriding a Profile's Security Configuration

Profile Overrides

A profile can have its own firewall policy, wireless client role policy, WEP shared key authentication, NAT policy and VPN policy (controllers and service platforms only) applied. If an existing firewall, client role or NAT policy is unavailable, an administrator can be navigated from the **Profiles** section of the UI to the **Configuration** > **Security** portion of the UI to create the required security policy configuration. Once created, a policy's configuration can have an override applied to meet the changing data protection requirements of a device's environment. However, in doing so the device must now be managed separately from the profile configuration shared by other devices within the managed network.

For more information on applying an override to an existing device profile, refer to the following sections:

- *Overriding a Profile's General Security Settings*
- *Overriding a Profile's Certificate Revocation List (CRL) Configuration*
- *Overriding a Profile's RADIUS Trustpoint Configuration*
- *Overriding a Profile's VPN Configuration*
- *Overriding a Profile's Auto IPSec Tunnel Configuration*
- *Overriding a Profile's NAT Configuration*
- *Overriding a Profile's Bridge NAT Configuration*
- *Overriding a Profile's Application Visibility Settings*

5.2.9.1 Overriding a Profile's General Security Settings

Overriding a Profile's Security Configuration

A profile can leverage existing firewall, wireless client role and WIPS policies and apply them to the profile's configuration. This affords each profile a truly unique combination of data protection policies best meeting the

data protection requirements the profile supports. However, as deployment requirements arise, an individual device may need some or all of its general security configuration overridden from the profile's settings.

To configure a profile's security settings and overrides:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Security** to expand its sub menu options.

5 Select **Settings.**

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

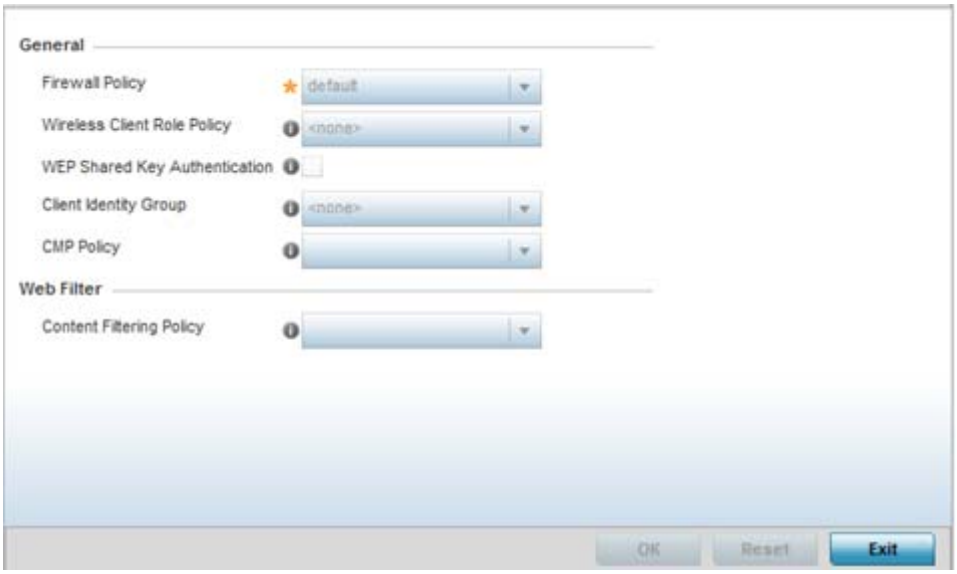


Figure 5-113 *Profile Overrides - General Security screen*

6 Refer to the **General** field to assign or override the following:

Firewall Policy	Use the drop-down menu to select an existing Firewall Policy to use as an additional security mechanism with this profile. All devices using this profile must meet the requirements of the firewall policy to access the network. A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms both blocking and permitting data traffic within the network. If an existing Firewall policy does not meet your requirements, select the *Create* icon to create a new firewall policy that can be applied to this profile. An existing policy can also be selected and edited as needed using the *Edit* icon.
Wireless Client Role Policy	Use the drop-down menu to select a client role policy used to strategically filter client connections based on a pre-defined set of filter rules and connection criteria. If an existing Wireless Client Role policy does not meet your requirements, select the *Create* icon to create a new configuration that can be applied to this profile. An existing policy can also be selected and edited as needed using the *Edit* icon.
WEP Shared Key Authentication	Select this option to require devices to use a WEP key to access the network using this profile. The controller or service platform use the key algorithm to convert an ASCII string to the same hexadecimal number. Clients without adapters need to use WEP keys manually configured as hexadecimal numbers. This option is disabled by default.
Client Identity Group	Select the client identity group to apply to this device profile. Client identity is a set of unique fingerprints used to identify a class of devices. A *Client identity group* is a set of client attributes that identify devices and apply specific permissions and restrictions on them.The information is used to configure permissions and access rules for that device class and can assist administrators by applying permissions and rules to multiple devices simultaneously.
CMP Policy	Use the drop down-menu to assign a CMP policy to allow a device to communicate to a CMP supported CA server, initiate a certificate request and download the required certificates from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting the certificates from the server. It can also auto update the certificates which are about to expire.

7 Use the **Web Filter** drop-down menu to select or override the URL Filter configuration applied to this virtual interface.

Web filtering is used to restrict access to resources on the Internet.

8 Select **OK** to save the changes or overrides. Select **Reset** to revert to the last saved configuration.

5.2.9.2 Overriding a Profile's Certificate Revocation List (CRL) Configuration

Overriding a Profile's Security Configuration

A *certificate revocation list* (CRL) is a list of revoked certificates that are no longer valid. A certificate can be revoked if the *certificate authority* (CA) had improperly issued a certificate, or if a private-key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.

To define a Certificate Revocation configuration or override:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points within the managed network.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Security** to expand its sub menu options.

5 Select **Certificate Revocation**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

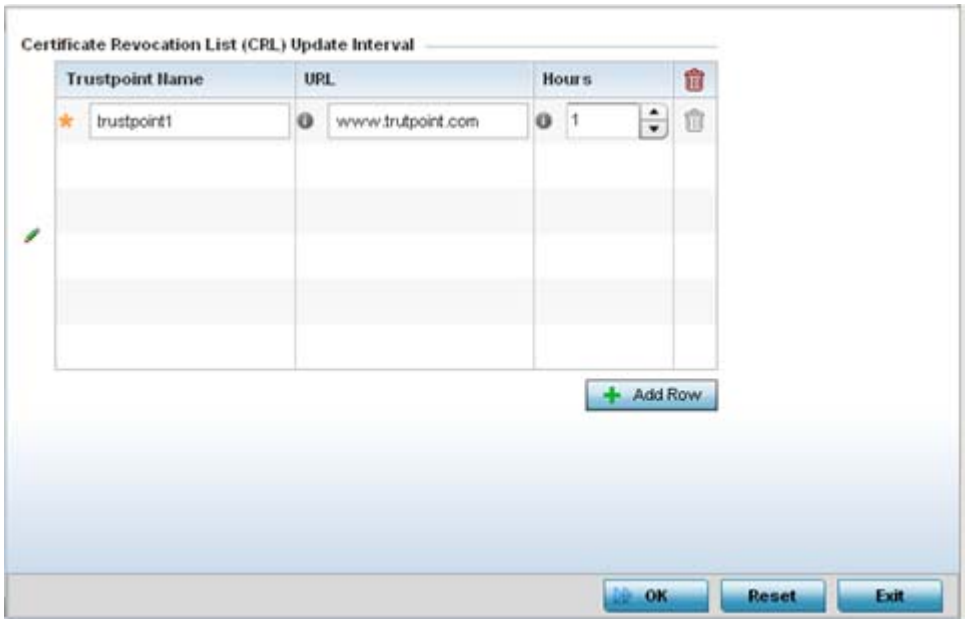


Figure 5-114 *Profile Overrides - Certificate Revocation screen*

6 Select the **+ Add Row** button to add a column within the **Certificate Revocation List (CRL) Update Interval** table to quarantine certificates from use in the managed network.

Additionally, a certificate can be placed on hold for a user defined period. If, for instance, a private key was found and nobody had access to it, its status could be reinstated.

a Provide the name of the trustpoint in question within the **Trustpoint Name** field. The name cannot exceed 32 characters.

b Enter the resource ensuring the trustpoint's legitimacy within the **URL** field.

c Use the spinner control to specify an interval (in hours) after which a device copies a CRL file from an external server and associates it with a trustpoint.

7 Select **OK** to save the changes and overrides made within the Certificate Revocation screen. Select **Reset** to revert to the last saved configuration.

5.2.9.3 Overriding a Profile's RADIUS Trustpoint Configuration

Overriding a Profile's Security Configuration

A RADIUS certificate links identity information with a public key enclosed in the certificate. A *certificate authority* (CA) is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate.

To define a RADIUS Trustpoint configuration, utilize an existing stored trustpoint or launch the certificate manager to create a new one:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points within the managed network.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Security** to expand its sub menu options.

5 Select **Trustpoints**.

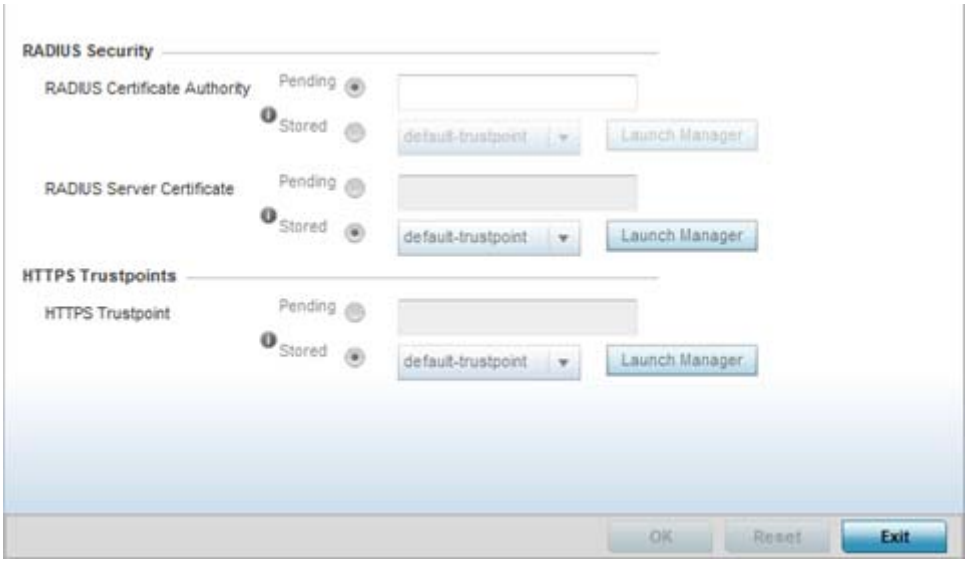


Figure 5-115 *Profile Overrides - Trustpoints screen*

6 Set the following **RADIUS Security** certificate settings:

RADIUS Certificate Authority	Either use the default-trustpoint or select the *Stored* radio button to enable a drop-down menu where an existing certificate can be leveraged. To leverage an existing certificate, select the *Launch Manager* button.
RADIUS Server Certificate	Either use the default-trustpoint or select the *Stored* radio button to enable a drop-down menu where an existing certificate/trustpoint can be used. To leverage an existing trustpoint, select the *Launch Manager* button.

7 Set the following **HTTPS Trustpoints**:

HTTPS Trustpoint	Either use the default trustpoint or select the Stored radio button to enable a drop-down menu where an existing certificate/trustpoint can be utilized. To use an existing certificate for this device, select the *Launch Manager* button. For more information, see *Certificate Management*.

8 Select **OK** to save the changes made within the RADIUS Trustpoints screen. Select **Reset** to revert to the last saved configuration.

5.2.9.4 Overriding a Profile's VPN Configuration

Overriding a Profile's Security Configuration

IPSec VPN provides a secure tunnel between two networked peer devices. Administrators can define which packets are sent within the tunnel, and how they're protected. When a tunnelled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination.

Tunnels are sets of *security associations* (SA) between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunnelled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

Use *crypto maps* to configure IPSec VPN SAs. Crypto maps combine the elements comprising IPSec SAs. Crypto maps also include *transform sets*. A transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic. One crypto map is utilized for each IPSec peer, however for remote VPN deployments one crypto map is used for all the remote IPSec peers.

Internet Key Exchange (IKE) protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs, and enables secure communications without time consuming manual pre-configuration.

To define a profile's VPN settings:

1 Select **Devices** from the Configuration tab.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Expand the **Security** menu and select **VPN**.

The profile's VPN configuration can be set or overridden using either a VPN setup wizard or by manually configuring the required advanced settings. WiNG provides two (2) wizards providing either minimal or more thorough administration.

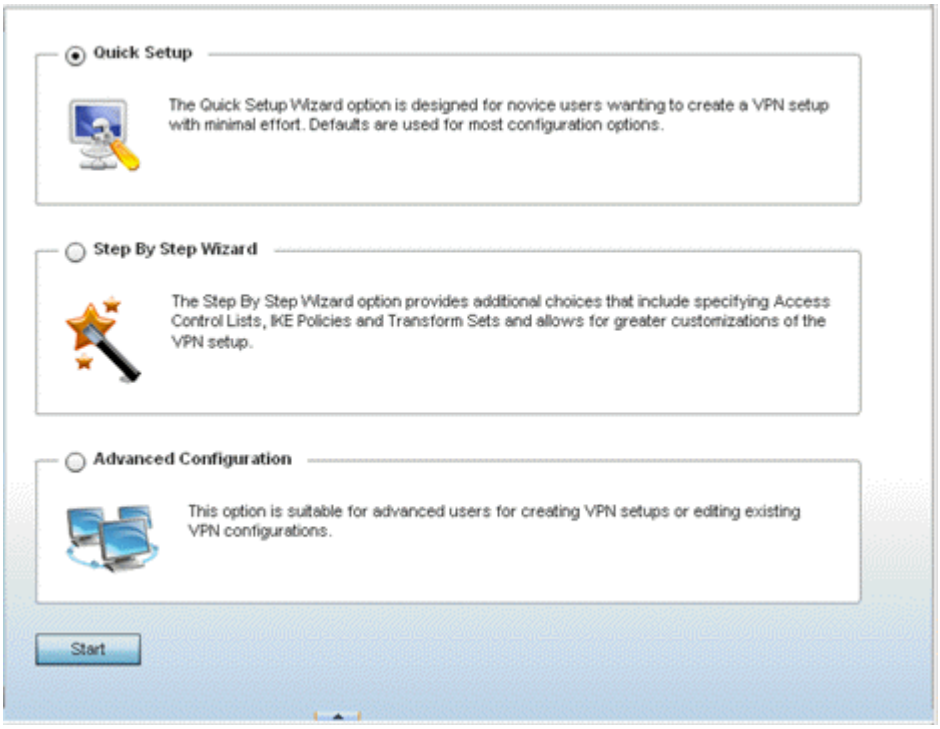


Figure 5-116 *VPN Setup Wizard*

- *Quick Setup Wizard* - Use the quick setup wizard to set a minimum number of basic VPN tunnel values. This wizard is designed for novice users, and enables them to setup a VPN configuration with minimum effort. This wizard uses default values for most parameters.
- *Step By Step Wizard* - Use the step-by-step wizard to create a VPN tunnel using settings updated from their minimum default values. This wizard is designed for intermediate users who require some VPN customization.
- *Advanced VPN Configuration* - The advanced VPN configuration option does not utilize a setup wizard. Rather, it utilizes and its own screen flow where just about every facet of a VPN tunnel configuration can be set by a qualified network administrator. For more information, see Setting the Profile's VPN Configuration on page 8-168.

5.2.9.4.4 Quick Setup Wizard

The *Quick Setup Wizard* creates a VPN configuration with minimum administration. Default values are retained for most parameters.

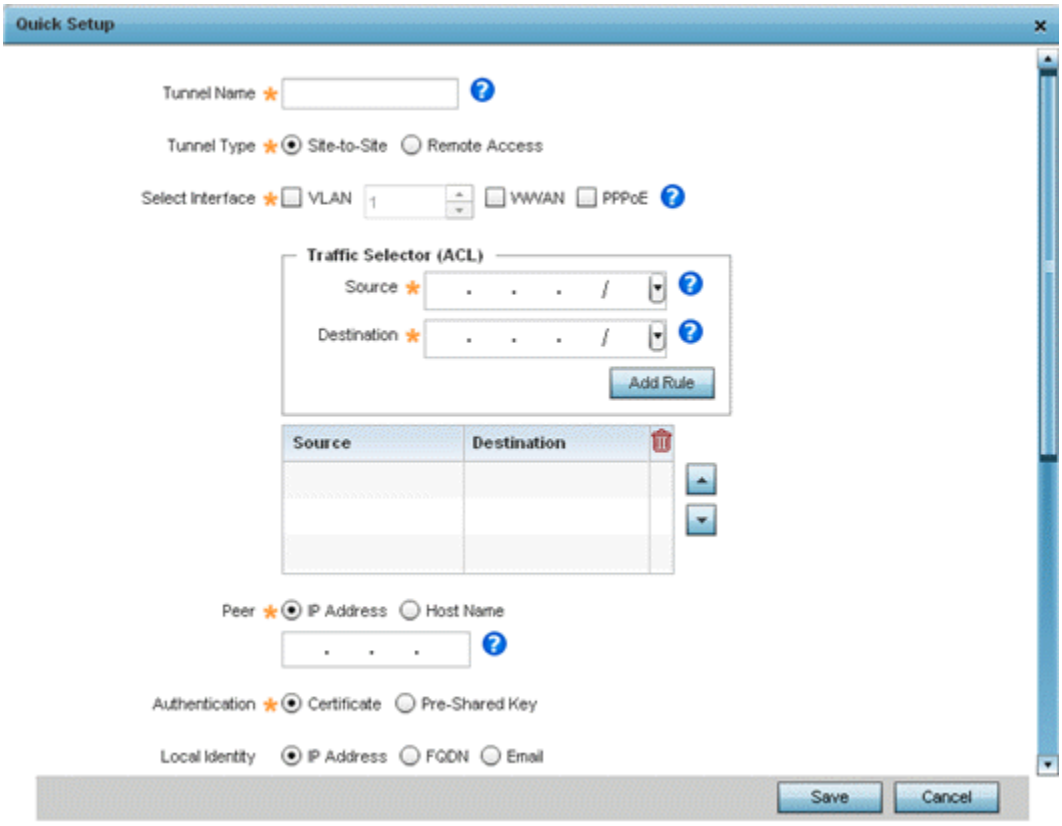


Figure 5-117 *VPN Quick Setup Wizard*

1 Select **Quick Setup** from the VPN Wizard screen.

2 Provide the following quick setup information to configure a VPN tunnel:

Tunnel Name	Provide a name for the tunnel. Tunnel name identifies the tunnel uniquely.
Tunnel Type	Configure the type of the tunnel. Tunnel can be one of the following types: • *Site-to-Site* – This tunnel provides a secured connection between two sites (default setting). • *Remote Access* – This tunnel provides access to a network to remote devices.
Select Interface	Configure the interface to use for creating the tunnel. The following options are available: • *VLAN* – Configure the tunnel over a Virtual LAN interface. Use the spinner to configure the VLAN number. • *WWAN* – Configure the tunnel over the WAN interface. • *PPPoE* – Configure the tunnel over the PPPoE interface.
Traffic Selector (ACL)	Configure ACLs that manage the traffic passing through the VPN tunnel. The following options are available: • *Source* – Provide the source network along with its mask • *Destination* – Provide the destination network along with its mask.

Peer	Configure the peer for this tunnel. The peer device can be specified either by its hostname or by its IP address.
Authentication	Set the authentication used to identify the peers with each other on opposite ends of the VPN tunnel connection. The following can be configured: • *Certificate* – Use a certificate to authenticate (default value). • *Pre-Shared Key* – Use a pre-shared key to authenticate. Enter the secret key in the space provided for it.
Local Identity	Configure the local identity used with this peer configuration for an IKE exchange with the target VPN IPSec peer. Options include *IP Address*, *Distinguished Name*, *FQDN*, *email* and *string*. The default setting is string.
Remote Identity	Configure the Access Point remote identifier used with this peer configuration for an IKE exchange with the target VPN IPSec peer. Options include *IP Address*, *Distinguished Name*, *FQDN*, *email* and *string*. The default setting is string.
IKE Policy	Configure the IKE policy to use. IKE is used to exchange authentication keys. Select from one of the following: • *All* – Use any IKE policy (default value). • *IKE1* – Use IKE 1 only • *IKE2* – Use IKE 2 only
Transform Set	Configure the transform set used to specify how traffic is protected within the crypto ACL defining the traffic that needs to be protected. Select the appropriate traffic set from the drop-down list.

3 Select **Save** to save the VPN quick setup tunnel configuration. To exit without saving, select **Cancel**.

5.2.9.4.5 Step By Step Wizard

The Step-By-Step wizard creates a VPN connection with more manual configuration than the Quick Setup Wizard. Use this wizard to manually configure *Access Control Lists*, *IKE Policy,* and *Transform Sets* to customize the VPN Tunnel.

1 Select the **Step-By-Step Wizard** option from the VPN screen.

2 Select the **Start** button.

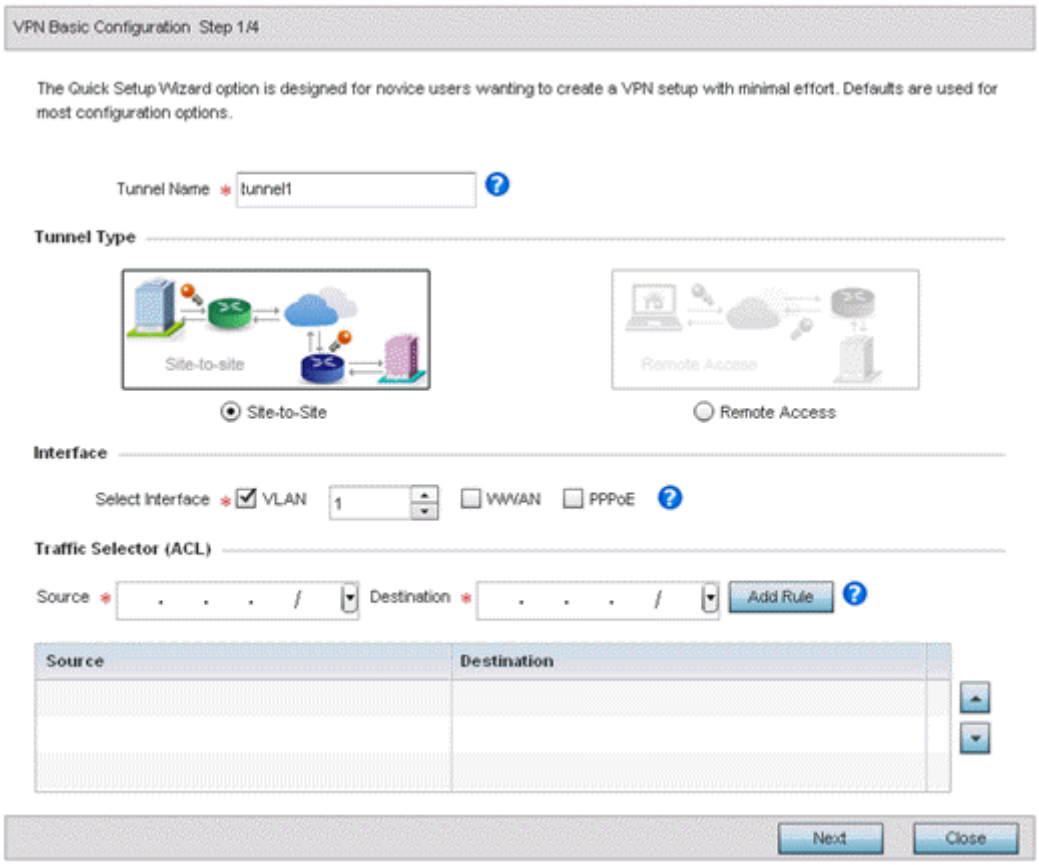


Figure 5-118 *VPN Step-By-Step Wizard - Step 1*

3 Set the following VPN values for step 1:

Tunnel Name	Provide a name for the tunnel in the *Tunnel Name* field.
Tunnel Type	Select the tunnel type being created. Two types of tunnels can be created. *Site to Site* (the default setting) is used to create a tunnel between two remote sites. *Remote Access* is used to create a tunnel between an user device and a network.
Interface	Select the interface to use. Interface can be a Virtual LAN (VLAN) or WWAN or PPPoE depending on the interfaces available on the device.
Traffic Selector	This field creates the *Access Control List* (ACL) that is used to control who uses the network. Provide the *Source* and *Destination* IP address ranges with their net mask. Click the *Add Rule* button to add the rule into the ACL.

4 Select the **Next** button to proceed to step 2.

If any of the required values within the step 1 screen are not set properly, the second wizard screen will not display until they are properly set.

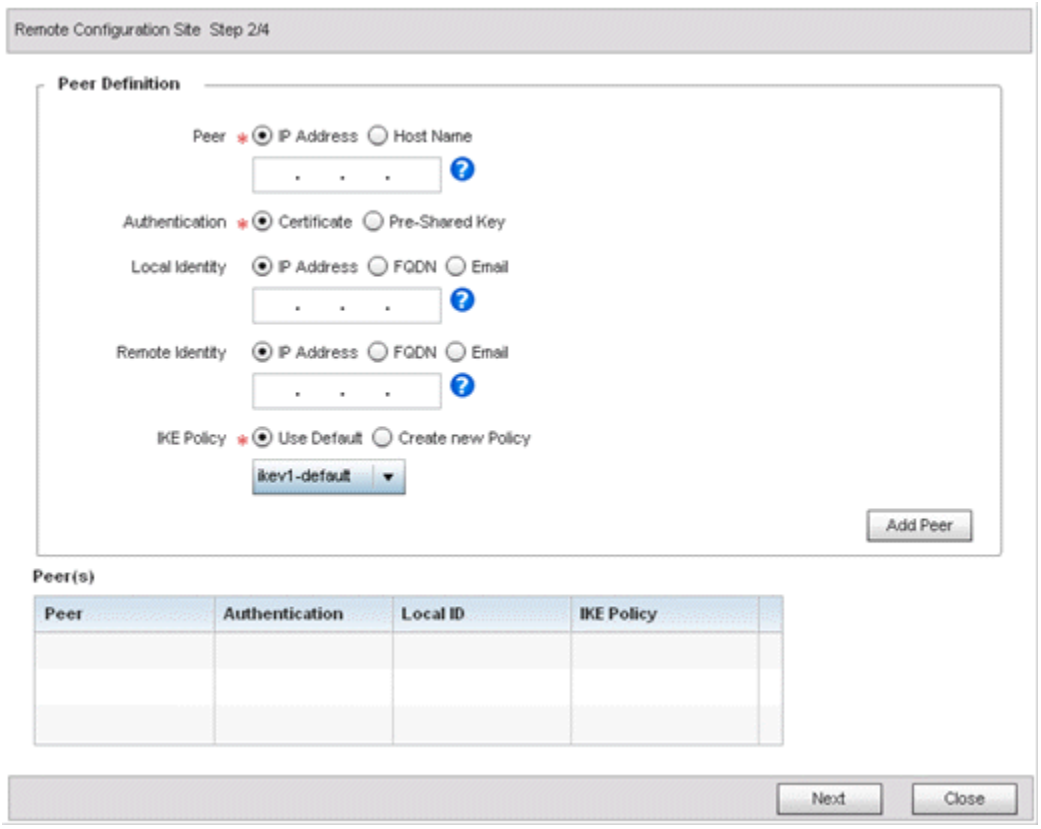


Figure 5-119 *VPN Step-By-Step Wizard - Step 2*

5 Set the following VPN quick setup values for step 2:

Peer	Select the type of peer for this device when forming a tunnel. Peer information can be either an *IP Address* (default value) or *hostname*. Provide the IP address or the host name of the peer device.
Authentication	Configure how devices authenticate on opposite ends of the tunnel connection. • *Certificate* – The devices use certificates to authenticate with each other (default value). • *Pre-Shared Key* – The devices use pre-shared key to authenticate.
Local Identity	Configure the local identity for the VPN tunnel. • *IP Address* – The local identity is an IP address (default value). • *FQDN* – The local identity is a *Fully Qualified Domain Name* (FQDN). • *Email* – The local identity is an E-mail address.
Remote Identity	Configure the remote identity for the VPN tunnel. • *IP Address* – The remote identity is an IP address (default value). • *FQDN* – The remote identity is a FQDN. • *Email* – The remote identity is an E-mail address.
IKE Policy	Configure an IKE policy to use when creating this VPN Tunnel. The following options are available: • *Use Default* – Select this option to use the default IKE profiles. • *Create new Policy* – Select this option to create a new IKE policy.

6 Click the **Add Peer** button to add the tunnel peer information into the *Peer(s)* table. This table lists all the peers set for the VPN Tunnel.

7 Select **Next** to proceed to the step 3 screen. Use the **Back** button to go to the previous step.

If any of the required values within the step 2 screen are not set properly, the third wizard screen will not display until they are properly set.

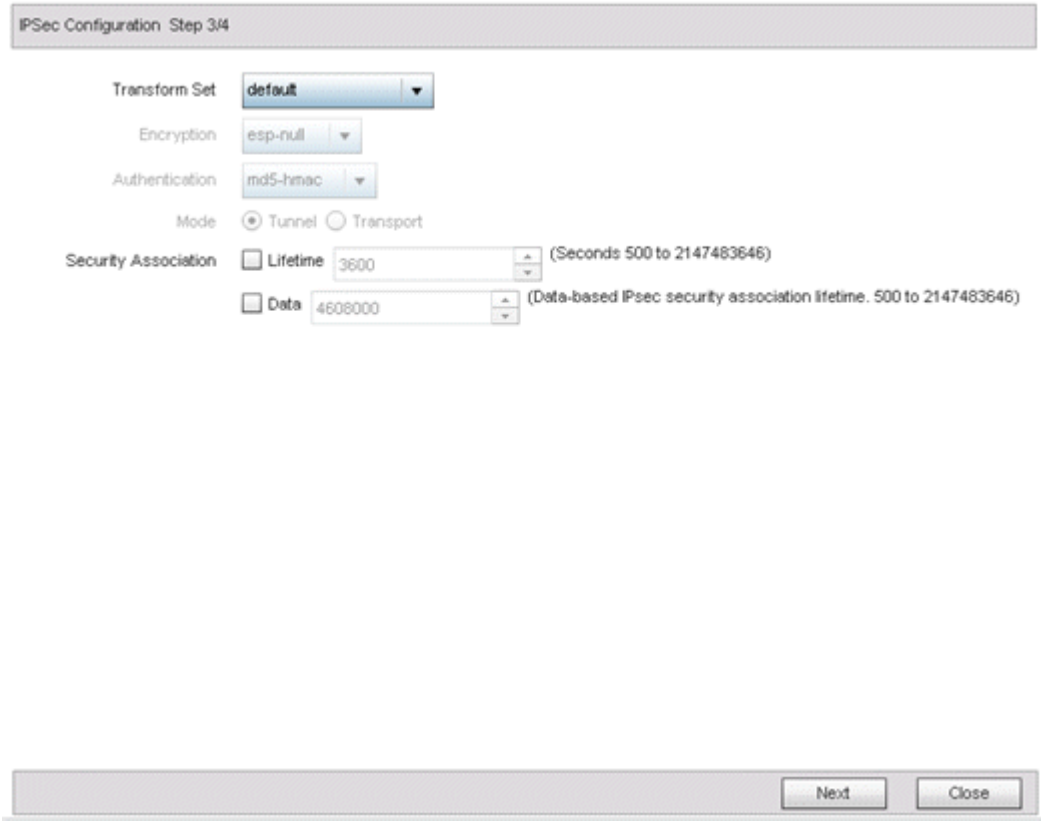


Figure 5-120 *VPN Step-By-Step Wizard - Step 3*

8 Set the following IPSec VPN values for step 3:

Transform Set	The transform set is a set of configurations for creating the VPN tunnel and imposes a security policy on the tunnel. Primarily, the transform set comprises the following: • *Encryption* – The encryption used for creating the tunnel. • *Authentication* – The authentication used to identify tunnel peers • *Mode* – The mode of the tunnel. This is the tunnel's operational mode. From the drop-down, select any pre-configured Transform Set or select *Create New Policy* to create a new transform set.
Encryption	This field is enabled when *Create New Policy* is selected in Transform Set field. This is the encryption used on data traversing through the tunnel. Select either *esp-null*, *des, 3des, aes, aes-192* or aes-*256*.
Authentication	This field is enabled when *Create New Policy* is selected in Transform Set field. This is how peers authenticate as the source of the packet to the other peers after a VPN tunnel has been created. Select either *MD5*, *SHA, SHA256 or AES-XCBC-HMAC-128.*

Mode	This field is enabled when *Create New Policy* is selected in *Transform Set* field. This indicates how packets are transported through the tunnel. • *Tunnel* – Use this mode when the Tunnel is between two routers or servers. • *Transport* – Use this mode when the Tunnel is created between a client and a server.
Security Association	Configures the lifetime of a security association (SA). Keys and SAs should be periodically renewed to maintain security of the tunnel. The field defines the parameters that set the lifetime of a security association. • *Lifetime* – Set the duration (in seconds) after which the keys should be changed. Set a value from 500-2,147,483,646 seconds. • *Data* – This is the amount of data in KBs the key can use. The key is changed after this quantity of data has be encrypted/decrypted. Set a value from 500-2,147,483,646 KBs.

9 Select **Next** to proceed to the fourth configuration screen. Use the **Back** button to navigate to the previous step. If any of the required values within the step 3 screen are not set properly, the fourth wizard screen will not display until they are properly set.

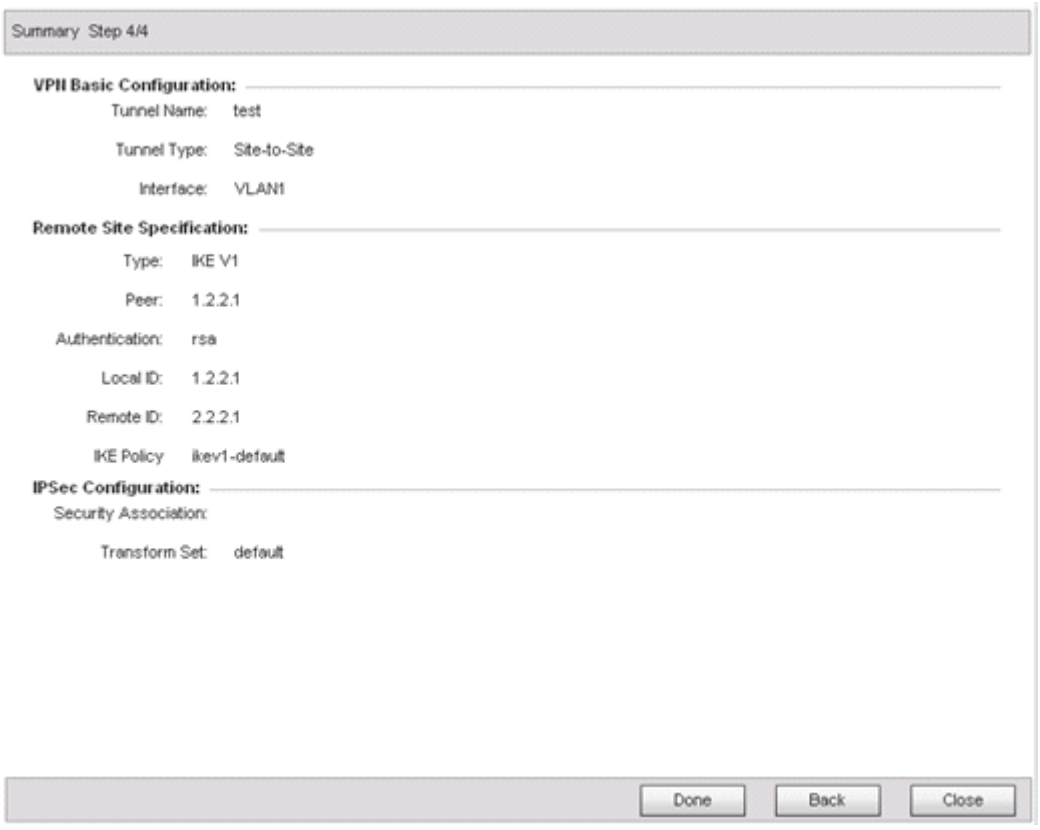


Figure 5-121 *VPN Step-By-Step Wizard - Step 4*

10 Review the configuration and select **Done** initiate the creation of the VPN tunnel. Use the **Back** button to navigate to the previous screen. Select **Close** to close the wizard without creating a VPN Tunnel.

5.2.9.4.6 Advanced VPN Configuration

The advanced VPN configuration option does not utilize a setup wizard. Rather, it utilizes and its own screen flow where just about every facet of a VPN tunnel configuration can be set by a qualified network administrator.

For detailed information on creating a VPN tunnel configuration, refer to Setting the Profile's VPN Configuration on page 8-168.

5.2.9.5 Overriding a Profile's Auto IPSec Tunnel Configuration

Overriding a Profile's Security Configuration

Auto IPSec tunneling provides a secure tunnel between two networked peer controllers or service platforms and associated Access Points which are within a range of valid IP addresses. Administrators can define which packets are sent within the tunnel, and how they're protected. When a tunnelled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination or associated Access Point

Tunnels are sets of *security associations* (SA) between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunnelled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (*AH* or *ESP*).

Internet Key Exchange (IKE) protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE enables secure communications without time consuming manual pre-configuration for auto IPSec tunneling.

To define an Auto IPSec Tunnel configuration or override that can be applied to a profile:

1 Select **Devices** from the Configuration tab.

  The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

  Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Security** to expand its sub menu options.

5 Select **Auto IPSec Tunnel**.

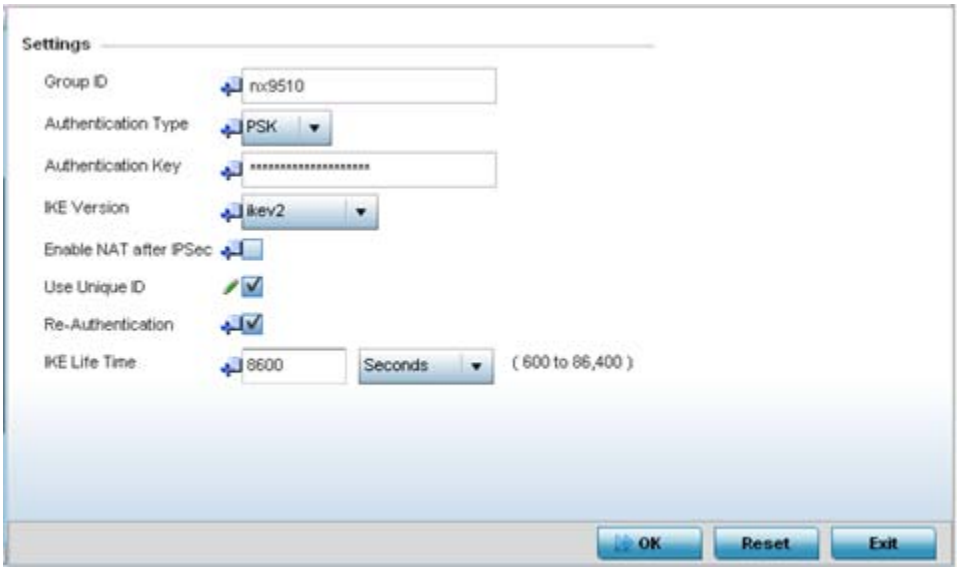


Figure 5-122 *Profile Overrides - Auto IPSec Tunnel screen*

The **Settings** field lists those Auto IPSec tunnel policies created thus far. Any of these policies can be selected and applied to a profile.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

Group ID	Define a 1 - 64 character identifier for an IKE exchange supporting auto IPSec tunnel secure peers.
Authentication Type	Use the drop-down menu to select either RSA or PSK (Pre Shared Key) as the authentication type for secure peer authentication on the auto IPSec secure tunnel. Rivest, Shamir, and Adleman (RSA) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing, as well as encryption. The default setting is RSA.
Authentication Key	Enter the 8 - 21 character shared key (password) used for auto IPSec tunnel secure peer authentication.
IKE Version	Use the drop-down menu to select the IKE version used for auto IPSec tunnel secure authentication with the IPSec gateway. IKEv2 is the default setting.
Enable NAT after IPSec	Select the checkbox to enable internal source port NAT on the auto IPSec secure tunnel.
Use Unique ID	Select this option to use a unique ID with auto IPSec secure authentication for the IPSec remote gateway (appending the MiNT ID). This setting is disabled by default.
Re-Authentication	Select this option to re-authenticate the key on a IKE rekey. This setting is enabled by default.
IKE Life Time	Set a lifetime in either *Seconds* (600 - 86,400), *Minutes* (10 - 1,440), *Hours* (1 - 24) or *Days* (1) for IKE security association duration. The default setting is 8600 seconds.

6 Select **OK** to save the changes made to the auto IPSec tunnel configuration. Select **Reset** to revert to the last saved configuration.

5.2.9.6 Overriding a Profile's NAT Configuration

Overriding a Profile's Security Configuration

Network Address Translation (NAT) is a technique to modify network address information within IP packet headers in transit. This enables mapping one IP address to another to protect wireless controller managed network address credentials. With typical deployments, NAT is used as an IP masquerading technique to hide private IP addresses behind a single, public facing, IP address.

Additionally, NAT is a process of modifying network address information in IP packet headers while in transit across a traffic routing device for the purpose of remapping one IP address to another. In most deployments NAT is used in conjunction with IP masquerading which hides RFC1918 private IP addresses behind a single public IP address.

NAT can provide a profile outbound Internet access to wired and wireless hosts connected to either an Access Point or a wireless controller. Many-to-one NAT is the most common NAT technique for outbound Internet access.

Many-to-one NAT allows an Access Point or wireless controller to translate one or more internal private IP addresses to a single, public facing, IP address assigned to a 10/100/1000 Ethernet port or 3G card.

To define a NAT configuration or override that can be applied to a profile:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points within the managed network.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Security** to expand its sub menu options.

5 Select **NAT**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

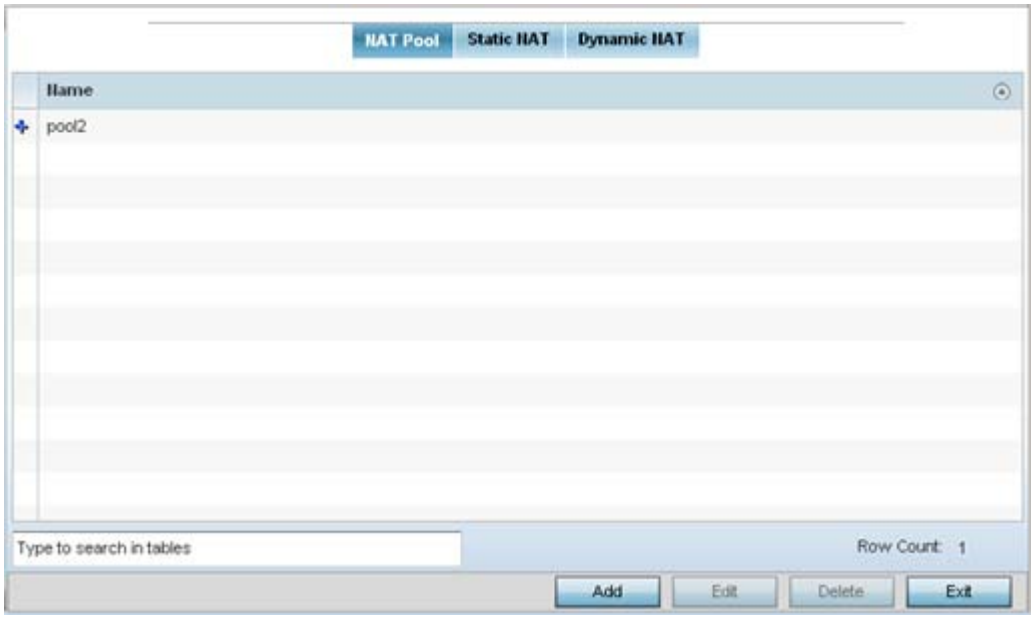


Figure 5-123 *Profile Overrides - NAT Pool screen*

The **NAT Pool** screen displays by default. The NAT Pool screen lists those NAT policies created thus far. Any of these policies can be selected and applied to a profile.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

6 Select **Add** to create a new NAT policy that can be applied to a profile. Select **Edit** to modify or override the attributes of a existing policy or select **Delete** to remove obsolete NAT policies from the list of those available to a profile.

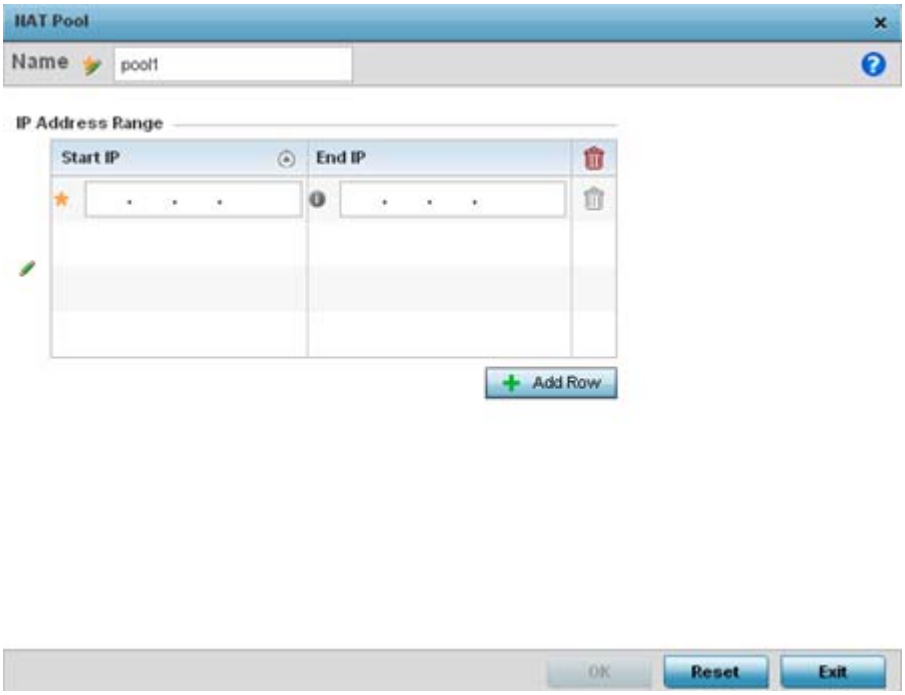


Figure 5-124 *NAT Pool screen*

7 If adding a new NAT policy or editing the configuration of an existing policy, define the following parameters:

Name	If adding a new NAT policy, provide a name to help distinguish it from others with similar configurations. The length cannot exceed 64 characters.
IP Address Range	Define a range of IP addresses that are hidden from the public Internet. NAT modifies network address information in the defined IP range while in transit across a traffic routing device. NAT only provides IP address translation and does not provide a firewall. A branch deployment with NAT by itself will not block traffic from being potentially routed through a NAT device. Consequently, NAT should be deployed with a stateful firewall.

8 Select the **+ Add Row** button as needed to append additional rows to the IP Address Range table.

9 Select **OK** to save the changes or overrides made to the profile's NAT Pool configuration. Select **Reset** to revert to the last saved configuration.

10 Select the **Static NAT** tab.

The Source tab displays by default and lists existing static NAT configurations. Existing static NAT configurations are not editable, but new configurations can be added or existing ones deleted as they become obsolete.

Static NAT creates a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a Web server on a perimeter interface with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host.

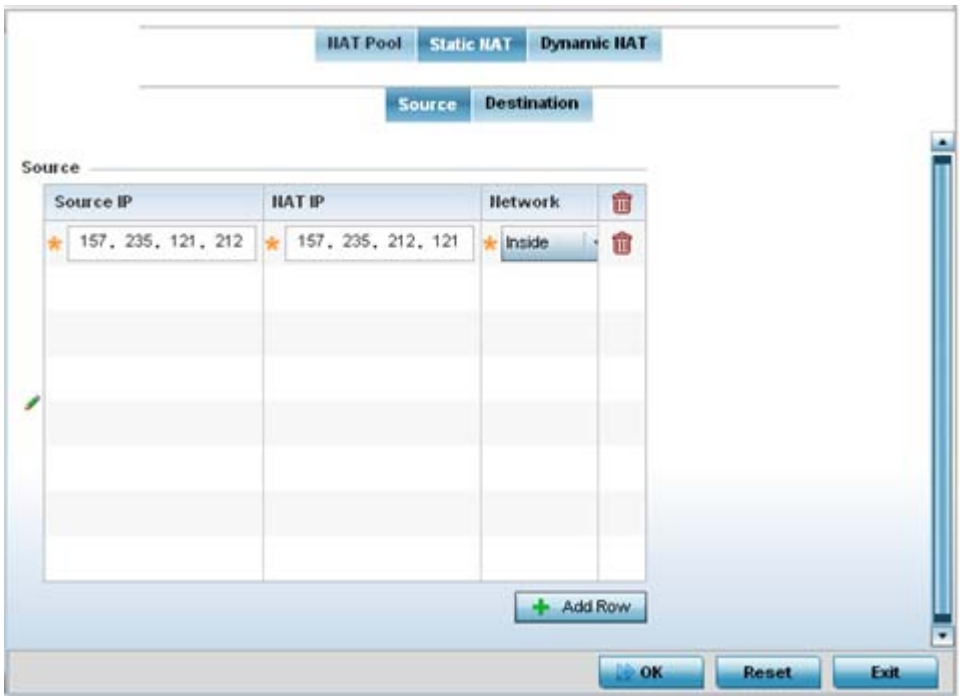


Figure 5-125 *Profile Overrides - Static NAT screen*

11 Select **+ Add Row** to create a new static NAT configuration.

12 Set or override the following **Source** configuration parameters:

Source IP	Enter the local address used at the origination of the static NAT configuration. This address (once translated) is not exposed to the outside world when the translation address is used to interact with the remote destination.
NAT IP	Enter the IP address of the matching packet to the specified value. The IP address modified can be either source or destination based on the direction specified.
Network	Select *Inside* or *Outside* NAT as the network direction. Select Inside to create a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a Web server on a perimeter interface with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host. Inside NAT is the default setting.Inside is the default setting.

13 Select the **Destination** tab to view destination NAT configurations and define packets passing through the NAT on the way back to the managed LAN are searched against to the records kept by the NAT engine. The destination IP address is changed back to the specific internal private class IP address to reach the LAN over the managed network.

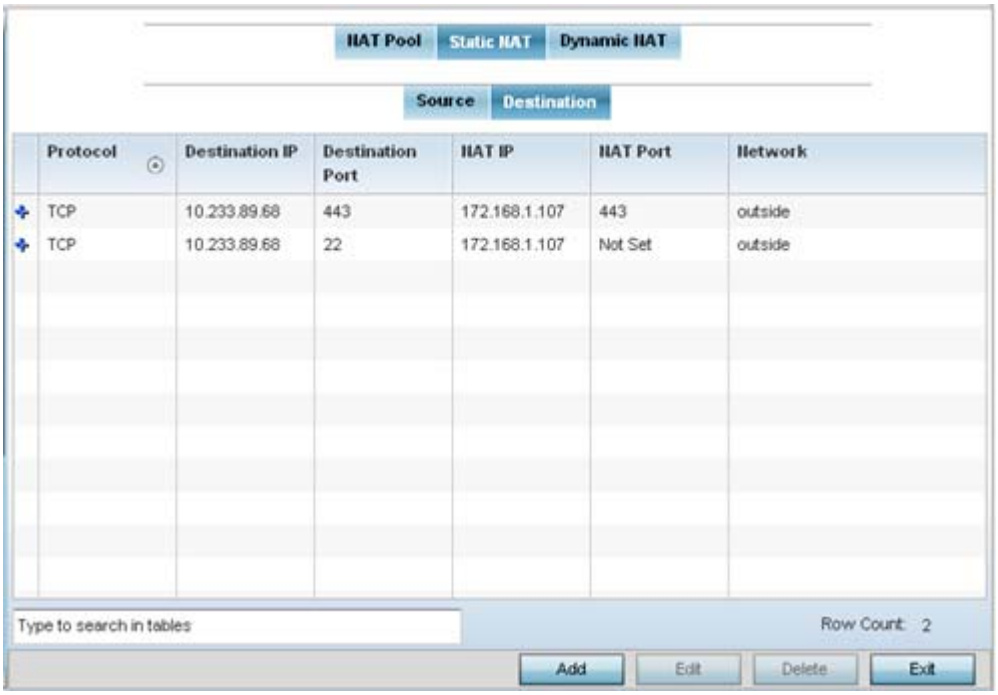


Figure 5-126 *NAT Destination screen*

14 Select **Add** to create a new NAT destination configuration or **Delete** to permanently remove a NAT destination. Existing NAT destinations cannot be edited.

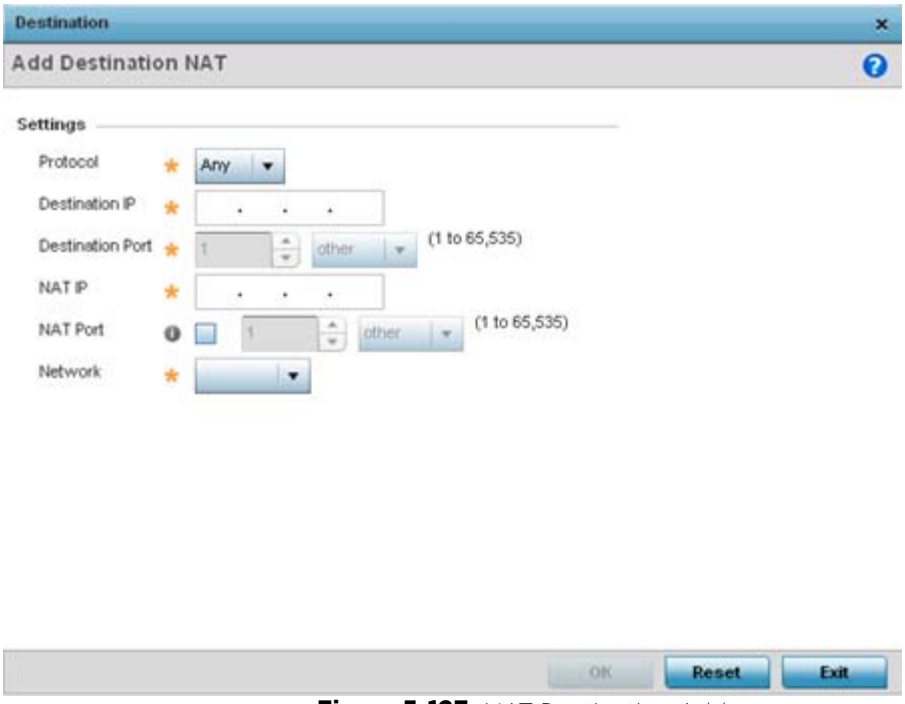


Figure 5-127 *NAT Destination Add screen*

15 Set or override the following **Destination** configuration parameters:

Static NAT creates a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a Web server on a perimeter interface with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the

actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host.

Protocol	Select the protocol for use with static translation (*TCP, UDP* and *Any* are available options). TCP is a transport layer protocol used by applications requiring guaranteed delivery. It's a sliding window protocol handling both time outs and retransmissions. TCP establishes a full duplex virtual connection between two endpoints. Each endpoint is defined by an IP address and a TCP port number. The *User Datagram Protocol* (UDP) offers only a minimal transport service, non-guaranteed datagram delivery, and provides applications direct access to the datagram service of the IP layer. UDP is used by applications not requiring the level of service of TCP, or are using communications services (multicast or broadcast delivery) not available from TCP. The default setting is Any.
Destination IP	Enter the local address used at the (source) end of the static NAT configuration. This address (once translated) is not exposed to the outside world when the translation address is used to interact with the remote destination.
Destination Port	Use the spinner control to set the local port number used at the (source) end of the static NAT configuration. The default value is port 1.
NAT IP	Enter the IP address of the matching packet to the specified value. The IP address modified can be either source or destination based on the direction specified.
NAT Port	Enter the port number of the matching packet to the specified value. This option is valid only if the direction specified is destination.
Network	Select *Inside* or *Outside* NAT as the network direction. Inside is the default setting.

16 Select **OK** to save the changes or overrides made to the static NAT configuration. Select **Reset** to revert to the last saved configuration.

17 Select the **Dynamic NAT** tab.

Dynamic NAT configurations translate the IP address of packets going out from one interface to another interface based on configured conditions. Dynamic NAT requires packets be switched through a NAT router to generate translations in the translation table.

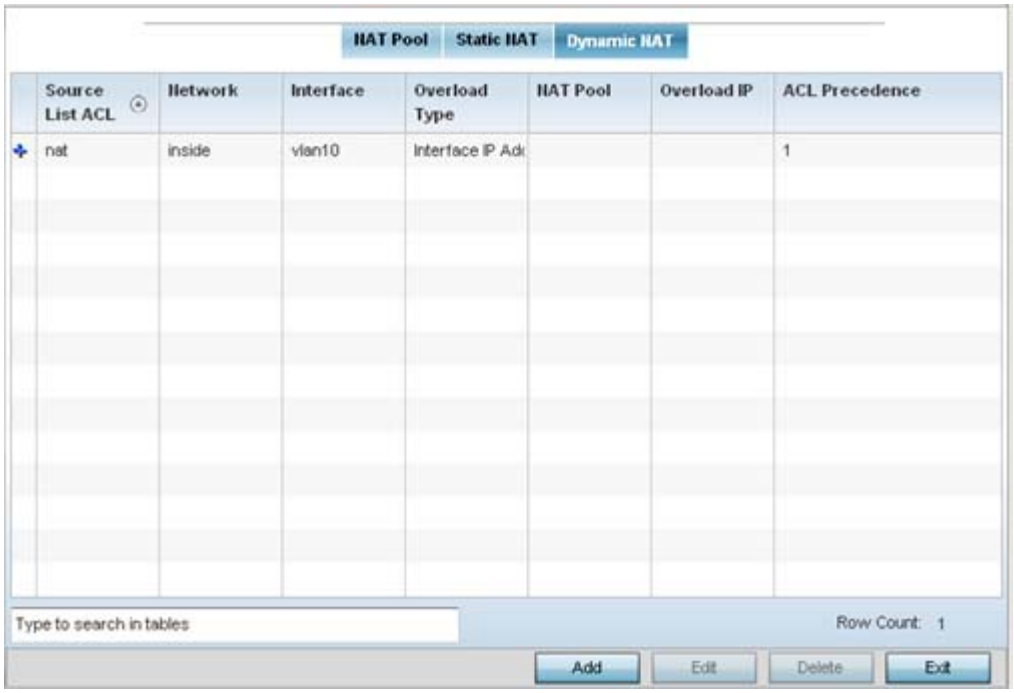


Figure 5-128 *Profile Overrides - Dynamic NAT screen*

18 Refer to the following to determine whether a new Dynamic NAT configuration requires creation, edit or deletion:

Source List ACL	Lists an ACL name to define the packet selection criteria for the NAT configuration. NAT is applied only on packets which match a rule defined in the access list. These addresses (once translated) are not exposed to the outside world when the translation address is used to interact with the remote destination.
Network	Displays *Inside* or *Outside* NAT as the network direction for the dynamic NAT configuration.
Interface	Lists the VLAN (from 1 - 4094) used as the communication medium between the source and destination points within the NAT configuration.
Overload Type	Displays the Overload Type utilized when several internal addresses are NATed to only one or a few external addresses. Options include *NAT Pool*, *One Global Address* and *Interface IP Address*. Interface IP Address is the default setting.
NAT Pool	Displays the name of an existing NAT pool used with the dynamic NAT configuration.
Overload IP	If One Global IP Address is selected as the Overload Type, define an IP address used a filter address for the IP ACL rule.
ACL Precedence	Lists the administrator assigned priority set for the listed source list ACL. The lower the value listed the higher the priority assigned to these ACL rules.

19 Select **Add** to create a new Dynamic NAT configuration, **Edit** to modify or override an existing configuration or **Delete** to permanently remove a configuration.

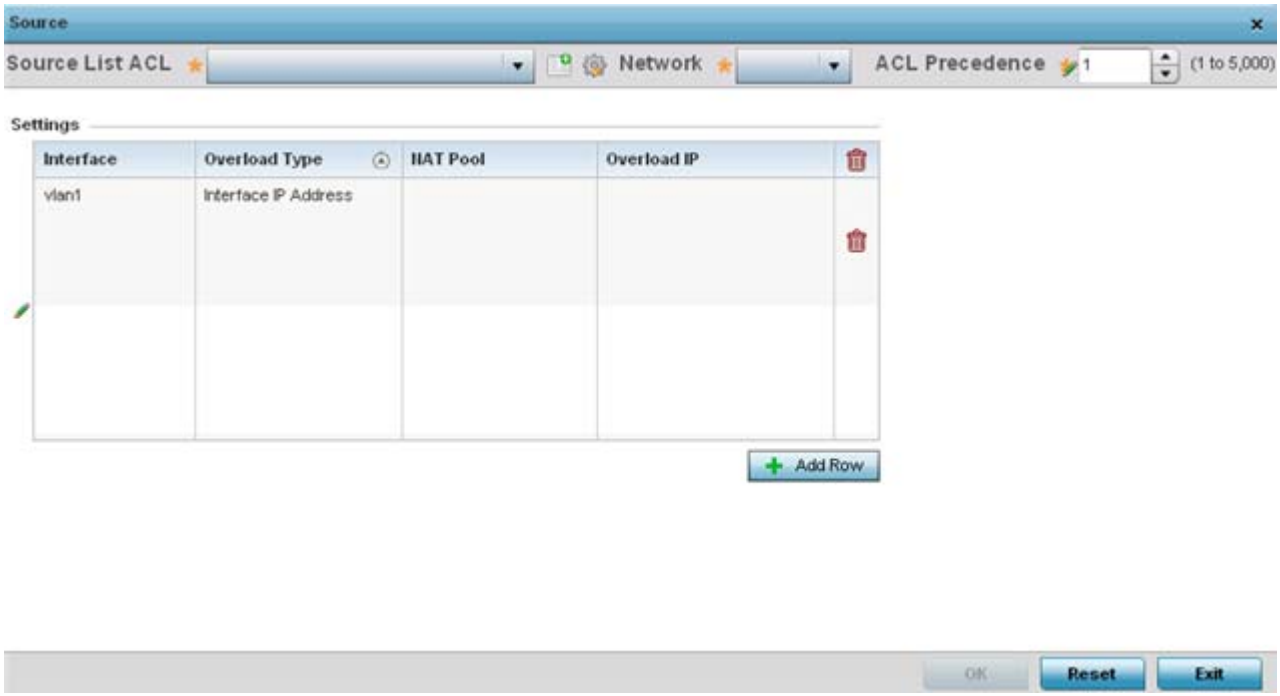


Figure 5-129 *Dynamic NAT Add screen*

20 Set or override the following to define the Dynamic NAT configuration:

Source List ACL	Use the drop-down menu to select an ACL name to define the packet selection criteria for NAT. NAT is applied only to packets which match a rule defined in the access list. These addresses (once translated) are not exposed to the outside world when the translation address is used to interact with a remote destination.
Network	Select *Inside* or *Outside* NAT as the network direction for the dynamic NAT configuration. Inside is the default setting.
ACL Precedence	Set the priority (from 1 - 5000) for the source list ACL. The lower the value, the higher the priority assigned to these ACL rules.
Interface	Use the drop-down menu to select the wireless WAN or VLAN ID (1 - 4094) used as the communication medium between the source and destination points within the NAT configuration. Ensure the VLAN selected represents the intended network traffic within the NAT supported configuration. VLAN1 is available by default.
Overload Type	Define the Overload Type utilized when several internal addresses are NATed to only one or a few external addresses. Options include *NAT Pool*, *One Global Address* and *Interface IP Address*. Interface IP Address is the default setting.
NAT Pool	Provide the name of an existing NAT pool for use with the dynamic NAT configuration.
Overload IP	If One Global IP Address is selected as the Overload Type, define an IP address used a filter address for the IP ACL rule.

21 Select **OK** to save the changes or overrides made to the dynamic NAT configuration. Select **Reset** to revert to the last saved configuration.

5.2.9.7 Overriding a Profile's Bridge NAT Configuration

Overriding a Profile's Security Configuration

Use *Bridge NAT* to manage Internet traffic originating at a remote site. In addition to traditional NAT functionality, Bridge NAT provides a means of configuring NAT for bridged traffic through an Access Point. NAT rules are applied to bridged traffic through the Access Point, and matching packets are NATed to the WAN link instead of being bridged on their way to the router.

Using Bridge NAT, a tunneled VLAN (extended VLAN) is created between the NoC and a remote location. When a remote client needs to access the Internet, Internet traffic is routed to the NoC, and from there routed to the Internet. This increases the access time for the end user on the client.

To resolve latency issues, Bridge NAT identifies and segregates traffic heading towards the NoC and outwards towards the Internet. Traffic towards the NoC is allowed over the secure tunnel. Traffic towards the Internet is switched to a local WLAN link with access to the Internet.

To define a NAT configuration or override that can be applied to a profile:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Security** to expand its sub menu options.

5 Select **Bridge NAT**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

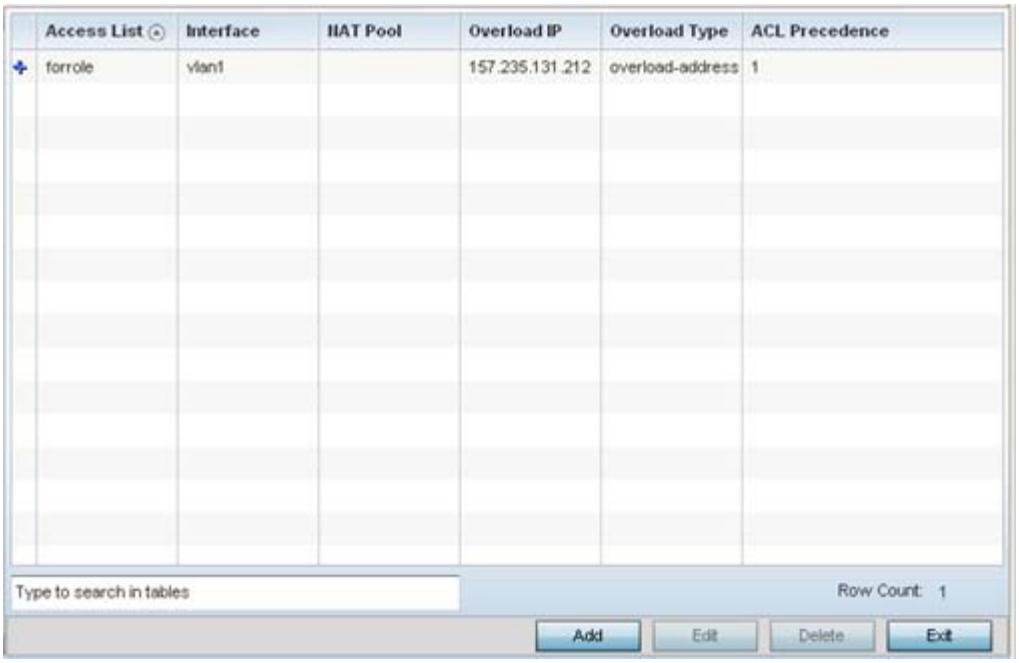


Figure 5-130 *Security Bridge NAT screen*

6 Review the following **Bridge NAT** configurations to determine whether a new Bridge NAT configuration requires creation or an existing configuration modified or removed.

Access List	Displays the access list applying IP address access/deny permission rules to the Bridge NAT configuration.
Interface	Lists the communication medium (outgoing layer 3 interface) between source and destination points. This is either the Access Point's *pppoe1* or *wwan1* interface or the VLAN used as the redirection interface between the source and destination.
NAT Pool	Lists the names of existing NAT pools used with the Bridge NAT configuration. This displays only when *Overload Type* is NAT Pool.
Overload IP	Lists the address used globally for numerous local addresses.
Overload Type	Define the overload type utilized when several internal addresses are NATed to only one or a few external addresses. Set as either *NAT Pool*, *One Global Address* or *Interface IP Address*.
ACL Precedence	Lists the administrator assigned priority set for the ACL. The lower the value listed the higher the priority assigned to these ACL rules.

7 Select **Add** to create a new Bridge VLAN configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.

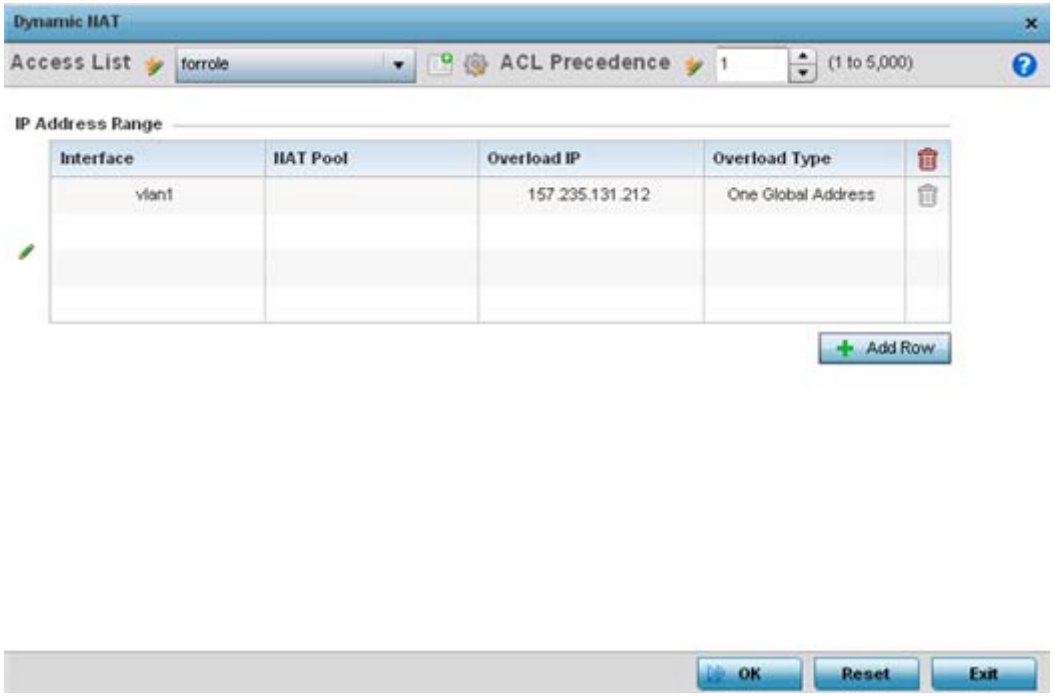


Figure 5-131 *Security Source Dynamic NAT screen*

8 Select the **ACL** whose IP rules are applied to the policy based forwarding rule. A new ACL can be defined by selecting the **Create** icon, or an existing set of IP ACL rules can be modified by selecting the **Edit** icon.

9 Use the **IP Address Range** table to configure IP addresses and address ranges that can used to access the Internet.

ACL Precedence	Set the priority (from 1 - 5000) for the ACL. The lower the value, the higher the priority assigned to these ACL rules.
Interface	Lists the outgoing layer 3 interface on which traffic is re-directed. The interface can be an Access Point *wwan* or *pppoe* interface. Traffic can also be redirected to a designated VLAN.
NAT Pool	Displays the NAT pool used by this Bridge NAT entry. A value is only displayed only when Overload Type has been set to *NAT Pool*.
Overload IP	Lists the single global address supporting numerous local addresses.
Overload Type	Lists the overload type utilized when several internal addresses are NATed to only one or a few external addresses. Options include *NAT Pool*, *One Global Address* and *Interface IP Address*. Interface IP Address is the default setting.

10 Select **+ Add Row** to set the interface, overload and NAT pool settings for the Bridge NAT configuration.

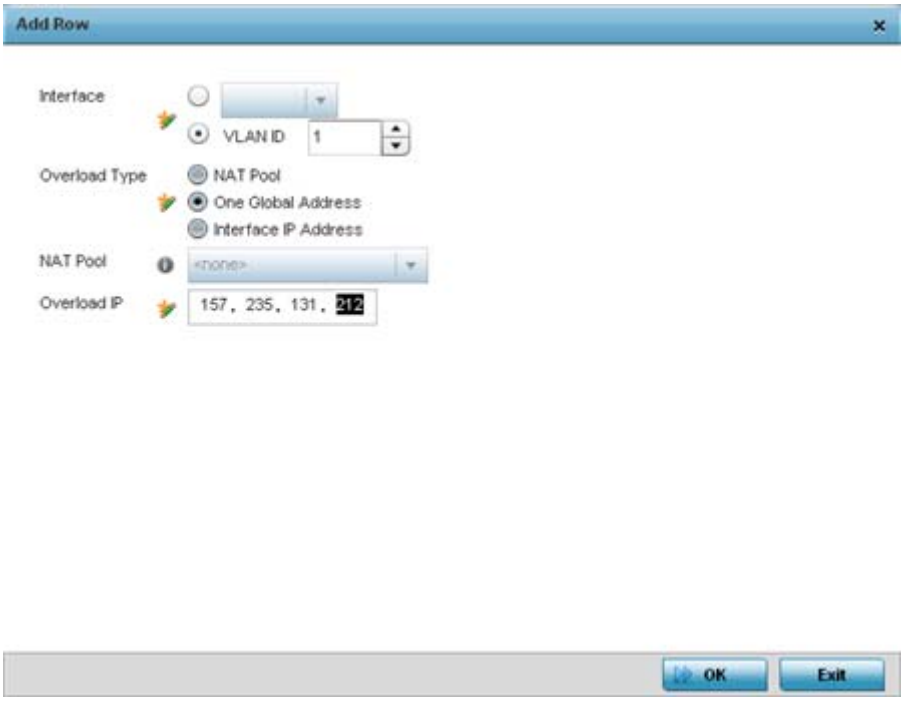


Figure 5-132 *Security Source Dynamic NAT screen*

11 Select **OK** to save the changes made within the Add Row and Source Dynamic NAT screen. Select **Reset** to revert to the last saved configuration.

5.2.9.8 Overriding a Profile's Application Visibility Settings

Overriding a Profile's Security Configuration

Deep Pocket Inspection (DPI) is an advanced packet analysis technique, which analyzes packet and packet content headers to determine the nature of network traffic. When DPI is enabled, packets of all flows are subjected to DPI to get accurate results. DPI identifies applications (such as, Netflix, Twitter, Facebook, etc.) and extracts metadata (such as, host name, server name, TCP-RTT, etc.) for further use by the WiNG firewall.

To configure a profile's application visibility settings and overrides:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Security** to expand its sub menu options.

5 Select **Application Visibility.**

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

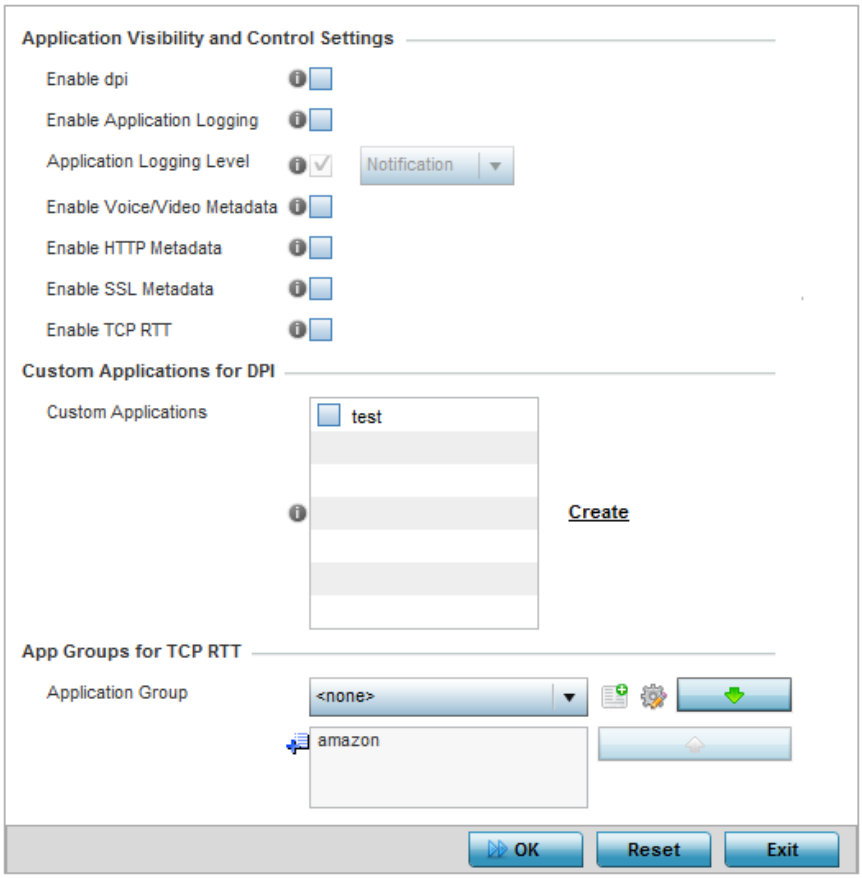


Figure 5-133 *Profile Overrides - Application Visibility screen*

6 Refer the following **Application Visibility and Control Settings**:

Enable dpi	Enable this setting to provide deep-packet inspection. When enabled, network flows are inspected at a granular level to identify applications (such as, Netflix, Twitter, Facebook, etc.) and extract metadata (such as, host name, server name, TCP-RTT, etc.) for further use by the WiNG firewall.
Enable Applications Logging	Select this option to enable event logging for DPI application recognition. This setting is disabled by default.
Application Logging Level	If enabling DPI application recognition event logging, set the logging level. Severity levels include *Emergency, Alert, Critical, Errors, Warning, Notice, Info* and *Debug*. The default logging level is Notification.
Enable Voice/Video Metadata	Select this option to enable the metadata extraction from voice and video classified flows. The default setting is disabled.

Enable HTTP Metadata	Select this option to enable the metadata extraction from HTTP flows. The default setting is disabled.
Enable SSL Metadata	Select this option to enable the metadata extraction from SSL flows. The default setting is disabled.
Enable TCP RTT	Select this option to enable extraction of RTT information from TCP flows. The default setting is disabled.

7 Review the **Custom Applications for DPI** field to select the custom applications available for this device profile. For information on creating custom applications and their categories, see Application on page 7-58.

8 If enabling TCP-RTT metadata collection, in the **App Groups for TCP RTT** field, specify the application groups for which TCP-RTT metadata collection is to be enabled. Select the *Application Groups* from the drop-down menu and use the green, down arrow to move the selection to the box below. Note, you can add maximum of 8 (eight) groups to the list. If the desired application group is not available, select the **Create** icon to define a new application group configuration or select the **Edit** icon to modify an existing application group. For information on creating custom application groups, see Application Group on page 7-60.

9 Select **OK** to save the changes or overrides. Select **Reset** to revert to the last saved configuration.

5.2.9.9 Overriding a Profile's VRRP Configuration

Profile Overrides

A default gateway is a critical resource for connectivity. However, it's prone to a single point of failure. Thus, redundancy for the default gateway is required by the Access Point. If WAN backhaul is available, and a router failure occurs, then the Access Point should act as a router and forward traffic on to its WAN link.

Define an external *Virtual Router Redundancy Protocol* (VRRP) configuration when router redundancy is required in a wireless network requiring high availability.

The election of a VRRP master is central to the configuration of VRRP. A VRRP master (once elected) performs the following functions:

- Responds to ARP requests
- Forwards packets with a destination link layer MAC address equal to the virtual router MAC address
- Rejects packets addressed to the IP address associated with the virtual router, if it is not the IP address owner
- Accepts packets addressed to the IP address associated with the virtual router, if it is the IP address owner or accept mode is true.

Nodes losing the election process enter a backup state where they monitor the master for any failures, and in case of a failure, one of the backups become the master and assumes the management of the designated virtual IPs. A backup does not respond to an ARP request, and discards packets destined for a virtual IP resource.

To define the configuration of a VRRP group:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of managed devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **VRRP**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

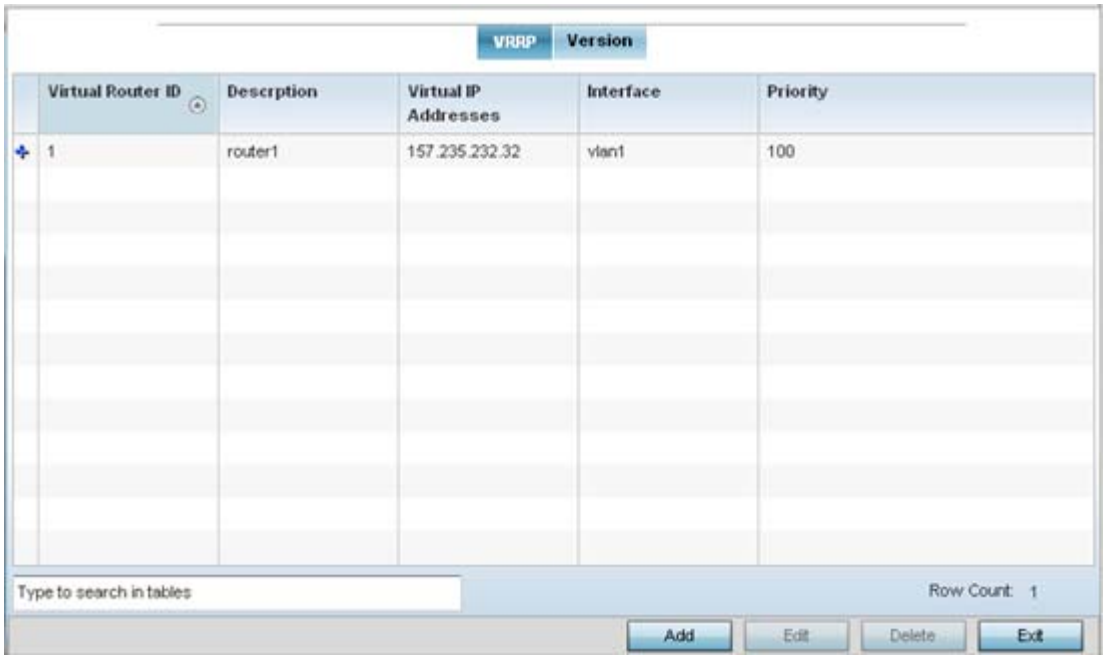


Figure 5-134 *Profile Overrides - VRRP screen*

5 Review the following VRRP configuration data to assess if a new VRRP configuration is required of is an existing VRRP configuration requires modification or removal:

Virtual Router ID	Lists a numerical index (1 - 255) used to differentiate VRRP configurations. The index is assigned when a VRRP configuration is initially defined. This ID identifies the virtual router a packet is reporting status for.
Description	Displays a description assigned to the VRRP configuration when it was either created or modified. The description is implemented to provide additional differentiation beyond the numerical virtual router ID.
Virtual IP Addresses	Lists the virtual interface IP address used as the redundant gateway address for the virtual route.
Interface	Displays the interfaces selected on the Access Point to supply VRRP redundancy fail over support.
Priority	Lists a numerical value (from 1 - 254) used for the virtual router master election process. The higher the numerical value, the higher the priority in the election process.

6 Select the **Version** tab to define the VRRP version scheme used with the configuration.

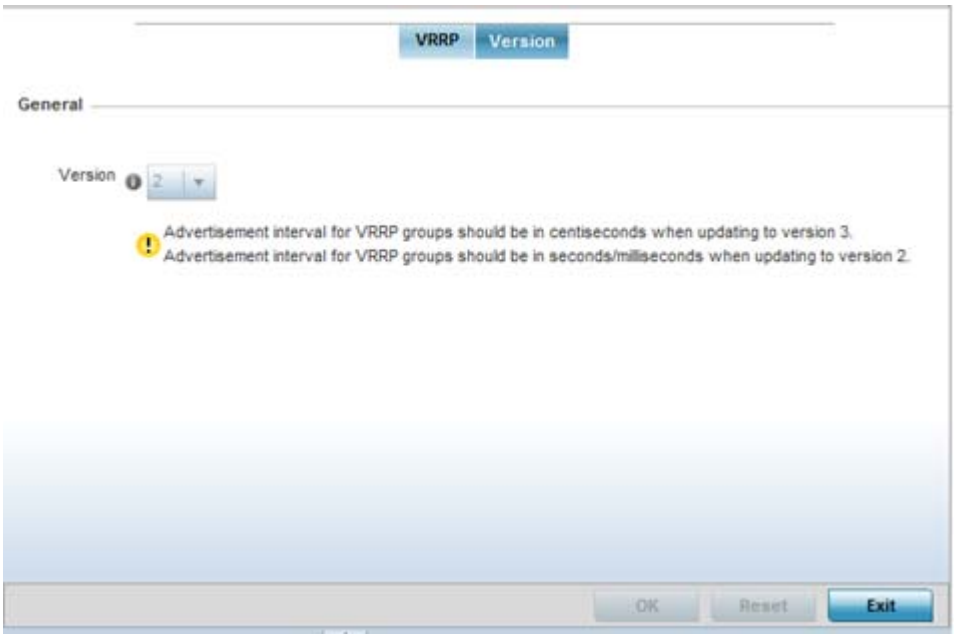


Figure 5-135 *VRRP screen - Version tab*

VRRP version 3 (RFC 5798) and 2 (RFC 3768) are selectable to set the router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP. For more information on the VRRP protocol specifications (available publicly) refer to http://www.ietf.org/rfc/rfc3768.txt (version 2) and http://www.ietf.org/rfc/rfc5798.txt (version 3).

7 From within VRRP tab, select **Add** to create a new VRRP configuration or **Edit** to modify the attributes of an existing VRRP configuration. If necessary, existing VRRP configurations can be selected and permanently removed by selecting **Delete**.

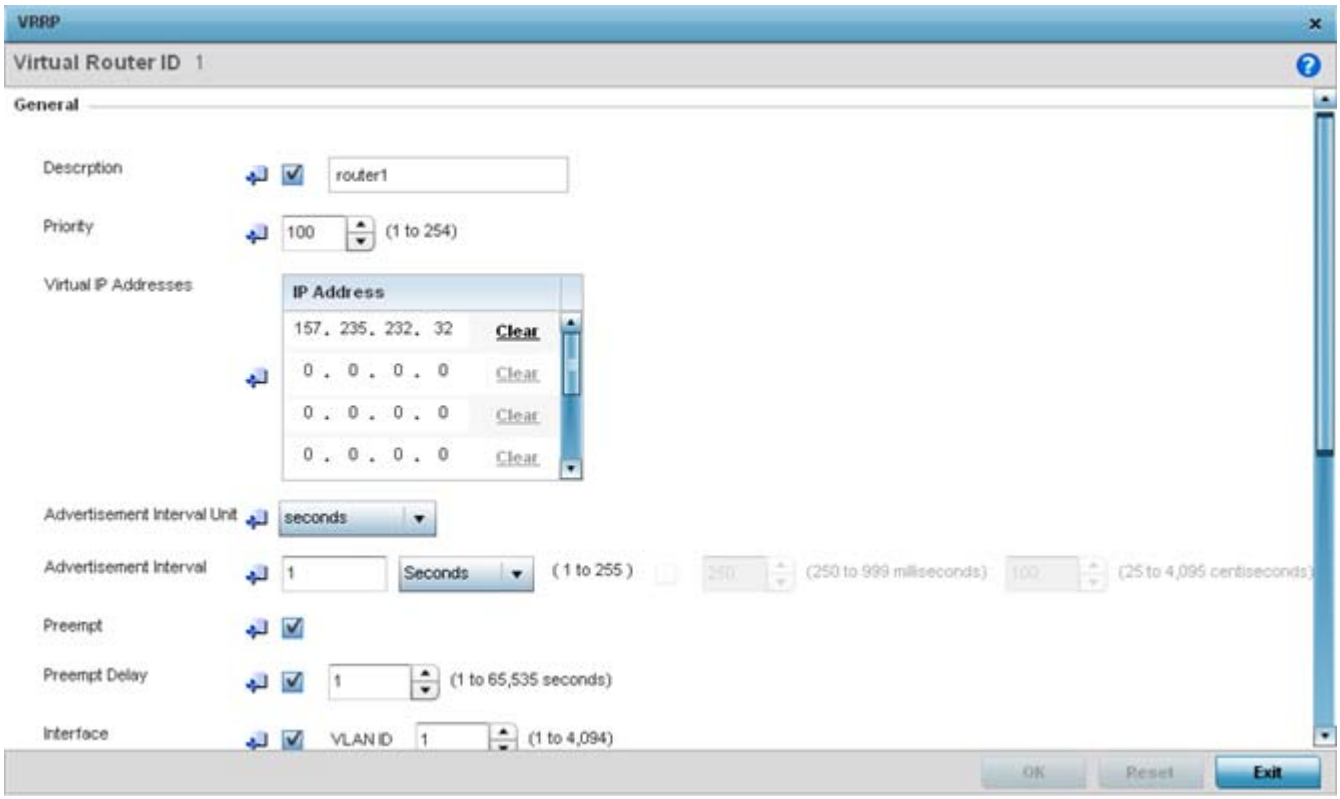


Figure 5-136 *VRRP screen*

8 If creating a new VRRP configuration, assign a **Virtual Router ID** from (1 - 255). In addition to functioning as numerical identifier, the ID identifies the virtual router a packet is reporting status for.

9 Define the following VRRP **General** parameters:

Description	In addition to an ID assignment, a virtual router configuration can be assigned a textual description (up to 64 characters) to further distinguish it from others with a similar configuration.
Priority	Use the spinner control to set a VRRP priority setting from 1 - 254. The controller or service platform uses the defined setting as criteria in selection of a virtual router master. The higher the value, the greater the likelihood of this virtual router ID being selected as the master.
Virtual IP Addresses	Provide up to 8 IP addresses representing the Ethernet switches, routers or security appliances defined as virtual router resources.
Advertisement Interval Unit	Select either *seconds*, *milliseconds* or *centiseconds* as the unit used to define VRRP advertisements. Once an option is selected, the spinner control becomes enabled for that *Advertisement Interval* option. The default interval unit is seconds. If changing the VRRP group version from 2 to 3, ensure the advertisement interval is in centiseconds. Use VRRP group version 2 when the advertisement interval is either in seconds or milliseconds.
Advertisement Interval	Once an *Advertisement Interval* unit has been selected, use the spinner control to set the interval the VRRP master sends out advertisements on each of its configured VLANs. The default setting is 1 second.

Preempt	Select this option to ensure a high priority backup router is available to preempt a lower priority backup router resource. The default setting is enabled. When selected, the *Preempt Delay* option becomes enabled to set the actual delay interval for pre-emption. This setting determines if a node with a higher priority can take over all the Virtual IPs from the nodes with a lower priority.
Preempt Delay	If the Preempt option is selected, use the spinner control to set the delay interval (in seconds) for pre-emption.
Interface	Select this value to enable/disable VRRP operation and define the VLAN (1 - 4,094) interface where VRRP will be running. These are the interfaces monitored to detect a link failure.

10 Refer to the **Protocol Extension** field to define the following:

Sync Group	Select the option to assign a VRRP sync group to this VRRP ID's group of virtual IP addresses. This triggers VRRP fail over if an advertisement is not received from the virtual masters that are part of this VRRP sync group. This setting is disabled b y default.
Network Monitoring: Local Interface	Select *wwan1*, *pppoe1* and *VLAN ID(s)* as needed to extend VRRP monitoring to these local Access Point interfaces. Once selected, these interfaces can be assigned an increasing or decreasing level or priority for virtual routing within the VRRP group.
Network Monitoring: Critical Resource	Assign the priority level for the selected local interfaces. Backup virtual routers can increase or decrease their priority in case the critical resources connected to the master router fail, and then transition to the master state themselves. Additionally, the master virtual router can lower its priority if the critical resources connected to it fails, so the backup can transition to the master state. This value can only be set on the backup or master router resource, not both. Options include *None*, *increment-priority*, *decrement priority*.
Network Monitoring: Critical Resource Name	Select each critical resource needed for monitoring. The action specified in the critical resource drop-down menu is applied to each selected critical resource.
Network Monitoring: Delta Priority	Use this setting to decrement the configured priority (by the set value) when the monitored interface is down. When critical resource monitoring, the value is incremented by the setting defined.

11 Select **OK** to save the changes made to the VRRP configuration. Select **Reset** to revert to the last saved configuration.

5.2.9.10 Overriding a Profile's Critical Resource Configuration

Profile Overrides

Critical resources are device IP addresses or destinations interopreted as critical to the health of the network. The critical resource feature allows for the continuous monitoring of these defined addresses. A critical resource, if not available, can result in the network suffering performance degradation. A critical resource can be a gateway, AAA server, WAN interface or any hardware or service on which the stability of the network depends. Critical resources are pinged regularly. If there's a connectivity issue, an event is generated stating a critical resource is unavailable. By default, there's no enabled critical resource policy and one needs to be created and implemented.

Critical resources can be monitored directly through the interfaces on which they're discovered. For example, a critical resource on the same subnet as the Access Point can be monitored by its IP address. However, a critical resource located on a VLAN must continue to monitored on that VLAN.

Critical resource can be configured for Access Points and wireless controllers using their respective profiles.

To define critical resources:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Critical Resources**.

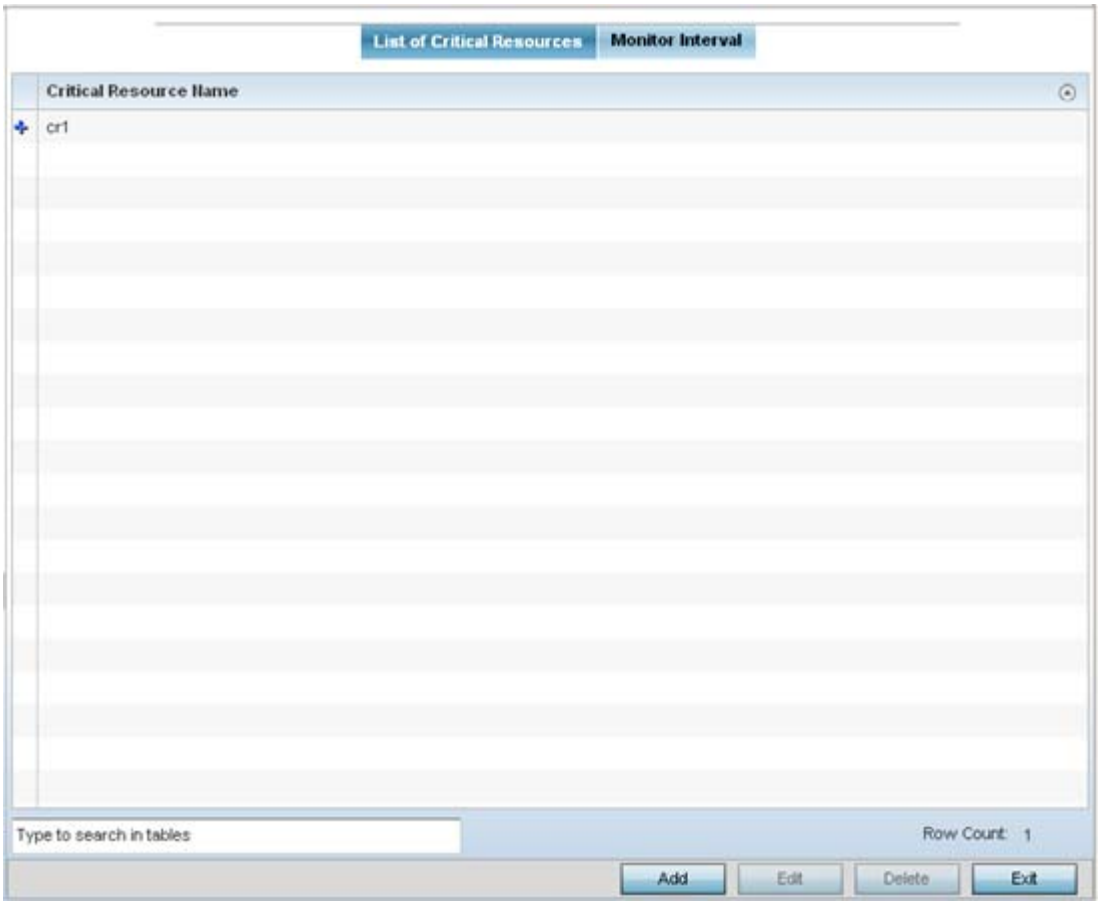


Figure 5-137 *Critical Resources screen - List of Critical Resources tab*

The screen lists the destination IP addresses or interfaces (VLAN, WWAN, or PPPoE) used for critical resource connection. IP addresses can be monitored directly by the controller, service platform or Access Point whereas a VLAN, WWAN or PPPoE must be monitored behind an interface.

5 The **Critical Resource Name** table displays the name of the resource(s) configured on this device.

6 Click the **Add** button at the bottom of the screen to add a new critical resource and connection method, or select an existing resource and select **Edit** to update the resource's configuration. If adding a new critical resource, assign it a name up to 32 characters.

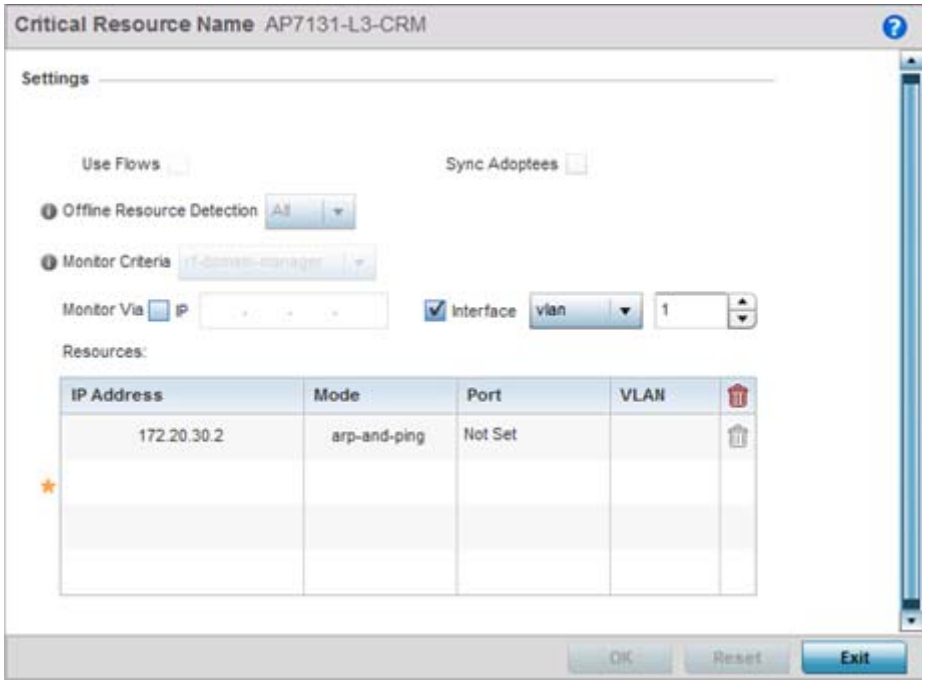


Figure 5-138 *Critical Resources screen - Adding a Critical Resource*

7 Select **Use Flows** to configure the critical resource to monitor using firewall flows for DHCP or DNS instead of ICMP or ARP packets to reduce the amount of traffic on the network. Select **Sync Adoptees** to sync adopted devices to state changes with a resource-state change message. These settings are disabled by default.

8 Use the **Offline Resource Detection** drop-down menu to define how critical resource event messages are generated. Options include *Any* and *All*. If selecting **Any**, an event is generated when the state of any single critical resource changes. If selecting **All**, an event is generated when the state of all monitored critical resources change.

9 Use the **Monitor Criteria** drop-down menu to select either *rf-domain-manager*, *cluster-master* or *All* as the resource for monitoring critical resources by one device and updating the rest of the devices in a group.

If selecting **rf-domain-manager**, the current rf-domain manager performs resource monitoring, and the rest of the devices do not. The RF-domain-manager updates any state changes to the rest of the devices in the RF Domain. With the **cluster-master** option, the cluster master performs resource monitoring and updates the cluster members with state changes. With a controller managed RF Domain, Monitoring Criteria should be set tor **All**, since the controller might not know the VLAN bridged locally by the devices in the RF Domain monitoring DHCP.

10 Select the **IP** option (within the **Monitor Via** field at the top of the screen) to monitor a critical resource directly (within the same subnet) using the provided IP address as a network identifier.

11 Select the **Interface** check box (within the Monitor Via field at the top of the screen) to monitor a critical resource using either the critical resource's VLAN, WWAN1 or PPPoE1 interface. If VLAN is selected, a spinner control is enabled to define the destination VLAN ID used as the interface for the critical resource.

12 Select **+ Add Row** to define the following for critical resource configurations:

IP Address	Provide the IP address of the critical resource. This is the address used by the Access Point to ensure the critical resource is available. Up to four addresses can be defined.

Mode	Set the ping mode used when the availability of a critical resource is validated. Select from: *arp-only* – Use the *Address Resolution Protocol* (ARP) for only pinging the critical resource. ARP is used to resolve hardware addresses when only the network layer address is known. *arp-and-ping* – Use both ARP and *Internet Control Message Protocol* (ICMP) for pining the critical resource and sending control messages (device not reachable, requested service not available, etc.).
Port	Define the interface on which to monitor critical resource. This field lists the available hardware interfaces. This option is only available if the selected mode is ARP Only.
VLAN	Define the VLAN on which the critical resource is available using the spinner control.

13 Select the **Monitor Interval** tab.

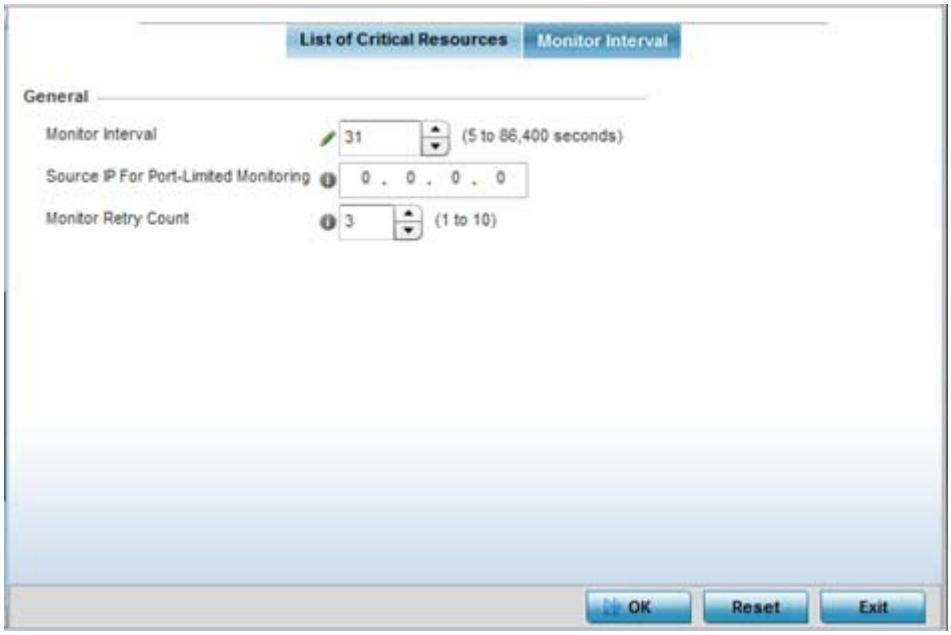


Figure 5-139 *Critical Resources screen - Monitor Interval tab*

Set **Monitor Interval** as the duration between two successive pings to the critical resource. Define this value in seconds from 5 - 86,400. The default setting is 30 seconds.

14 Set the **Source IP for Port-Limited Monitoring** to define the IP address used as the source address in ARP packets used to detect a critical resource on a layer 2 interface. Generally, the source address 0.0.0.0 is used in the APR packets used to detect critical resources. However, some devices do not support the above IP address and drop the ARP packets. Use this field to provide an IP address specifically used for this purpose. The IP address used for Port-Limited Monitoring must be different from the IP address configured on the device.

15 Set the **Monitoring Retries before Marking Resource as DOWN** for the number of retry connection attempts (1 - 10) permitted before this device connection is defined as down (offline). The default setting is three connection attempts.

16 Select **OK** to save the changes to the critical resource configuration and monitor interval. Select **Reset** to revert to the last saved configuration.

5.2.9.11 Overriding a Profile's Services Configuration

Profile Overrides

A profile can contain specific guest access (captive portal), DHCP server and RADIUS server configurations supported by the controller, service platform or Access Point's own internal resources. These access, IP assignment and user authorization resources can be defined uniquely as profile requirements dictate.

To define or override a profile's services configuration:

1 Select **Devices** from the Configuration tab.

The *Device Configuration* screen displays a list of devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Select **Services**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

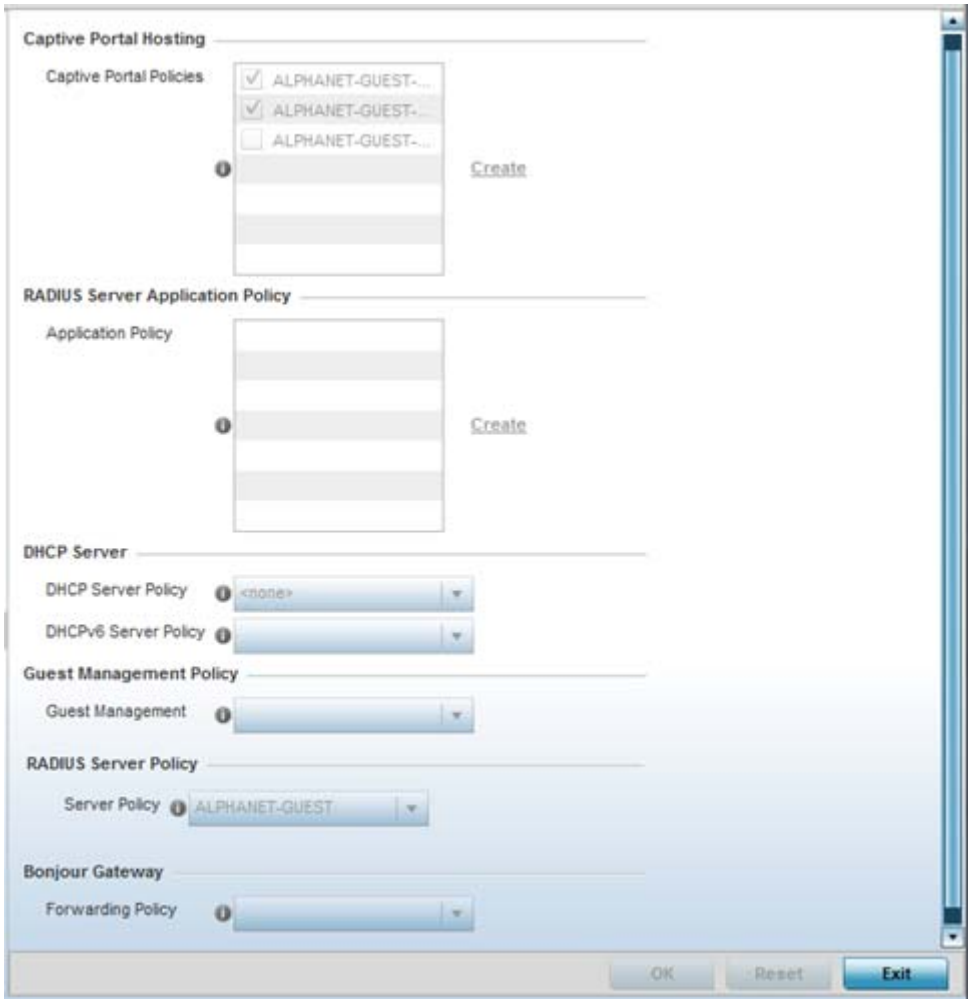


Figure 5-140 *Profile Overrides - Services screen*

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

5 Refer to the **Captive Portal Hosting** field to set or override the guest access configuration (captive portal) for this profile.

A *captive portal* is an access policy for providing guests temporary and restrictive access to the wireless network.

A captive portal configuration provides secure authenticated controller or service platform access using a standard Web browser. Hotspots provides authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the wireless network. Once logged into the captive portal additional *Agreement*, *Welcome* and *Fail* pages provide the administrator with a number of options on the hotspot's screen flow and user appearance.

Either select an existing captive portal policy, use the default captive portal policy or select the **Create** link to create a new configuration that can be applied to this profile. For more information, see Configuring Captive Portal Policies on page 11-1.

6 Use the **RADIUS Server Application Policy** drop-down menu to select an application policy to authenticate users and authorize access to the network. A RADIUS policy provides the centralized management of authentication data (usernames and passwords). When an client attempts to associate, the controller or service platform sends the authentication request to the RADIUS server.

If an existing RADIUS server policy does not meet your requirements, select the **Create** link to create a new policy.

7 Use the **DHCP Server Policy** drop-down menu assign this profile a DHCP server policy. If an existing DHCP policy does not meet the profile's requirements, select the Create icon to create a new policy configuration that can be applied to this profile or the Edit icon to modify the parameters of an existing DHCP Server policy.

Dynamic Host Configuration Protocol (DHCP) allows hosts on an IP network to request and be assigned IP addresses as well as discover information about the network where they reside. Each subnet can be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool. When the onboard DHCP server allocates an address for a DHCP client, the client is assigned a lease, which expires after an pre-determined interval. Before a lease expires, wireless clients (to which leases are assigned) are expected to renew them to continue to use the addresses. Once the lease expires, the client is no longer permitted to use the leased IP address. The profile's DHCP server policy ensures all IP addresses are unique, and no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired).

8 Use the **DHCPv6 Server Policy** drop-down menu assign this profile a DHCPv6 server policy. If an existing DHCP policy for IPv6 does not meet the profile's requirements, select the Create icon to create a new policy configuration that can be applied to this profile or the Edit icon to modify the parameters of an existing DHCP Server policy.

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. DHCP in IPv6 works in with IPv6 router discovery. With the proper RA flags, DHCPv6 works like DHCP for IPv4. The central difference is the way a device identifies itself if assigning addresses manually instead of selecting addresses dynamically from a pool.

For more information, see Configuring Captive Portal Policies on page 11-1.

9 Use the **Guest Management Policy** drop-down menu to select an existing Guest Management policy to use as a mechanism to manage guest users with this profile.

10 Use the **RADIUS Server Policy** drop-down menu to select an existing RADIUS server policy to use as a user validation security mechanism with this profile.

A profile can have its own unique RADIUS server policy to authenticate users and authorize access to the network. A profile's RADIUS policy provides the centralized management of controller or service platform authentication data (usernames and passwords). When an client attempts to associate, an authentication request is sent to the RADIUS server.For more information, see Configuring RADIUS Server Policies on page 11-57.

11 Set **Bonjour Gateway** settings. Bonjour is Apple's implementation of zero-configuration networking (Zeroconf). Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates devices such as printers, other computers and services that these computers offer over a local network.

Bonjour provides a general method to discover services on a local area network (LAN). It allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with special DNS configuration, it can be extended to find services across broadcast domains.

12 From the **Forwarding Policy** drop-down, select the Bonjour Gateway forwarding policy. n.

13 Select **OK** to save the changes or overrides made to the profile's services configuration. Select **Reset** to revert to the last saved configuration.

5.2.9.12 Overriding a Profile's Management Configuration

Profile Overrides

Controllers and service platforms have mechanisms to allow/deny management access to the network for separate interfaces and protocols (*HTTP, HTTPS*, *Telnet*, *SSH* or *SNMP*). These management access configurations can be applied strategically to profiles as resource permissions dictate. Additionally, overrides can be applied to customize a device's management configuration, if deployment requirements change an a devices configuration must be modified from its original device profile configuration.

Additionally, an administrator can define a profile with unique configuration file and device firmware upgrade support. In a clustered environment, these operations can be performed on one controller or service platform, then propagated to each member of the cluster and onwards to devices managed by each cluster member.

To define or override a profile's management configuration:

1 Select **Devices** from the Configuration tab.

The Device Configuration screen displays a list of devices or peer controllers, service platforms or Access Points.

2 Select a target device (by double-clicking it) from amongst those displayed within the Device Configuration screen.

Devices can also be selected directly from the Device Browser in the lower, left-hand, side of the UI.

3 Select **Profile Overrides** from the Device menu to expand it into sub menu options.

4 Expand the **Management** menu item and select **Settings**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

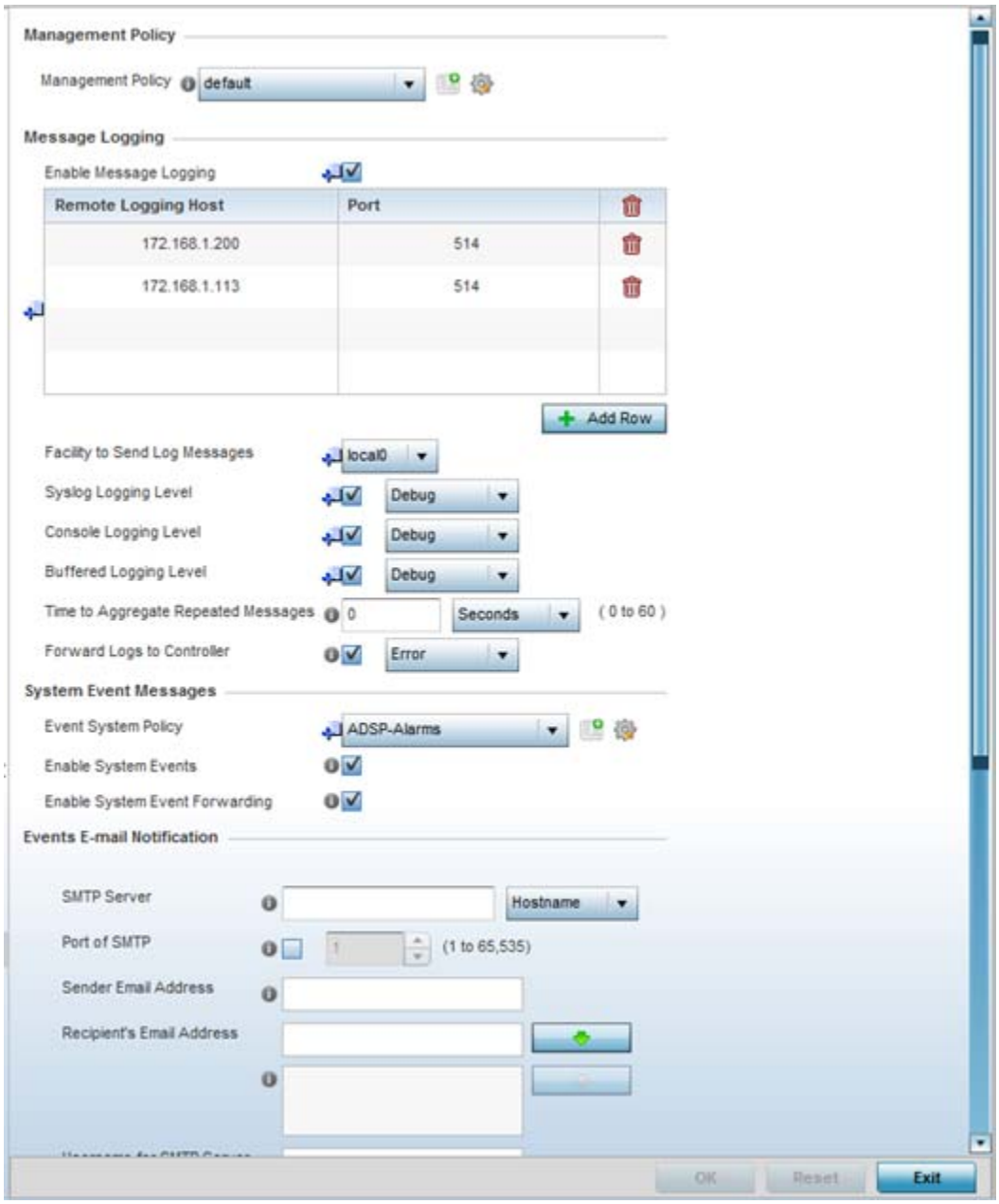


Figure 5-141 *Profile Overrides - Management Settings screen*

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

5 Refer to the **Management Policy** field to set or override a management configuration for this profile. A default management policy is also available if no existing policies are usable.

Use the drop-down menu to select an existing management policy to apply to this profile. If no management policies exist meeting the data access requirements of this profile, select the **Create** icon to access screens used to define administration, access control and SNMP configurations. Select an existing policy and select the

Edit icon to modify the configuration of an existing management policy. For more information, see Viewing Management Access Policies on page 12-1.

6 Refer to the **Message Logging** field to define how the profile logs system events. It's important to log individual events to discern an overall pattern potentially impacting performance.

Enable Message Logging	Select this option to enable the profile to log system events to a log file or a syslog server. Selecting this check box enables the rest of the parameters required to define the profile's logging configuration. This option is disabled by default.
Remote Logging Host	Use this table to define numerical (non DNS) IP addresses for up to three external resources where logged system events can be sent on behalf of the profile. Select the *Delete* icon as needed to remove an IP address.
Facility to Send Log Messages	Use the drop-down menu to specify the local server (if used) for profile event log transfers.
Syslog Logging Level	Event severity coincides with the syslog logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include 0 - *Emergency,* 1 - *Alert*, 2 - *Critical*, 3 - *Errors*, 4 - *Warning*, 5 - *Notice*, 6 - *Info* and 7 - *Debug*. The default logging level is 4.
Console Logging Level	Event severity coincides with the syslog logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include 0 - *Emergency,* 1 - *Alert*, 2 - *Critical*, 3 - *Errors*, 4 - *Warning*, 5 - *Notice*, 6 - *Info* and 7 - *Debug*. The default logging level is 4.
Buffered Logging Level	Event severity coincides with the syslog logging level defined for the profile. Assign a numeric identifier to log events based on criticality. Severity levels include 0 - *Emergency,* 1 - *Alert*, 2 - *Critical*, 3 - *Errors*, 4 - *Warning*, 5 - *Notice*, 6 - *Info* and 7 - *Debug*. The default logging level is 4.
Time to Aggregate Repeated Messages	Define the increment (or interval) system events are logged on behalf of the profile. The shorter the interval, the sooner the event is logged. Either define an interval in *Seconds* (0 - 60) or *Minutes* (0 -1). The default value is 0 seconds.
Forward Logs to Controller	Select the check box to define a log level for forwarding event logs. Log levels include *Emergency, Alert*, *Critical*, *Error*, *Warning*, *Notice*, *Info* and *Debug*. The default logging level is Error.

7 Refer to the **System Event Messages** section to define or override how controller or service platform system messages are logged and forwarded on behalf of the profile.

Event System Policy	Select an *Event System Policy* from the drop-down menu. If an appropriate policy does not exist, select the *Create* button to make a new policy.
Enable System Events	Select the *Enable System Events* check box to allow the profile to capture system events and append them to a log file. It's important to log individual events to discern an overall pattern that may be negatively impacting controller or service platform performance. This setting is enabled by default.
Enable System Event Forwarding	Select the *Enable System Event Forwarding* radio button to forward system events to another controller, service platform or cluster member. This setting is enabled by default.

8 Refer to the **Events E-mail Notification** section to define or override how system event notification Emails are sent.

SMTP Server	Specify either the *Hostname* or *IP Address* of the outgoing SMTP server where notification Emails are originated. Hostnames cannot include an underscore character.
Port of SMTP	If a non-standard SMTP port is used on the outgoing SMTP server, select this option and specify a port from 1 - 65,535 for the outgoing SMTP server to use.
Sender E-mail Address	Specify the Email address from which notification Email is originated. This is the *from* address on notification Email.
Recipient's E-mail Address	Specify up to 6 Email addresses to be the recipient's of event Email notifications.
Username for SMTP Server	Specify the sender username on the outgoing SMTP server. Many SMTP servers require users to authenticate with a *username* and *password* before sending Email through the server.
Password for SMTP Server	Specify the password associated with the username of the sender on the outgoing SMTP server. Many SMTP servers require users to authenticate with a *username* and *password* before sending Email through the server.

9 Refer to the **Persist Configurations Across Reloads** section to define or override how configuration settings are handled after reloads.

Configure	Use the drop-down menu to configure whether configuration overrides should persist when the device configuration is reloaded. Available options are *Enabled*, *Disabled* and *Secure*.

10 Refer to the **HTTP Analytics** field to define analytic compression settings and update intervals.

Compress	Select this option to use compression to when sending updates to the controller. This option is disabled by default.
Update Interval	Define an interval in either *Seconds* (1 - 3,600), *Minutes* (1 - 60) or *Hours* (1) for interval to push buffered packets. The default setting in 1 minute.

11 Refer to the **External Analytics Engine** section to define or override analytics engine login information for an external host.

The Guest Access & Analytics software module is a site-wide Enterprise License available only on service platforms. When a customer visits a store, they connect to the Wireless LAN via guest access using a mobile device. The user needs to authenticate only on their first visit, and will automatically connect to the network for subsequent visits. The Analytics module helps gather data about customer behavior such as web sites visited, search terms used, mobile device types, number of new users vs. repeat users. This data provides a better understanding of pricing strategies and promotions being run by competitors. The data can be exported for additional in-depth analysis.

Controller	Select this option to provide service platform analytics to a local device. This setting is enabled by default.
URL	When using an external analytics engine with a NX9000 series service platform, enter the IP address or *uniform resource locator* (URL) for the system providing external analytics functions.
User Name	Enter the user name needed to access the external analytics engine.

Password	Enter the password associated with the username on the external analytics engine.
Update Interval	Set the interval in either *Seconds* (1 - 3,600), *Minutes* (1 - 60) or *Hours* (1) to forward buffered information to an external server resource, even when the buffers are not full. The default setting in 1 minute.

12 Select **OK** to save the changes and overrides made to the profile's Management Settings. Select **Reset** to revert to the last saved configuration.

13 Select **Firmware** from the Management menu.

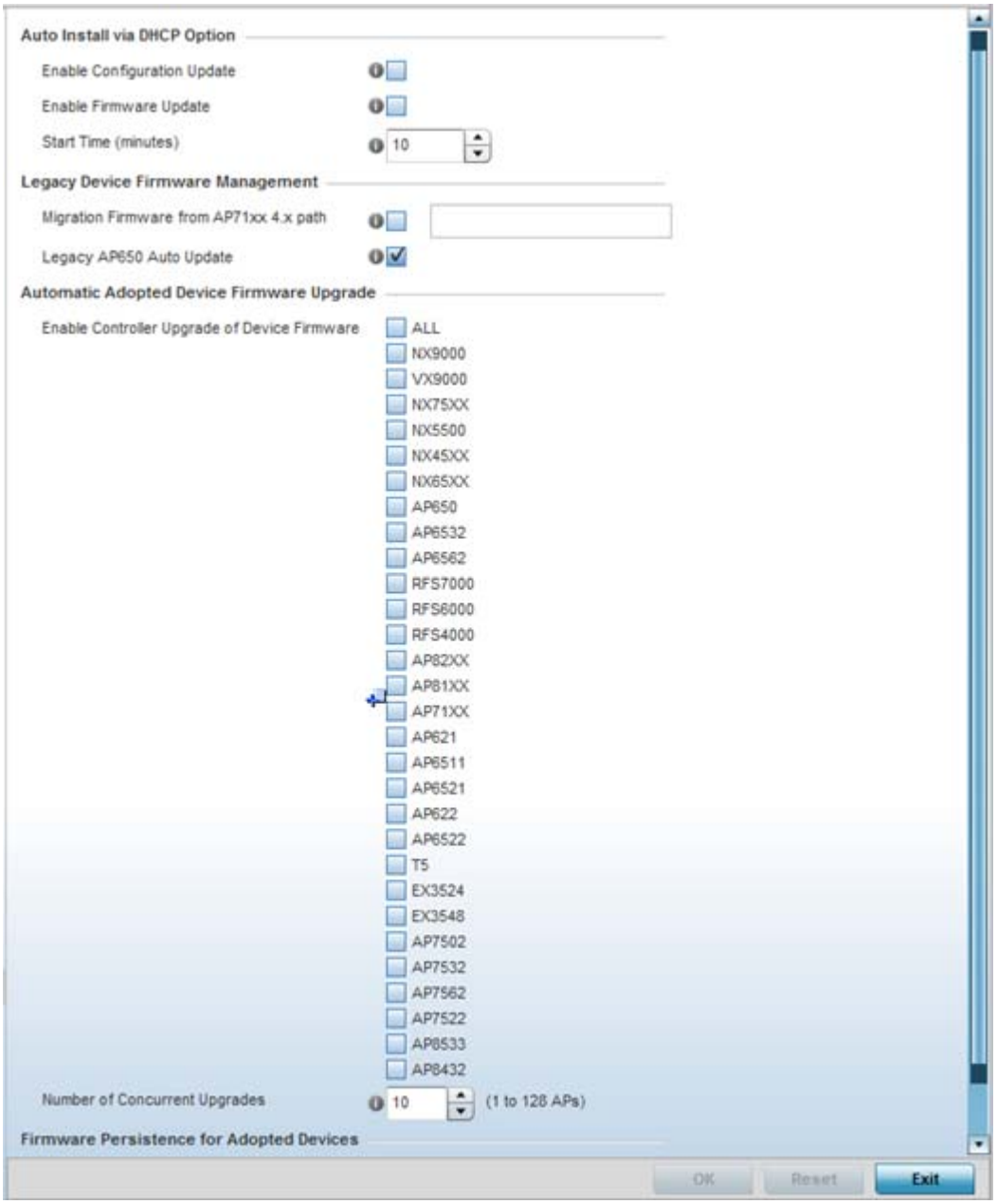


Figure 5-142 *Profile Overrides - Management Firmware screen*

14 Refer to the **Auto Install via DHCP Option** field to configure automatic configuration file and firmware updates.

Enable Configuration Update	Select *Enable Configuration Update* (from within the Automatic Configuration Update field) to enable automatic profile configuration file updates from an external location. If enabled (the setting is disabled by default), provide a complete path to the target configuration file used in the update.
Enable Firmware Update	Select this option to enable automatic firmware upgrades (for this profile) from a user defined remote location. This value is disabled by default.
Start Time (minutes)	Use the spinner control to set the number of minutes to delay the start of an auto upgrade operation. Stagger the start of an upgrade operation as needed in respect to allowing an Access Point to complete its current client support activity before being rendered offline during the update operation. The default setting is 10 minutes.

15 Refer to the parameters within the **Legacy Device Firmware Management** field to set legacy Access Point firmware provisions:

Migration Firmware from AP71xx 4.x path	Provide a path to a firmware image used to provision AP71xx model Access Points currently utilizing a 4.x version legacy firmware file. Once a valid path is provided, the update is enabled to the version maintained locally for AP71xx models.
Legacy AP650 Auto Update	Select this option to provision AP650 model Access Points from their legacy firmware versions to the version maintained locally for that model. This setting is enabled by default, making updates to AP650 models automatic if a newer AP650 image is maintained locally.

16 Use the parameters within the **Automatic Adopted AP Firmware Upgrade** section to define an automatic firmware upgrade from a local file.

Enable Controller Upgrade of Device Firmware	Select the device model to upgrade using the most recent firmware file on the controller, service platform or Virtual Controller AP. This parameter is enabled by default. Select All to update all the listed device types
Number of Concurrent Upgrades	Use the spinner control to define the maximum number (1 - 128) of adopted APs that can receive a firmware upgrade at the same time. The default value is 10. Keep in mind that during a firmware upgrade, the Access Point is offline and unable to perform its normal client support role until the upgrade process is complete.

17 Select the **Persist AP Images on Controller** button (from within the **Firmware Persistence for Adopted Devices** field) to enable the RF domain manager to retain and store the new image of an Access Point selected for a firmware update. The image is only stored on the RF domain manager when there's space to accommodate it.

The upgrade sequence is different depending on whether the designated RF domain manager is a controller/ service platform or Access Point.

- *When the RF domain manager is an Access Point* - The NOC uploads a provisions an Access Point model's firmware on to the Access Point RF domain manager. The NOC initiates an auto-update for Access Points using that model's firmware. If the **Persist Image on Controller** option is selected, the RF domain manager retains the image for that model. The NOC then provisions the firmware of the next Access Point type to the RF domain manager. The auto-update process is then repeated for that model. Once all the selected models have been updated, the RF domain manager's model is updated last.
- *When the RF domain manager is a controller or service platform* - The NOC adopts controllers to the NOC's cluster within its RF domain. The NOC triggers an update on active controllers or service platforms and reboots them as soon as the update is complete. As soon as the active nodes come back up, the NOC

triggers an update on standby controllers or service platforms and reboots them as soon as the update is complete. When the standby controllers or service platforms come back up the following conditions apply:

- *If the reboot is not scheduled* - The Access Points adopted to RF domain members are not updated. It's expected the controllers and service platforms have auto-upgrade enabled which will update the Access Points when re-adopted.
- *If the reboot is scheduled* - The NOC pushes the first Access Point model's firmware to the RF domain manager. The NOC initiates an Access Point upgrade on all Access Points on the RF domain manager for that model. If the **Persist Image on Controller** option is selected, the RF domain manager retains the image for that model. The NOC then provisions the firmware of the next Access Point type to the RF domain manager. This process is repeated until each selected Access Point model is updated.

The Firmware Persistence feature is *enabled* for all controller and service platform RF domain managers with the flash memory capacity to store firmware images for the selected Access Point models they provision. This feature is *disabled* for Access Point RF Domain managers that do not typically have the flash memory capacity needed.

18 Select **Heartbeat** from the Management menu. Select the **Service Watchdog** option to implement heartbeat messages to ensure associated devices are up and running and capable of effectively interoperating. The Service Watchdog is enabled by default.

19 Select OK to save the changes and overrides made to the profile's configuration. Select Reset to revert to the last saved configuration.

5.2.9.13 Overriding a Profile's Mesh Point Configuration

Profile Overrides

Mesh points are Access Points dedicated to mesh network support. Mesh networking enables users to access broadband applications anywhere (including moving vehicles).

To set or override an Access Point profile's Mesh Point configuration:

1 Select **Devices** from the Web UI.

2 Select **Device Configuration** to expand its menu items.

3 Select **Mesh Point**.

NOTE: A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click the **Clear Overrides** button. This removes all overrides from the device.

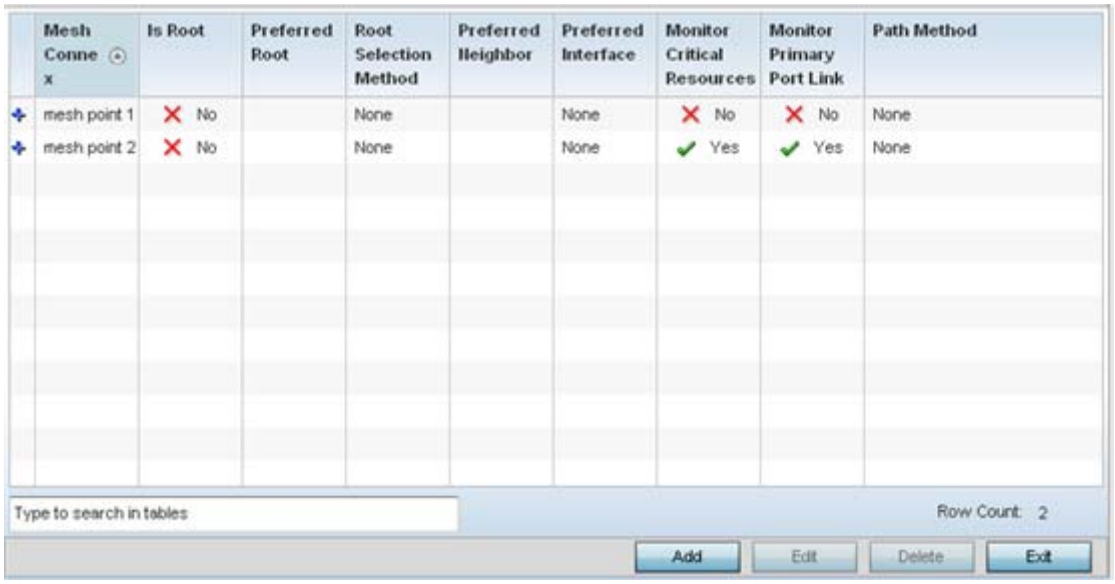


Figure 5-143 *Profile Overrides - Mesh Point screen*

4 Refer to the **Mesh Point** screen to view existing Mesh Point overrides. If an existing Mesh Point override does not meet your requirements, select the **Add** button to create a new override or the **Edit** button to modify the parameters of an existing override. The Mesh Point screen displays the **Settings** tab by default.

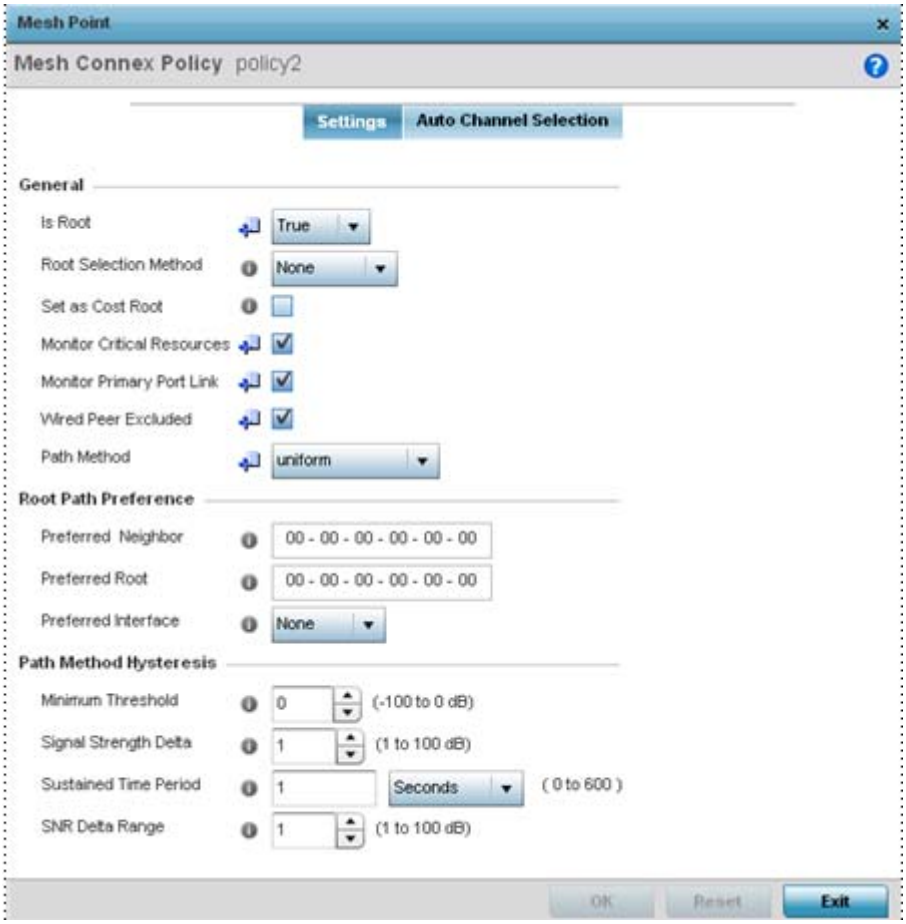


Figure 5-144 *Mesh Point - Settings Screen*

5 Define the following settings from within the **General** field:

MeshConnex Policy	If adding a new policy, specify a name for the MeshConnex Policy. The name cannot be edited later with other configuration parameters. Until a viable name is provided, the Settings tab cannot be enabled for configuration.
Is Root	Select the root behavior of this mesh point. Select *True* to indicate this mesh point is a root node for this mesh network. Select *False* to indicate this mesh point is not a root node for this mesh network.
Root Selection Method	Use the drop-down menu to determine whether this meshpoint is the root or non-root meshpoint. Select either *None, auto-mint* or *auto-proximity*. The default setting is None. When auto-mint is selected, root selection is based on the total cost to the root. Cost to the root is measured as total cost through hops to the root node. Root selection occurs for the root with the least path cost. When auto-proximity is selected, root selection is based on signal strength of candidate roots. None indicates no preference in root selection.
Set as Cost Root	Select this option to set the mesh point as the cost root for meshpoint root selection. This setting is disabled by default.
Monitor Critical Resources	Enable this feature to allow dynamic conversion of a mesh point from root to non-root when there is a critical resource failure. This option is disabled by default.
Monitor Primary Port Link	Enable this feature to allow dynamic conversion of a mesh point from root to non-root during a link down event. This option is disabled by default.
Wired Peer Excluded	Select this option to exclude a mesh from forming a link with another mesh device that's a wired peer. This option is disabled by default.
Path Method	From the drop-down menu, select the method to use for path selection in a mesh network. The available options are: *None* – Select this to indicate no criteria used in root path selection. *uniform* – Select this to indicate that the path selection method is uniform. When selected, two paths will be considered equivalent if the average value is the same for these paths. *mobile-snr-leaf* – Select this if this Access Point is mounted on a vehicle or a mobile platform (AP7161 models only). When selected, the path to the route will be selected based on the *Signal To Noise Ratio* (SNR) to the neighbor device. *snr-leaf* – Select this to indicate the path with the best signal to noise ratio is always selected. *bound-pair* – Select this option to bind one mesh point connection at a time. Once established, other mesh point connection requests are denied.

NOTE: An AP7161 model Access Point can be deployed as a *vehicular mounted modem* (VMM) to provide wireless network access to a mobile vehicle (car, train etc.). A VMM provides layer 2 mobility for connected devices. VMM does not provide layer 3 services, such as IP mobility. For VMM deployment considerations, see Vehicle Mounted Modem (VMM) Deployment Considerations on page 5-253.

NOTE: When using 4.9GHz, the root preferences selection for the radio's preferred interface still displays as 5GHz.

6 Set the following **Root Path Preference** values:

Preferred Neighbor	Specify the MAC address of a preferred neighbor to override mesh point settings.
Preferred Root	Specify the MAC address of a a preferred root device to override mesh point settings.
Preferred Interface	Use the drop-down menu to override the preferred mesh point interface to *2.4GHz*, *4.9 GHz* or *5.0GHz*. None defines the interface as open to any radio band.

7 Set the following **Path Method Hysteresis**:

Minimum Threshold	Enter the minimum value for SNR above which a candidate for the next hop in a dynamic mesh network is considered for selection. This field along with *Signal Strength Delta* and *Sustained Time Period* are used to dynamically select the next hop in a dynamic mesh network. The default setting is 0 dB.
Signal Strength Delta	Enter a delta value in dB. A candidate for selection as a next hop in a dynamic mesh network must have a SNR value that is higher than the value configured here. This field along with the *Minimum Threshold* and *Sustained Time Period* are used to dynamically select the next hop in a dynamic mesh network. The default setting is 1 dB.
Sustained Time Period	Enter the duration (in seconds or minutes) for the duration a signal must sustain the constraints specified in the *Minimum Threshold* and *Signal Strength Delta* path hysteresis values. These values are used to dynamically select the next hop in a dynamic mesh network. The default setting is 1 second.
SNR Delta Range	Select the root selection method hysteresis (from 1 - 100dB) SNR delta range a candidate must sustain. The default setting is 1 dB.

8 Select the **Auto Channel Selection** tab.

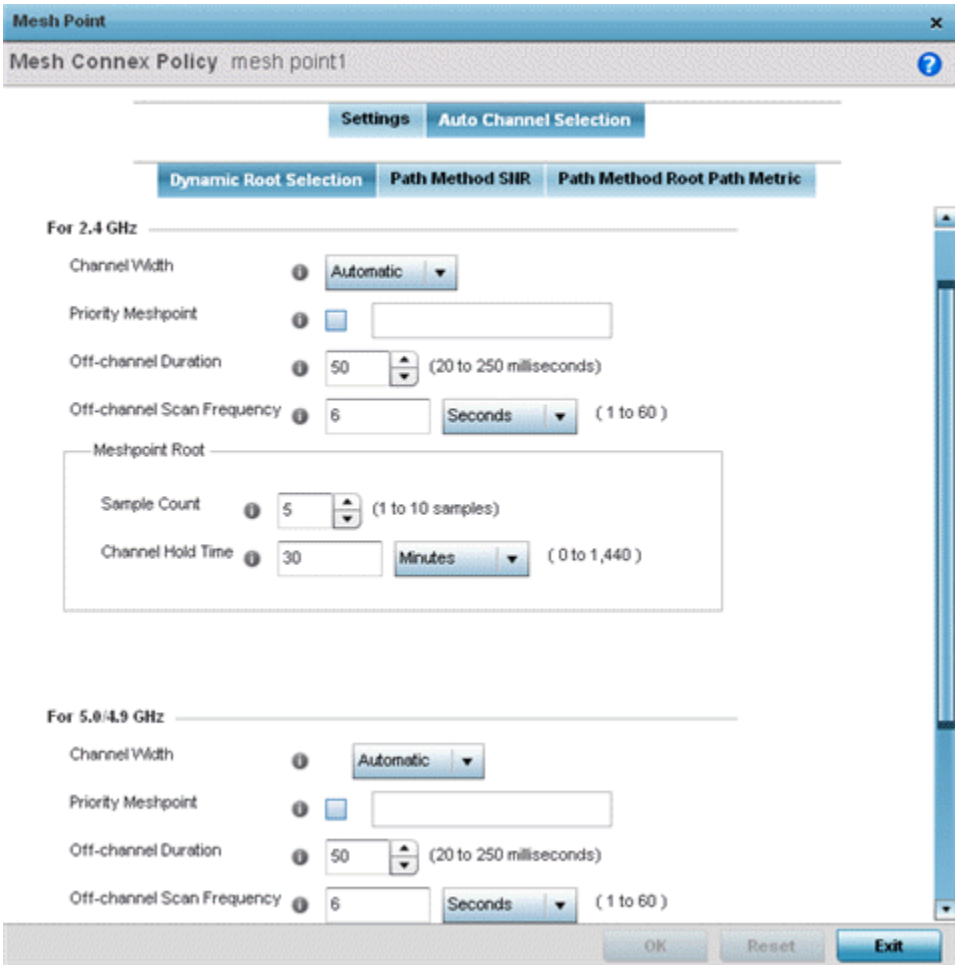


Figure 5-145 *Mesh Point Auto Channel Selection - Dynamic Root Selection screen*

The **Dynamic Root Selection** screen displays by default. The Dynamic Root Selection screen provides configuration for the 2.4 GHz and 5.0/4.9 GHz frequencies.

9 Refer to the following. These descriptions are common for configuring either the 2.4 GHZ and 5.0/4.9 GHz frequencies

Channel Width	Set the channel width the meshpoint's automatic channel scan assigns to the selected radio. Available options include: • *Automatic* – Defines the channel width is calculated automatically. This is the default value. • *20 MHz* – Sets the width between two adjacent channels as 20 MHz. • *40 MHz* – Sets the width between two adjacent channels as 40 MHz. • *80 MHz* – Utilized for 802.11ac Access Points in the 5 GHz frequency.
Priority Meshpoint	Configure the meshpoint monitored for automatic channel scans. This is the meshpoint assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a meshpoint is automatically selected. This setting is disabled by default.
Off-channel Duration	Set the duration (from 20 - 250 milliseconds) the scan dwells on each channel when performing an off channel scan. The default is 50 milliseconds.

Off-channel Scan Frequency	Set the duration (from 1- 60 seconds) between two consecutive off channel scans. The default is 6 seconds.
Meshpoint Root: Sample Count	Configure the number of scan samples (from 1- 10) for data collection before a mesh channel is selected. The default is 5.
Meshpoint Root: Channel Hold Time	Configure the duration (from 0 - 1440 minutes) to remain on a channel before channel conditions are reassessed for a possible channel change. Set this value to zero (0) to prevent an automatic channel selection from occurring. The default setting is 30 minutes.

10 Select the **Path Method SNR** tab to configure *signal to noise* (SNR) ratio values when selecting the path to the meshpoint root.

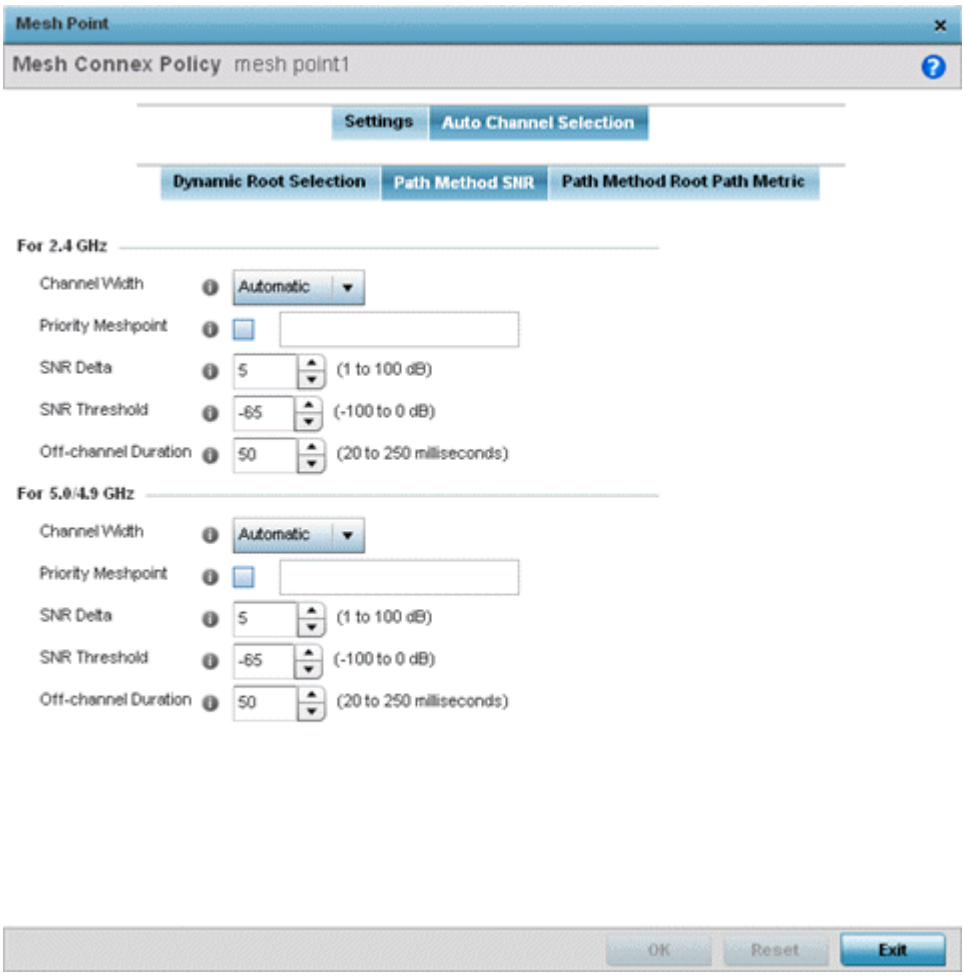


Figure 5-146 *Mesh Point Auto Channel Selection - Path Method SNR screen*

11 Set the following **2.4 GHz** and **5.0/4.9 GHz** path method SNR data:

Channel Width	Set the channel width the meshpoint automatic channel scan assigns to the selected radio. Available options include: • *Automatic* – Defines the channel width calculation automatically. This is the default value. • *20 MHz* – Sets the width between two adjacent channels as 20 MHz. • *40 MHz* – Sets the width between two adjacent channels as 40 MHz. • *80 MHz* – Utilized for 802.11ac Access Points in the 5 GHz frequency.

Priority Meshpoint	Set the meshpoint monitored for automatic channel scans. This is the meshpoint assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a meshpoint is automatically selected. This setting is disabled by default.
SNR Delta	Set the *signal to noise* (SNR) ratio delta (from 1 - 100 dB) for mesh path selections. When path selection occurs, the defined value is utilized for selecting the optimal path. A better candidate, on a different channel, must have a signal strength that exceeds this delta value when compared to the signal strength of the next hop in the mesh network. The default setting is 5 dB.
SNR Threshold	Set the SNR threshold for mesh path selections (from -100 to 0 dB). If the signal strength of the next mesh hop falls below this set value, a scan is triggered to select a better next hop. the default setting is -65 dB.
Off-channel Duration	Configure the duration (from 20 - 250 milliseconds) for scan dwells on each channel, when performing an off channel scan. The default setting is 50 milliseconds.

12 Select the **Path Method Root Path Metric** tab to calculate root path metrics.

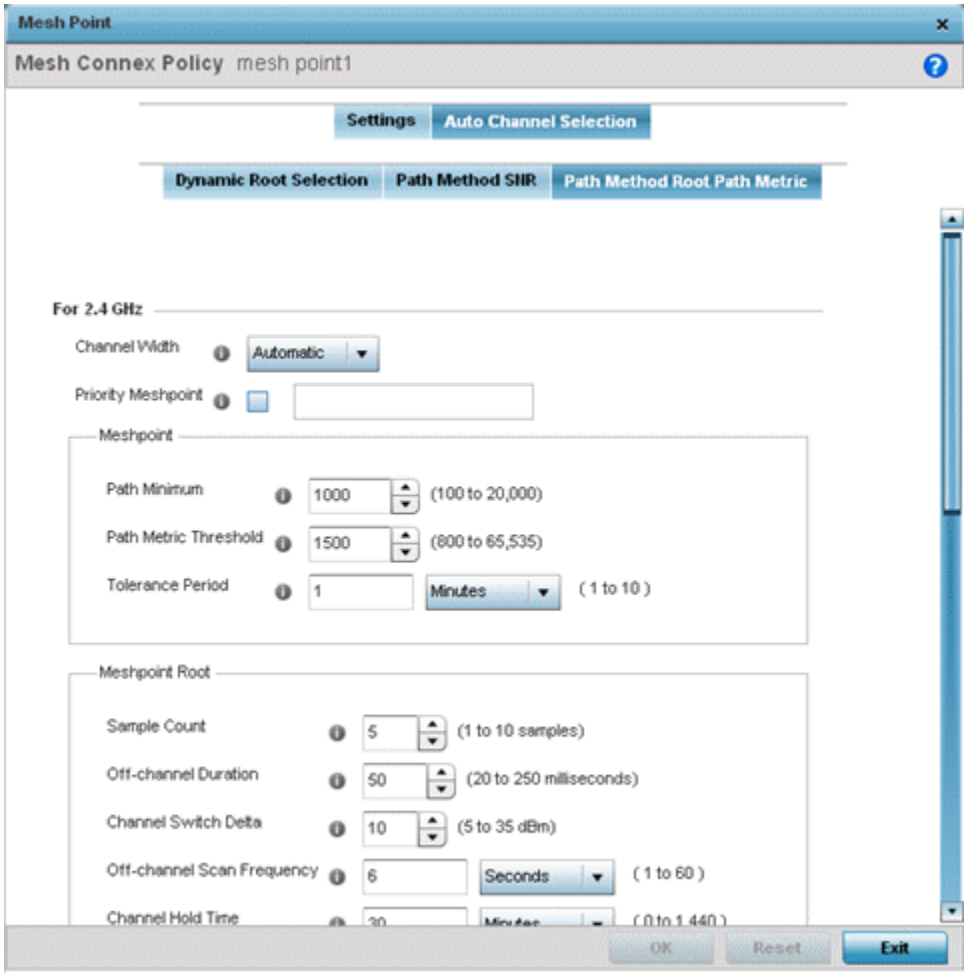


Figure 5-147 *Mesh Point Auto Channel Selection - Root Path Metric screen*

13 Set the following **Path Method Root Path Metrics** (applying to both the 2.4 GHz and 5.0/4.9 GHz frequencies):

Channel Width	Set the channel width meshpoint automatic channel scan should assign to the selected radio. The available options are: • *Automatic* – Defines the channel width as calculated automatically. This is the default value. • *20 MHz* – Set the width between two adjacent channels as 20 MHz. • *40 MHz* – Set the width between two adjacent channels as 40 MHz • *80 MHz* – Utilized for 802.11ac Access Points in the 5 GHz frequency.
Priority Meshpoint	Define the meshpoint assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a meshpoint is automatically selected.
Meshpoint: Path Minimum	Set the minimum path metric (from 100 - 20,000) for mesh connection establishment. The default setting is 1000.
Meshpoint: Path Metric Threshold	Configure a minimum threshold (from 800 - 65535) for triggering an automatic channel selection for meshpoint selection. The default is 1500.
Meshpoint: Tolerance Period	Configure a duration to wait before triggering an automatic channel selection for the next mesh hop. The default is one minute.
Meshpoint Root: Sample Count	Set the number of scans (from 1- 10) for data collection before a mesh point root is selected. The default is 5.
Meshpoint Root: Off-channel Duration	Configure the duration in the range of 20 - 250 milliseconds for the *Off Channel Duration* field. This is the duration the scan dwells on each channel when performing an off channel scan. The default is 50 milliseconds.
Meshpoint Root: Channel Switch Delta	Configure the delta (from 5 - 35 dBm) that triggers a meshpoint root automatic channel selection when exceeded. The default is 10 dBm.
Meshpoint Root: Off-channel Scan Frequency	Configure the duration (from 1 -60 seconds) between two consecutive off channel scans for meshpoint root. The default is 6 seconds.
Meshpoint Root: Channel Hold Time	Set the minimum duration (from 0 - 1440 minutes) to remain on a selected channel before channel conditions are reassessed for a possible channel change. Set this value to zero (0) to prevent an automatic channel selection from occurring. The default is 30 minutes.

14 Select **OK** to save the updates or overrides to the Mesh Point configuration. Select **Reset** to revert to the last saved configuration.

5.2.9.13.7 Vehicle Mounted Modem (VMM) Deployment Considerations

Before defining a VMM configuration (mounting an AP7161 mesh point on a moving vehicle), refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Disable layer 2 stateful packet inspection from the firewall policy. For more information, see Firewall Policy Advanced Settings on page 10-10.
- Set the RTS threshold value to 1 on all mesh devices. The default is 2347. For more information on defining radio settings, refer to Access Point Radio Configuration on page 8-55.
- Use *Opportunistic* as the rate selection setting for the AP7161 radio. The default is Standard. For more information on defining this setting, see *Radio Override Configuration*.
- Disable Dynamic Chain Selection (radio setting). The default is enabled. This setting can be disabled in the CLI using the dynamic-chain-selection command, or in the UI (refer to *Radio Override Configuration*).

- Disable A-MPDU Aggregation if the intended vehicular speed is greater than 30 mph. For more information, see *Radio Override Configuration*.
- Set a misconfiguration recovery time for the non-root AP profile. This configuration should delay the rejection of the newest configuration push from the controller, potentially causing adoption loss.

  The additional delay is to support cases when the new configuration from the controller causes the root AP to move from current channel to other channels, resulting in a mesh link going down, and in turn non-root APs losing adoption. This delay accommodates the time needed for the non-root AP to scan all channels and finding the best root node. The non-root AP can begin operating on the new channel, and establish the mesh link re-adopt to the controller. (For countries using DFS, the scan time is also factored in for the configured value). If the AP fails to find a suitable root node within this time, this new config is a misconfigured and the device would reject the latest config.

  For outdoor APs, it is recommended the misconfiguration-recovery-time be disabled. This can be accomplished by setting the value to 0. Update non root ap71xx profiles on the controller to include this change.

  Using an appropriate console terminal and or connection to your device log on to the CLI and follow these steps:

```
rfs6000-xxxxxx>enable
rfs6000-xxxxxx #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
rfs6000-xxxxxx (config)#profile ap71xx Non-Root-AP71xx
rfs6000-xxxxxx (config-profile-Non-Root-AP71xx)#misconfiguration-recovery-time
0
rfs6000-xxxxxx (config-profile-Non-Root-AP71xx)#
```

5.2.9.14 Overriding a Profile's Environmental Sensor Configuration (AP8132 Only)

Profile Overrides

A sensor module is a USB environmental sensor extension to an AP8132 model Access Point. It provides a variety of sensing mechanisms, allowing the monitoring and reporting of the Access Point's radio coverage area. The output of the sensor's detection mechanisms are viewable using either the Environmental Sensor screen.

To set or override an environmental sensor configuration for an AP8132 model Access Point:

1 Select the **Configuration** > **Devices** from the Web UI.

2 Select **Profile Overrides** to expand its menu items

3 Select **Environmental Sensor**.

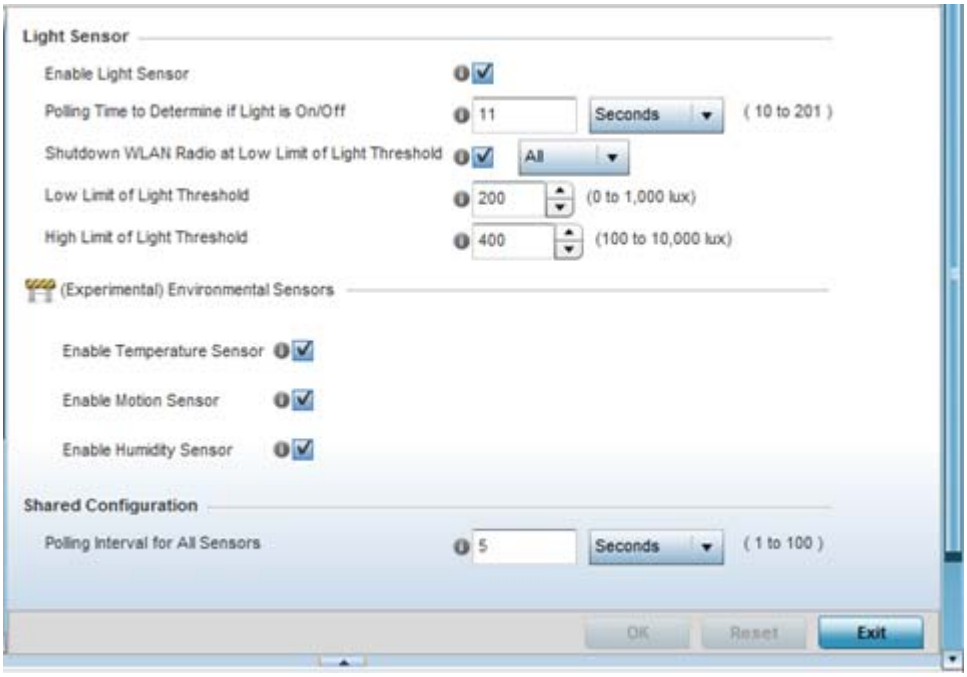


Figure 5-148 *Profile Overrides - Environmental Sensor screen*

4 Set the following **Light Sensor** settings for the sensor module:

Enable Light Sensor	Select this option to enable the light sensor on the module. This setting is enabled by default. The light sensor reports whether the deployment location has its lights powered on or off.
Polling Time to Determine if Light is On/Off	Define an interval in *Seconds* (2 - 201) or *Minutes* (1 - 4) for the sensor module to poll its environment to assess light intensity to determine whether lighting is on or off. The default polling interval is 11 seconds. Light intensity is used to determine whether the Access Point's deployment location is currently populated with clients.
Shutdown WLAN Radio at Low Limit of Light Threshold	Select this option to power off the Access Point's radio if the light intensity dims below the set threshold. If enabled, select *All* (both radios), *radio-1* or *radio-2*.
Low Limit of Light Threshold	Set the low threshold limit (from 0 - 1,000 lux) to determine whether the lighting is off in the Access Point's deployment location. The default is 200. In daytime, the light sensor's value is between 350-450. The default values for the low threshold is 200, i.e., the radio is turned off if the average reading value is lower than 200.
High Limit of Light Threshold	Set the upper threshold limit (from 100 - 10,000 lux) to determine whether the lighting is on in the Access Point's deployment location. The default high threshold is 400. The radios are turned on when the average value is higher than 400.

5 Enable or disable the following **Environmental Sensors**:

Enable Temperature Sensor	Select this option to enable the module's temperature sensor. Results are reported back to the Access Point's Environment screens within the Statistics node. This setting is enabled by default.
Enable Motion Sensor	Select this option to enable the module's motion sensor. Results are reported back to the Access Point's Environment screens within the Statistics node. This setting is enabled by default.
Enable Humidity Sensor	Select this option to enable the module's humidity sensor. Results are reported back to the Access Point's Environment screens within the Statistics node. This setting is enabled by default.

6 Define or override the following **Shared Configuration** settings:

Polling Interval for All Sensors	Set an interval in either *Seconds* (1 - 100) or *Minutes* (1 - 2) for the time between sensor environmental polling (both light and environment). The default setting is 5 seconds.

7 Select **OK** to save the changes and overrides made to the environmental sensor screen. Select **Reset** to revert to the last saved configuration.

5.2.9.15 Overriding a Profile's Advanced Configuration

Profile Overrides

Refer to profile's advanced set of configuration screens to set client load balance calculations and ratios, set a MiNT configuration and set other miscellaneous settings. For more information, refer to the following:

- *Advanced Profile Client Load Balance Configuration*
- *Advanced MiNT Protocol Configuration*
- *Advanced Profile Miscellaneous Configuration*

5.2.9.15.8 Advanced Profile Client Load Balance Configuration

Overriding a Profile's Advanced Configuration

Set a the ratios and calculation values used by Access Points to distribute client loads both amongst neighbor devices and the 2.4 and 5 GHz radio bands.

To define Access Point client load balance algorithms:

1 Select the **Configuration** > **Devices** from the Web UI.

2 Select **Profile Overrides** to expand its menu items

3 Select **Advanced** to expand its sub menu items.

4 Select **Client Load Balancing** from the Advanced menu item.

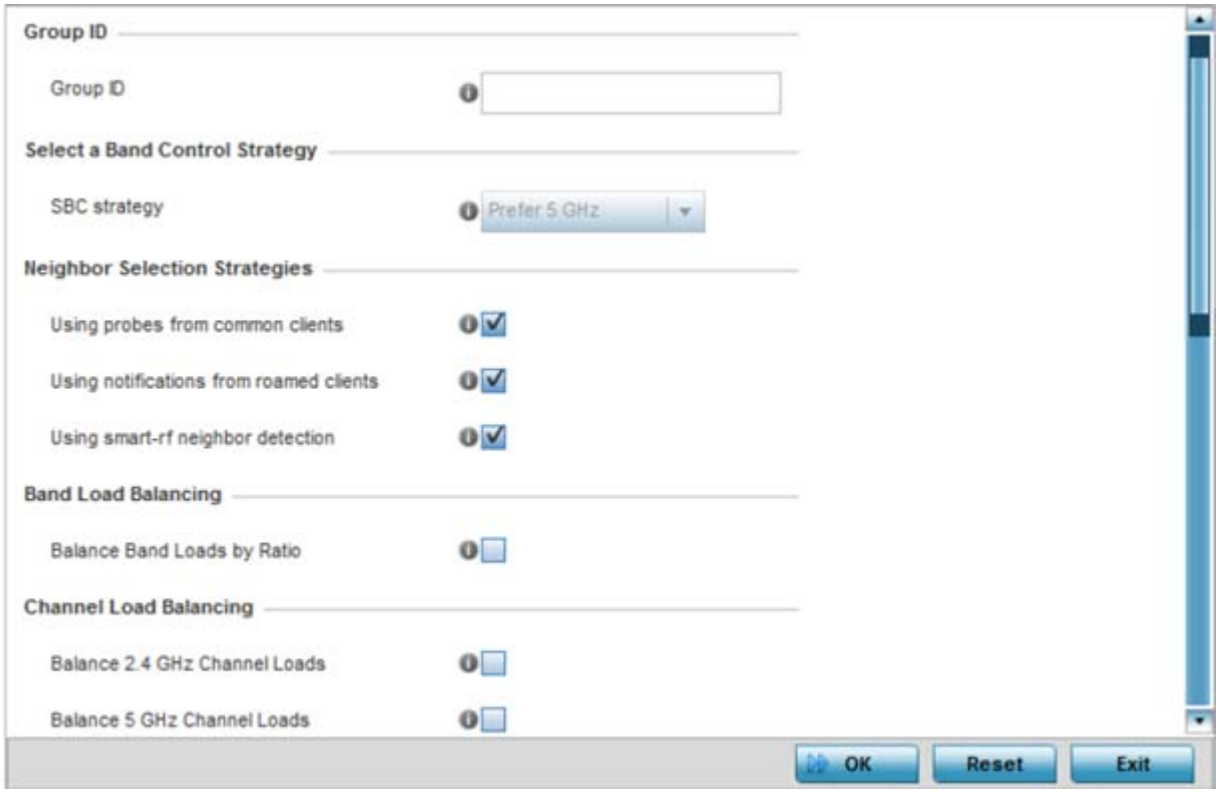


Figure 5-149 *Advanced Profile Overrides - Client Load Balancing screen*

5 Use the **Group ID** field to define a group ID of up to 32 characters to differentiate the ID from others with similar configurations.

6 Select the **SBC strategy** from the drop-down menu to determine how band steering is conducted.

Band steering directs 5 GHz-capable clients to that band. When an Access Point hears a request from a client to associate on both the 2.4 GHz and 5 GHz bands, it knows the client is capable of operation in 5 GHz. Band steering steers the client by responding only to the 5 GHz association request and not the 2.4 GHz request. The client only associates in the 5 GHz band.

7 Set the following **Neighbor Selection Strategies**:

Using probes from common clients	Select this option to select neighbors (peer devices) using probes from common clients. This setting is enabled by default.
Using notifications from roamed clients	Select this option to select neighbors (peer devices) using roam notifications from roamed clients. This setting is enabled by default.
Using smart-rf neighbor detection	Select this option to select neighbors (peer devices) using Smart RF. This setting is enabled by default.

8 Enable **Balance Band Loads by Radio** (within the **Band Load Balancing** field) to distribute an Access Points client traffic load across both the 2.4 and 5 GHz radio bands.

9 Set the following **Channel Load Balancing** settings:

Balance 2.4 GHz Channel Loads	Select this option to balance an Access Point's 2.4 GHz client load across all channels. This setting is enabled by default.
Balance 5 GHz Channel Loads	Select this option to balance an Access Point's 5 GHz client load across all channels. This setting is enabled by default.

10 Enable **Balance AP Loads** (within the **AP Load Balancing** field) to distribute client traffic evenly amongst neighbor Access Points.

11 Set the following **Advanced Parameters for** client load balancing:

Max. 2.4 GHz Difference Considered Equal	Set the maximum load difference (from 1 - 100%) considered equal when comparing 2.4 GHz client loads. The default setting is 1%.
Min. Value to Trigger 2.4 Ghz Channel Balancing	Set the threshold (from 1 - 100%) beyond which channel load balancing is triggered in the 2.4 GHz radio band. The default setting is 5%.
Weightage given to Client Count	Set the weightage (from 1- 100%) applied to client count calculations in the 2.4 GHz radio band. The default setting is 90%.
Weightage given to Throughput	Set the weightage (from 1- 100%) applied to client throughput calculations in the 2.4 GHz radio band. The default setting is 10%.
Max. 5 GHz Difference Considered Equal	Set the maximum load difference (from 1 - 100%) considered equal when comparing 5 GHz client loads. The default setting is 1%.
Min. Value to Trigger 5 Ghz Channel Balancing	Set the threshold (from 1 - 100%) beyond which channel load balancing is triggered in the 5 GHz radio band. The default setting is 5%.
Weightage given to Client Count	Set the weightage (from 1- 100%) applied to client count calculations in the 5 GHz radio band. The default setting is 90%.
Weightage given to Throughput	Set the weightage (from 1- 100%) applied to client throughput calculations in the 5 GHz radio band. The default setting is 10%.

12 Define the following **AP Load Balancing** settings:

Min. Value to Trigger Balancing	Set a value (from 1 - 100%) used to trigger client load balancing when exceeded. The default setting is 5%.
Max. AP Load Difference Considered Equal	Set the maximum load balance differential (from 1 - 100%) considered equal when comparing neighbor Access Point client loads. The default setting is 1%.
Weightage given to Client Count	Set the weightage (from 1- 100%) applied to client count in an Access Point's overall load calculation. The default setting is 90%.
Weightage given to Throughout	Set the weightage (from 1- 100%) applied to client throughput in an Access Point's overall load calculation. The default setting is 10%.

13 Set the following **Band Control** values:

Max. Band Load Difference Considered Equal	Set the maximum load difference (from 1 - 100%) considered equal when comparing band loads. The default setting is 1%.
Band Ratio (2.4 GHz)	Set the relative load for the 2.4 GHz radio band as a leveled ratio from 1 - 10. The default setting is 0.
Band Ratio (5 GHz)	Set the relative load for the 5 GHz radio band as a leveled ratio from 1 - 10. The default setting is 0.
5 GHz load at which both bands enabled	Define the 5 GHz radio load value (from 1 - 100%) above which the 5 GHz radio is equally preferred in the overall load balance distribution. The default is 75%.
2.4 GHz load at which both bands enabled	Define the 2.4 GHz radio load value (from 1 - 100%) above which the 2.4 GHz radio is equally preferred in the overall load balance distribution. The default is 75%.

14 Define the following **Neighbor Selection** settings

Minimal signal strength for common clients	Define the minimum signal strength value (from -100 to 30 dBm) that must be exceeded for an Access Point's detected client to be considered a common client. The default setting is -100 dBi.
Minimum number of clients seen	Set the minimum number of clients (from 0 - 256) that must be common to two or more Access Points for the Access Points to regard one another as neighbors using the common client neighbor detection strategy. The default setting is 0.
Max confirmed neighbors	Set the maximum number (from 1 - 16) of neighbor Access Points that must be detected amongst peer Access Point to initiate load balancing. The default setting is 16.
Minimum signal strength for smart-rf neighbors	Set the minimal signal strength value (from -100 to 30 dBm) for an Access Point detected using Smart RF to qualify as a neighbor Access Point. The default setting is - 65 dBm.

15 Select **OK** to save the changes made to the profile's Advanced client load balance configuration. Select **Reset** to revert to the last saved configuration.

5.2.9.15.9 Advanced MiNT Protocol Configuration

Overriding a Profile's Advanced Configuration

MINT provides the means to secure profile communications at the transport layer. Using MINT, a device can be configured to only communicate with other authorized (MINT enabled) devices. Keys can also be generated externally using any application (like openssl). These keys must be present on the device managing the domain for key signing to be integrated with the UI. A device needing to communicate with another first negotiates a security context with that device.

The security context contains the transient keys used for encryption and authentication. A secure network requires users to know about certificates and PKI. However, administrators do not need to define security parameters for Access Points to be adopted (secure WISPe being an exception, but that isn't a commonly used feature). Also, users can replace any device on the network or move devices around and they continue to work. Default security parameters for MiNT are such that these scenarios continue to function as expected, with minimal user intervention required only when a new network is deployed

To define or override a profile's MINT configuration:

1 Select the **Configuration** > **Devices** from the Web UI.

2 Select **Profile Overrides** to expand its menu items

3 Select **Advanced** to expand its sub menu items.

4 Select **MINT Protocol** from the Advanced menu item.

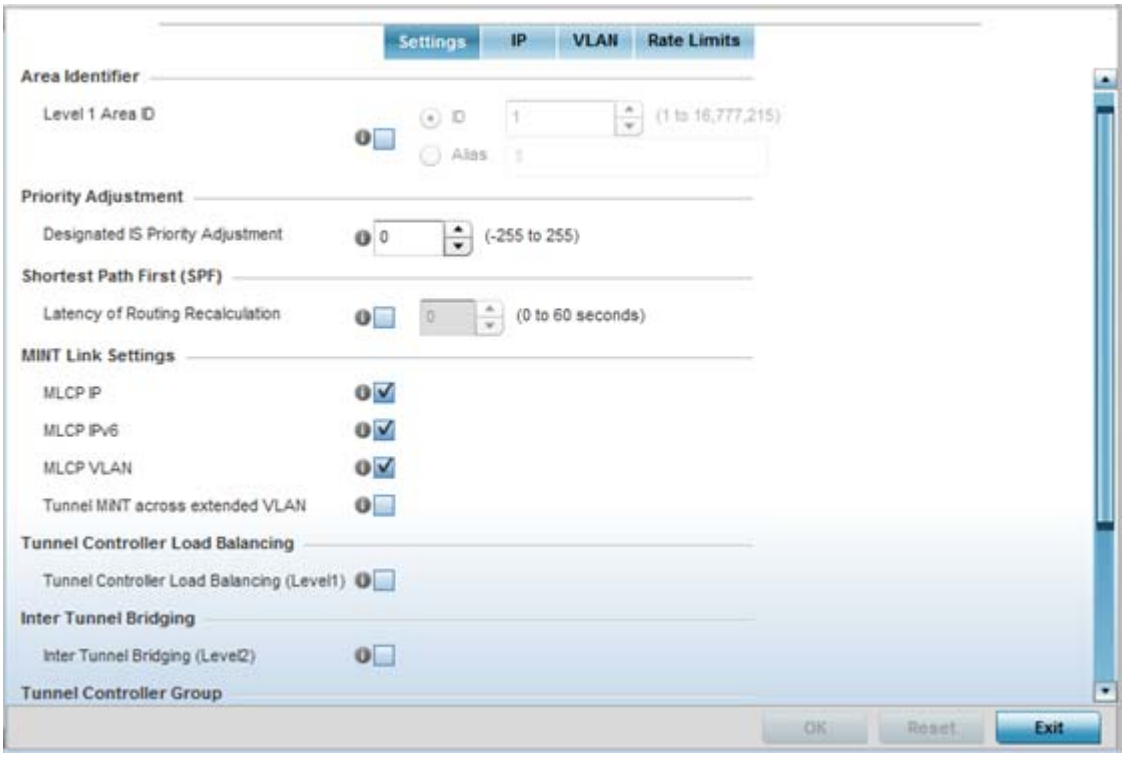


Figure 5-150 *Advanced Profile Overrides MINT screen - Settings tab*

The **Settings** tab displays by default.

5 Refer to the **Area Identifier** field to define or override the Level 1 and Level 2 Area IDs used by the profile's MINT configuration.

Level 1 Area ID	Select this option to either use a spinner control for setting the Level 1 Area ID (1 - 16,777,215) or create an alias for the ID. An alias enables an administrator to define a configuration item, such as a this area ID, as an alias once and use the alias across different configuration items. The default value is disabled.

6 Define or override the following **Priority Adjustment** in respect to devices supported by the profile:

Designated IS Priority Adjustment	Use the spinner control to set a *Designated IS Priority Adjustment* setting. This is the value added to the base level DIS priority to influence the *Designated IS* (DIS) election. A value of +1 or greater increases DISiness. The default setting is 0.

7 Select the **Latency of Routing Recalculation** option (within the **Shortest Path First (SPF)** field) to enable the spinner control used for defining or overriding a latency period (from 0 - 60 seconds). The default setting is disabled.

8 Define or override the following **MINT Link Settings** in respect to devices supported by the profile:

MLCP IP	Check this box to enable *MINT Link Creation Protocol* (MLCP) by IP Address. MLCP is used to create one UDP/IP link from the device to a neighbor. The neighboring device does not need to be a controller or service platform, it can be another Access Point with a path to the controller or service platform. This setting is enabled by default.
MLCP IPv6	Check this box to enable MLCP for automated MiNT UDP/IP link creation. This setting is enabled by default.

MLCP VLAN	Check this box to enable MLCP by VLAN. MLCP is used to create one VLAN link from the device to a neighbor. That neighboring device does not need to be a controller or service platform, it can be another Access Point with a path to the controller or service platform. This setting is enabled by default.
Tunnel MiNT across extended VLAN	Select this option to tunnel MiNT protocol packets across an extended VLAN. This setting is disabled by default.

9 Select **Tunnel Controller Load Balancing (Level 1)** to enable load balance distribution via a WLAN tunnel controller. This setting is disabled by default.

10 Select **Inter Tunnel Bridging (Level 2)** to enable inter tunnel bridging. This setting is disabled by default.

11 Enter a 64 character maximum **Tunnel Controller Name** for this tunneled-WLAN-controller interface.

12 Enter a 64 character maximum **Preferred Tunnel Controller Name** this Access Point prefers to tunnel traffic to via an extended VLAN.

13 Select **OK** to save the updates and overrides to the MINT Protocol configuration. Select **Reset** to revert to the last saved configuration.

14 Select the **IP** tab to display the link IP network address information shared by the devices managed by the MINT configuration.

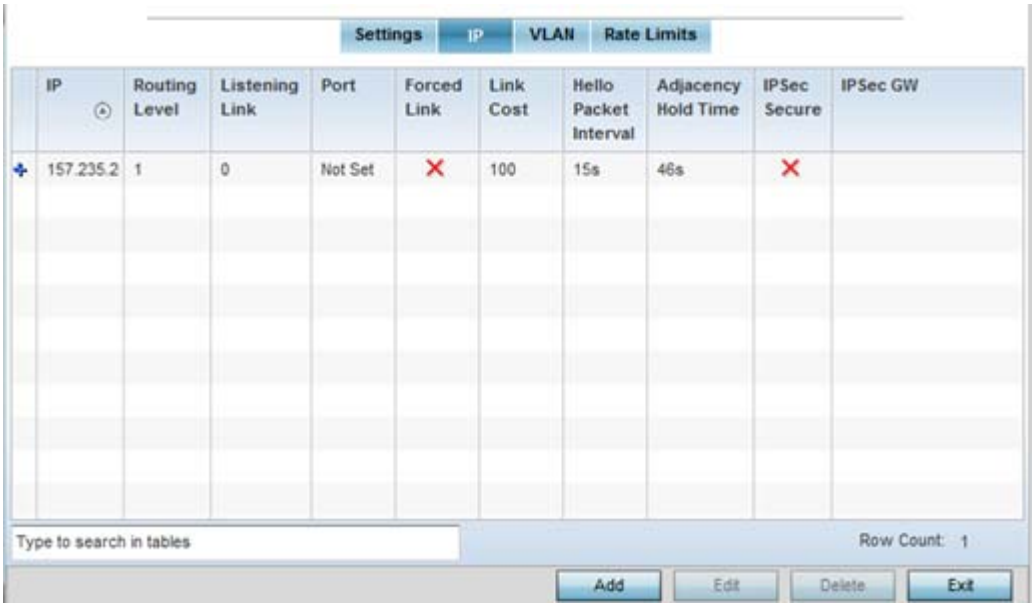


Figure 5-151 *Advanced Profile MINT screen - IP tab*

15 The IP tab displays the **IP** address, **Routing Level**, **Listening Link**, **Port**, **Forced Link**, **Link Cost**, **Hello Packet Interval**, **Adjacency Hold Time** and IPSec Secure, and IPSec GW settings that devices use to securely communicate amongst one another. Select **Add** to create a new Link IP configuration or **Edit** to override an existing MINT configuration.

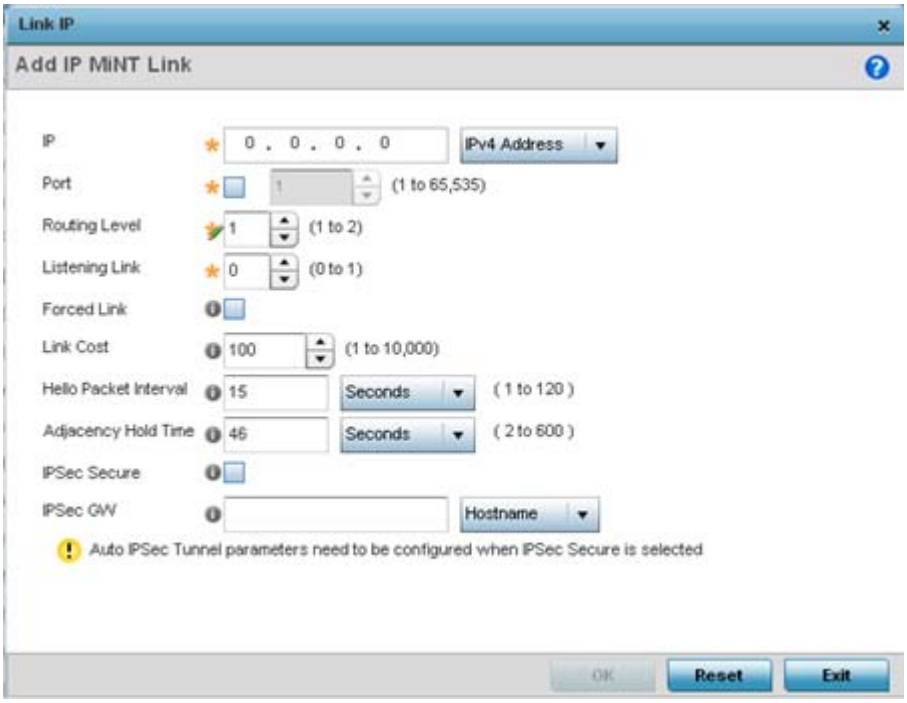


Figure 5-152 *Advanced Profile MINT screen - Link IP tab*

16 Set the following **Link IP** parameters to complete the MINT network address configuration:

IP	Define or override the IP address used by peers for interoperation when supporting the MINT protocol. Use the drop-down to select the type of IP address provided. The available choices are *IPv4 Address* and *IPv6 Address*.
Port	To specify a custom port for MiNT links, select this option and use the spinner control to define or override the port number (1 - 65,535).
Routing Level	Use the spinner control to define or override a routing level of either *1* or *2*.
Listening Link	Specify a listening link of either 0 or 1. UDP/IP links can be created by configuring a matching pair of links, one on each end point. However, that is error prone and doesn't scale. So UDP/IP links can also listen (in the TCP sense), and dynamically create connected UDP/IP links when contacted. The typical configuration is to have a listening UDP/IP link on the IP address S.S.S.S, and for all the APs to have a regular UDP/IP link to S.S.S.S.
Forced Link	Check this box to specify the MiNT link as a forced link.
Link Cost	Use the spinner control to define or override a link cost from 1 - 10,000. The default value is 100.
Hello Packet Interval	Set or override an interval in either *Seconds* (1 - 120) or *Minutes* (1 - 2) for the transmission of hello packets. The default interval is 15 seconds.
Adjacency Hold Time	Set or override a hold time interval in either *Seconds* (2 - 600) or *Minutes* (1 - 10) for the transmission of hello packets. The default interval is 46 seconds.
IPSec Secure	Enable this option to provide IPSec secure peer authentication on the MiNT connection (link). This option is disabled by default.
IPSec GW	Select the numerical IP address or administrator defined hostname of the IPSec gateway. Hostnames cannot include an underscore character.

17 Select **OK** to save the updates and overrides to the MINT Protocol's network address configuration. Select **Reset** to revert to the last saved configuration.

18 Select the **VLAN** tab to display link IP VLAN information shared by the devices managed by the MINT configuration.

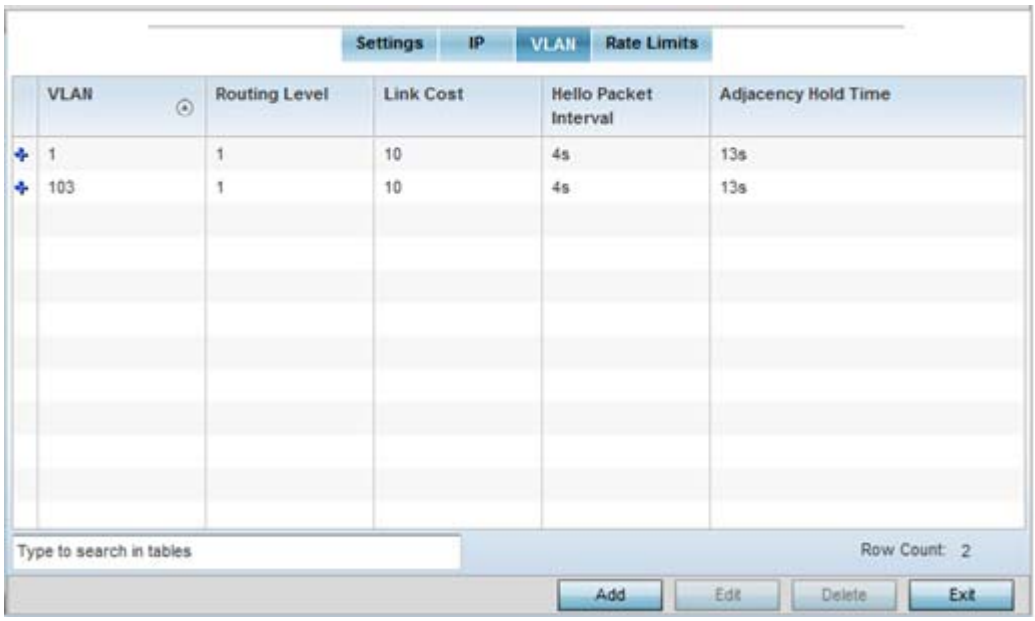


Figure 5-153 *Advanced Profile MINT screen - VLAN tab*

The VLAN tab displays the **VLAN**, **Routing Level**, **Link Cost**, **Hello Packet Interval** and **Adjacency Hold Time** devices use to securely communicate amongst one another. Select **Add** to create a new VLAN link configuration or **Edit** to override an existing MINT VLAN configuration.

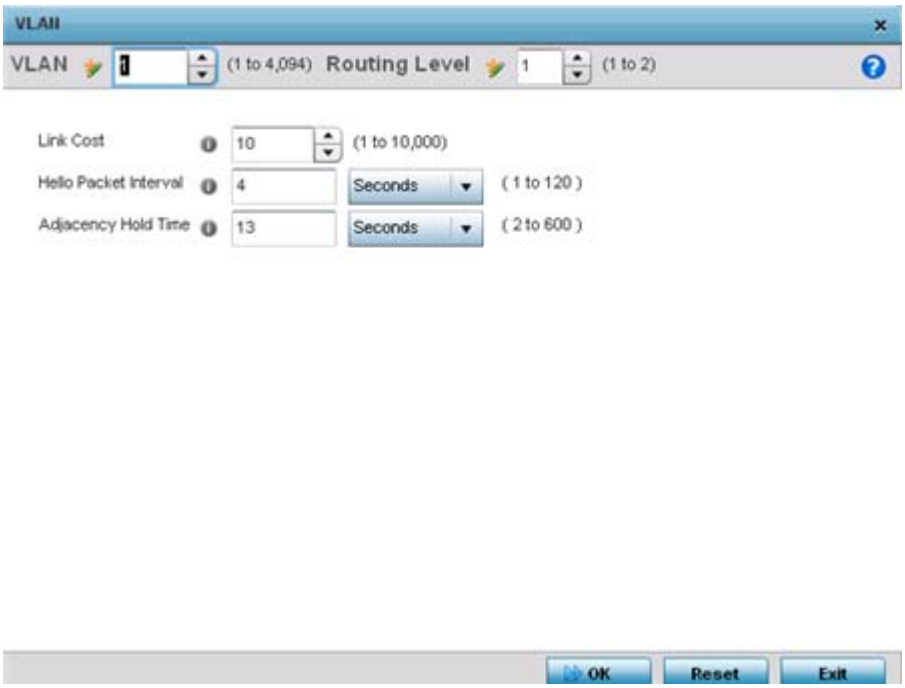


Figure 5-154 *Advanced Profile MINT screen - Add/Edit VLAN*

19 Set the following **VLAN** parameters for the MINT configuration:

VLAN	Define a VLAN ID from 1 - 4,094 used by peers for interoperation when supporting the MINT protocol.
Routing Level	Use the spinner control to define or override a routing level of either *1* or *2*.
Link Cost	Use the spinner control to define or override a link cost from 1 - 10,000. The default value is 100.
Hello Packet Interval	Set or override an interval in either *Seconds* (1 - 120) or *Minutes* (1 - 2) for the transmission of hello packets. The default interval is 15 seconds.
Adjacency Hold Time	Set or override a hold time interval in either *Seconds* (2 - 600) or *Minutes* (1 - 10) for the transmission of hello packets. The default interval is 46 seconds.

20 Select **OK** to save the updates and overrides to the MINT Protocol configuration. Select **Reset** to revert to the last saved configuration.

21 Select the **Rate Limits** tab to display data rate limits configured on extended VLANs and optionally add or edit rate limit configurations.

Excessive traffic can cause performance issues on an extended VLAN. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that has infected on one or more devices. Rate limiting reduces the maximum rate sent or received per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. Uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. Rate limits are extracted from the RADIUS server's response. When such attributes are not present, the settings defined on the controller, service platform or Access Point are applied. An administrator can set separate QoS rate limit configurations for data types transmitted from the network (upstream) and data transmitted from a wireless clients back to associated radios (downstream).

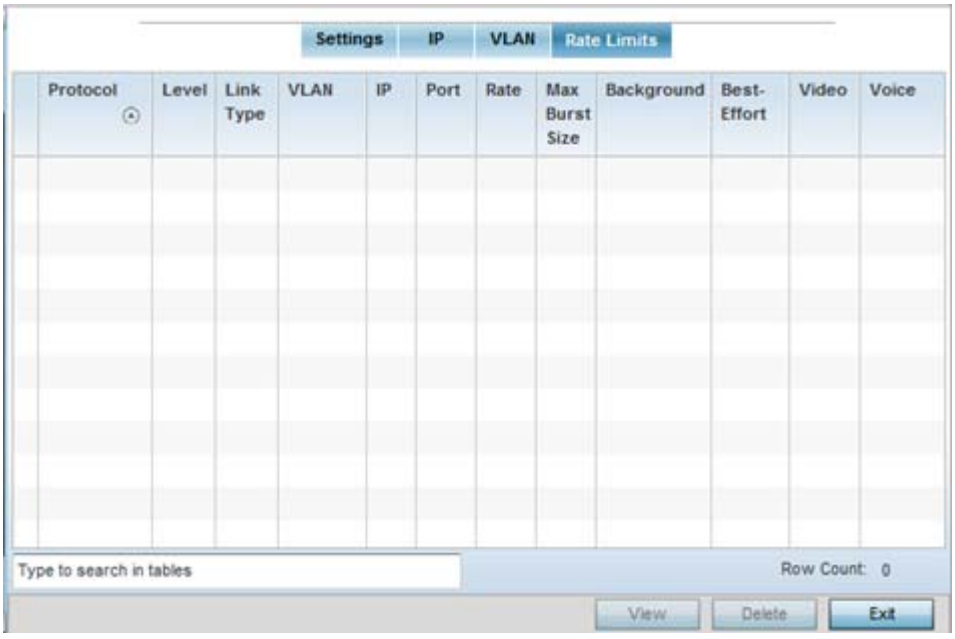


Figure 5-155 *Advanced Profile MINT screen - Rate Limit tab*

Existing rate limit configurations display along with their virtual connection protocols and data traffic QoS customizations.

22 Select **Add** to create a new rate limit configuration.

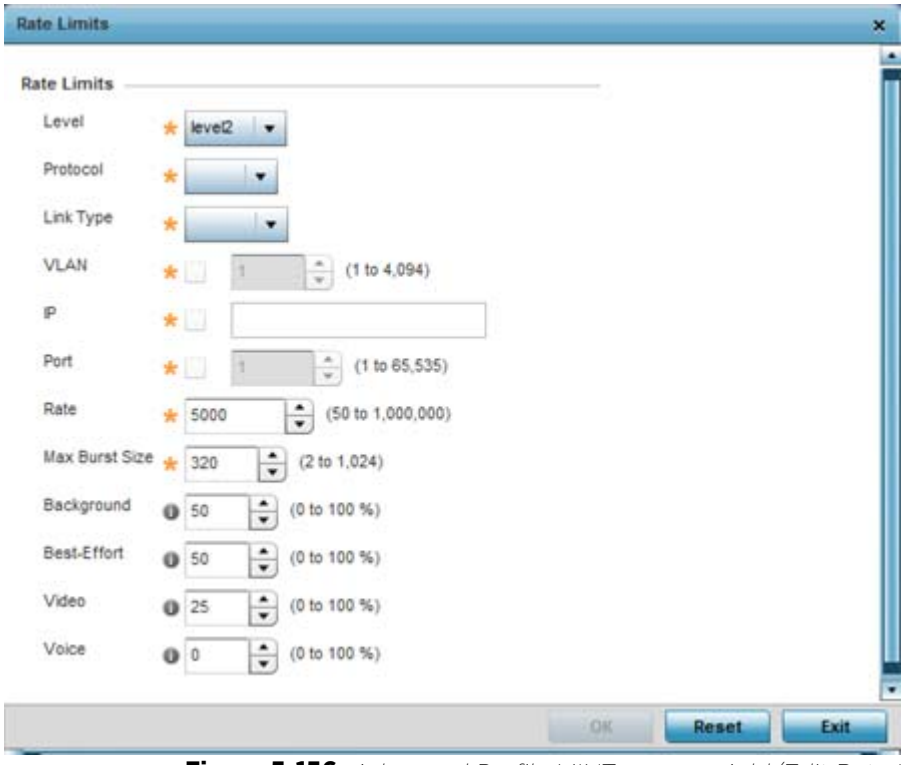


Figure 5-156 *Advanced Profile MINT screen - Add/Edit Rate Limit*

23 Set the following **Rate Limits** to complete the MINT configuration:

Level	Select *level2* to apply rate limiting for all links on level2.
Protocol	Select either *mlcp* or *link* as this configuration's rate limit protocol. *Mint Link Creation Protocol* (MLCP) creates a UDP/IP link from the device to a neighbor. The neighboring device does not need to be a controller or service platform, it can be an Access Point with a path to the controller or service platform. Select *link* to rate limit using statically configured MiNT links.
Link Type	Select either *VLAN*, to configure a rate limit configuration on a specific virtual LAN, or *IP* to set rate limits on a static IP address/Port configuration.
VLAN	When the Protocol is set to *link* and the Link Type is set to *VLAN*, use the spinner control to select a virtual LAN from 1 - 4094 to refine the rate limiting configuration to a specific VLAN.
IP	When the Protocol is set to *link* and the Link Type is set to *VLAN*, enter the IP address as the network target for rate limiting.
Port	When the Protocol is set to *link* and the Link Type is set to *VLAN*, use the spinner control to set the virtual port (1 - 65,535) used for rate limiting traffic.
Rate	Define a rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.

Max Burst Size	Use the spinner to set the maximum burst size from 0 - 1024 kb. The smaller the burst, the less likely the upstream packet transmission will result in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should add a 10% margin (minimally) to allow for traffic bursts. The default burst size is 320 kbytes.
Background	Configures the random early detection threshold (as a percentage) for low priority background traffic. Background packets are dropped and a log message generated if the rate exceeds the set value. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default setting is 50%.
Best-Effort	Configures the random early detection threshold (as a percentage) for low priority best-effort traffic. Best-effort packets are dropped and a log message generated if the rate exceeds the set value. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 50%.
Video	Configures the random early detection threshold (as a percentage) for high priority video traffic. Video packets are dropped and a log message generated if the rate exceeds the set value. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 25%.
Voice	Configures the random early detection threshold (as a percentage) for high priority voice traffic. Voice packets are dropped and a log message generated if the rate exceeds the set value. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 0%.

24 Select **OK** to save the updates and overrides to the MINT Protocol's rate limit configuration. Select **Reset** to revert to the last saved configuration.

5.2.9.15.10 Advanced Profile Miscellaneous Configuration

Overriding a Profile's Advanced Configuration

Refer to the advanced profile's Miscellaneous menu item to set or override a profile's NAS configuration. The profile database on the RADIUS server consists of user profiles for each connected *network access server* (NAS) port. Each profile is matched to a username representing a physical port. When the wireless controller authorizes users, it queries the user profile database using a username representative of the physical NAS port making the connection. Access Point LED behavior and RF Domain management can also be defined from within the Miscellaneous screen.

1 Select the **Configuration** > **Devices** from the Web UI.

2 Select **Profile Overrides** to expand its menu items

3 Select **Advanced** to expand its sub menu items.

4 Select **Miscellaneous** from the Advanced menu item.

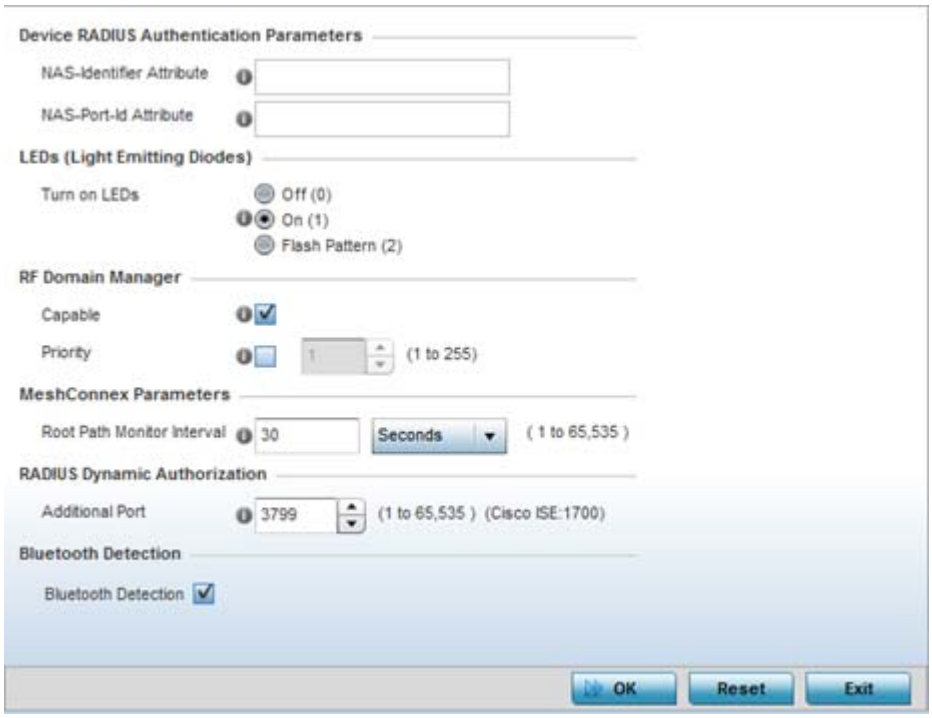


Figure 5-157 *Advanced Profile Overrides - Miscellaneous screen*

5 Set a **NAS-Identifier Attribute** up to 253 characters in length.

6 This is the RADIUS NAS-Identifier attribute that typically identifies the controller, service platform or Access Point where a RADIUS message originates.

7 Set a **NAS-Port-Id Attribute** up to 253 characters in length.

8 This is the RADIUS NAS port ID attribute which identifies the device port where a RADIUS message originates.

9 Select the **Turn on LEDs** option (within the **LEDs (Light Emitting Diodes)** section) to enable the LEDs on Access Point. This parameter is not available for controllers or service platforms.

Select the **Flash Pattern(2)** option (within the **LEDs (Light Emitting Diodes)** field) to flash an Access Point's LED's in a distinct manner (different from its operational LED behavior) to allow an administrator to validate an Access Point has received its configuration from its managing controller or service platform.

Enabling this feature allows an administrator to validate an Access Point has received its configuration (perhaps remotely at the site of deployment) without having to log into the managing controller or service platform. This feature is disabled by default.

10 Select the **Capable** check box (within the **RF Domain Manager** section) to designate this specific device as being the RF Domain manager for a particular RF Domain. The default value is enabled.

11 Select the **Priority** check box (within the **RF Domain Manager** section) to set a priority value for this specific profile managed device. Once enabled, use the spinner control to set a device priority between 1 - 255. The higher the number set, the higher the priority in the RF Domain manager election process.

12 Configure a **Root Path Monitor Interval** (from1 - 65,535 seconds) to specify how often to check if the mesh point is up or down.

13 Set the **Additional Port** value (within the **RADIUS Dynamic Authorization** field) from 1-65,535 to enable a CISCO *Identity Services Engine* (ISE) *Authentication, Authorization and Accounting* (AAA) server to dynamically authenticate a client.

When a client requests access to a CISCO ISE RADIUS server supported network, the server presents the client with a URL where a device's compliance is checked for definition file validity (this form of file validity checking is called *posture*). If the client device complies, it is allowed access to the network.

14 Enable **Bluetooth Detection** to scan for Bluetooth devices over the WiNG managed 2.4 GHz Access Point radio. Bluetooth is a technology for exchanging data over short distances using short-wavelength UHF radio waves in the 2.4 GHz band from mobile wireless clients.

NOTE: Enabling Bluetooth detection results in interference on the Access Point's 2.4 GHz radio when in WLAN mode. WLANs are susceptible to sources of interference by Bluetooth devices.

15 Select **OK** to save the changes made to the profile's Advanced Miscellaneous configuration. Select **Reset** to revert to the last saved configuration.

5.3 Auto Provisioning Policies

Device Configuration

Wireless devices can adopt other wireless devices. For example, a wireless controller can adopt an number of Access Points. When a device is adopted, the device configuration is determined by the adopting device. Since multiple configuration policies are supported, an adopting device needs to determine which configuration policies should be used for a given adoptee. Auto Provisioning Policies determine which configuration policies are used for an adoptee based on some of its properties. For example, a configuration policy could be assigned based on MAC address, IP address, CDP snoop strings, etc.

Once created an auto provisioning policy can be used in profiles or device configuration objects. An auto provisioning policy contains a set of ordered by precedence rules that either *deny* or *allow* adoption based on potential adoptee properties and a catch-all variable that determines if the adoption should be allowed when none of the rules is matched. All rules (both deny and allow) are evaluated sequentially starting with the rule with the lowest precedence. The evaluation stops as soon as a rule has been matched, no attempt is made to find a better match further down in the set.

The evaluation is performed using various matching criteria. The matching criteria supported include:

MAC	Matches the MAC address of a device attempting to be adopted. Either a single MAC address or a range of MAC addresses can be specified.
VLAN	Matches when adoption over a Layer 2 link matches the VLAN ID of an adoption request. Note that this is a VLAN ID as seen by the recipient of the request, in case of multiple hops over different VLANs this may different from VLAN ID set by the sender. A single VLAN ID is specified in the rule. This rule is ignored for adoption attempts over Layer 3.
IP Address	Matches when adoption is using a Layer 3 link matches the source IP address of an adoption request. In case of NAT the IP address may be different from what the sender has used. A single IP, IP range or IP/mask is specified in the rule. This rule is ignored for adoption attempts over Layer 2.
Serial Number	Matches exact serial number (case insensitive).
Model	Matches exact model name (case insensitive).

DHCP Option	Matches the value found in DHCP vendor option 191 (case insensitive). DHCP vendor option 191 can be setup to communicate various configuration parameters to an AP. The value of the option in a string in the form of tag=value separated by a semicolon, e.g.'tag1=value1;tag2=value2;tag3=value3'. The Access Point includes the value of tag'rf-domain', if present. This value is matched against the auto provisioning policy.
FQDN	Matches a substring to the FQDN of a device (case insensitive).
CDP	Matches a substring in a list of CDP snoop strings (case insensitive). For example, if an Access Point snooped 3 devices: controller1.extremenetworks.com, controller2.extremenetworks.com and controller3.extremenetworks.com,'controller1','extremenetworks', 'extremenetworks.com', are examples of the substrings that will match.
LLDP	Matches a substring in a list of LLDP snoop strings (case insensitive). For example, if an Access Point snooped 3 devices: controller1.extremenetworks.com, controller2.extremenetworks.com and controller3.extremenetworks.com,'controller1', 'extremenetworks', 'extremenetworks.com', are substrings match.

Auto Provisioning is the process to discover controllers or service platforms available in the network, pick the most desirable controller or service platform, establish an association, optionally obtain an image upgrade and obtain its configuration.

At adoption, an Access Point solicits and receives multiple adoption responses from controllers and service platforms available on the network. These adoption responses contain loading policy information the Access Point uses to select the optimum controller or service platform for adoption. By default, an auto provisioning policy generally distributes AP adoption evenly amongst available controller or service platform. Modify existing adoption policies or create a new one as needed to meet the adoption requirements of a device and their assigned profile.

NOTE: A device configuration does not need to be present for an auto provisioning policy to take effect. Once adopted, and the device's configuration is defined and applied by the controller or service platform, the auto provisioning policy mapping does not have impact on subsequent adoptions by the same device.

An auto provisioning policy enables an administrator to define adoption rules an Access Point's adoption by a wireless controller.

Auto provisioning policies set the different restrictions on how an Access Point gets adopted to a wireless controller.

To review existing Auto Provisioning Policy configurations:

1 Select **Configuration** > **Devices** > **Auto Provisioning Policy**.

2 The **Auto-Provisioning** screen displays by default.

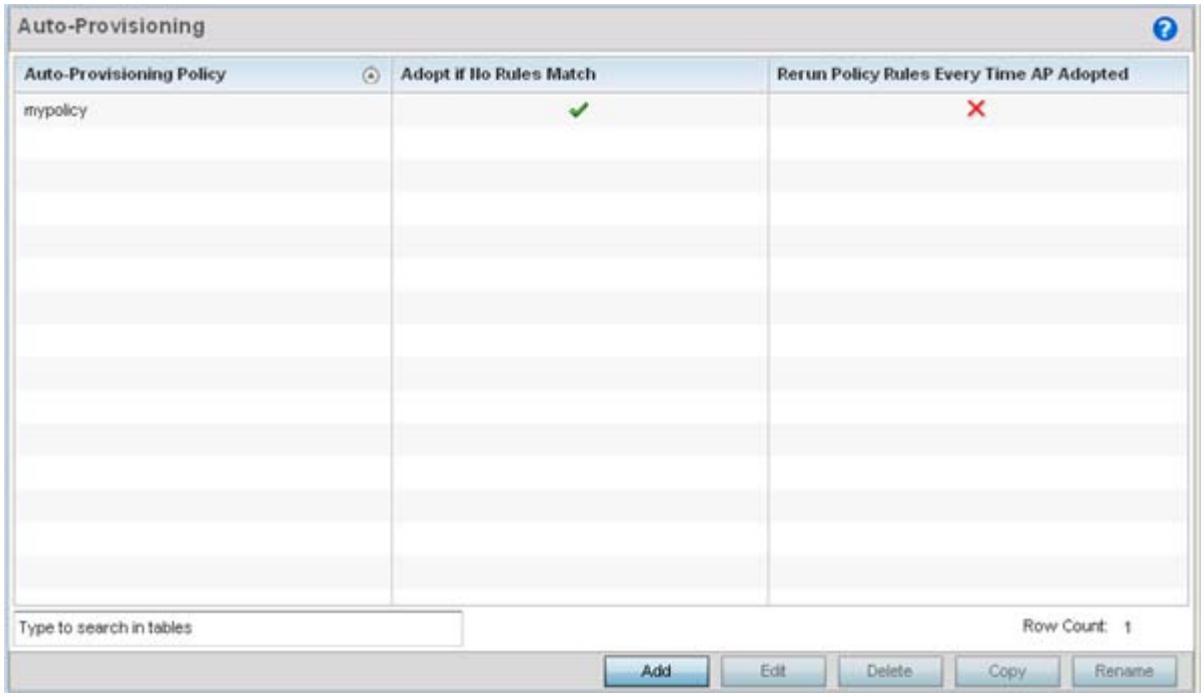


Figure 5-158 *Auto-Provisioning screen*

Use the **Auto-Provisioning** screen to determine whether an existing policy can be used as is, a new Auto Provisioning Policy requires creation or an existing policy requires edit or deletion.

3 Review the following **Auto-Provisioning** parameters:

Auto-Provisioning Policy	Lists the name of each policy when it was created. It cannot be modified as part of the Auto Provisioning Policy's edit process.
Adopt if No Rules Match	Displays whether this policy will adopt devices if no adoption rules apply. Double-click within this column to launch the edit screen where rules can be defined for device adoption. This feature is disabled by default.
Rerun Policy Rules Every Time AP Adopted	Displays whether this policy will be run every time an AP is adopted. Double-click within this column to launch the edit screen where this option can be modified. This feature is disabled by default.

4 Select **Add** to create a new Auto Provisioning Policy, **Edit** to revise an existing Auto Provisioning Policy or **Delete** to permanently remove a policy. For instructions on either adding or editing an Auto Provisioning Policy, see Configuring an Auto-Provisioning Policy on page 5-270.

5.3.1 Configuring an Auto-Provisioning Policy

- *Cluster Configuration Overrides (Controllers and Service Platforms Only)*

Auto-Provisioning Policies can be created or refined as unique deployment requirements dictate changes in the number of Access Point radios within a specific radio coverage area.

To add a new Auto Provisioning Policy or edit an existing Auto-Provisioning Policy configuration:

1 From the **Adoption** screen, either select **Add** or select an existing Auto-Provisioning Policy and select **Edit**.

2 If adding a new Auto-Provisioning Policy, provide a name in the **Auto-Provisioning Policy** field. The name must not exceed 32 characters. Select **Continue** to enable the remaining parameters of the Auto-Provisioning Policy screen.

The **Rules** tab displays by default.

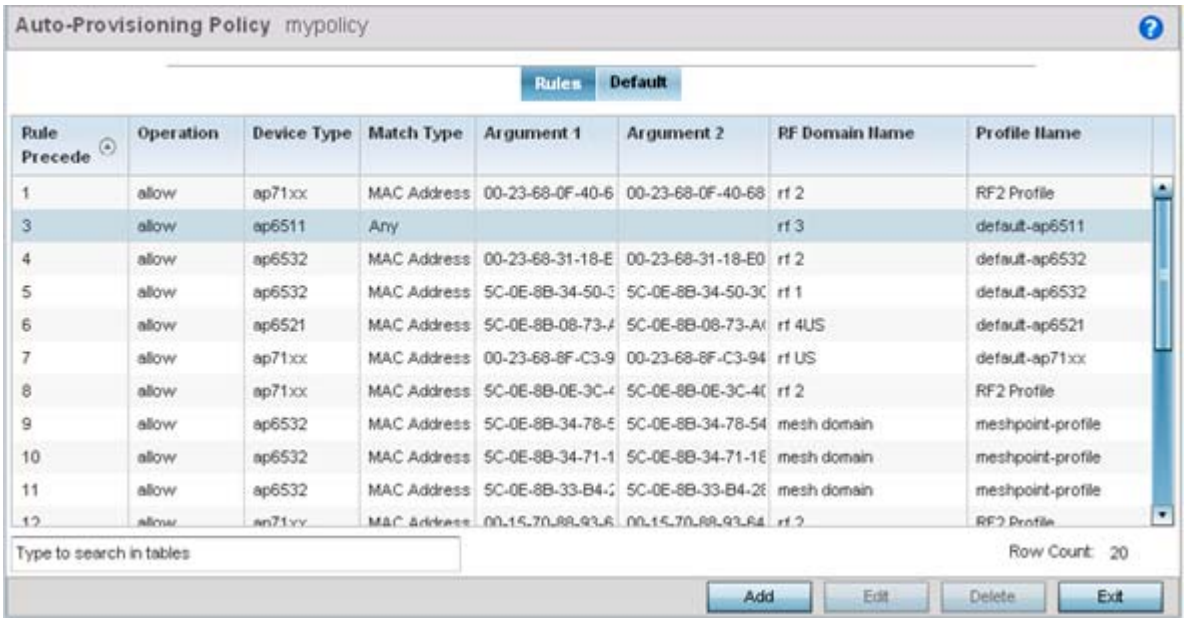


Figure 5-159 *Auto-Provisioning Policy screen - Rules tab*

3 Review the following **Auto-Provisioning Policy** rule data to determine whether a rule can be used as is, requires edit or whether new rules need to be defined:

Rule Precedence	Displays the precedence (sequence) the Adoption Policies rules are applied. Rules with the lowest precedence receive the highest priority. This value is set (from 1 - 1000) when adding a new Auto Provisioning Policy rule configuration.
Operation	Lists the operation taken upon receiving an adoption request from an Access Point: The following operations are available: *allow* – Allows the normal provisioning of connected Access Points upon request. *deny* – Denies (prohibits) the provisioning of connected Access Point upon request. *redirect* – When selected, an Access Point seeks a steering controller (upon adoption request), that will forward the network credentials of a designated controller resource that initiates the provisioning process. *upgrade* – Conducts the provisioning of requesting Access Points from this controller resource.
Device Type	Sets the Access Point model for which this policy applies. Adoption rules are specific to the selected model.

Match Type	Lists the matching criteria used in the policy. This is like a filter and further refines the APs that can be adopted. The Match Type can be one of the following: *MAC Address* – The filter type is a MAC Address of the selected Access Point model. *IP Address* – The filter type is the IP address of the selected Access Point model. *VLAN* – The filter type is a VLAN. *Serial Number* – The filter type is the serial number of the selected Access Point model. *Model Number* – The filter type is the Access Point model number. *DHCP Option* – The filter type is the DHCP option value of the selected Access Point model.
Argument 1	The number of arguments vary on the Match Type. This column lists the first argument value. This value is not set as part of the rule creation or edit process.
Argument 2	The number of arguments vary on the Match Type. This column lists the second argument value. This value is not set as part of the rule creation or edit process.
RF Domain Name	Sets the name of the RF Domain to which the device is adopted automatically. Select the *Create* icon to define a new RF Domain configuration or select the *Edit* icon to revise an existing configuration.
Profile Name	Defines the name of the profile used when the Auto Provisioning Policy is applied to a device. Select the *Create* icon to define a new Profile configuration or the *Edit* icon to revise an existing configuration. For more information, see General Profile Configuration on page 8-5.

4 If a rule requires addition or modification, select either **Add** or **Edit** to define the required parameters using the Rule screen.

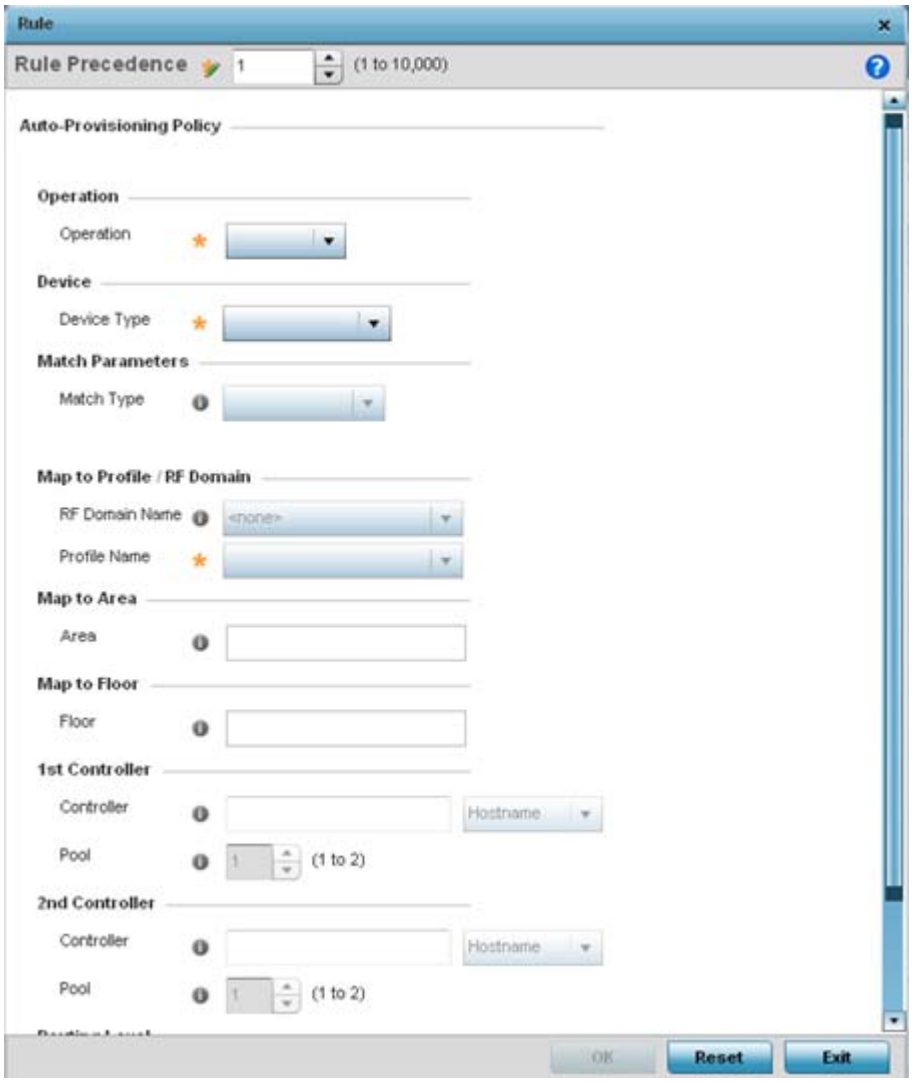


Figure 5-160 *Auto Provisioning Policy Rule screen*

5 Specify the following parameters in the **Rule** screen:

Rule Precedence	Assign a priority from 1 - 10,000 for the application of the auto-provisioning policy rule. Rules with thlowest value have priority.
Operation	Define the operation taken upon receiving an adoption request from an Access Point: the following operations are available: *Allow* – Allows the normal provisioning of connected Access Points upon request. *Deny* – Denies (prohibits) the provisioning of connected Access Point upon request. *Redirect* – When selected, an Access Point seeks a steering controller (upon adoption request), that will forward the network credentials of a designated controller resource that initiates the provisioning process. *Upgrade* – Conducts the provisioning of requesting Access Points from this controller resource.
Device Type	Set the Access Point model for which this policy applies. Adoption rules are specific to the selected model, as radio configurations are often unique to specific models.

Match Type	Set the matching criteria used in the policy. This is like a filter and further refines Access Points capable of adoption. The Match Type can be one of the following: *MAC Address* – The filter type is a MAC Address of the selected Access Point model. *IP Address* – The filter type is the IP address of the selected Access Point model. *VLAN* – The filter type is a VLAN. *Serial Number* – The filter type is the serial number of the selected Access Point model. *Model Number* – The filter type is the Access Point model number. *DHCP Option* – The filter type is the DHCP option value of the selected Access Point model.
RF Domain Name	Set the RF Domain to which the device is adopted automatically. Select the *Create* icon to define a new RF Domain configuration or select the *Edit* icon to revise an existing configuration. For more information, see to General Profile Configuration on page 8-5.
Profile Name	Define the profile used when an Auto Provisioning Policy is applied to a device. Select the *Create* icon to define a new Profile configuration or select the *Edit* icon to revise an existing configuration. For more information, see General Profile Configuration on page 8-5.
Area	Enter a 64 character maximum deployment area name assigned to this policy.
Floor	Enter a 32 character maximum deployment floor name assigned to this policy.
1st Controller	When *redirect* is selected as the operation, provide a 1st choice steering controller *Hostname* or *IP Address* and port to forward network credentials for a controller resource to initiate the provisioning process.
2nd Controller	When *redirect* is selected as the operation, provide a 2nd choice steering controller *Hostname* or *IP Address* and port to forward network credentials for a controller resource to initiate the provisioning process.
Routing Level	When *redirect* is selected as the operation, specify the routing level as *1* or *2*.

6 Select **OK** to save the updates and overrides to the Auto-Provisioning policy rule configuration. Select **Reset** to revert to the last saved configuration.

7 Select the **Default** tab to define the Auto Provisioning Policy's rule matching adoption configuration.

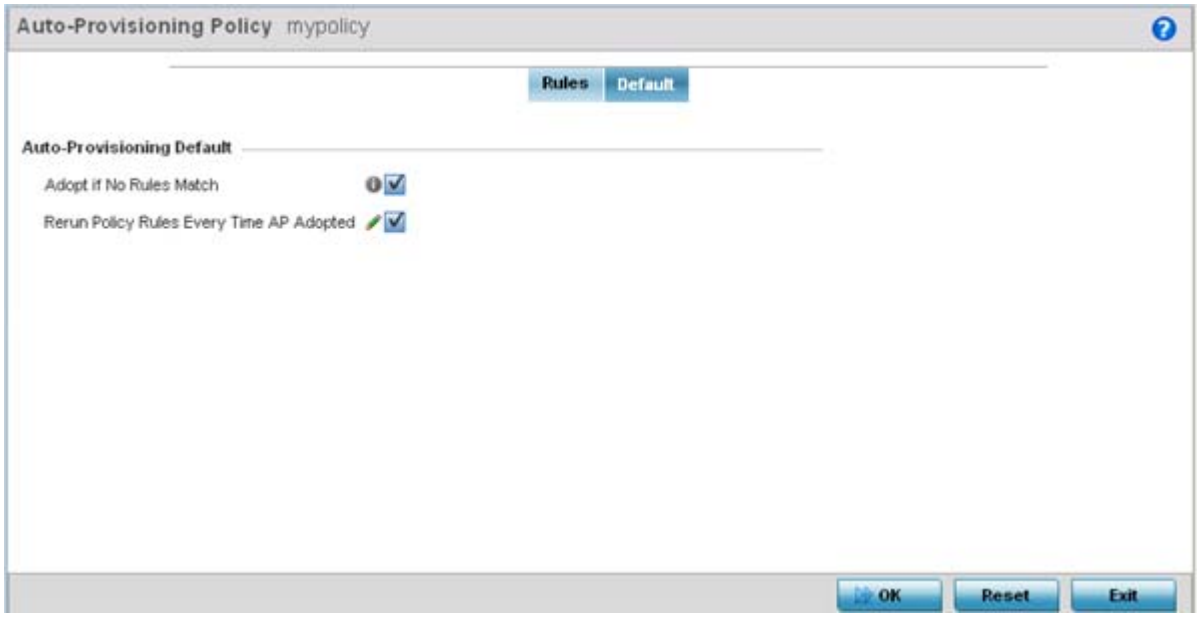


Figure 5-161 *Auto Provisioning Policy screen - Default tab*

8 Select **Adopt if No Rules Match** to adopt when no matching filter rules apply. This setting is disabled by default.

9 Select **Rerun Policy Rules Every Time AP Adopted** to run this policy and apply its rule set every time an Access Point is adopted. This setting is disabled by default.

10 Select **OK** to save the updates to the screen. Selecting **Reset** reverts the screen to the last saved configuration.

5.4 Managing an Event Policy

Device Configuration

Event Policies enable an administrator to create specific notification mechanisms using one, some or all of the SNMP, syslog, forwarding or e-mail notification options available to the controller or service platform. Each listed event can have customized notification settings defined and saved as part of an event policy. Thus, policies can be configured and administrated in respect to specific sets of client association, authentication/encryption and performance events. Once policies are defined, they can be mapped to device profiles strategically as the likelihood of an event applies to particular devices. By default, there's no enabled event policy and one needs to be created and implemented.

When initially displayed, the Event Policy screen lists interfaces. Existing policies can have their event notification configurations modified as device profile requirements warrant.

To define an event policy:

1 Select **Configuration** > **Devices** > **Event Policy**.

2 Select **Add** to create a new event policy or **Edit** to modify an existing policy. Use the **Delete** button to remove existing event policy.

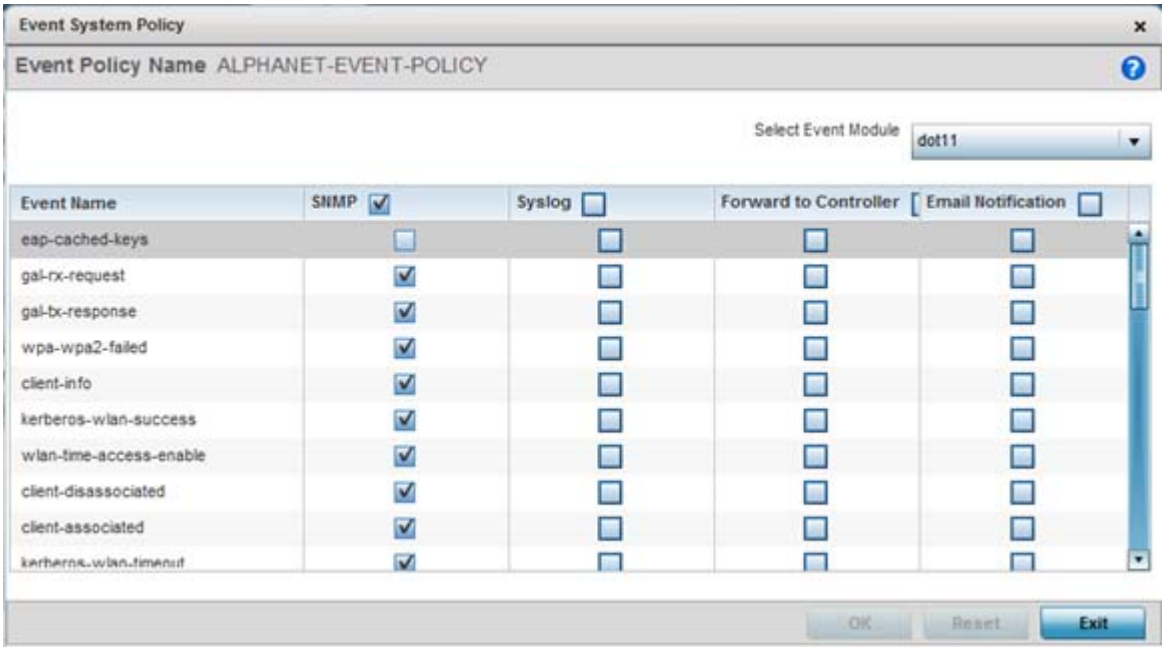


Figure 5-162 *Event Policy screen*

3 Ensure the button is selected to enable the screen for configuration for a specific event category. This option needs to remain selected to apply the event policy configuration to the profile.

4 Refer to the **Select Event Module** drop-down menu on the top right-hand side of the screen and select an event module used to track the occurrence of each list event.

5 Review each event and select (or deselect) the *SNMP*, *Syslog*, *Forward to Controller* or *Email Notification* option as required for the event. Map an existing policy to a device profile as needed. Select Profile from the Map drop-down menu in the lower-left hand side of the screen. Expand the list of device profiles available, and apply the event policy as required.

6 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration. **Delete** obsolete rows as needed.

5.5 Managing MINT Policies

Device Configuration

To add or modify a MINT Policy:

1 Select **Configuration** > **Devices > MINT Policy** to display the MINT Policy screen.

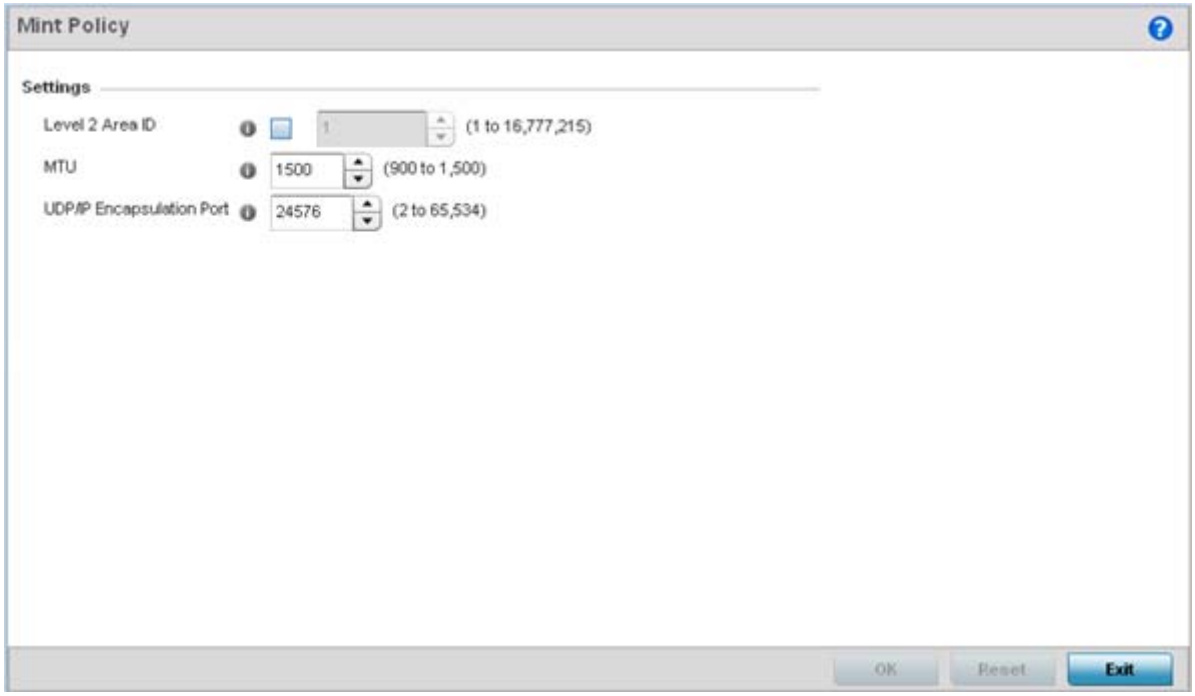


Figure 5-163 *MINT Policy Configuration screen*

2 Configure the following parameters to configure the MINT policy:

Level 2 Area ID	Define a Level 2 Area ID for the Mint Policy. The Level 2 Area ID is the global mint area identifier. This area identifier separates two overlapping mint networks and need only be configured if the administrator has two mint networks that share the same packet broadcast domain.
MTU	Specify a MTU value for the mint policy between 900 and 1,500. The MTU setting specifies the maximum packet size that will be used for mint packets. Larger packets will be fragmented so they fit within this packet size limit. The administrator may want to configure this parameter if the mint backhaul network requires or recommends smaller packet sizes. The default value is 1500.
UDP/IP Encapsulation Port	Specify the port to use for UDP/IP encapsulation between 2 and 65,534. This value specifies an alternate UDP port to be used by mint packets and must be an even number. This port number will be used by mint control packets, and this port value plus 1 will be used to carry mint data packets. The default value is 24576.

3 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

6 Wireless Configuration

A *Wireless Local Area Network* (WLAN) is a data-communications system and wireless local area network that flexibly extends the functionalities of a wired LAN. A WLAN links two or more computers or devices using spread-spectrum or OFDM modulation based technology. A WLAN does not require lining up devices for line-of-sight transmission, and are thus, desirable for wireless networking. Roaming users can be handed off from one wireless controller connected Access Point to another, like a cellular phone system. WLANs can therefore be configured around the needs of specific user groups, even when they are not in physical proximity.

WLANs can be used to provide an abundance of services, including data communications (allowing mobile devices to access applications), E-mail, file and print services or even specialty applications (such as guest access control and asset tracking).

Each wireless controller WLAN configuration contains encryption, authentication and QoS policies and conditions for user connections. Connected Access Point radios transmit periodic beacons for each BSS. A beacon advertises the SSID, security requirements, supported data rates of the wireless network to enable clients to locate and connect to the WLAN.

WLANs are mapped to radios on each connected Access Point. A WLAN can be advertised from a single Access Point radio or can span multiple Access Points and radios. WLAN configurations can be defined to only provided service to specific areas of a site. For example a guest access WLAN may only be mapped to a 2.4GHz radio in a lobby or conference room providing limited coverage while a data WLAN is mapped to all 2.4GHz and 5GHz radios at the branch site providing complete coverage.

RFS4000 and RFS6000 series wireless controllers and NX4500 and NX6500 series service platforms support a maximum of 32 WLANs. The NX7500 service platforms support up to 256 WLANs. NX9000 series service platforms support up to 1000 WLANs.

The wireless configuration is comprised the following policies:

- *Wireless LAN Policy*
- *Configuring WLAN QoS Policies*
- *Radio QoS Policy*
- *Association ACL*
- *Smart RF Policy*
- *MeshConnex Policy*
- *Mesh QoS Policy*
- *Passpoint Policy*
- *Sensor Policy*

These policies can be separately selected within the **Configuration > Wireless** pane located in top, left-hand, side of the UI.

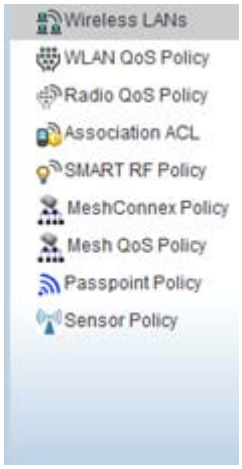


Figure 6-1 *Configuration > Wireless pane*

6.1 Wireless LAN Policy

To review the attributes of existing WLANs and, if necessary, modify their configurations:

1 Select **Configuration** > **Wireless** > **Wireless LANs** to display a high-level display of the existing WLANs.

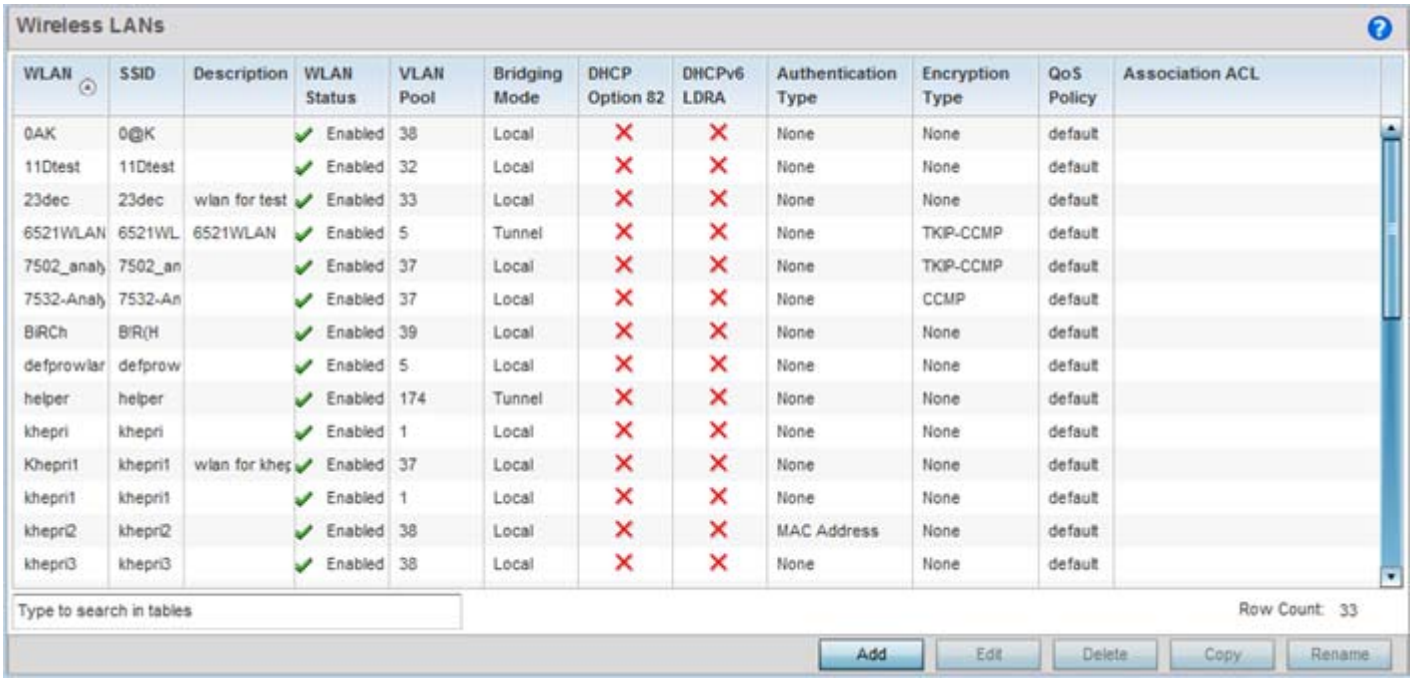


Figure 6-2 *Wireless LANs screen*

2 Refer to the following (read only) information to assess the attributes of the each WLAN available to the wireless controller:

WLAN	Displays the name of each available WLAN. Individual WLANs can selected and their SSID and client management properties modified. RFS4000 and RFS6000 series wireless controllers and NX4500 and NX6500 series service platforms support a maximum of 32 WLANs. The NX7500 service platforms support up to 256 WLANs. NX9000 series service platforms support up to 1000 WLANs.
SSID	Displays the name of the SSID assigned to the WLAN when created or last modified. Optionally, select a WLAN and click the *Edit* button to update the WLAN's SSID.
Description	Displays the brief description set for each listed WLAN when it was either created or modified.
WLAN Status	Lists each WLAN's current status as either *Active* or *Shutdown*. A green check mark defines the WLAN as available to clients on all radios where it has been mapped. A red "X" defines the WLAN as shutdown, meaning even if the WLAN is mapped to radios, it's not available for clients to associate.
VLAN Pool	Lists each WLAN's current VLAN mapping. The wireless controller permits mapping a WLAN to more than one VLANs. When a client associates with a WLAN, the client is assigned a VLAN by load balance distribution. The VLAN is picked from a pool assigned to the WLAN. Keep in mind however, typical deployments only map a single VLAN to a WLAN. The use of a pool is strictly optional.
Bridging Mode	Displays the bridging mode used by each WLAN. Available bridging modes are Local and Tunnel.
DHCP Option 82	DHCP Option 82 is commonly used in large enterprise deployments to provide client physical attachment information. Option 82 is used in distributed DHCP server/relay environments, where relays insert additional information to identify the client's point of attachment. A red "X" defines DHCP option 82 as disabled, a green check means its enabled.
DHCPv6 LDRA	*Lightweight DHCPv6 Relay Agent* (LDRA) is used to insert relay-agent options in DHCPv6 message exchanges that identify client-facing interfaces. These relay agents are deployed to forward DHCPv6 messages between clients and servers when they are not on the same IPv6 link. A red "X" indicates this WLAN acts as a DHCPv6 LDRA.
Authentication Type	Displays the name of the authentication scheme this WLAN is using to secure its client membership transmissions. *None* is listed if authentication is not used within this WLAN. Refer to the Encryption type column if no authentication is used to verify there is some sort of data protection used with the WLAN or risk no protection at all.
Encryption Type	Displays the name of the encryption scheme this WLAN is using to secure its client membership transmissions. *None* is listed if encryption is not used within this WLAN. Refer to the Authentication type column if no encryption is used to verify there is some sort of data protection used with the WLAN or risk using this WLAN with no protection at all.

QoS Policy	Lists the QoS policy applied to each listed WLAN. A QoS policy needs to be custom selected (or created) for each WLAN in respect to the WLAN's intended client traffic and the voice, video or normal data traffic it supports.
Association ACL	Lists the Association ACL policy applied to each listed WLAN. An Association ACL is a policy-based *Access Control List* (ACL) that either prevents or allows wireless clients from connecting to a WLAN. The mapping of an Association ACL is strictly optional.

Use the sequential set of WLAN screens to define a unique configuration for each WLAN. Refer to the following to set WLAN configurations:

- *Basic WLAN Configuration*
- *Configuring WLAN Security*
- *Configuring WLAN Firewall Support*
- *Configuring Client Settings*
- *Configuring WLAN Accounting Settings*
- *Configuring WLAN Service Monitoring Settings*
- *Configuring Client Load Balancing Settings*
- *Configuring Advanced WLAN Settings*
- *Configuring Auto Shutdown Settings*

6.1.1 Basic WLAN Configuration

Wireless LAN Policy

When creating or modifying a WLAN, the Basic Configuration screen is the first screen that displays as part of the WLAN configuration screen flow. is the Use this screen to enable a WLAN and define its SSID, client behavior and VLAN assignments.

1 Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display a high-level display of the existing WLANs.

2 Select the **Add** button to create an additional WLAN, or select an existing WLAN then **Edit** to modify its properties.

RFS4000 and RFS6000 model wireless controllers support a maximum of 32 WLANs. The NX7500 service platform support up to 256 WLANs. The NX9000 Series supports up to 1000 WLANs.

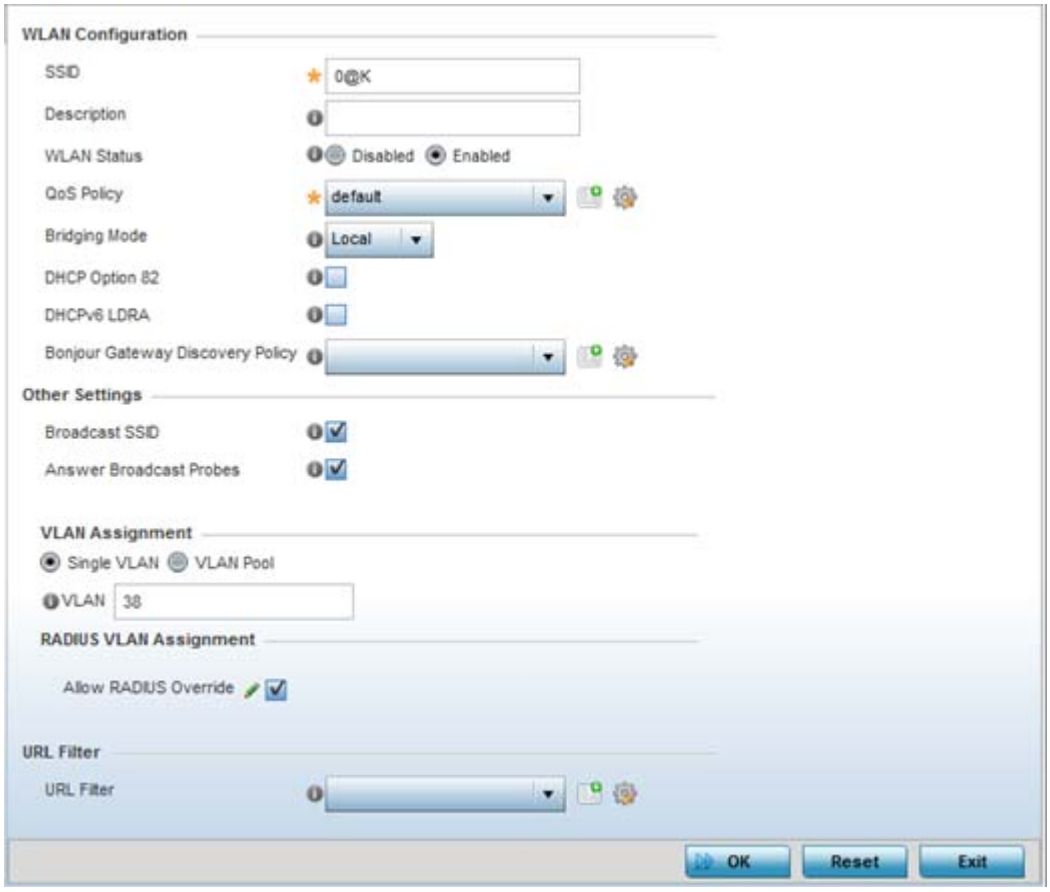


Figure 6-3 *WLAN Policy Basic Configuration screen*

3 Refer to the **WLAN Configuration** field to define the following:

WLAN	If adding a new WLAN, enter its name in the space provided. Spaces between words are not permitted. The name could be a logical representation of the WLAN coverage area (engineering, marketing etc.). If editing an existing WLAN, the WLAN's name appears at the top of the screen and cannot be modified. The name cannot exceed 32 characters.
SSID	Enter or modify the *Services Set Identification* (SSID) associated with the WLAN. The maximum number of characters that can be used for the SSID is 32.
Description	Provide a textual description for the WLAN to help differentiate it from others with similar configurations. The description can be up to 64 characters.
WLAN Status	Select the *Enabled* radio button to make this WLAN active and available to clients on all radios where it has been mapped. Select the *Disabled* radio button to make this WLAN inactive, meaning even if the WLAN is mapped to radios, it's not available for clients to associate and use.

QoS Policy	Use the drop-down menu to assign an existing QoS policy to the WLAN or select the *Create* icon to define a new QoS policy or select the *Edit* icon to modify the configuration of the selected QoS Policy. QoS helps ensure each WLAN receives a fair share of the overall bandwidth, either equally or per the proportion configured. For information on creating a QoS policy that can be applied to WLAN, see *Configuring WLAN QoS Policies*.
Bridging Mode	Use the drop-down menu to specify a bridging mode for the WLAN. Available bridging policy modes are *Local*, *Tunnel* or *split-tunnel*.
DHCP Option 82	Select this option to enable DHCP option 82. DHCP Option 82 provides client physical attachment information. This setting is disabled by default.
DHCPv6 LDRA	Select this option to enable the DHCPv6 relay agent. The DHCPv6 LDRA (*Lightweight DHCP Relay Agent*) allows for DHCPv6 messages to be transmitted on existing networks that do not currently support IPv6 or DHCPv6.
Bonjour Gateway Discovery Policy	Select an existing Bonjour configuration to apply to the WLAN configuration. Bonjour provides a method to discover services on a WLAN. Bonjour allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.

4 Refer to the **Other Settings** field to define broadcast behavior within this specific WLAN.

Broadcast SSID	Select this check box to enable the wireless controller to broadcast SSIDs within beacons. If a hacker tries to isolate and hack a client SSID via a client, the ESSID will display since the ESSID is in the beacon. This feature is enabled by default.
Answer Broadcast Probes	Select this check box to associate a client with a blank SSID (regardless of which SSID the wireless controller is currently using). This feature is enabled by default.

5 Refer to the **VLAN Assignment** field to add or remove VLANs for the selected WLAN, and define the number of clients permitted. Remember, users belonging to separate VLANs can share the same WLAN. It's not necessary to create a new WLAN for every VLAN in the network.

Single VLAN	Select the *Single VLAN* radio button to assign just one VLAN to this WLAN. Enter the name of the VLAN within the VLAN parameter field when the Single VLAN radio button is selected. Utilizing a single VLAN per WLAN is a more typical deployment scenario than using a VLAN pool.
VLAN Pool	Select the *VLAN Pool* radio button to display a table with VLAN and wireless client columns (representing configurable options). Define the VLANs available to this WLAN. Additionally, define the number of wireless clients supported by each VLAN. Use the radio button's on the left-hand side of the table to enable or disable each VLAN and wireless client configuration for the WLAN. Select the *+ Add Row* button to add additional VLANs to the WLAN.

6 Select the **Allow Radius Override** check box in the RADIUS VLAN Assignment to allow an override to the WLAN configuration. If, as part of the authentication process, the RADIUS server returns a client's VLAN-ID in a

RADIUS Access-Accept packet, and this feature is enabled, all client traffic is forward on that VLAN. If disabled, the RADIUS server returned VLAN-ID is ignored and the VLAN configuration (defined above) is used.

7 Use the **URL Filter** field to configure user access restrictions to resources on the controller or service platform managed Internet. User access is controlled with URL Filters. Use the **URL Filter** drop down menu to select a preconfigured URL Filter. To create a new URL Filter, use the **Create** button. To edit an existing URL Filter, use the **Edit** button.

8 Select **OK** when completed to update the WLAN's basic configuration. Select **Reset** to revert the screen back to the last saved configuration.

6.1.2 Configuring WLAN Security

- *Wireless LAN Policy*

A WLAN can be assigned a security policy supporting authentication, captive portal (hotspot) or encryption schemes.

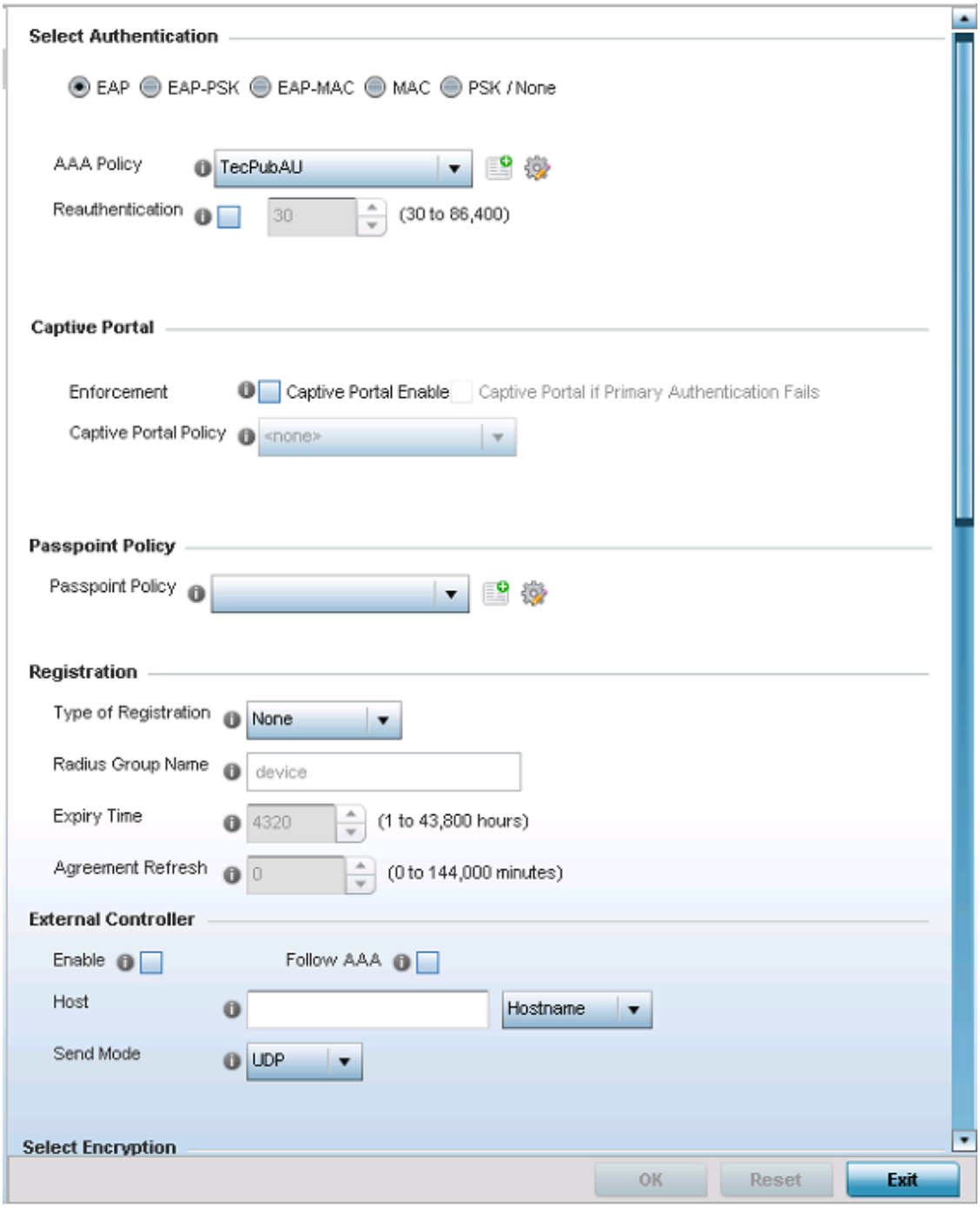


Figure 6-4 *WLAN Policy Security screen*

Authentication ensures only known and trusted users or devices access a WLAN. Authentication is enabled per WLAN to verify the identity of both users and devices. Authentication is a challenge and response procedure for validating user credentials such as username, password and sometimes secret-key information.

A client must authenticate to an Access Point to receive resources from the network. Controllers and service platforms support *EAP*, *EAP PSK, EAP-MAC, MAC* and PSK/None authentication options.

Refer to the following to configure an authentication scheme for a WLAN:

- *802.1x EAP, EAP-PSK and EAP MAC*
- *MAC Authentication*
- *PSK / None*

Secure guest access to the network is referred to as *captive portal* access. A captive portal is guest access policy for providing guests temporary and restrictive access to the wireless network. Existing captive portal policies can be applied to a WLAN to provide secure guest access as needed.

A captive portal configuration provides secure authenticated access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Once logged into captive portal, additional *Agreement, Welcome* and *Fail* pages provide the administrator with a number of options on captive portal screen flow and user appearance. Refer to *Captive Portal on page 6-13* for information on assigning a captive portal policy to a WLAN.

A *passpoint* policy provides an interoperable platform for streamlining Wi-Fi access to Access Points deployed as public hotspots. Passpoint is supported across a wide range of wireless network deployment scenarios and client devices. For more information, see *Passpoint Policy*.

Encryption is central for WLAN security, as it provides data privacy for traffic forwarded over a WLAN. When the 802.11 specification was introduced, Wired Equivalent Privacy (WEP) was the primary encryption mechanism. WEP has since been interpreted as flawed in many ways, and is not considered an effective standalone encryption scheme for securing a wireless controller WLAN. WEP is typically used WLAN deployments designed to support legacy clients. New device deployments should use either WPA or WPA2 encryption.

Encryption applies a specific algorithm to alter its appearance and prevent unauthorized hacking. Decryption applies the algorithm in reverse, to restore the data to its original form. A sender and receiver must employ the same encryption/decryption method to interoperate. When both TKIP and CCMP are both enabled a mix of clients are allowed to associate with the WLAN. Some use TKIP, others use CCMP. Since broadcast traffic needs to be understood by all clients, the broadcast encryption type in this scenario is TKIP.

TKIP-CCMP, WPA2-CCMP, WEP 64, WEP 128 and Keyguard encryption options are supported.

Refer to the following to configure an encryption scheme for a WLAN:

- *TKIP-CCMP*
- *WPA2-CCMP*
- *WEP 64*
- *WEP 128*
- *Keyguard*
- *T5 Controller Security*

6.1.2.1 802.1x EAP, EAP-PSK and EAP MAC

Configuring WLAN Security

The *Extensible Authentication Protocol* (EAP) is the de-facto standard authentication method used to provide secure authenticated access to WLANs. EAP provides mutual authentication, secured credential exchange, dynamic keying and strong encryption. 802.1X EAP can be deployed with WEP, WPA or WPA2 encryption schemes to further protect user information forwarded over WLANs.

The EAP process begins when an unauthenticated supplicant (client device) tries to connect with an authenticator (in this case, the authentication server). An Access Point passes EAP packets from the client to an authentication

server on the wired side of the Access Point. All other packet types are blocked until the authentication server (typically, a RADIUS server) verifies the client's identity.

802.1X EAP provides mutual authentication over the WLAN during authentication. The 802.1X EAP process uses credential verification to apply specific policies and restrictions to WLAN users to ensure access is only provided to specific wireless controller resources.

802.1X requires a 802.1X capable RADIUS server to authenticate users and a 802.1X client installed on each devices accessing the EAP supported WLAN. An 802.1X client is included with most commercial operating systems, including Microsoft Windows, Linux and Apple OS X.

The RADIUS server authenticating 802.1X EAP users can reside either internally or externally to a controller, service platform or Access Point. User account creation and maintenance can be provided centrally using ADSP or individually maintained on each device. If an external RADIUS server is used, EAP authentication requests are forwarded.

When using PSK with EAP, the controller, service platform or Access Point sends a packet requesting a secure link using a pre-shared key. The authenticating device must use the same authenticating algorithm and passcode during authentication. EAP-PSK is useful when transitioning from a PSK network to one that supports EAP. The only encryption types supported with this are TKIP, CCMP and TKIP-CCMP.

To configure EAP on a WLAN:

1 Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN, or select and existing WLAN and **Edit** to modify the security properties of an existing WLAN.

3 Select **Security**.

4 Select **EAP, EAP-PSK** or **EAP-MAC** as the authentication type.

Either option enables the radio buttons for various encryption mechanisms as an additional measure of security with the WLAN.

Figure 6-5 *EAP, EAP-PSK or EAP MAC Authentication screen*

5 Either select an existing **AAA Policy** from the drop-down menu or select the **Create** icon to the right of the AAA Policy parameter to display a screen where new AAA policies can be created. Select the **Edit** icon to modify the configuration of the selected AAA policy.

Authentication, authorization, and *accounting* (AAA) is a framework for intelligently controlling access to the network, enforcing user authorization policies and auditing and tracking usage. These combined processes are central for securing wireless client resources and wireless network data flows.

6 Select the **Reauthentication** check box to force EAP supported clients to reauthenticate. Use the spinner control set the number of seconds (from 30 - 86,400) that, once exceeded, forces the EAP supported client to reauthenticate to use the resources supported by the WLAN.

7 Select **OK** when completed to update the WLAN's EAP configuration. Select **Reset** to revert back to the last saved configuration.

EAP, EAP-PSK and EAP MAC Deployment Considerations

802.1x EAP, EAP-PSK and EAP MAC

Before defining a 802.1x EAP, EAP-PSK or EAP MAC supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- A valid certificate should be issued and installed on devices providing 802.1X EAP. The certificate should be issued from an Enterprise or public certificate authority to allow 802.1X clients to validate the identity of the authentication server prior to forwarding credentials.
- If using an external RADIUS server for EAP authentication, the round trip delay over the WAN should not exceed 150ms. Excessive delays over a WAN can cause authentication and roaming issues and impact wireless client performance. If experiencing excessive delays, consider using local RADIUS resources.

6.1.2.2 MAC Authentication

Configuring WLAN Security

MAC is a device level authentication method used to augment other security schemes when legacy devices are deployed using static WEP.

MAC authentication can be used for device level authentication by permitting WLAN access based on device MAC address. MAC authentication is typically used to augment WLAN security options that do not use authentication (such as static WEP, WPA-PSK and WPA2-PSK) MAC authentication can also be used to assign VLAN memberships, Firewall policies and time and date restrictions.

MAC authentication can only identify devices, not users. MAC authentication only references a client wireless interface card MAC address when authenticating the device, it does not distinguish the device's user credentials. MAC authentication is somewhat poor as a standalone data protection technique, as MAC addresses can be easily spoofed by hackers who can provide a device MAC address to mimic a trusted device within the network.

MAC authentication is enabled per WLAN profile, augmented with the use of a RADIUS server to authenticate each device. A device's MAC address can be authenticated against the local RADIUS server built into the device or centrally (from a datacenter). For RADIUS server compatibility, the format of the MAC address can be forwarded to the RADIUS server in non-delimited and or delimited formats:

To configure MAC on a WLAN:

1 Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN, or select and existing WLAN and **Edit** to modify the security properties of an existing WLAN.

3 Select **Security**.

4 Select **MAC** as the Authentication Type.

Selecting MAC enables the radio buttons for each encryption option as an additional measure of security for the WLAN.

Figure 6-6 *MAC Authentication screen*

5 Either select an existing AAA Policy from the drop-down menu or select the **Create** icon to the right of the AAA Policy parameter to display a screen where new AAA policies can be created. A default AAA policy is also available if configuring a WLAN for the first time and there's no existing policies. Select the **Edit** icon to modify the configuration of a selected AAA policy.

Authentication, authorization, and *accounting* (AAA) is a framework for intelligently controlling access to the wireless client, enforcing user authorization policies and auditing and tracking usage. These combined processes are central for securing wireless client resources and wireless network data flows.

6 Select the **Reauthentication** option to force MAC supported clients to reauthenticate. Use the spinner control set the number of minutes (30 - 86,400) that, once exceeded, forces the EAP supported client to reauthenticate in order to use the resources supported by the WLAN.

7 Select **OK** when completed to update the WLAN's MAC configuration. Select **Reset** to revert the screen back to the last saved configuration.

MAC Authentication Deployment Considerations

MAC Authentication

Before defining a MAC authentication configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- MAC authentication can only be used to identify end-user devices, not the users themselves.
- MAC authentication is somewhat poor as a standalone data protection technique, as MAC addresses can be easily spoofed by hackers who can provision a MAC address on their device to mimic a trusted device.

6.1.2.3 PSK / None

Configuring WLAN Security

Open-system authentication can be referred to as no authentication, since no actual authentication and user credential validation takes place. A client user requests (and is granted) authentication with no credential exchange.

Figure 6-7 *PSK / None Settings screen*

NOTE: Although *None* implies no authentication, this option is also used when pre-shared keys are used for encryption (thus the PSK in the description).

6.1.2.4 Captive Portal

Configuring WLAN Security

A *captive portal* is an access policy for providing guests temporary and restrictive access to the controller, service platform or Access Point managed network. For an overview of the Captive Portal process and information on how to define a captive portal policy, see *Configuring Captive Portal Policies on page 11-1*.

To assign a captive portal policy to a WLAN:

1 Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN or select an existing WLAN and select **Edit** to modify the properties of an existing wireless controller WLAN.

3 Select **Security**.

4 Refer to the **Captive Portal** field within the WLAN Policy security screen.

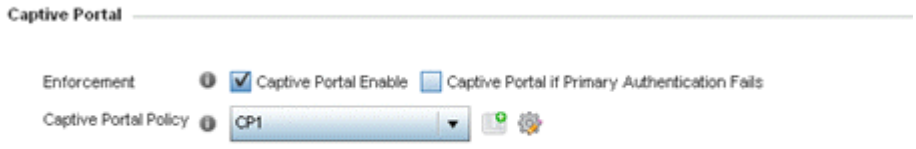


Figure 6-8 *WLAN Policy Security screen - Captive Portal Field*

5 Select the **Captive Portal Enable** option if authenticated guest access is required with the selected WLAN. This feature is disabled by default.

6 Select the **Captive Portal if Primary Authentication Fails** checkbox to enable the captive portal policy if the primary authentication is unavailable. This option is only enabled when **Captive Portal Enable** is selected.

7 Select the **Captive Portal Policy** to use with the WLAN from the drop-down menu. If no relevant policies exist, select the **Create** icon to define a new policy to use with this WLAN or the **Edit** icon to update the configuration of an existing Captive Portal policy. For more information, see *Configuring Captive Portal Policies on page 11-1*.

8 Select **OK** when completed to update the Captive Portal configuration. Select **Reset** to revert the WLAN Policy Security screen back to the last saved configuration.

6.1.2.5 Passpoint

Configuring WLAN Security

A *passpoint* policy provides an interoperable platform for streamlining Wi-Fi access to Access Points deployed as public hotspots (captive portals). Passpoint is supported across a wide range of wireless network deployment scenarios and client devices.

To assign a passpoint policy to a WLAN:

1 Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN or select an existing WLAN and select **Edit** to modify the properties of an existing wireless controller WLAN.

3 Select **Security**.

4 Refer to the **Passpoint** field within the WLAN Policy security screen.

Figure 6-9 *WLAN Policy Security screen - Passpoint Policy*

5 Select an existing **Passpoint Policy** from the drop down menu to apply it to the WLAN. If no relevant policies exist, select the **Create** icon to define a new policy to use with this WLAN or the **Edit** icon to update the configuration of an existing passpoint policy. For more information, see *Passpoint Policy on page 6-104*.

6 Select **OK** when completed to update the Captive Portal configuration. Select **Reset** to revert the WLAN Policy Security screen back to the last saved configuration.

6.1.2.6 Registration

Configuring WLAN Security

Registration requires the validation of devices by address to continue the authentication process.

To assign a Registration to a WLAN:

1 Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN or select an existing WLAN and select **Edit** to modify the properties of an existing wireless controller WLAN.

3 Select **Security**.

4 Refer to the **Registration** section within the WLAN Policy security screen.

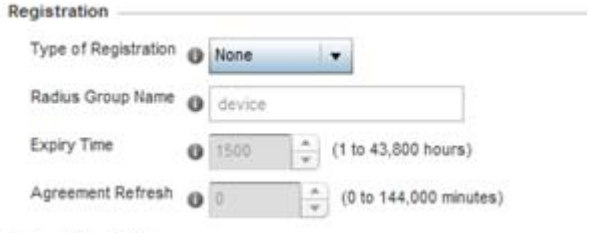


Figure 6-10 *WLAN Policy Security screen - MAC Registration*

5 Use the **Type of Registration** drop-down menu to set the self-registration type for the selected WLAN. Options include *None, device, user* and *device-OTP*.

When captive portal guest users are authenticating using their User ID (Email Address/Mobile Number/ Member ID) and the received pass code in order to complete the registration process. The WLAN authentication type should be MAC-Authentication and the WLAN registration type should be configured as **device-OTP**.

When captive portal device registration is through social media, the WLAN registration type should be set as **device** registration, and the captive portal needs to be configured for guest user social authentication.

Enter a 64 character maximum **RADIUS Group Name** to which the registering user associates. When left blank, users are not associated with a RADIUS group.

Use the **Expiry Time** spinner control to set the amount of time (from 1 - 43,800 hours) before registration addresses expire and must be re-entered.

Set the **Agreement Refresh** as the amount of time (from 0 - 144,000 minutes) before the agreement page is displayed if the user has not been logged during the specified period. The default setting is 0 days.

6 Select **OK** when completed to update the Registration settings. Select **Reset** to revert the WLAN Policy Security screen back to the last saved configuration.

6.1.2.7 External Controller

Configuring WLAN Security

To set the WLAN's external controller or service platform security configuration:

1 Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN or select an existing WLAN and select **Edit** to modify its properties.

3 Select **Security**.

4 Refer to the **External Controller** section within the WLAN Policy security screen

Figure 6-11 *WLAN Policy Security screen - External Controller Field*

5 Select the **Enable** option if WLAN authentication is handled using an external resource. This feature is disabled by default.

Select the **Follow AAA** option if the resource handling WLAN authentication and accounting is an external RADIUS server specified within an AAA policy. However, ensure that an AAA policy identifying the authentication and accounting server exists and is associated with the WLAN.

Note, in case of EGuest deployment, the authenticating and accounting server specified in the AAA policy should point to the EGuest server host.

6 If using an external resource, other than the AAA RADIUS server, use the drop-down menu to select either **Hostname** or **IP Address** and enter the server information in the **Host** field. Hostnames cannot include an underscore character.

7 Select the **Send Mode** as either **UDP**, **HTTP** or **HTTPS**. The default setting is **UDP**.

8 Select **OK** when completed to update the **External Controller** configuration. Select **Reset** to revert the WLAN Policy Security screen back to the last saved configuration.

6.1.2.8 TKIP-CCMP

Configuring WLAN Security

CCMP is a security standard used by the *Advanced Encryption Standard* (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a *Message Integrity Check* (MIC) using the proven *Cipher Block Chaining* (CBC) technique. Changing just one bit in a message produces a totally different result.

The encryption method is *Temporal Key Integrity Protocol* (TKIP). TKIP addresses WEP's weaknesses with a re-keying mechanism, a per-packet mixing function, a message integrity check and an extended initialization vector. However TKIP also has vulnerabilities.

To configure TKIP-CCMP encryption on a WLAN:

1 Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN or select an existing WLAN and **Edit** to modify its properties.

3 Select **Security**.

4 Select the **TKIP-CCMP** radio button from within the Select Encryption field.

The screen populates with the parameters required to define a WLAN's TKIP-CCMP configuration for the new or existing WLAN.

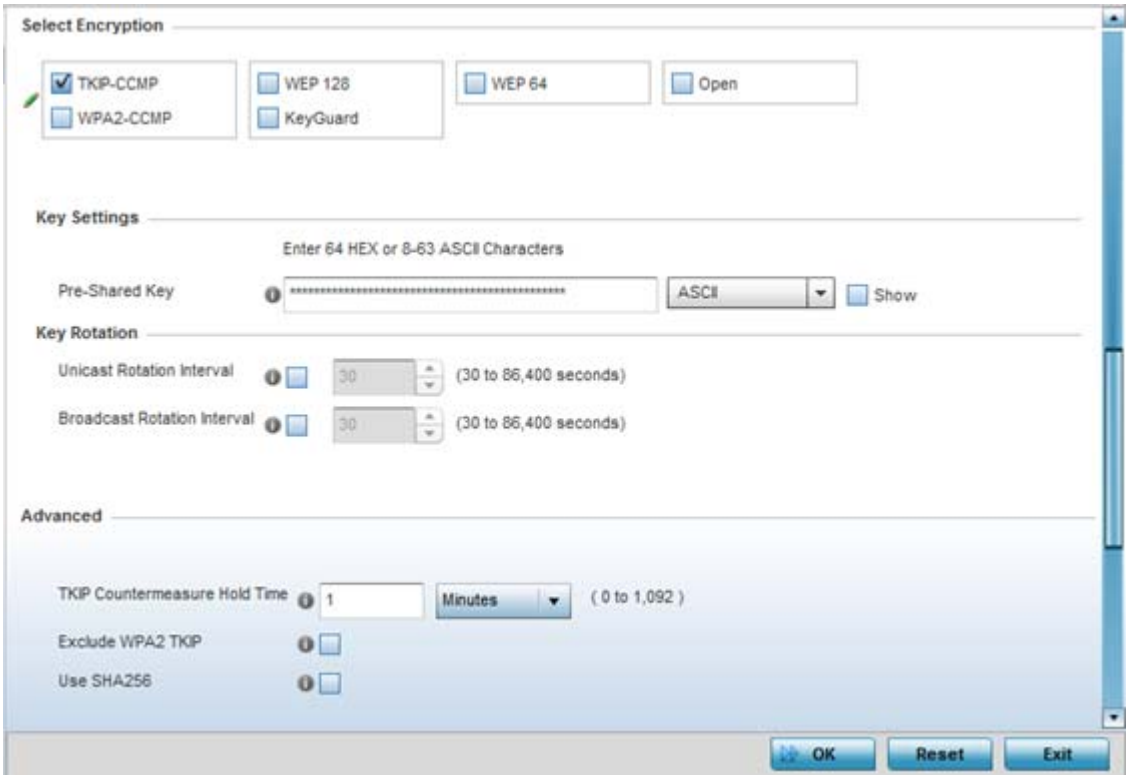


Figure 6-12 *TKIP-CCMP screen*

5 Define **Key Settings**.

Pre-Shared Key	Enter either an alphanumeric string of 8 to 63 ASCII characters or 64 HEX characters as the primary string both transmitting and receiving authenticators must share. The alphanumeric string allows character spaces. The string is converted into a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

6 Define **Key Rotation** values.

Unicast messages are addressed to a single device on the network. *Broadcast* messages are addressed to multiple devices. When using WPA2, a wireless client can use 2 keys, one unicast key, for its own traffic to and from an Access Point, and one broadcast key, the common key for all the clients in that subnet.

Rotating the keys is recommended the keys so a potential hacker would not have enough data using a single key to attack the deployed encryption scheme.

Unicast Rotation Interval	Define an interval for unicast key transmission in seconds (30 -86,400). Some clients have issues using unicast key rotation, so ensure you know which kind of clients are impacted before using unicast keys. This feature is disabled by default.
Broadcast Rotation Interval	When enabled, the key indices used for encrypting/decrypting broadcast traffic are alternatively rotated based on the defined interval. Define an interval for broadcast key transmission in seconds (30-86,400). Key rotation enhances the broadcast traffic security on the WLAN. This feature is disabled by default.

7 Set the following **Advanced** settings for the WPA/WPA2-TKIP encryption scheme

TKIP Countermeasure Hold Time	The TKIP countermeasure hold-time is the time during which the use of the WLAN is disabled if TKIP countermeasures have been invoked on the WLAN. Use the drop-down menu to define a value in either *Hours* (0-18), *Minutes* (0-1,093) or *Seconds* (0-65,535). The default setting is 1 second.
Exclude WPA2 TKIP	Select this option for an Access Point to advertise and enable support for only WPA-TKIP. This option can be used if certain older clients are not compatible with the newer WPA2-TKIP information elements. Enabling this option allows backwards compatibility for clients that support WPA-TKIP and WPA2-TKIP but do not support WPA2-CCMP. Enabling this feature is recommended if WPA-TKIP or WPA2-TKIP supported clients operate in a WLAN populated by WPA2-CCMP enabled clients. This feature is disabled by default.
Use SHA256	Select to enable use of the SHA-256 hash algorithms with WPA2. This is optional when using WPA2 without 802.11w Protected Management Frames (PMF) enabled. This is mandatory when PMF is enabled.

8 Select **OK** when completed to update the WLAN's TKIP-CCMP encryption configuration. Select **Reset** to revert the screen back to its last saved configuration.

6.1.2.8.1 TKIP-CCMP Deployment Considerations

Before defining a TKIP-CCMP supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- TKIP-CCMP should only be enabled for legacy device support when WPA2-CCMP support is not available.
- Though TKIP offers better security than WEP, it can be vulnerable to certain attacks.

- When both TKIP and CCMP are both enabled a mix of clients are allowed to associate with the WLAN. Some use TKIP, others use CCMP. Since broadcast traffic needs to be understood by all clients, the broadcast encryption type in this scenario is TKIP.

6.1.2.9 WPA2-CCMP

Configuring WLAN Security

WPA2 is a newer 802.11i standard that provides even stronger wireless security than *Wi-Fi Protected Access* (WPA) and WEP. CCMP is the security standard used by the *Advanced Encryption Standard* (AES). AES serves the same function TKIP does for WPA-TKIP. CCMP computes a *Message Integrity Check* (MIC) using the proven *Cipher Block Chaining* (CBC) technique. Changing just one bit in a message produces a totally different result.

WPA2/CCMP is based on the concept of a *Robust Security Network* (RSN), which defines a hierarchy of keys with a limited lifetime (similar to TKIP). Like TKIP, the keys the administrator provides are used to derive other keys. Messages are encrypted using a 128-bit secret key and a 128-bit block of data. The end result is an encryption scheme as secure as any the wireless controller provides for its associated clients.

To configure WPA2-CCMP encryption on a WLAN:

1 Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN or select an existing WLAN and choose **Edit** to modify the properties of an existing WLAN.

3 Select **Security**.

4 Select the **WPA2-CCMP** check box from within the select Select Encryption field.

The screen populates with the parameters required to define a WPA2-CCMP configuration for the new or existing WLAN.

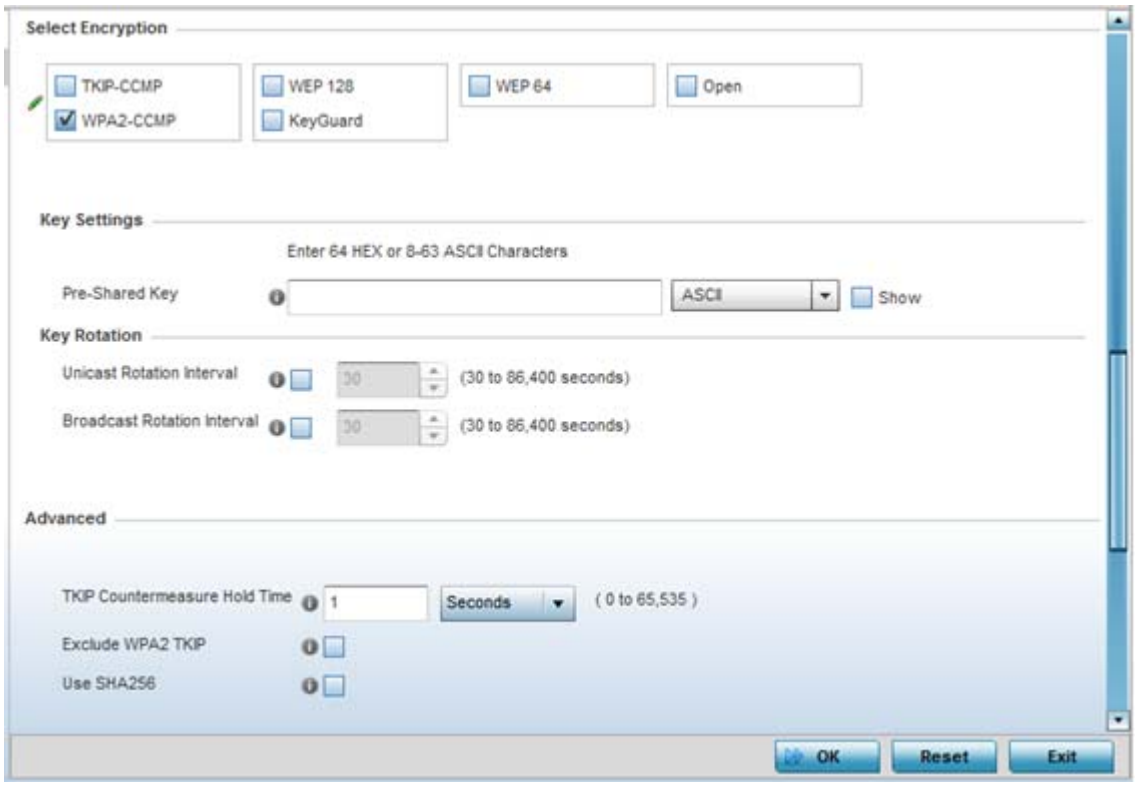


Figure 6-13 *WPA2-CCMP screen*

5 Define **Key Settings**.

Pre-Shared Key	Enter either an alphanumeric string of 8 to 63 ASCII characters or 64 HEX characters as the primary string both transmitting and receiving authenticators must share. The alphanumeric string allows character spaces. The string is converted to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

6 Define **Key Rotation** values.

Unicast messages are addressed to a single device on the network. *Broadcast* messages are addressed to multiple devices. When using WPA2-CCMP, a wireless client can use 2 keys: one unicast key, for its own traffic to and from an Access Point, and one broadcast key, the common key for all the clients in that subnet.

Rotating these keys is recommended so a potential hacker will not have enough data using a single key to attack the deployed encryption scheme.

Unicast Rotation Interval	Define an interval for unicast key transmission in seconds (30 -86,400). Some clients have issues using unicast key rotation, so ensure you know which clients are impacted before using unicast keys. This value is disabled by default.
Broadcast Rotation Interval	When enabled, the key indices used for encrypting/decrypting broadcast traffic are alternatively rotated based on the defined interval. Define an interval for broadcast key transmission in seconds (30-86,400). Key rotation enhances the broadcast traffic security on the WLAN. This value is disabled by default.

7 Set the following **Advanced** for the WPA2-CCMP encryption scheme.

TKIP Countermeasure Hold Time	The TKIP countermeasure hold-time is the time during which the use of the WLAN is disabled if TKIP countermeasures have been invoked on the WLAN. Use the drop-down menu to define a value in either *Hours* (0-18), *Minutes* (0-1,092) or *Seconds* (0-65,535). The default setting is 60 seconds.
Exclude WPA2-TKIP	Select this option for an Access Point to advertise and enable support for only WPA-TKIP. Select this option if certain older clients are not compatible with the newer WPA2-TKIP information elements. Enabling this option allows backwards compatibility for clients that support WPA-TKIP and WPA2-TKIP but do not support WPA2-CCMP. Consider enabling this feature if WPA-TKIP or WPA2-TKIP supported clients operate in a WLAN populated by WPA2-CCMP enabled clients. This feature is disabled by default.
Use SHA256	Select this option for an Access Point to advertise and enable support for only WPA-TKIP. Select this option if certain older clients are not compatible with the newer WPA2-TKIP information elements. Enabling this option allows backwards compatibility for clients that support WPA-TKIP and WPA2-TKIP but do not support WPA2-CCMP. Consider enabling this feature if WPA-TKIP or WPA2-TKIP supported clients operate in a WLAN populated by WPA2-CCMP enabled clients. This feature is disabled by default.

8 Select **OK** when completed to update the WLAN's WPA2-CCMP encryption configuration. Select **Reset** to revert back to its last saved configuration.

WPA2-CCMP Deployment Considerations

WPA2-CCMP

Before defining a WPA2-CCMP supported configuration on a wireless controller WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- WPA2-CCMP should be configured for all new (non visitor) WLANs requiring encryption, as it's supported by the majority of the hardware and client vendors using wireless networking equipment.
- WPA2-CCMP supersedes WPA-TKIP and implements all the mandatory elements of the 802.11i standard. WPA2-CCMP introduces a new AES-based algorithm called CCMP which replaces TKIP and WEP and is considered significantly more secure.

6.1.2.10 WEP 64

Configuring WLAN Security

Wired Equivalent Privacy (WEP) is a security protocol specified in the IEEE *Wireless Fidelity* (Wi -Fi) standard. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN.

WEP can be used with open, shared, MAC and 802.1 X EAP authentications. WEP is optimal for WLANs supporting legacy deployments when also used with 802.1X EAP authentication to provide user and device authentication and dynamic WEP key derivation and periodic key rotation. 802.1X provides authentication for devices and also reduces the risk of a single WEP key being deciphered. If 802.1X support is not available on the legacy device, MAC authentication should be enabled to provide device level authentication.

WEP 64 uses a 40 bit key concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. WEP 64 is a less robust encryption scheme than WEP 128 (containing a shorter WEP algorithm for a hacker to potentially duplicate), but networks that require more security are at risk from a WEP flaw. WEP is only recommended if there

are client devices incapable of using higher forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys.

To configure WEP 64 encryption on a WLAN:

1 Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN or select **Edit** to modify the properties of an existing WLAN.

3 Select **Security**.

4 Select the **WEP 64** check box from within the Select Encryption field.
The screen populates with the parameters required to define a WEP 64 configuration for the WLAN.

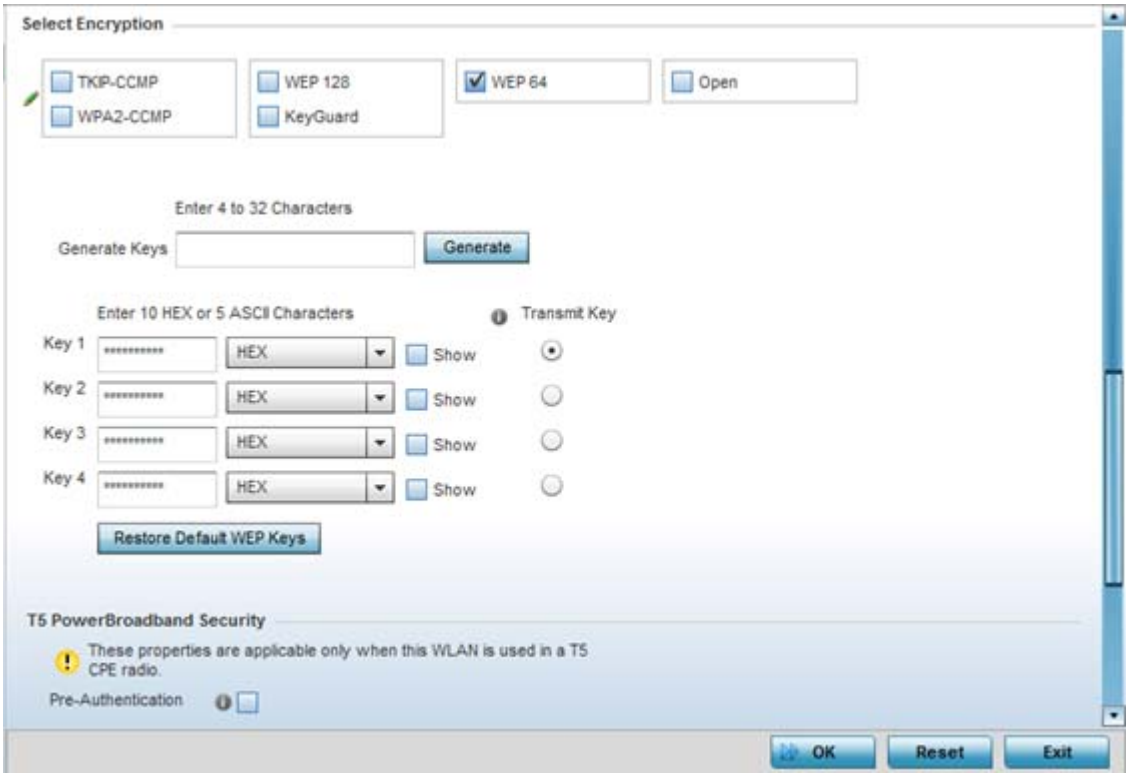


Figure 6-14 *WEP 64 screen*

5 Configure the following WEP 64 settings:

Generate Keys	Specify a 4 to 32 character Pass Key and click the *Generate* button. The pass key can be any alphanumeric string. Wireless devices and their connected clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without adapters need to use WEP keys manually configured as hexadecimal numbers.
Keys 1-4	Use the Key #1-4 fields to specify key numbers. For WEP 64 (40-bit key), the keys are 10 hexadecimal characters in length. Select one of these keys for default activation by clicking its radio button. Selecting *Show* displays a key in exposed plain text.
Restore Default WEP Keys	If you feel it necessary to restore the WEP algorithm back to its default settings, click the *Restore Default WEP Keys* button.

Default WEP 64 keys are as follows:

- Key 1 1011121314
- Key 2 2021222324
- Key 3 3031323334
- Key 4 4041424344

6 Select **OK** when completed to update the WLAN's WEP 64 encryption configuration. Select **Reset** to revert the screen back to its last saved configuration.

WEP 64 Deployment Considerations

Before defining a WEP 64 supported configuration on a wireless controller WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Additional layers of security (beyond WEP) should be enabled to minimize the likelihood of data loss and security breaches. WEP enabled WLANs should be mapped to an isolated VLAN with firewall policies restricting access to hosts and suspicious network applications.
- WEP enabled WLANs should only be permitted access to resources required by legacy devices.
- If WEP support is needed for WLAN legacy device support, 802.1X EAP authentication should be also configured in order for the WLAN to provide authentication and dynamic key derivation and rotation.

6.1.2.11 WEP 128

Configuring WLAN Security

Wired Equivalent Privacy (WEP) is a security protocol specified in the IEEE *Wireless Fidelity* (Wi -Fi) standard. WEP is designed to provide a WLAN with a level of security and privacy comparable to that of a wired LAN.

WEP can be used with open, shared, MAC and 802.1 X EAP authentications. WEP is optimal for WLANs supporting legacy deployments when also used with 802.1X EAP authentication to provide user and device authentication and dynamic WEP key derivation and periodic key rotation. 802.1X provides authentication for devices and also reduces the risk of a single WEP key being deciphered. If 802.1X support is not available on the legacy device, MAC authentication should be enabled to provide device level authentication.

WEP 128 uses a 104 bit key which is concatenated with a 24-bit initialization vector (IV) to form the RC4 traffic key. WEP may be all a small-business user needs for the simple encryption of wireless data. However, networks that require more security are at risk from a WEP flaw. WEP is only recommended if there are client devices incapable of using higher forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys.

WEP 128 provides a more robust encryption algorithm than WEP 64 by requiring a longer key length and pass key. Thus, making it harder to hack through the replication of WEP keys.

To configure WEP 128 encryption on a WLAN:

1 Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN or select **Edit** to modify the properties of an existing WLAN.

3 Select **Security**.

4 Select the **WEP 128** check box from within the Select Encryption field.

The screen populates with the parameters required to define a WEP 128 configuration for the WLAN.

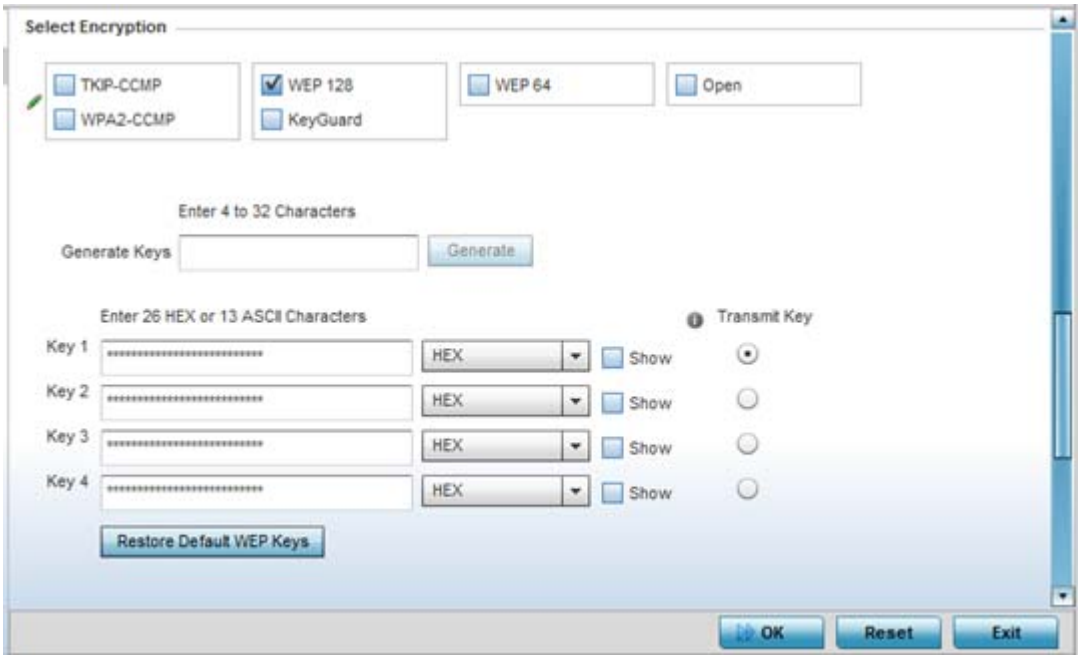


Figure 6-15 *WEP 128 screen*

5 Configure the following WEP 128 settings:

Generate Keys	Specify a 4 to 32 character Pass Key and click the *Generate* button. The pass key can be any alphanumeric string. Wireless devices and their connected clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without adapters need to use WEP keys manually configured as hexadecimal numbers.
Keys 1-4	Use the Key #1-4 areas to specify key numbers. For WEP 128 (104-bit key), the keys are 26 hexadecimal characters in length. Select one of these keys for default activation by clicking its radio button. Selecting *Show* displays a key in exposed plain text.
Restore Default WEP Keys	If you feel it necessary to restore the WEP algorithm back to its default settings, click the *Restore Default WEP Keys* button.

Default WEP 128 keys are as follows:

- Key 1 101112131415161718191A1B1C
- Key 2 202122232425262728292A2B2C
- Key 3 303132333435363738393A3B3C
- Key 4 404142434445464748494A4B4C

6 Select **OK** when completed to update the WLAN's WEP 128 encryption configuration. Select **Reset** to revert the screen back to its last saved configuration.

WEP 128 Deployment Considerations

WEP 128

Before defining a WEP 128 supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Additional layers of security (beyond WEP) should be enabled to minimize the likelihood of data loss and security breaches. WEP enabled WLANs should be mapped to an isolated VLAN with firewall policies restricting access to hosts and suspicious network applications.
- WEP enabled WLANs should only be permitted access to resources required by legacy devices.
- If WEP support is needed for WLAN legacy device support, 802.1X EAP authentication should be also configured in order for the WLAN to provide authentication and dynamic key derivation and rotation.

6.1.2.12 Keyguard

Configuring WLAN Security

Keyguard is a form of WEP, and could be all a small business needs for the simple encryption of wireless data.

KeyGuard is a proprietary encryption method, and an enhancement to WEP encryption, and was developed before the finalization of WPA-TKIP. The Keyguard encryption implementation is based on the IEEE Wi-Fi standard, 802.11i.

To configure Keyguard encryption on a WLAN:

1 Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN or select **Edit** to modify the properties of an WLAN.

3 Select **Security**.

4 Select the **Keyguard** check box from within the Select Encryption field.
The screen populates with the parameters required to define a KeyGuard configuration for the WLAN.

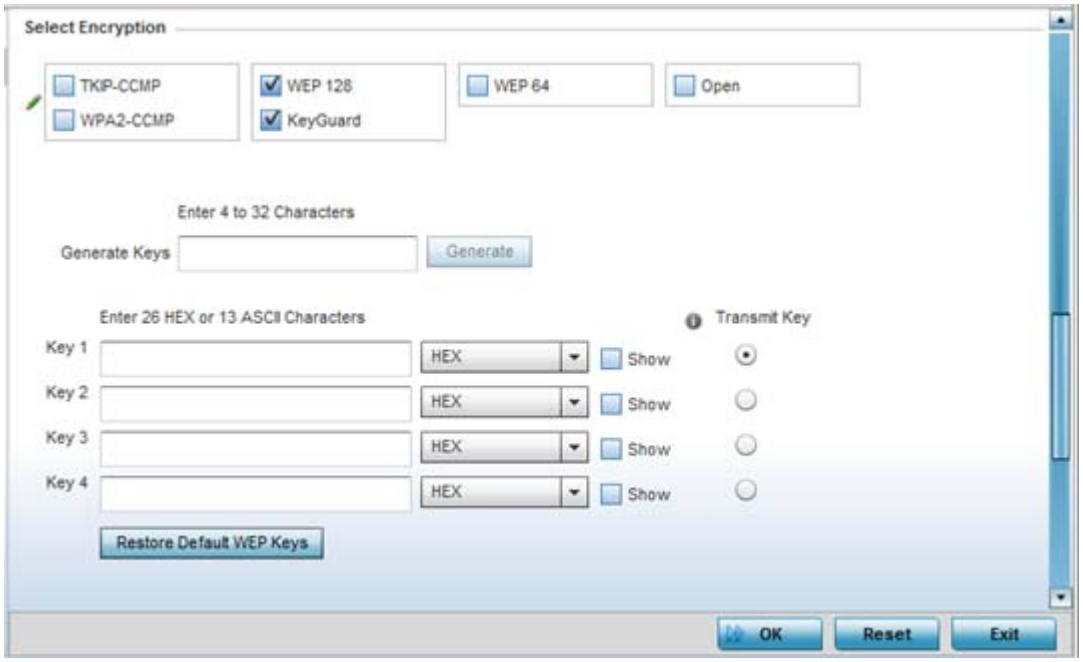


Figure 6-16 *WLAN KeyGuard Configuration screen*

5 Configure the following Keyguard settings:

Generate Keys	Specify a 4 to 32 character Pass Key and click the *Generate* button. The pass key can be any alphanumeric string. Clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without adapters need to use keys manually configured as hexadecimal numbers.

Keys 1-4	Use the Key #1-4 areas to specify key numbers. For Keyguard (104-bit key), the keys are 26 hexadecimal characters in length. Select one of these keys for default activation by clicking its radio button. Selecting *Show* displays a key in exposed plain text.
Restore Default WEP Keys	If you feel it necessary to restore the Keyguard algorithm back to its default settings, click the *Restore Default WEP Key*s button. This may be the case if the latest defined algorithm has been compromised and no longer provides its former measure of data security.

Default WEP Keyguard keys are as follows:

- Key 1 101112131415161718191A1B1C
- Key 2 202122232425262728292A2B2C
- Key 3 303132333435363738393A3B3C
- Key 4 404142434445464748494A4B4C

6 Select **OK** when completed to update the WLAN's Keyguard encryption configuration. Select **Reset** to revert the screen back to its last saved configuration.

KeyGuard Deployment Considerations

Keyguard

Before defining a Keyguard configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Authentication techniques can also be enabled on WLANs supporting other proprietary techniques, such as KeyGuard.
- A WLAN using KeyGuard to support legacy devices should also use largely limited to the support of just those legacy clients using KeyGuard.

6.1.2.13 T5 Controller Security

Configuring WLAN Security

A T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The *Customer Premises Equipment* (CPEs) are the T5 controller managed radio devices. These CPEs use *Digital Subscriber Line* (DSL) as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

To configure WLAN security settings for a T5 controller and its connected CPEs:

1 Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN or select **Edit** to modify the properties of an WLAN.

3 Select **Security**.

4 Refer to the **T5 PowerBroadband Security** field at the bottom of the screen.

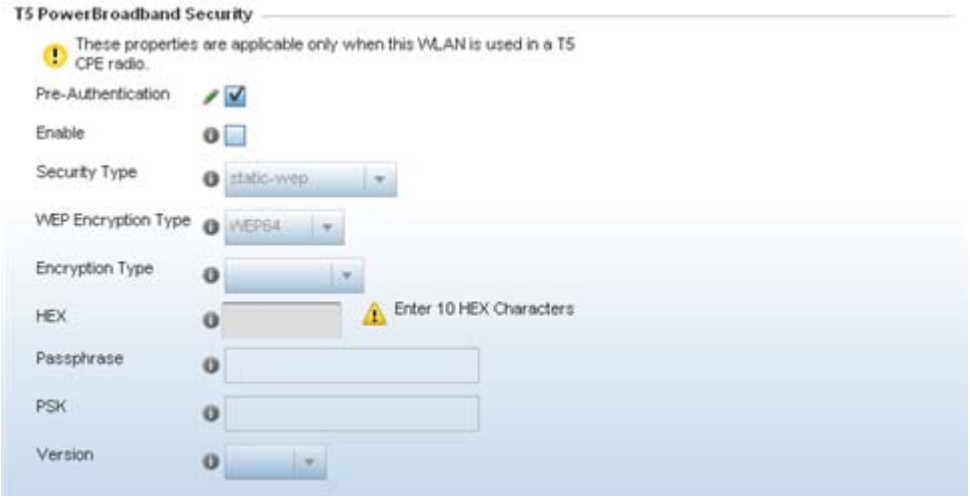


Figure 6-17 *T5 PowerBroadband Security screen*

5 Configure the following **T5 PowerBroadband Security** settings (available only when the WLAN supports T5 controllers and their connected CPEs radio devices):

Pre-Authentication	Select this option to invoke the use of pre-authentication 802.11i fast roaming. This setting is disabled by default.
Enable	Select this option to enable the *Security Type* and *WEP Encryptions Type* drop-down menus used to define and apply different encryption and authentication settings to the T5 WLAN security configuration.
Security Type	Use the drop-down menu to select the security type to apply to the WLAN. Options include *static-wep* (default), *wpa-enterprise* and *wpa-personal*.
WEP Encryption Type	If *static-wep* is selected as the Encryption Type, use this setting to apply either a WEP64 or WEP128 encryption algorithm to the T5 support WLAN configuration.
Encryption Type	If *wpa-enterprise* or *wpa-personal* are selected as the Encryption Type, use this setting to apply either a CCMP, TKIP or TKIP-CCMP encryption algorithm to the T5 controller WLAN security configuration.
HEX	If using *static-wep,* provide the 10-26 character Hex password used to derive the security key.
Passphrase	If using *static-wep,* enter either an alphanumeric string of 8 to 63 ASCII characters or 64 HEX characters as the primary string both transmitting and receiving authenticators must share. The alphanumeric string allows character spaces. The string is converted into a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.
PSK	Enter either an alphanumeric string as the primary string both transmitting and receiving authenticators must share. The alphanumeric string allows character spaces. The string is converted into a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.
Version	If *wpa-enterprise* or *wpa-personal* are selected as the Encryption Type, use this setting to apply a WPA or WPA2 encryption scheme to the T5 support WLAN configuration.

6 Select **OK** when completed to update the T5 PowerBroadband Security configuration. Select **Reset** to revert the screen back to its last saved configuration.

6.1.3 Configuring WLAN Firewall Support

- *Wireless LAN Policy*

A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms both blocking and permitting data traffic. For an overview of firewalls, see *Wireless Firewall on page 10-1*.

WLANs use firewalls like *Access Control Lists* (ACLs) to filter/mark packets based on the WLAN from which they arrive, as opposed to filtering packets on Layer 2 ports. An ACL contains an ordered list of *Access Control Entries* (ACEs). Each ACE specifies an action and a set of conditions (rules) a packet must satisfy to match the ACE. The order of conditions in the list is critical since filtering is stopped after the first match.

IPv4 and IPv6 based firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC.

Additionally, administrators can filter Layer 2 traffic on a physical Layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to WLAN packet traffic.

Keep in mind IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

To review access policies, create a new policy or edit the properties of an existing policy:

1 Select **Configuration** > **Wireless LANs** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create a new WLAN or **Edit** to modify the properties of an existing WLAN.

3 Select **Firewall** from the Wireless LAN Policy options.

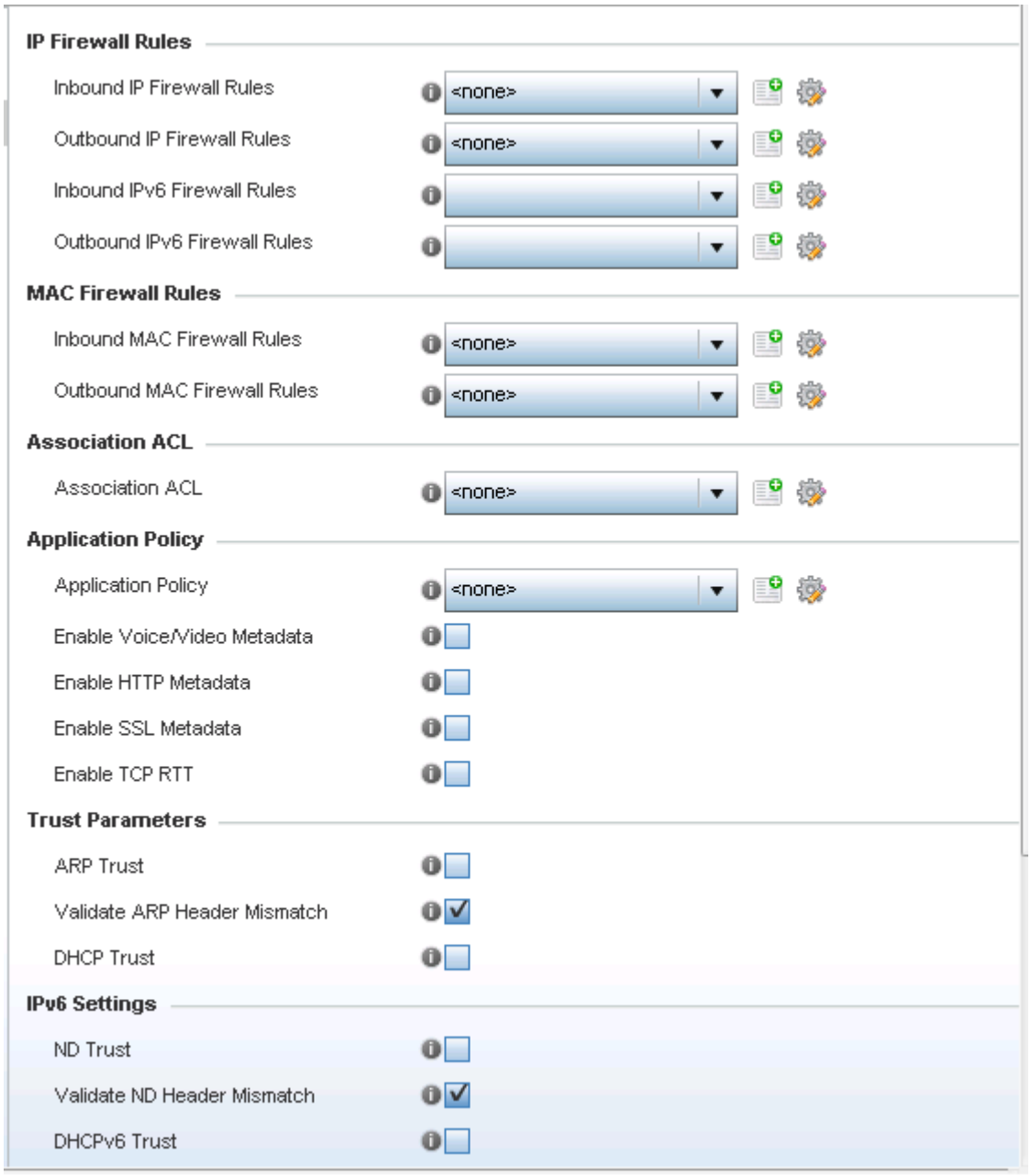


Figure 6-18 *WLAN Policy Firewall screen*

The screen displays editable fields for *IP Firewall Rules*, *MAC Firewall Rules*, *Trust Parameters, IPv6 Settings* and *Wireless Client Deny* limits.

Select an existing **Inbound IP Firewall Rule** and **Outbound IP Firewall Rule** using the drop-down menu. If no rules exist, select the **Create** icon to display a screen where Firewall rules can be created. Select the **Edit** icon to modify the configuration of a selected Firewall policy configuration.

4 If creating a new IP firewall rule, provide a name up to 32 characters.

5 Select the **Add** button.

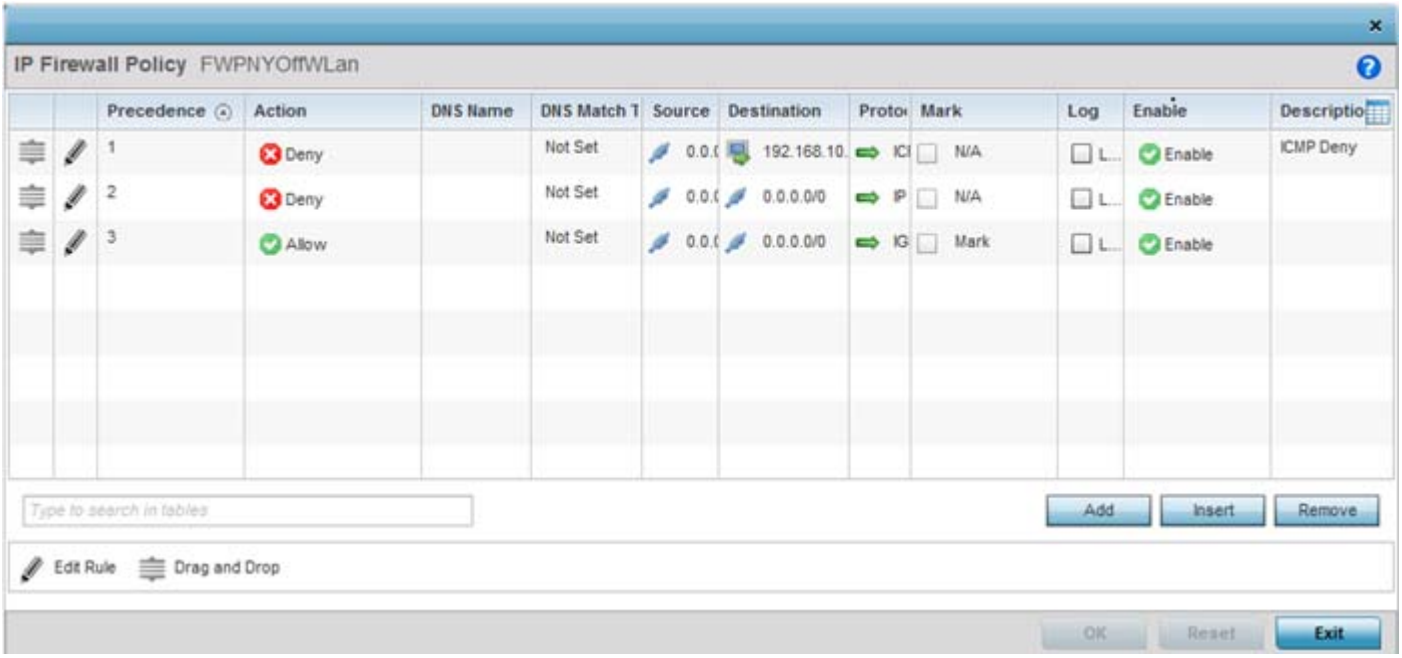


Figure 6-19 *IP Firewall Rules screen*

6 IP firewall rule configurations can either be modified as a collective group of variables or selected and updated individually as their filtering attributes require a more refined update.

a. Select the **Edit Rule** icon to the left of a particular IP firewall rule configuration to update its parameters collectively.

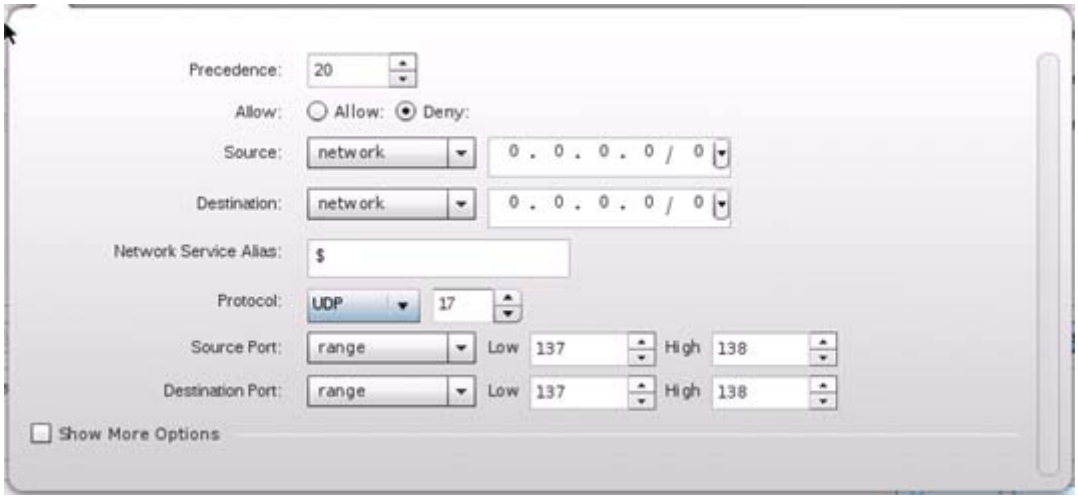


Figure 6-20 *IP Firewall Rules Add Criteria screen*

b. Click the icon within the **Description** column (top right-hand side of the screen) and select IP filter values as needed to add criteria into the configuration of the IP ACL.

Figure 6-21 *IP Firewall Rules Add Criteria screen*

NOTE: Only those selected IP ACL filter attributes display. Each value can have its current setting adjusted by selecting that IP ACL's column to display a pop-up to adjust that one value.

7 Define the following IP firewall rule settings as required:

Precedence	Specify or modify a precedence for this IP policy between 1-5000. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.
Action	Every IP Firewall rule is made up of matching criteria rules. The action defines the packet's disposition if it matches the specified criteria. The following actions are supported: *Deny* - Instructs the Firewall to restrict a packet from proceeding to its destination. *Allow* - Instructs the Firewall to allow a packet to proceed to its destination.
DNS Name	Specify the DNS Name which may be a full domain name, a portion of a domain name or a suffix. This name is used for the DNS Match Type criteria.
DNS Match Type	Specify the DNS matching criteria that the DNS Name can be matched against. This can be configured as an exact match for a DNS domain name, a suffix for the DNS name or a domain that contains a portion of the DNS name. If traffic matches the configured criteria in the DNS Match Type, that rule will be applied to the ACL.
Source	Select the source IP address or network group configuration used as basic matching criteria for this IP ACL rule.
Destination	Determine whether filtered packet destinations for this IP firewall rule do not require any classification (*any*), are designated as a set of configurations consisting of protocol and port mappings (an *alias*), set as a numeric IP address (*host*) or defined as *network* IP and mask. Selecting alias requires a destination network group alias be available or created.
Network Service Alias	The *service alias* is a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Set an alphanumeric service alias (beginning with a $) and include the protocol as relevant. Selecting either *tcp* or *udp* displays an additional set of specific TCP/UDP source and destinations port options.

Source Port	If using either *tcp* or *udp* as the protocol, define whether the source port for incoming IP ACL rule application is *any*, *equals* or an administrator defined *range*. If not using tcp or udp, this setting displays as N/A. This is the data local origination port designated by the administrator. Selecting *equals* invokes a spinner control for setting a single numeric port. Selecting *range* displays spinner controls for *Low* and *High* numeric range settings. A source port cannot be a destination port.
Destination Port	If using either *tcp* or *udp* as the protocol, define whether the destination port for outgoing IP ACL rule application is *any, equals* or an administrator defined *range*. If not using tcp or udp, this setting displays as N/A. This is the data destination virtual port designated by the administrator. Selecting *equals* invokes a spinner control for setting a single numeric port. Selecting *range* displays spinner controls for *Low* and *High* numeric range settings.
ICMP Type	Selecting *ICMP* as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. The *Internet Control Message Protocol* (ICMP) uses messages identified by numeric *type*. ICMP messages are used for packet flow control or generated in IP error responses. ICMP errors are directed to the source IP address of the originating packet. Assign an ICMP type from 1-10.
ICMP Code	Selecting *ICMP* as the protocol for the IP rule displays an additional set of ICMP specific options for ICMP type and code. Many ICMP types have a corresponding *code*, helpful for troubleshooting network issues (0 - *Net Unreachable,* 1 *Host Unreachable*, 2 *Protocol Unreachable* etc.).
Start VLAN	Select a Start VLAN icon within a table row to set (apply) a start VLAN range for this IP ACL filter. The Start VLAN represents the virtual LAN beginning numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply.
End VLAN	Select an End VLAN icon within a table row to set (apply) an end VLAN range for this IP ACL filter. The End VLAN represents the virtual LAN end numeric identifier arriving packets must adhere to in order to have the IP ACL rules apply.
Mark	Select an IP Firewall rule's *Mark* checkbox to enable or disable event marking and set the rule's 8021p or dscp level (from 0 - 7).
Log	Select an IP Firewall rule's *Log* checkbox to enable or disable event logging for this rule's usage.
Enable	Select an IP Firewall rule's *Enable* or *Disable* icon to determine this rule's inclusion with the IP firewall policy.
Description	Lists the administrator assigned description applied to the IP ACL rule. Select a description within the table to modify its character string as filtering changes warrant. Select the icon within the Description table header to launch a *Select Columns* screen used to add or remove IP ACL criteria from the table.

8 Select existing inbound and outbound **MAC Firewall Rules** using the drop-down menu. If no rules exist, select **Create** to display a screen where Firewall rules can be created. MAC firewall rules can also be applied to an EX3500 Ethernet PoE switch connected and utilized by a WiNG managed device.

9 Select the **+ Add Row** button.

10 Select the added row to expand it into configurable parameters.

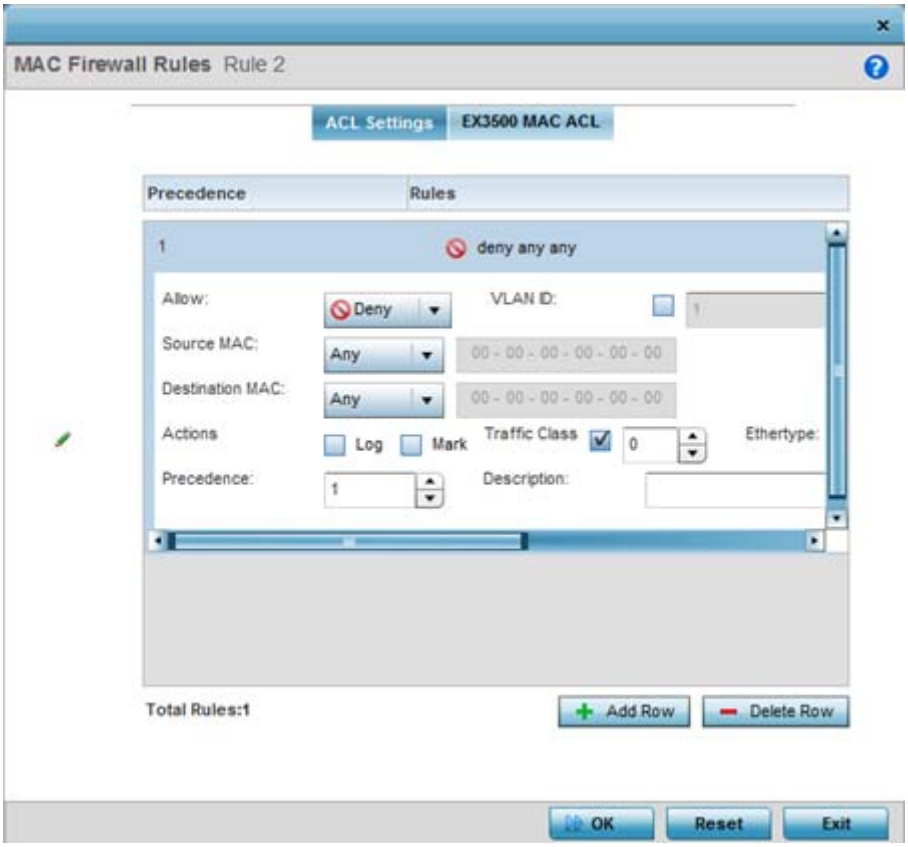


Figure 6-22 *MAC Firewall Rules screen*

11 Define the following parameters for either the inbound or outbound MAC Firewall Rules for either a WiNG managed device or an EX3500 switch connected to a WiNG managed device:

Allow	Every IP Firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported: *Deny* - Instructs the Firewall to deny a packet from proceeding to its destination. *Permit* - Instructs the Firewall to allow a packet to proceed to its destination.
VLAN ID	Enter a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the local RADIUS server). The VLAN ID can be between 1 - 4094. EX3500 PoE switches utilize a VLAN Mask option (from 0 - 4095) to mask the exposure of the VLAN ID.
Match 802.1P	Configures IP DSCP to 802.1p priority mapping for untagged frames. Use the spinner control to define a setting between 0-7.
Source and Destination MAC	Enter both *Source* and *Destination* MAC addresses. The wireless controller uses the source IP address, destination MAC address as basic matching criteria. Provide a subnet mask if using a mask.

Action	The following actions are supported: *Log* - Creates a log entry that a Firewall rule has allowed a packet to either be denied or permitted. *Mark* - Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit. *Mark, Log* - Conducts both mark and log functions.
Traffic Class	Sets an ACL traffic classification value for the packets identified by this inbound MAC filter. Traffic classifications are used for QoS purposes. Use the spinner to define a traffic class from 1- 10.
Ethertype	Use the drop-down menu to specify an Ethertype of either *ipv6*, *arp*, *wisp* or *monitor 8021q*. An EtherType is a two-octet field within an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet frame. EX3500 PoE switches utilize an Ether Mask option (from 0 - 65535) to mask the exposure of the Ethertype.
Precedence	Use the spinner control to specify a precedence for this MAC Firewall rule between 1-1500. Access policies with lower precedence are always applied first to packets.
Description	Provide an ACL setting description (up to 64 characters) for the rule to help differentiate the it from others with similar configurations.

12 If creating a new **Association ACL**, provide a name specific to its function. Avoid naming it after a WLAN it may support. The name cannot exceed 32 characters.

13 Assign an **Application Policy** to the firewall and set the following metadata extraction rules:

Application Policy	Use the drop-down menu to assign an application policy to the WLAN's firewall configuration. When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that specific application. An application policy defines the rules or actions executed on recognized HTTP, SSL and voice/video applications. For more information, refer to *Application Policy on page 7-54*.
Voice/Video Metadata	Select this option to enable the extraction of voice and video metadata flows. When enabled, administrators can track voice and video calls by extracting parameters (packets transferred and lost, jitter, audio codec and application name). Most Enterprise VoIP applications like facetime, skype for business and VoIP terminals can be monitored for call quality and visualized on the NSight dashboard in manner similar to HTTP and SSL. Call quality and metrics can only be determined from calls established unencrypted. This setting is disabled by default.
HTTP Metadata	Select this option to enable the extraction of HTTP flows. When enabled, administrators can track HTTP Websites accessed by both internal and guest clients and visualize HTTP data usage, hits, active time and total clients on the NSight application's dashboard. This setting is disabled by default.
SSL Metadata	Select this option to enable the extraction of SSL flows. When enabled, administrators can track SSL Websites accessed by both internal and guest clients and visualize SSL data usage, hits, active time and total clients on the NSight application's dashboard.This setting is disabled by default.

Enable TCP RTT	Select this option to enable the extraction of *Round Trip Time* (RTT) from *Transmission Control Protocol (TCP)* flows. When enabled, the RTT information from TCP flows detected on the VLAN interface associated with the WLAN is extracted and forwarded to the NSight server by Access Points. However, this TCP-RTT metadata is viewable only on the NSight dashboard. Therefore, ensure the NSight server is up, an NSight policy (pointing to the NSight server) is applied on the Access Point's RF Domain, and NSight analytics data collection is enabled. This setting is disabled by default.

14 Set the following **Trust Parameters**:

ARP Trust	Select the check box to enable ARP Trust on this WLAN. ARP packets received on this WLAN are considered trusted and information from these packets is used to identify rogue devices within the network. This setting is disabled by default.
Validate ARP Header Mismatch	Select this option to verify the mismatch for source MAC in the ARP and Ethernet headers. By default, mismatch verification is enabled.
DHCP Trust	Select the check box to enable DHCP trust on this WLAN. This setting is disabled by default.

15 Set the following **IPv6 Settings**:

ND Trust	Select this option to enable the trust of neighbor discovery requests on an IPv6 supported firewall on this WLAN. This setting is disabled by default.
Validate ND Header Mismatch	Select this option to enable a mismatch check for the source MAC within the ND header and Link Layer Option. This setting is enabled by default.
DHCPv6 Trust	Select this option to enable the trust all DHCPv6 responses on this WLAN's firewall. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is disabled by default.
RA Guard	Select this option to enable router advertisements or ICMPv6 redirects on this WLAN's firewall. This setting is disabled by default.

16 Set the following **Wireless Client Deny** configuration:

Wireless Client Denied Traffic Threshold	If enabled, any associated client which exceeds the thresholds configured for storm traffic is either deauthenticated or blacklisted depending on the selected action. The threshold range is 1-1000000 packets per second. This feature is disabled by default.
Action	If enabling a wireless client threshold, use the drop-down menu to determine whether clients are deauthenticated when the threshold is exceeded or blacklisted from connectivity for a user defined interval. Selecting *None* applies no consequence to an exceeded threshold.
Blacklist Duration	Select the check box and define a setting between 0 - 86,400 seconds. Once the blacklist duration has been exceeded, offending clients can reauthenticate once again.

17 Set a **Firewall Session Hold Time** in either *Seconds* (1 - 300) or *Minutes* (1 - 5). This is the hold time for caching user credentials and firewall state information when a client roams. The default setting is 30 seconds.

18 Select **OK** when completed to update this WLAN's Firewall settings. Select **Reset** to revert the screen back to its last saved configuration.

WLAN Firewall Deployment Considerations

Before defining an access control configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC ACL to the interface.

6.1.4 Configuring Client Settings

Wireless LAN Policy

Each WLAN can maintain its own unique client support configuration. These include wireless client inactivity timeouts and broadcast settings.

1 Select **Configuration** > **Wireless** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN, or select and existing WLAN and **Edit** to modify its properties.

3 Select the **Client Settings** tab.

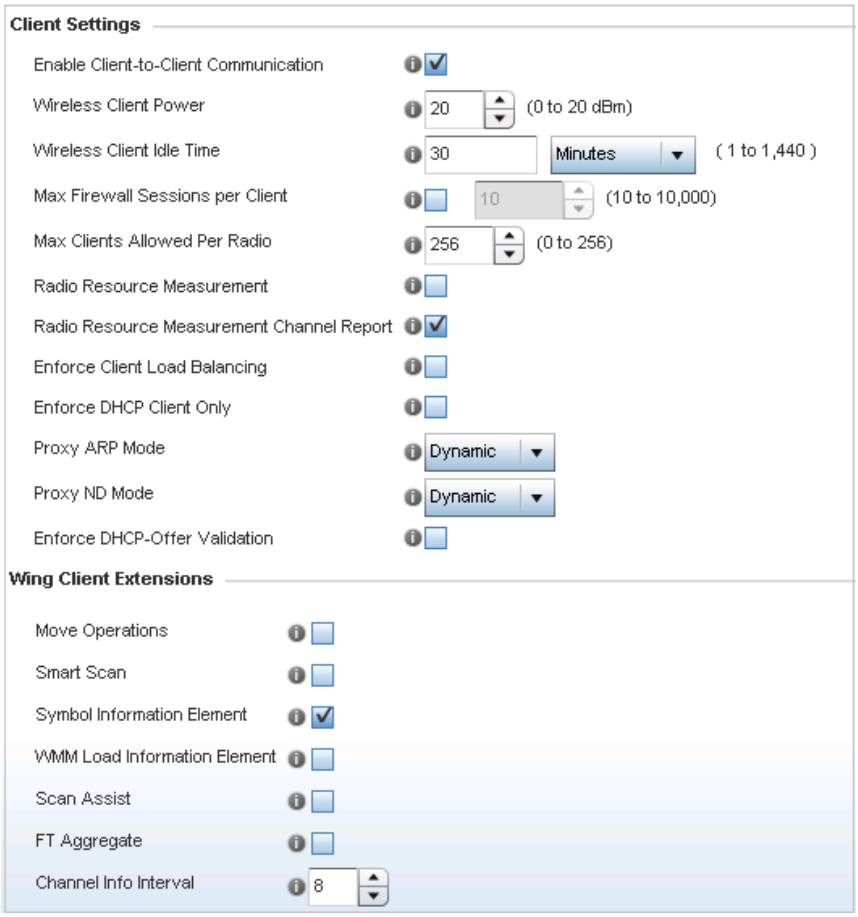


Figure 6-23 *WLAN Policy Client Settings screen*

4 Define the following **Client Settings** for the WLAN:

Enable Client-to-Client Communication	Select this option to enable client to client communication within this WLAN. The default is enabled, meaning clients are allowed to exchange packets with other clients. It does not necessarily prevent clients on other WLANs from sending packets to this WLAN, but as long as this setting also disabled on that WLAN, clients are not permitted to interoperate.
Wireless Client Power	Use this parameter to set the maximum transmit power (between 0 - 20 dBm) communicated to wireless clients for transmission within the network. The default value is 20 dBm.
Wireless Client Idle Time	Set the maximum amount of time wireless clients are allowed to be idle within this WLAN. Set the idle time in either *Seconds* (60 - 86,400), *Minutes* (1 - 1,440), *Hours* (1 - 24) or *Days* (1). When this setting is exceeded, the client is no longer able to access resources and must re-authenticate. The default value is 1,800 seconds.
Max Firewall Sessions per Client	Select this option to set the maximum amount of sessions (between 10 - 10,000) clients within the network over the Firewall. When enabled, this parameter limits the number of simultaneous sessions allowed by the Firewall per wireless client. This feature is disabled by default.
Max Clients Allowed Per Radio	Use the spinner control to set the maximum number of clients (from 0 - 256) allowed to associate to each radio within this WLAN. The default setting is 256.
Radio Resource Measurement	Select this option to enable radio resource measurement capabilities (IEEE 802.11k) on this WLAN. 802.11k improves how traffic is distributed. In a WLAN, each device normally connects to an Access Point with the strongest signal. Depending on the number and locations of the clients, this arrangement can lead to excessive demand on one Access Point and underutilization others, resulting in degradation of overall network performance. With 802.11k, if the Access Point with the strongest signal is loaded to its capacity, a client connects to a underutilized Access Point. Even if the signal is weaker, the overall throughput is greater since it's an efficient use of the network's resources. This setting is disabled by default.
Radio Resource Measurement Channel Report	Select this option to enable radio resource measurement channel reporting (IEEE 802.11k) on this WLAN. This setting is disabled by default.
Enforce Client Load Balancing	Select the check box to distribute clients evenly amongst associated Access Point radios. This feature is disabled by default. Loads are balanced by ignoring association and probe requests. Probe and association requests are not responded to, forcing a client to associate with another Access Point radio.
Enforce DHCP Client Only	Select the check box to enforce that the firewall only allows packets from clients if they used DHCP to obtain an IP address, disallowing static IP addresses. This feature is disabled by default.
Proxy ARP Mode	Use the drop-down menu to define the proxy ARP mode as either *Strict* or *Dynamic*. Proxy ARP is the technique used to answer ARP requests intended for another system. By faking its identity, the Access Point accepts responsibility for routing packets to the actual destination. Dynamic is the default value.

Proxy ND Mode	Use the drop-down menu to define the proxy *neighbor discovery* (ND) mode for WLAN member clients as either *Strict* or *Dynamic*. ND Proxy is used in IPv6 to provide reachability by allowing the a client to act as proxy. Proxy certificate signing can be done either dynamically (requiring exchanges of identity and authorization information) or statically when the network topology is defined. Dynamic is the default value.
Enforce DHCP-Offer Validation	Select the check box to enforce DHCP offer validation. The default setting is disabled.

5 Define the following **Wing Client Extensions** to potentially increase client roaming reliability and handshake speed:

Move Operations	Select the check box to enable the use of *Hyper-Fast Secure Roaming* (HFSR) for clients utilizing this WLAN. This feature applies only to certain client devices. This feature is disabled by default.
Smart Scan	Enable smart scan to adjust clients channel scans to a few channels as opposed to all available channels. This feature is disabled by default.
Symbol Information Element	Select the check box to support the Symbol Information Element with legacy Symbol Technology clients, thus making them optimally interoperable with the latest Extreme Networks Access Points. The default setting is enabled.
WMM Load Information Element	Select the check box to support a WMM Load Information Element in radio transmissions with legacy clients. The default setting is disabled.
Scan Assist	Enable scan assist to achieve faster roams on DFS channels by eliminating passive scans. Clients would get channel information directly from possible roam candidates. This setting is disabled by default.
FT Aggregate	Enable *fast transition* (FT) aggregate to increase roaming speed by eliminating separate key exchange handshake frames with potential roam candidates. Enable fast transition to complete an initial FT over DS handshake with multiple roam candidates (up to 6) at once, eliminating the need to send separate FT over DS handshakes to each roam candidate. This setting is disabled by default.
Channel Info Interval	Configure the channel information interval to periodically retrieve channel information directly from potential roam candidates without making a scan assist request.

6 Define the following **Coverage Hole Detection** settings to determine how detected coverage holes are managed:

Enable	Enable this setting to inform an Access Point when it experiences a coverage hole (area of poor wireless coverage). This setting is disabled by default.
Use 11k Clients	Optionally enable this setting to also use 802.11k-only-capable clients to detect coverage holes. This is a reduced set of coverage hole detection capabilities (only standard 11k messages and behaviors). This setting is disabled by default.
Threshold	Use the spinner control to set the Access Point signal strength (as seen by the client) below which a coverage hole incident is reported. The threshold can be set from -80 to -60.

Offset	Use the spinner control to set the offset added to the threshold to obtain the Access Point signal strength (as seen by the client) considered adequate. The offset can be set from 5 to 20.

7 Set the following **AP Attributes Information**:

Enable	Select this option to include the AP-Attributes information element in the beacon. The information element helps clients recognize which wing-extensions are supported by the AP. This setting is enabled by default.
Include Hostname	Select this option to include the AP's hostname in the AP-Attributes information element. This setting is disabled by default.

8 Define the following **Timeout Settings** for the WLAN:

Credential Cache Timeout	Set a timeout period for the credential cache in *Days*, *Hours*, *Minutes* or *Seconds*.
VLAN Cache Timeout	Set a timeout period for the VLAN cache in *Days*, *Hours*, *Minutes* or *Seconds*.

9 Select **Controller Assisted Mobility,** within the **Mobility** field, to use a controller or service platform's mobility database to assist in roaming between RF Domains. This feature is disabled by default.

10 Use the **Device ID** settings, within the **OpenDNS** field, to specify a 16 character maximum OpenDNS device ID forwarded in a DNS query. OpenDNS extends DNS by adding additional features such as misspelling correction, phishing protection, and optional content filtering.

11 Select **Client Isolation**, within the **T5 PowerBroadband Client Settings** field, to disallow clients connecting to the WLAN to communicate with one another. This setting applies exclusively to CPE devices managed by a T5 controller and is disabled by default.

Use the **Inactivity Time Out** field to define the inactivity timeout specific to T5 clients. Set the maximum amount of time T5 clients are allowed to be idle within this WLAN. Set the idle time in either Seconds (60 - 86,400), Minutes (1 - 1,440), Hours (0 - 24) or Days (0 - 1). When this setting is exceeded, the client is no longer able to access resources and must reauthenticate. The default value is 1,800 seconds.

A T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices. The *Customer Premises Equipment* (CPEs) are the T5 controller managed radio devices. These CPEs use a *Digital Subscriber Line* (DSL) as their high speed Internet access mechanism using the CPE's physical wallplate connection and phone jack.

12 Select **OK** when completed to update the WLAN's client setting configuration. Select **Reset** to revert the screen back to the last saved configuration.

6.1.4.1 WLAN Client Setting Deployment Considerations

Configuring Client Settings

Before defining a WLAN's client settings, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Clients on the same WLAN associated with an AAP can communicate locally at the AP Level without going through the controller or service platform. If this is undesirable, an Access Point's Client-to-Client Communication option should be disabled.
- When the wireless client idle time setting is exceeded, the client is no longer able to access WLAN resources and must re-authenticate. The default value is 1,800 seconds.

6.1.5 Configuring WLAN Accounting Settings

Accounting is the method of collecting and sending security server information for billing, auditing, and reporting user data; such as start and stop times, executed commands (such as PPP), number of packets and number of bytes. Accounting enables wireless network administrators to track the services users are accessing and the network resources they are consuming. When accounting is enabled, the network access server reports and logs user activity to a RADIUS security server in the form of accounting records. Each accounting record is comprised of AV pairs and is stored on a local access control server. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA.

Accounting can be enabled and applied to WLANs, to uniquely log accounting events specific to the WLAN. Accounting logs contain information about the use of remote access services by users. This information is of great assistance in partitioning local versus remote users and how to best accommodate each. Remote user information can be archived to an external location for periodic network and user permission administration.

To configure WLAN accounting settings:

1 Select **Configuration** > **Wireless LANs** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN or select **Edit** to modify the properties of an existing WLAN.

3 Select **Accounting**.

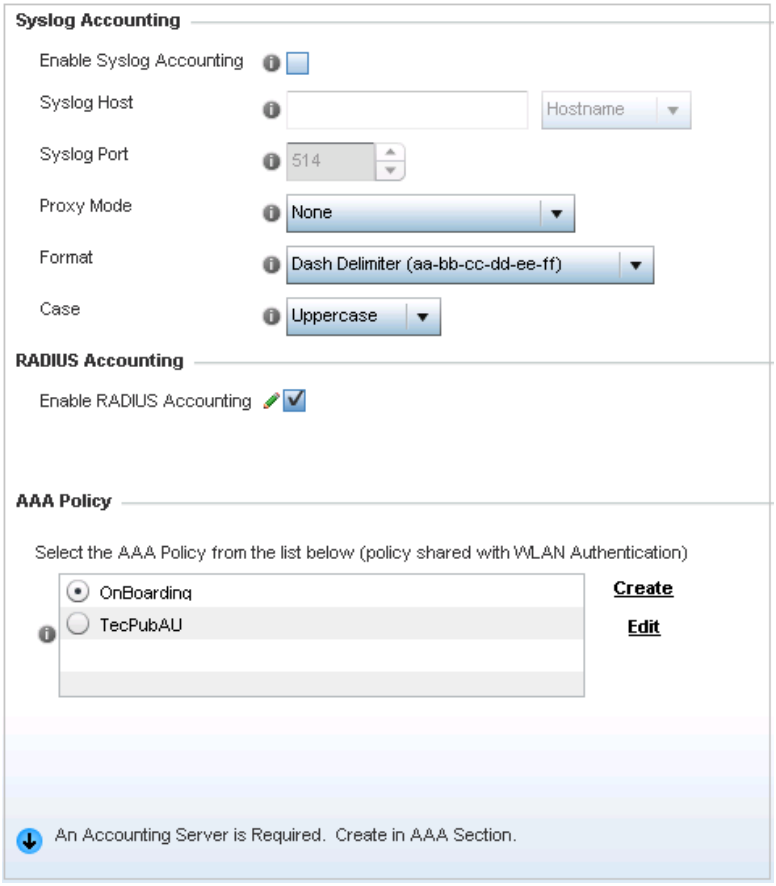


Figure 6-24 *WLAN Policy Accounting screen*

4 Set the following **System Log Accounting** information:

Enable Syslog Accounting	Use this option to generate accounting records in standard syslog format (RFC 3164). The feature is disabled by default.
Syslog Host	Specify the IP address or hostname of the external syslog host where accounting records are routed. Hostnames cannot include an underscore character.
Syslog Port	Use the spinner control to set the destination UDP port number of the external syslog host where the accounting records are routed.
Proxy Mode	If a proxy is needed to connect to the syslog server choose a proxy mode of *Through RF Domain Manager* or *Through Wireless Controller.* If no proxy is needed, select *None*.
Format	Specify the delimiter format for the MAC address to be packed in the syslog request. Available formats are No Delimiter (aabbccddeeff), Colon Delimiter (aa:bb:cc:dd:ee:ff), Dash Delimiter (aa-bb-cc-dd-ee-ff), Dot Delimiter (aabb.ccdd.eeff) and Middle Dash Delimiter (aabbcc-ddeeff).
Case	Specify to send the MAC addresses in either Uppercase or Lowercase for syslog requests.

5 Select the **Enable RADIUS Accounting** check box to use an external RADIUS resource for AAA accounting. When the check box is selected, a **AAA Policy** field displays. Either use the default AAA policy with the WLAN, or select **Create** to define a new AAA configuration that can be applied to the WLAN. This setting is disabled by default.

6 Select **OK** when completed to update this WLAN's accounting settings. Select **Reset** to revert the screen to its last saved configuration.

6.1.5.1 *Accounting Deployment Considerations*

Before defining a WLAN AAA configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- When using RADIUS authentication, the WAN port round trip delay should not exceed 150ms. Excessive delay over a WAN can cause authentication and roaming issues. When excessive delays exists, a distributed RADIUS service should be used.
- Authorization policies should be implemented when users need to be restricted to specific WLANs, or time and date restrictions need to be applied.
- Authorization policies can also apply bandwidth restrictions and assign Firewall policies to users and devices.

6.1.6 Configuring WLAN Service Monitoring Settings

Wireless LAN Policy

Service Monitoring is a mechanism for administrating external AAA server, captive portal server, Access Point adoption, and DHCP server activity for WLANs. Service monitoring enables an administrator to better notify users of a service's availability and make resource substitutions. Service monitoring can be enabled and applied to log activity as needed for specific WLANs.

External services can be rendered unavailable due to any of the following instances:

- When the RADIUS authentication server becomes unavailable. The RADIUS server could be local or external to the controller, service platform or Access Point.

- When an externally hosted captive portal is unavailable (for any reason)
- If an Access Point's connected controller or service platform becomes unavailable
- When a monitored DHCP server resource becomes unavailable

To configure WLAN service monitoring:

1 Select **Configuration** > **Wireless LANs** > **Wireless LAN Policy** to display a high-level display of the existing WLANs.

2 Select the **Add** button to create an additional WLAN or select **Edit** to modify the properties of an existing WLAN.

3 Select **Service Monitoring**.

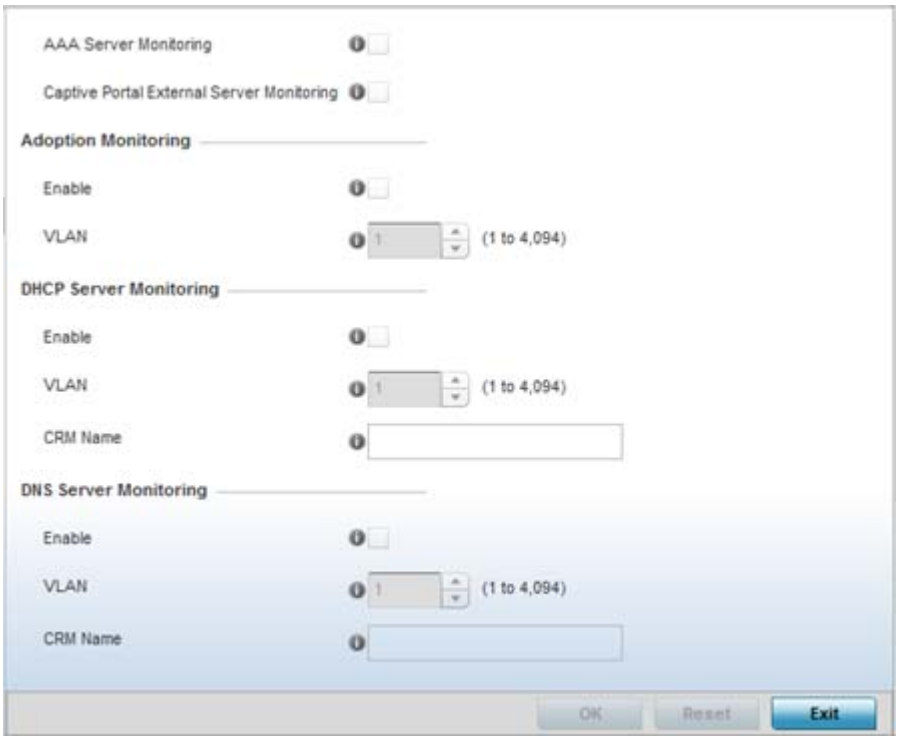


Figure 6-25 *WLAN Policy Service Monitoring screen*

4 Select the **AAA Server monitoring** option to monitor a dedicated external RADIUS server and ensure its adoption resource availability. This setting is disabled by default.

5 Select the **Captive Portal External Server monitoring** option to monitor externally hosted captive portal activity, and temporary and restrictive user access to the controller or service platform managed network. This setting is disabled by default.

6 Refer to the **Adoption Monitoring** field to set the WLAN's adoption service monitoring configuration.

Enable	Enable adoption monitoring to check Access Point adoptions to the controller or service platform. When the connection is lost, captive portal users are migrated to a defined VLAN. This feature is disabled by default, so it must be enabled to monitor WLAN specific adoption data.
VLAN	Select the VLAN users are migrated to when an Access Point's connection to its adopting controller or service platform is lost. The available range is from 1 - 4,094.

7 Refer to the **DHCP Server Monitoring** field to set the WLAN's adoption service monitoring configuration.

Enable	Select enable to monitor activity over the defined DHCP Server. When the connection to the DHCP server is lost, captive portal users are automatically migrated a defined VLAN. The feature is disabled by default.
VLAN	Select the VLAN users are migrated to when the defined DHCP server resource becomes unavailable. The available range is from 1 - 4,094.
CRM Name	Enter the DHCP server to monitor for availability. When this DHCP server resource becomes unavailable, the device falls back to defined VLAN. This VLAN has a DHCP server configured that provides a pool of IP addresses and with a lease time less than the main DHCP server.

8 Refer to the **DNS Server Monitoring** field to set the WLAN's DNS service monitoring configuration.

Enable	Select enable to monitor activity over the defined DNS Server. When the connection to the DNS server is lost, captive portal users are automatically migrated a defined VLAN. The feature is disabled by default.
VLAN	Select the VLAN users are migrated to when the defined DNS server resource becomes unavailable. The available range is from 1 - 4,094.
CRM Name	Enter the DNS server to monitor for availability. When this DNS server resource becomes unavailable, the device falls back to defined VLAN. This VLAN has a DNS server configured that provides DNS address resolution till the main DNS server becomes available.

9 Select **OK** when completed to update this WLAN's service monitor settings. Select **Reset** to revert the screen back to its last saved configuration.

6.1.7 Configuring Client Load Balancing Settings

Wireless LAN Policy

To configure WLAN client load balance settings:

1 Select **Configuration** > **Wireless LANs** > **Wireless LAN Policy** to display a high-level display of the existing WLANs.

2 Select the **Add** button to create an additional WLAN or select **Edit** to modify the properties of an existing wireless controller WLAN.

3 Select **Client Load Balancing**.

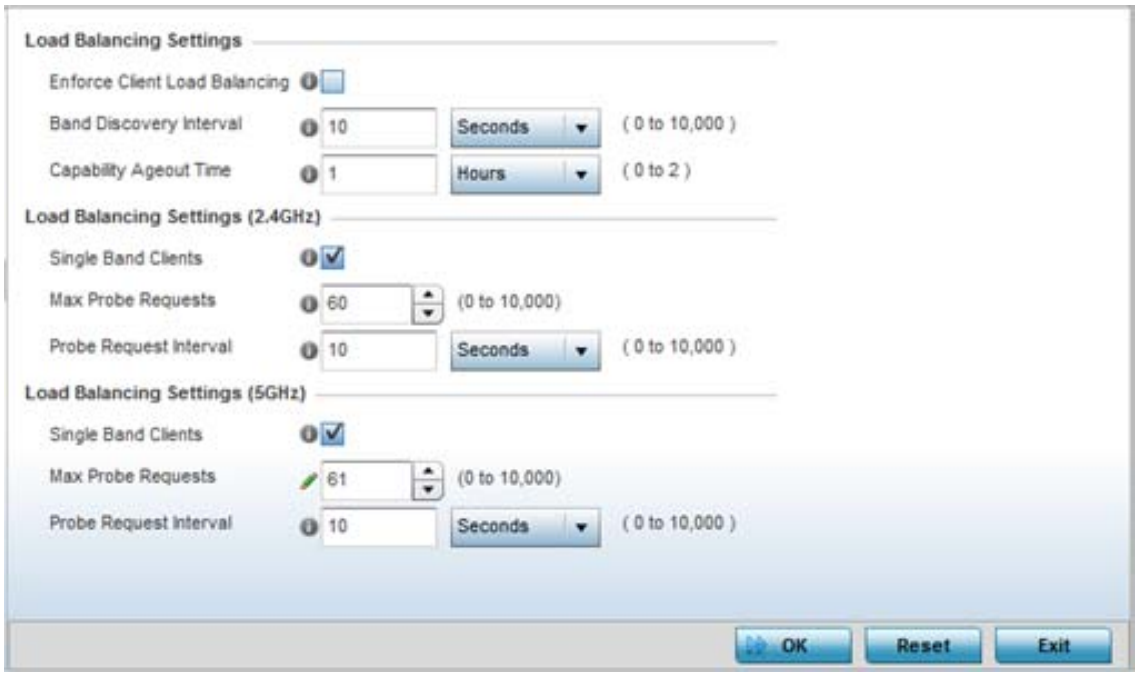


Figure 6-26 *WLAN Policy Client Load Balancing screen*

4 Refer to the **Load Balancing Settings** section to configure load balancing for the WLAN.

Enforce Client Load Balancing	Select this option to enforce a client load balance distribution on this WLAN's Access Point radios. AP6522, AP6532, AP6562, AP7161, AP81XX and AP8232 models can support 256 clients per Access Point. AP6521 model can support up to 128 clients per Access Point. Loads are balanced by ignoring association and probe requests. Probe and association requests are not responded to, forcing a client to associate with another Access Point radio.This setting is disabled by default.
Band Discovery Interval	Enter a value (from 0 - 10,000 seconds) to set the interval dedicated to discover a client's radio band capability before its Access Point radio association. The default setting is 24 seconds.
Capability Ageout Time	Define a value in either *Seconds* (0 - 10,000), *Minutes* (0 -166) or *Hours* (0 -2) to ageout a client's capabilities from the internal table. The default is 24 seconds.

5 Refer to the **Load Balancing Settings (2.4GHz)** section to configure load balancing for the 2.4 GHz WLAN.

Single Band Clients	Select this option to enable association for single band clients on the 2.4GHz frequency, even if load balancing is available. This setting is enabled by default.
Max Probe Requests	Enter a value from 0 - 10,000 for the maximum number of probe requests for clients using the 2.4GHz frequency. The default value is 60.
Probe Request Interval	Enter a value in seconds between 0 - 10,000 to configure the interval for client probe requests beyond which it is allowed to associate for clients on the 2.4GHz network. The default is 10 seconds.

6 Refer to the **Load Balancing Settings (5GHz)** section to configure load balancing for the 5 GHz WLAN.

Single Band Clients	Select this option to enable the association of single band clients on 5GHz, even if load balancing is available. This setting is enabled by default.
Max Probe Requests	Enter a value from 0 - 10,000 for the maximum number of probe requests for clients using 5GHz. The default value is 60.
Probe Request Interval	Enter a value in seconds from 0 - 10,000 to configure the interval for client probe requests. When exceeded, clients can associate using 5GHz. The default setting is 10 seconds.

7 Select **OK** when completed to update this WLAN's advanced settings. Select **Reset** to revert the screen back to its last saved configuration.

6.1.8 Configuring Advanced WLAN Settings

Wireless LAN Policy

To configure advanced settings on a WLAN:

1 Select **Configuration** > **Wireless LANs** > **Wireless LAN Policy** to display available WLANs.

2 Select the **Add** button to create an additional WLAN or select **Edit** to modify the properties of an existing WLAN.

3 Select **Advanced**.

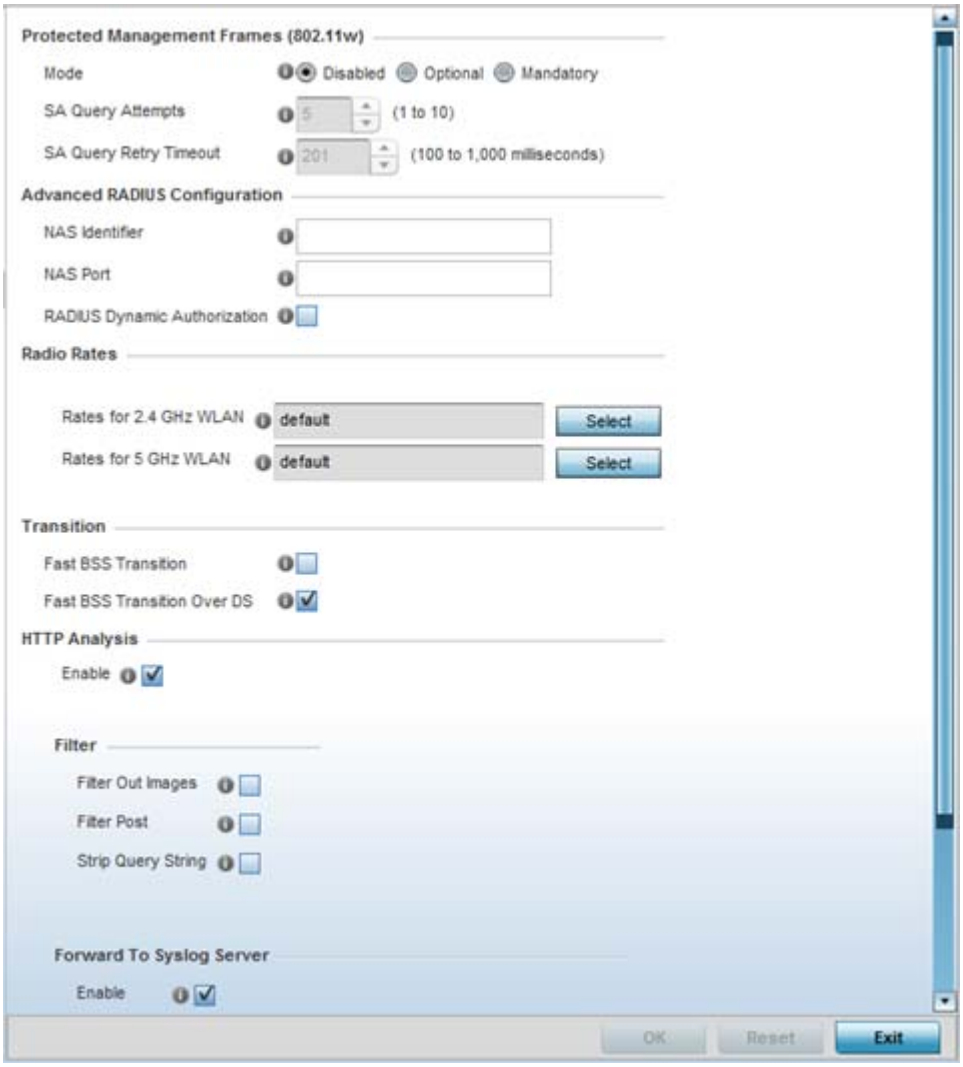


Figure 6-27 *WLAN Policy Advanced screen*

4 Refer to the **Protected Management Frames (802.11w)** field to set a frame protection mode and security association for the WLAN's advanced configuration.

Mode	Select a radio button for the mode (either *Disabled*, *Optional* or *Mandatory*). Disabled is the default setting.
SA Query Attempts	Use the spinner control to set the number of security association query attempts between 1-10. The default value is 5.
SA Query Retry Timeout	Set the timeout (from 100-1,000 milliseconds) for waiting for a response to a SA query before resending it. The default is 201 milliseconds.

5 Refer to the **Advanced RADIUS Configuration** field to set the WLAN's NAS configuration and RADIUS Dynamic Authorization.

NAS Identifier	Specify what's included in the RADIUS NAS-Identifier field for authentication and accounting packets relating to this WLAN. Configuring a value is optional, and defaults are used if not configured.

NAS Port	The profile database on the RADIUS server consists of user profiles for each connected *network access server* (NAS) port. Each profile is matched to a username representing a physical port. When authorizing users, it queries the user profile database using a username representative of the physical NAS port making the connection. Set the numeric port value from 0-4,294,967,295.
RADIUS Dynamic Authorization	Select the check box to enable a mechanism that extends the RADIUS protocol to support unsolicited messages sent from the RADIUS server. These messages allow administrators to issue *change of authorization* (CoA) messages, which affect session authorization, or *Disconnect Messages (DM)*, which terminated a session immediately. This feature is disabled by default.

6 Refer to the **Radio Rates** field to define selected data rates for both the 2.4 and 5.0 GHz bands.

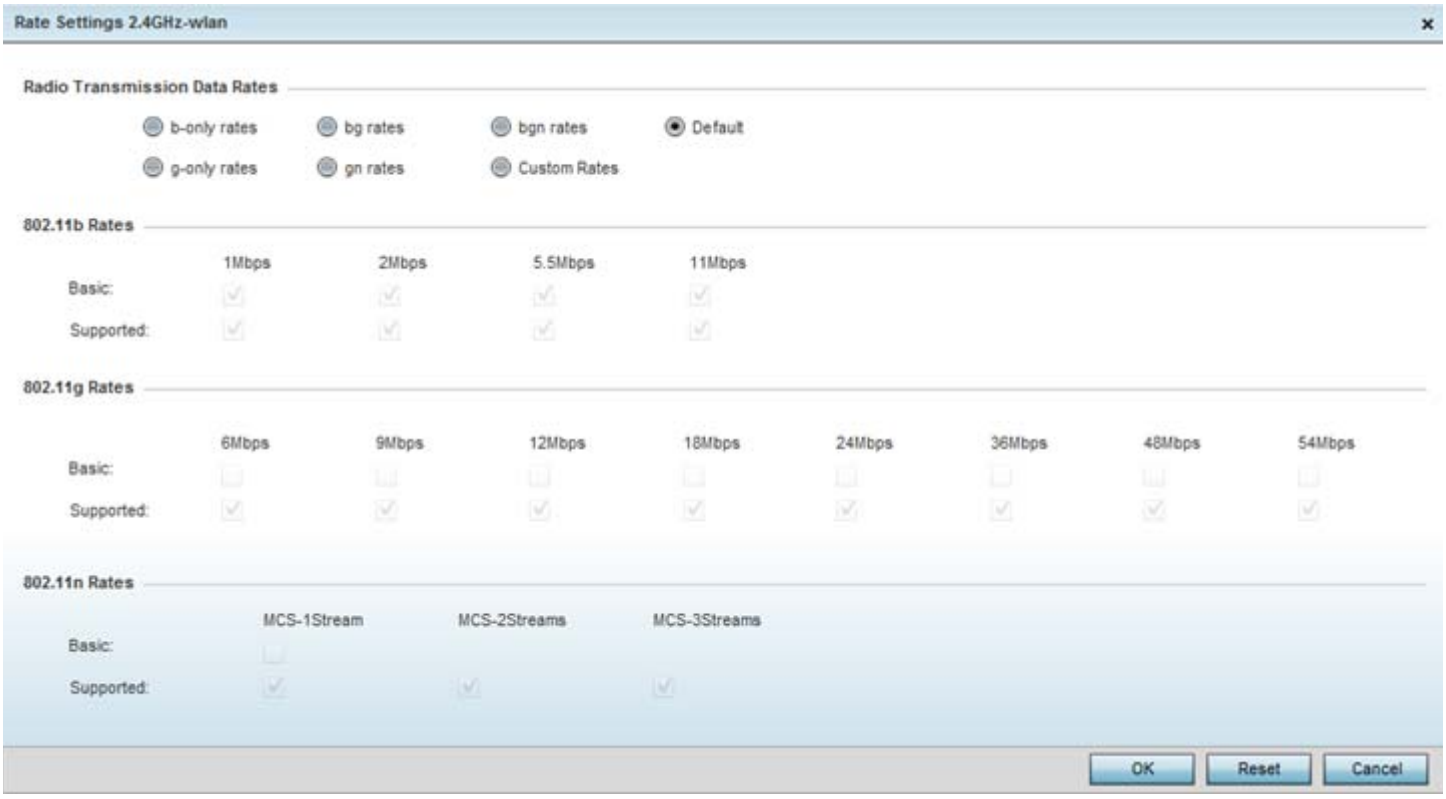


Figure 6-28 *Advanced WLAN Rate Settings 2.4 GHz screen*

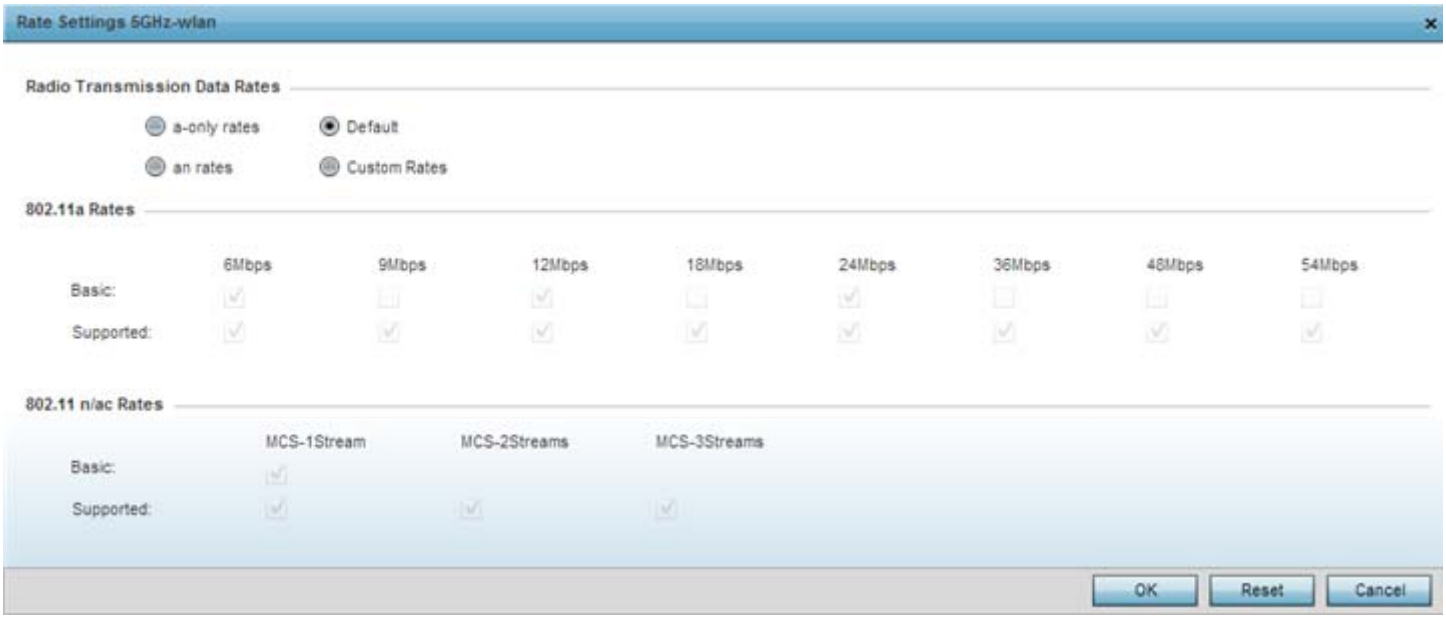


Figure 6-29 *Advanced WLAN Rate Settings 5 GHz screen*

Define both minimum *Basic* and optimal *Supported* rates as required for the 802.11b rates, 802.11g rates and 802.11n supported by the 2.4 GHz band and the 802.11a and 802.11n rates supported by the 5.0 GHz band. These are the supported client rates within this WLAN.

802.11n MCS rates are defined as follows both with and without *short guard intervals* (SGI):

Table 6.1 *MCS-1Stream*

MCS Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40MHz With SGI
0	1	6.5	7.2	13.5	15
1	1	13	14.4	27	30
2	1	19.5	21.7	40.5	45
3	1	26	28.9	54	60
4	1	39	43.4	81	90
5	1	52	57.8	108	120
6	1	58.5	65	121.5	135
7	1	65	72.2	135	150

Table 6.2 *MCS-2Stream*

MCS Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40MHz With SGI
0	2	13	14.4	27	30
1	2	26	28.9	54	60
2	2	39	43.4	81	90
3	2	52	57.8	108	120
4	2	78	86.7	162	180
5	2	104	115.6	216	240

Table 6.2 *MCS-2Stream*

MCS Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40MHz With SGI
6	2	117	130	243	270
7	2	130	144.4	270	300

Table 6.3 *MCS-3Stream*

MCS Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40MHz With SGI
0	3	19.5	21.7	40.5	45
1	3	39	43.3	81	90
2	3	58.5	65	121.5	135
3	3	78	86.7	162	180
4	3	117	130.7	243	270
5	3	156	173.3	324	360
6	3	175.5	195	364.5	405
7	3	195	216.7	405	450

802.11ac MCS rates are defined as follows both with and without *short guard intervals* (SGI):

Table 6.4 *MCS-802.11ac (theoretical throughput for single spatial streams)*

MCS Index	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40MHz With SGI	80 MHz No SGI	80MHz With SGI
0	6.5	7.2.	13.5	15	29.3	32.5
1	13	14.4	27	30	58.5	65
2	19.5	21.7	40.5	45	87.8	97.5
3	26	28.9	54	60	117	130
4	39	43.3	81	90	175.5	195
5	52	57.8	108	120	234	260
6	58.5	65	121.5	135	263.3	292.5
7	65	72.2	135	150	292.5	325
8	78	86.7	162	180	351	390
9	n/a	n/a	180	200	390	433.3

7 Set the following **Transition** options:

Fast BSS Transition	If needed, select the *Fast BSS Transition* check box to enable 802.11r fast roaming on this WLAN. This setting is disabled by default. 802.11r is an attempt to undo the burden that security and QoS added to the handoff process, and restore it back to an original four message exchange process. The central application for the 802.11r standard is VOIP using mobile phones within wireless Internet networks.
Fast BSS Transition Over DS	Optionally select the *Fast BSS Transition Over DS* check box to enable 802.11r over DS fast roaming on this WLAN. This setting is enabled by default.

8 Enable **HTTP Analysis** for log file analysis on this WLAN. This setting is disabled by default.

9 Set the following HTTP analysis **Filter** settings for the WLAN:

Filter Out Images	Select this option to filter images out of this WLAN's log files. This setting is disabled by default.
Filter Post	Select this option to filter posts out of this WLAN's log files. This setting is disabled by default.
Strip Query String	Select this option to filter query strings out of this WLAN's log files. This setting is disabled by default.

10 Set the following **Forward to Syslog Server** settings for HTTP analysis on this WLAN:

Enable	Select the check box to forward any firewall HTTP Analytics to a specified syslog server for this WLAN. This setting is disabled by default.
Host	Enter a *Hostname* or *IP Address* for the syslog server to forward HTTP Analytics. Hostnames cannot include an underscore character.
Port	Specify the port number utilized by the syslog server. The default port is 514.
Proxy Mode	If a proxy is needed to connect to the syslog server, select a proxy mode of either *Through RF Domain Manager* or *Through Wireless Controller*. If no proxy is needed, select *None*.

11 Select **OK** when completed to update this WLAN's advanced settings. Select **Reset** to revert the screen back to its last saved configuration.

6.1.9 Configuring Auto Shutdown Settings

Wireless LAN Policy

The *Auto Shutdown* feature set the WLAN to shutdown when certain criteria are met. It also allows administrators to set the operating days and hours of certain WLANs for security or bandwidth purposes.

To configure advanced settings on a WLAN:

1 Select **Configuration** > **Wireless LANs** > **Wireless LAN Policy** available WLANs.

2 Select the **Add** button to create an additional WLAN or select **Edit** to modify the properties of an existing WLAN.

3 Select **Auto Shutdown**.

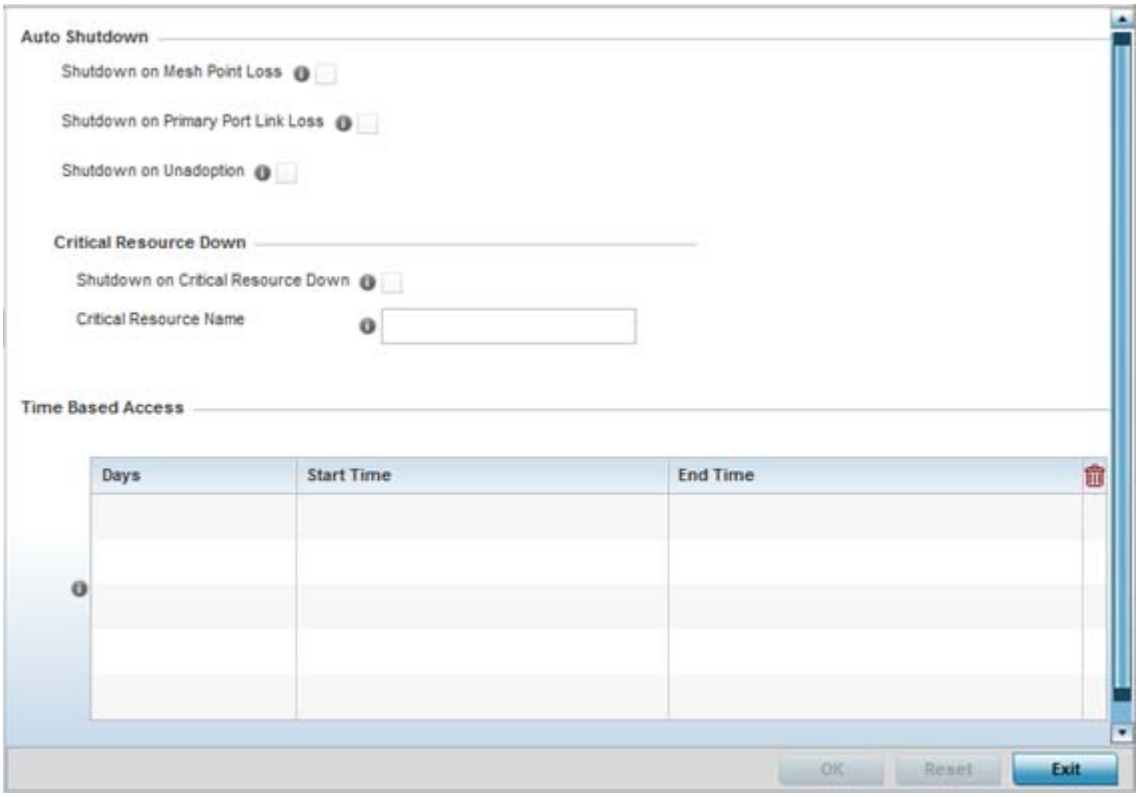


Figure 6-30 *WLAN Policy Auto Shutdown screen*

4 Refer to the **Auto Shutdown** field to set the WLANs shutdown criteria.

Shutdown on Mesh Point Loss	Select this option to automatically disable the WLAN when its associated mesh point is unreachable. This setting is disabled by default.
Shutdown on Primary Port Link Loss	Select this option to automatically disable the WLAN when its primary port link is unreachable. This setting is disabled by default.
Shutdown on Unadoption	Select this option to automatically disable the WLAN when associated Access Points are unadopted. This setting is disabled by default.

5 Set the following **Critical Resource Down** settings to determine whether a WLAN auto shutdown is enabled when a defined critical resource goes offline:

Shutdown on Critical Resource Down	Enable this feature to bring the selected WLAN offline when a defined critical resource goes offline. This setting is disabled by default.
Critical Resource Name	When enabled, enter a 127 character maximum critical resource name.This is the resource that must remain online to render the selected WLAN online.

6 To configure **Time Based Access** for this WLAN, click **+ Add Row** and configure each of the following options.

Days	Use the drop-down menu to select a day of the week to apply this access policy. Selecting *All* will apply the policy every day. Selecting *weekends* will apply the policy on Saturdays and Sundays only. Selecting *weekdays* will apply the policy on Monday, Tuesday, Wednesday, Thursday and Friday only. Selecting individual days of the week will apply the policy only on the selected day.

Start Time	This value sets the starting time the WLAN is activated. Use the spinner controls to select the hour and minute, in a 12h time format. Then use the radio button to choose *AM* or *PM*.
End Time	This value sets the ending time of day(s) that the WLAN will be disabled. Use the spinner controls to select the hour and minute, in a 12h time format. Then use the radio button to choose *AM* or *PM*.

7 Select **OK** when completed to update the auto shutdown settings. Select **Reset** to revert the screen back to its last saved configuration.

6.2 Configuring WLAN QoS Policies

- *Wireless LAN Policy*

QoS provides a data traffic prioritization scheme. QoS reduces congestion from excessive traffic. If there is enough bandwidth for all users and applications (unlikely because excessive bandwidth comes at a very high cost), then applying QoS has very little value. QoS provides policy enforcement for mission-critical applications and/or users that have critical bandwidth requirements when bandwidth is shared by different users and applications.

QoS helps ensure each WLAN receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards clients are classified into categories such as Video, Voice and Data. Packets within each category are processed based on the weights defined for each WLAN.

The Quality of Service screen displays a list of QoS policies available to WLANs. If none of the exiting QoS policies supports an ideal QoS configuration for the intended data traffic of this WLAN, select the **Add** button to create new policy. Select the radio button of an existing WLAN and select **Ok** to map the QoS policy to the WLAN displayed in the banner of the screen.

Use the WLAN *Quality of Service* (QoS) Policy screen to add a new QoS policy or edit the attributes of an existing policy.

NOTE: WLAN QoS configurations differ significantly from QoS policies configured for radios. WLAN QoS configurations are designed to support the data requirements of wireless clients, including the data types they support and their network permissions. Radio QoS policies are specific to the transmit and receive characteristics of the connected radio's themselves, independent from the wireless clients the Access Point radios supported.

1 Select **Configuration** > **Wireless** > **WLAN QoS Policy** to display existing QoS policies available to WLANs.

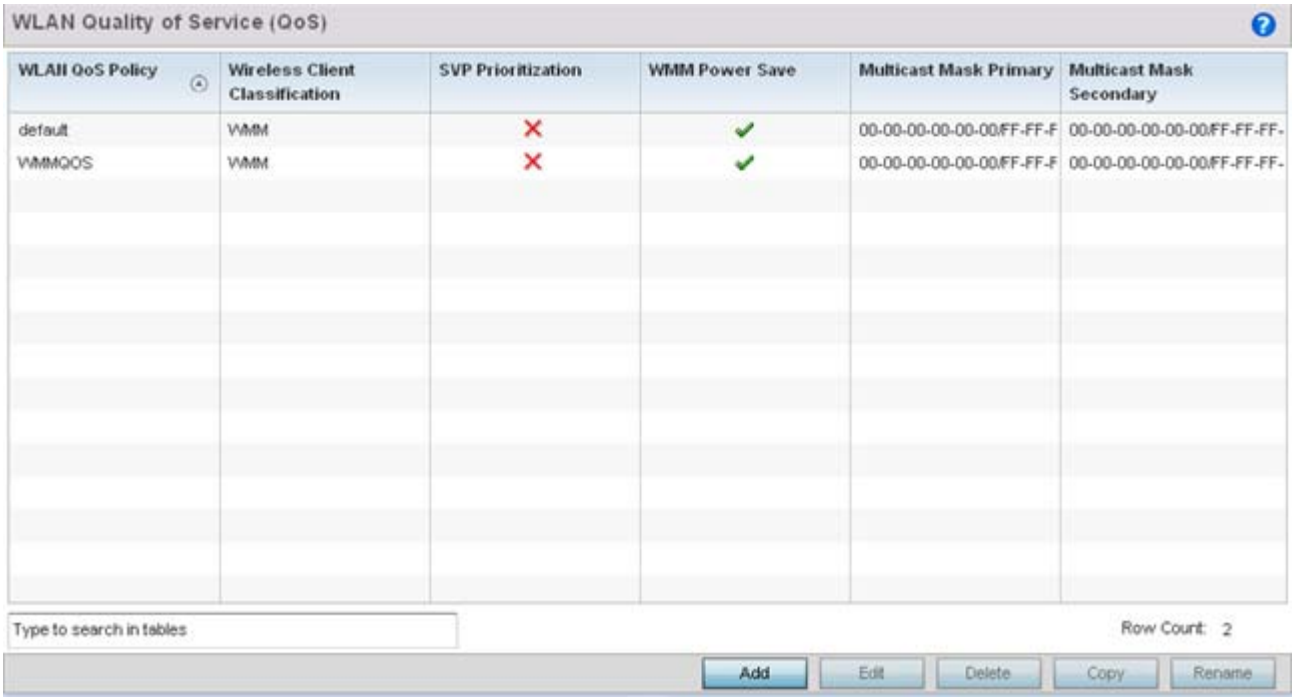


Figure 6-31 *WLAN QoS Policy screen*

2 Refer to the following read-only information on each listed QoS policy to determine whether an existing policy can be used as is, an existing policy requires edit or a new policy requires creation:

WLAN QoS Policy	Displays the name assigned to this WLAN QoS policy when it was initially created. The assigned policy name cannot be modified as part of the edit process.
Wireless Client Classification	Lists each policy's *Wireless Client* Classification as defined for this WLAN's intended traffic. The Classification Categories are the different WLAN-WMM options available to a radio. Classification types include: *WMM* – Implies WiFi Multimedia QoS extensions are enabled on this radio. This allows different traffic streams between the wireless client and the Access Point to be prioritized according to the type of traffic (voice, video etc). WMM classification is required to support the high throughput data rates required of 802.11n device support. *Voice* – Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio. *Video* – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio. *Normal* – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio. *Low* – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio. *Non-Unicast* – Optimized for non-Unicast traffic. Implies all traffic on this WLAN is designed for broadcast or multicast.

SVP Prioritization	A green check mark defines the policy as having *Spectralink Voice Prioritization* (SVP) enabled to allow the wireless controller to identify and prioritize traffic from Spectralink/Polycomm phones using the SVP protocol. Phones using regular WMM and SIP are not impacted by SVP prioritization. A red "X" defines the QoS policy as not supporting SVP prioritization.
WMM Power Save	Enables support for the WMM based power-save mechanism, also known as *Unscheduled Automatic Power Save Delivery* (U-APSD). This is primarily used by voice devices that are WMM capable. The default setting is enabled.
Multicast Mask Primary	Displays the primary multicast mask defined for each listed QoS policy. Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, the administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional and only needed if there are traffic types requiring special handling.
Multicast Mask Secondary	Displays the secondary multicast mask defined for each listed QoS policy.

NOTE: When using a wireless client classification other than WMM, only legacy rates are supported on that WLAN.

3 Either select the **Add** button to define a new WLAN QoS policy, or select an existing WLAN QoS policy and select **Edit** to modify its existing configuration. Existing QoS policies can be selected and deleted as needed. Optionally **Copy** a policy or **Rename** a WLAN QoS Policy as needed.

A *Quality of Service* (QoS) policy screen displays for the new or selected WLAN. The screen displays the WMM tab by default, but additional tabs also display for WLAN and wireless client rate limit configurations. For more information, refer to the following:

- *Configuring a WLAN's QoS WMM Settings*
- *Configuring Rate Limit Settings*

6.2.1 Configuring a WLAN's QoS WMM Settings

Using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for both home networks and Enterprises to decide which data streams are most important and assign them a higher traffic priority.

WMM's prioritization capabilities are based on the four access categories. The higher the access category, the higher the probability to transmit this kind of traffic over the WLAN. Access categories were designed to correspond to 802.1d priorities to facilitate interoperability with QoS policy management mechanisms. WMM enabled wireless controllers/Access Points coexist with legacy devices (not WMM-enabled).

Packets not assigned to a specific access category are categorized by default as having best effort priority. Applications assign each data packet to a given access category packets are then added to one of four independent transmit queues (one per access category - voice, video, best effort or background) in the client. The

client has an internal collision resolution mechanism to address collision among different queues, which selects the frames with the highest priority to transmit.

The same mechanism deals with external collision, to determine which client(s) should be granted the *opportunity to transmit* (TXOP). The collision resolution algorithm responsible for traffic prioritization is probabilistic and depends on two timing parameters that vary for each access category.

- The minimum interframe space, or *Arbitrary Inter-Frame Space Number* (AIFSN)
- The contention window, sometimes referred to as the random backoff wait

Both values are smaller for high-priority traffic. The value of the contention window varies through time. Initially the contention window is set to a value that depends on the AC. As frames with the highest AC tend to have the lowest backoff values, they are more likely to get a TXOP.

After each collision the contention window is doubled until a maximum value (also dependent on the AC) is reached. After successful transmission, the contention window is reset to its initial, AC dependant value. The AC with the lowest backoff value gets the TXOP.

To configure a WMM configuration for a WLAN:

1 Select **Configuration** > **Wireless** > **WLAN QoS Policy** to display existing QoS Policies.

2 Select the **Add** button to create a new QoS policy or **Edit** to modify the properties of an existing WLAN QoS policy.

The **WMM** tab displays by default.

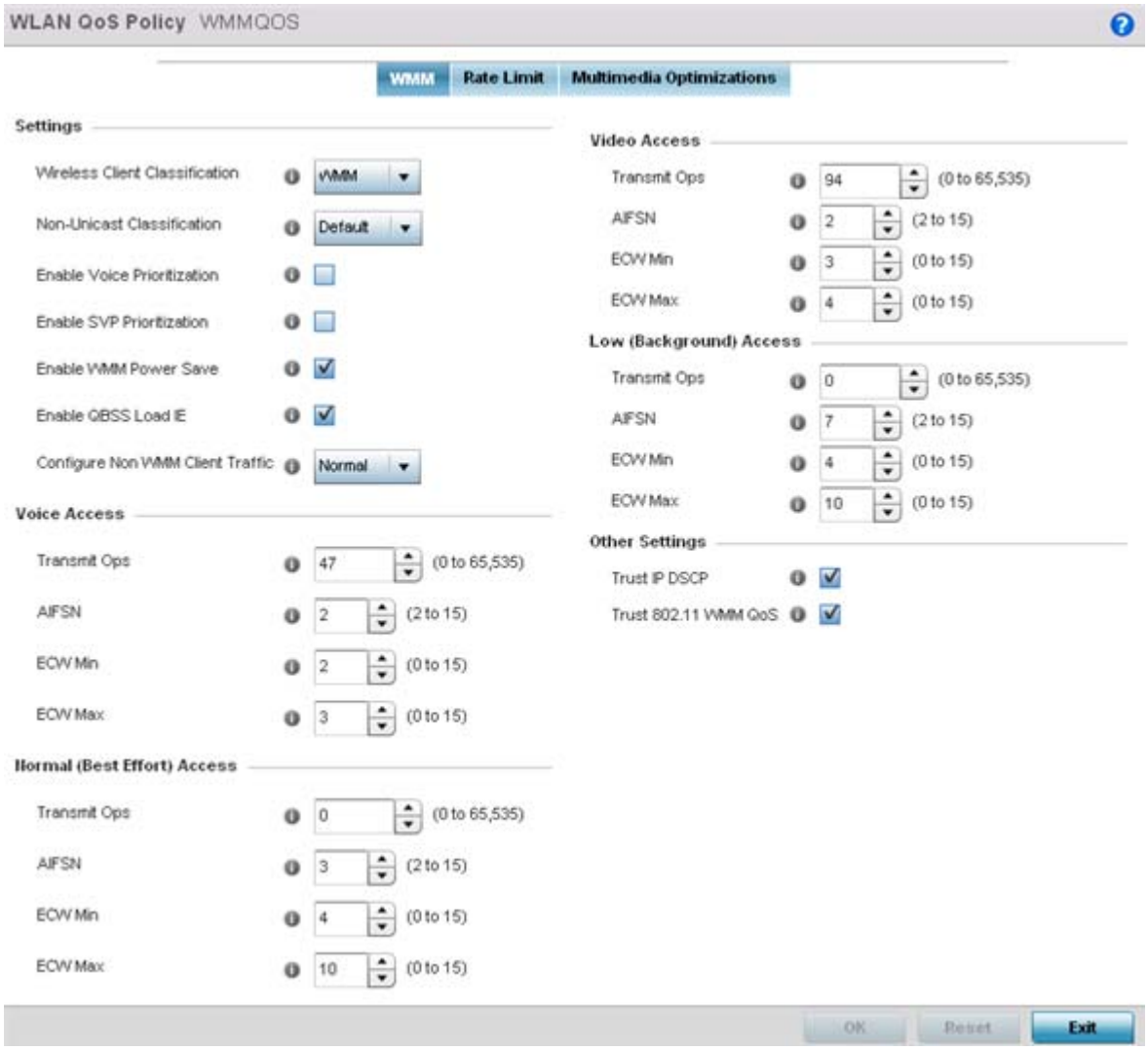


Figure 6-32 *WLAN QoS Policy - WMM screen*

3 Configure the following in respect to the WLAN's intended WMM radio traffic and user requirements:

Wireless Client Classification	Use the drop-down menu to select the *Wireless Client* Classification for this WLAN's intended traffic type. The classification categories are the different WLAN-WMM options available to the radio. Classification types include: *WMM* – Implies WiFi Multimedia QoS extensions are enabled on this radio. This allows different traffic streams between the wireless client and the Access Point to be prioritized according to the type of traffic (voice, video etc). The WMM classification is required to support the high throughput data rates required of 802.11n device support. WMM is the default setting. *Voice* – Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio. *Video* – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio. *Normal* – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio. *Low* – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.
Non-Unicast Classification	Use the drop-down menu to select the Non-Unicast Classification for this WLAN's intended traffic. Non-unicast classification types include: *Voice* – Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio. *Video* – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio. *Normal* – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio. *Low* – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.
Enable Voice Prioritization	Select this option if Voice traffic is prioritized on the WLAN. This gives priority to voice and voice management packets supported only on certain legacy VOIP phones. This feature is disabled by default.
Enable SVP Prioritization	Enabling *Spectralink Voice Prioritization* (SVP) allows the identification and prioritization of traffic from Spectralink/Polycomm phones. This gives priority to voice on certain legacy VOIP phones. If the wireless client classification is WMM, non WMM devices recognized as voice devices have their traffic transmitted at voice priority. Devices are classified as voice when they emit SIP, SCCP, or H323 traffic. Thus, selecting this option has no effect on devices supporting WMM. This feature is disabled by default.
Enable WMM Power Save	Enables support for the WMM based power-save mechanism, also known as *Unscheduled Automatic Power Save Delivery* (U-APSD). This is primarily used by voice devices that are WMM capable. The default setting is enabled.
Enable QBSS Load IE	Check this option to enable a QoS Basis Service Set (QBSS) information element (IE) in beacons and probe response packets advertised by Access Points. The default value is enabled.

Configure Non WMM Client Traffic	Use the drop-down menu to select the Non-WMM client traffic Classification. Non-WMM classification types include: *Voice* – Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio. *Video* – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio. *Normal* – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio. *Low* – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.

4 Set the following **Voice Access** settings for the WLAN's QoS policy:

Transmit Ops	Use the slider to set the maximum device transmit duration after obtaining a transmit opportunity. The default value is 47.
AIFSN	Set the current *Arbitrary Inter-frame Space Number* (AIFSN) between 2-15. Higher-priority traffic voice categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 2.
ECW Min	The ECW Min is combined with the ECW Max to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 2.
ECW Max	The ECW Max is combined with the ECW Min to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 3.

5 Set the following **Normal (Best Effort) Access** settings for the WLAN's QoS policy:

Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default value is 0.
AIFSN	Set the current AIFSN between 2-15. Lower priority traffic categories should have higher AIFSNs than higher priority traffic categories. This will cause lower priority traffic to wait longer before attempting access. The default value is 3.
ECW Min	The ECW Min is combined with the ECW Max to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Normal). The available range is from 0-15. The default value is 4.
ECW Max	The ECW Max is combined with the ECW Min to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Normal). The available range is from 0-15. The default value is 10.

6 Set the following **Video Access** settings for the WLAN's QoS policy:

Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. The default values is 94.
AIFSN	Set the current *Arbitrary Inter-frame Space Number* (AIFSN) between 2-15. Higher-priority traffic video categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 2.
ECW Min	The ECW Min is combined with the ECW Max to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 3.
ECW Max	The ECW Max is combined with the ECW Min to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 4.

7 Set the following **Low (Background) Access** settings for the WLAN's QoS policy:

Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number. The default value is 0.
AIFSN	Set the current AIFSN between 2-15. Lower priority traffic categories should have higher AIFSNs than higher priority traffic categories. This will cause lower priority traffic to wait longer before attempting access. The default value is 7.
ECW Min	The ECW Min is combined with the ECW Max to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Low). The available range is from 0-15. The default value is 4.
ECW Max	The ECW Max is combined with the ECW Min to create the contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Low). The available range is from 0-15. The default value is 10.

8 Set the following **Other Settings** for the WLAN's QoS policy:

Trust IP DSCP	Select this option to trust IP DSCP values for WLANs. The default value is enabled.
Trust 802.11 WMM QoS	Select this option to trust 802.11 WMM QoS values for WLANs. The default value enabled.

9 Select **OK** when completed to update this WLAN's QoS settings. Select **Reset** to revert the screen back to its last saved configuration.

6.2.2 Configuring Rate Limit Settings

Excessive traffic can cause performance issues or bring down the network entirely. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that

has infected on one or more devices. Rate limiting reduces the maximum rate sent or received from the wireless network (and WLAN) per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. The uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. Rate limits are extracted from the RADIUS server's response. When such attributes are not present, the settings defined on the controller, service platform or Access Point are applied. An administrator can set separate QoS rate limit configurations for data transmitted from the network (upstream) and data transmitted from a WLAN's wireless clients back to associated radios (downstream).

Before defining rate limit thresholds for WLAN upstream and downstream traffic, define the normal number of ARP, broadcast, multicast and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) will be dropped resulting in intermittent outages and performance problems.

Connected wireless clients can also have QoS rate limit settings defined in both the *upstream* and *downstream* direction.

To configure a QoS rate limit configuration for a WLAN:

1 Select **Configuration** > **Wireless** > **WLAN QoS Policy** to display existing QoS policies available to WLANs.

2 Either select the **Add** button to define a new WLAN QoS policy, or select an existing WLAN QoS policy and select **Edit** to modify its existing configuration.

3 Select the **Rate Limit** tab.

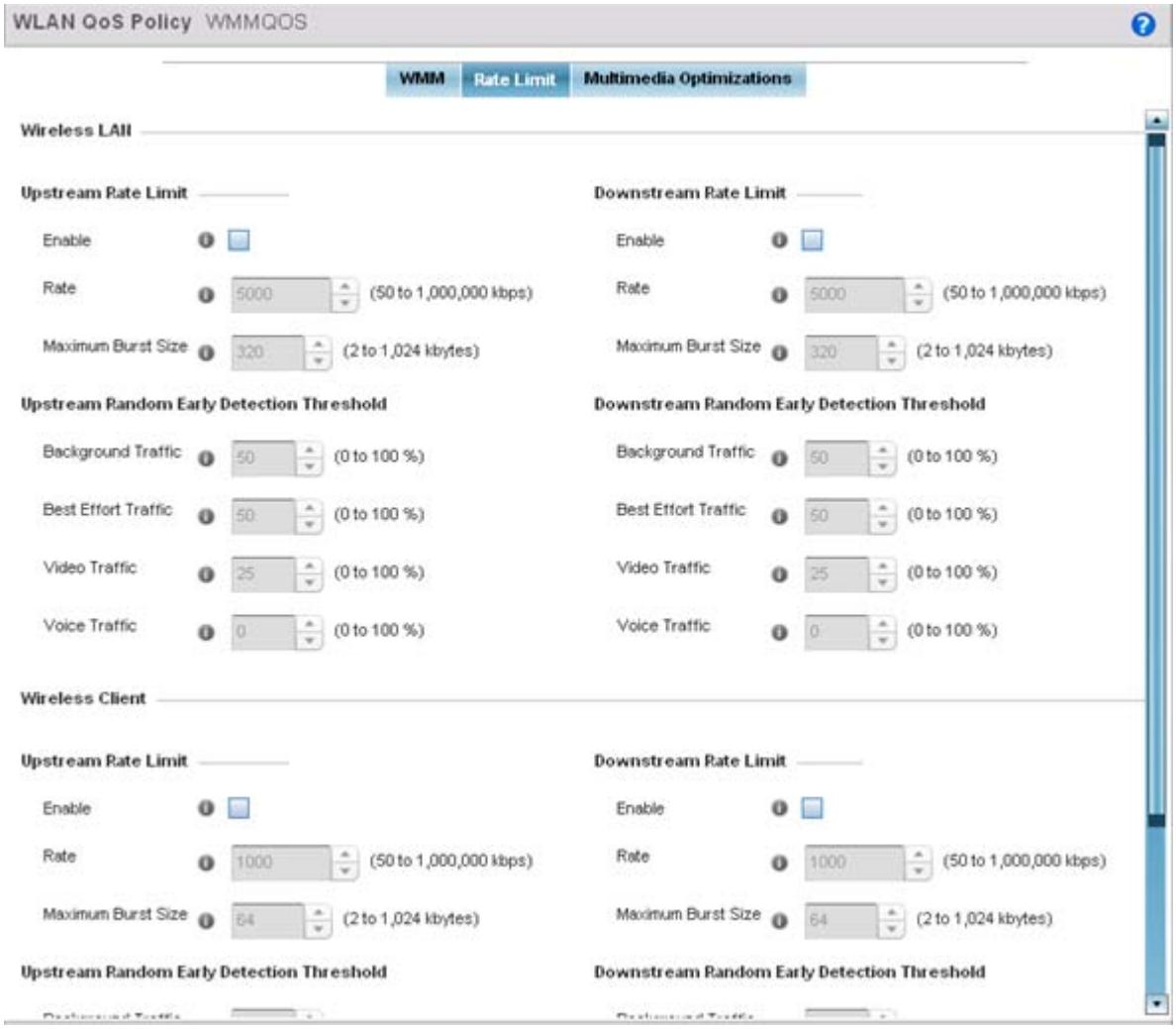


Figure 6-33 *QoS Policy WLAN Rate Limit screen*

4 Configure the following parameters in respect to the intended WLAN **Upstream Rate Limit,** or traffic from the controller or service platform to associated Access Point radios and connected wireless clients:

Enable	Select the *Enable* check box to enable rate limiting for data transmitted from the controller or service platform to associated Access Point radios and connected wireless clients. Enabling this option does not invoke rate limiting for data traffic in the downstream direction. This feature is disabled by default.
Rate	Define an upstream rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the WLAN (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.

Maximum Burst Size	Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the upstream packet transmission will result in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should add a 10% margin (minimally) to allow for traffic bursts. The default burst size is 320 kbytes.

5 Set the following WLAN **Upstream Random Early Detection Threshold** settings for each access category. An early random drop is done when a traffic stream falls below the set threshold.

Background Traffic	Set a percentage value for background traffic in the upstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
Best Effort Traffic	Set a percentage value for best effort traffic in the upstream direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
Video Traffic	Set a percentage value for video traffic in the upstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.
Voice Traffic	Set a percentage value for voice traffic in the upstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%.

6 Configure the following parameters in respect to the intended WLAN **Downstream Rate Limit,** or traffic from wireless clients to associated Access Point radios and the controller or service platform:

Enable	Select the *Enable* radio button to enable rate limiting for data transmitted from the controller or service platform to its associated Access Point radios and connected wireless clients. Enabling this option does not invoke rate limiting for data traffic in the upstream direction. This feature is disabled by default.

Rate	Define an upstream rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the WLAN (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.
Maximum Burst Size	Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the downstream packet transmission will result in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should add a 10% margin (minimally) to allow for traffic bursts. The default burst size is 320 kbytes.

7 Set the following WLAN **Downstream Random Early Detection Threshold** settings for each access category. An early random drop is done when the amount of tokens for a traffic stream falls below the set threshold.

Background Traffic	Set a percentage value for background traffic in the downstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
Best Effort Traffic	Set a percentage value for best effort traffic in the downstream direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
Video Traffic	Set a percentage value for video traffic in the downstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general downstream rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.
Voice Traffic	Set a percentage value for voice traffic in the downstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. 0% means no early random drops will occur.

8 Configure the following parameters in respect to the intended Wireless Client **Upstream Rate Limit**:

Enable	Select the *Enable* radio button to enable rate limiting for data transmitted from the client to its associated Access Point radio and connected wireless controller. Enabling this option does not invoke client rate limiting for data traffic in the downstream direction. This feature is disabled by default.

Rate	Define an upstream rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped by the client and a log message is generated. The default rate is 1,000 kbps.
Maximum Burst Size	Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the upstream packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.

9 Set the following Wireless Client **Upstream Random Early Detection Threshold** settings for each access category:

Background Traffic	Set a percentage value for background traffic in the upstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.
Best Effort Traffic	Set a percentage for best effort traffic in the upstream direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.
Video Traffic	Set a percentage value for video traffic in the upstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 25%.
Voice Traffic	Set a percentage value for voice traffic in the downstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 0%.0% implies no early random drops occur.

10 Configure the following parameters in respect to the intended Wireless Client **Downstream Rate Limit** (traffic from a controller or service platform to associated Access Point radios and the wireless client):

Enable	Select the Enable radio button to enable rate limiting for data transmitted from connected wireless clients to the controller or service platform. Enabling this option does not invoke rate limiting for data traffic in the upstream direction. This feature is disabled by default.
Rate	Define a downstream rate limit between 50 - 1,000,000 kbps.This limit constitutes a threshold for the maximum the number of packets transmitted or received by the client. Traffic that exceeds the defined rate is dropped and a log message is generated. The default rate is 1,000 kbytes.
Maximum Burst Size	Set a maximum burst size between 2 - 64 kbytes. The smaller the burst, the less likely the downstream packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.

11 Set the following Wireless Clients **Downstream Random Early Detection Threshold** settings:

Background Traffic	Set a percentage value for background traffic in the downstream direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default is 50%.

Best Effort Traffic	Set a percentage value for best effort traffic in the downstream direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default is 50%.
Video Traffic	Set a percentage value for video traffic in the downstream direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default is 25%.
Voice Traffic	Set a percentage value for voice traffic in the downstream direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 0%.0% means no early random drops occur.

12 Select **OK** to update this WLAN's QoS rate limit settings. Select **Reset** to revert to the last saved configuration.

6.2.3 Configuring Multimedia Optimization Settings

Multimedia optimizations customize the size and speed of multimedia content (voice, video etc.) to deliver WLAN traffic strategically to the WLAN's managed clients and their defined QoS requirements.

To configure multimedia optimizations for a controller, service platform or Access Point managed WLAN:

1 Select **Configuration** > **Wireless** > **WLAN QoS Policy** to display existing QoS policies available to WLANs.

2 Either select the **Add** button to define a new WLAN QoS policy, or select an existing WLAN QoS policy and select **Edit** to modify its existing configuration.

3 Select the **Multimedia Optimizations** tab.

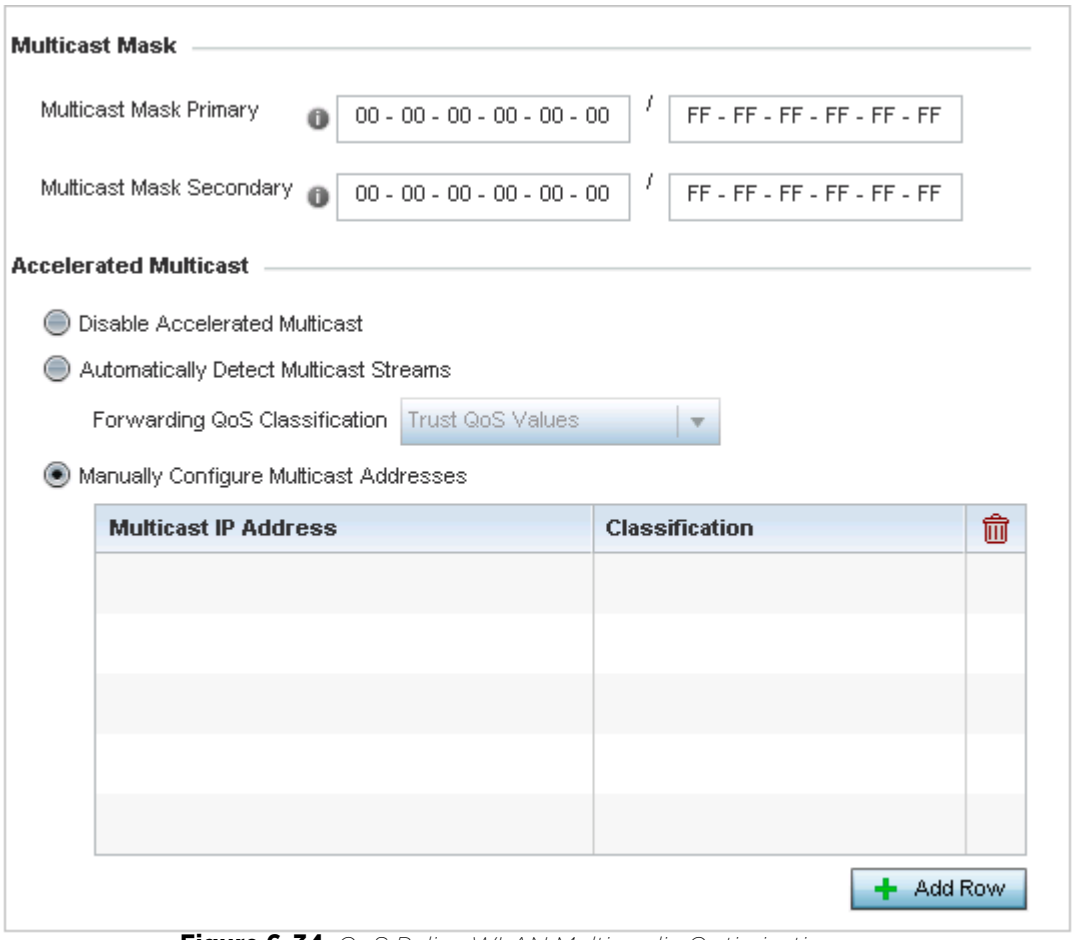


Figure 6-34 *QoS Policy WLAN Multimedia Optimizations screen*

4 Configure the following parameters in respect to the intended **Multicast Mask**:

Multicast Mask Primary	Configure the primary multicast mask defined for each listed QoS policy. Normally all multicast and broadcast packets are buffered until the periodic DTIM interval (indicated in the 802.11 beacon frame), when clients in power save mode wake to check for frames. However, for certain applications and traffic types, an administrator may want the frames transmitted immediately, without waiting for the DTIM interval. By configuring a primary and secondary multicast mask, an administrator can indicate which frames are transmitted immediately. Setting masks is optional and only needed if there are traffic types requiring special handling.
Multicast Mask Secondary	Set a secondary multicast mask for the WLAN QoS policy in case the primary becomes unavailable.

5 Set the following **Accelerated Multicast** settings:

Disable Multicast Streaming	Select this option to disable all Multicast Streaming on the WLAN.

Automatically Detect Multicast Streams	Select this option to have multicast packets converted to unicast to provide better overall airtime utilization and performance. The administrator can either have the system automatically detect multicast streams and convert all detected multicast streams to unicast, or specify which multicast streams are converted to unicast. When the stream is converted and queued for transmission, there are a number of classification mechanisms that can be applied to the stream and the administrator can select what type of classification they wan.
Manually Configure Multicast Adddresses	Select this option and specify a list of multicast addresses and classifications. Packets are accelerated when the destination addresses matches.

6 Select **OK** when completed to update this WLAN's Multimedia Optimizations settings. Select Reset to revert the screen back to its last saved configuration.

6.2.4 WLAN QoS Deployment Considerations

Before defining a QoS configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- WLAN QoS configurations differ significantly from QoS policies configured for wireless controller associated Access Point radios. WLAN QoS configurations are designed to support the data requirements of wireless clients, including the data types they support and their network permissions. Radio QoS policies are specific to the transmit and receive characteristics of the connected radio's themselves, independent from the wireless clients these Access Point radios support.
- Enabling WMM support on a WLAN only advertises WMM capability to wireless clients. The wireless clients must be also able to support WMM and use the parameters correctly while accessing the wireless network to truly benefit.
- Rate limiting is disabled by default on all WLANs. To enable rate limiting, a threshold must be defined for WLAN.
- Before enabling rate limiting on a WLAN, a baseline for each traffic type should be performed. Once a baseline has been determined, a minimum 10% margin should be added to allow for traffic bursts.
- The bandwidth required for real-time applications such as voice and video are very fairly easy to calculate as the bandwidth requirements are consistent and can be realistically trended over time. Applications such as Web, database and Email are harder to estimate, since bandwidth usage varies depending on how the applications are utilized.

6.3 Radio QoS Policy

Without a dedicated QoS policy, a wireless network operates on a best-effort delivery basis, meaning all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped!

When configuring a QoS policy for a radio, select specific network traffic, prioritize it, and use congestion-management and congestion-avoidance techniques to provide deployment customizations best suited to each QoS policy's intended wireless client base.

Wireless devices, associated Access Point radios and connected clients support several *Quality of Service* (QoS) techniques enabling real-time applications (such as voice and video) to co-exist simultaneously with lower priority background applications (such as Web, E-mail and file transfers). A well designed QoS policy should:

- Classify and mark data traffic to accurately prioritize and segregate it (by access category) throughout the network.
- Minimize the network delay and jitter for latency sensitive traffic.
- Ensure higher priority traffic has a better likelihood of delivery in the event of network congestion.
- Prevent the ineffective utilization of Access Points degrading session quality by configuring admission control mechanisms within each radio QoS policy

Wireless clients supporting low and high priority traffic contend with one another for access and data resources. The IEEE 802.11e amendment has defined *Enhanced Distributed Channel Access* (EDCA) mechanisms stating high priority traffic can access the network sooner then lower priority traffic. The EDCA defines four traffic classes (or access categories); *voice* (highest), *video* (next highest), *best effort* and *background* (lowest).The EDCA has defined a time interval for each traffic class, known as the *Transmit Opportunity* (TXOP). The TXOP prevents traffic of a higher priority from completely dominating the wireless medium, thus ensuring lower priority traffic is still supported by controller or service platform associated Access Points and their connected radios.

IEEE 802.11e includes an advanced power saving technique called *Unscheduled Automatic Power Save Delivery* (U-APSD) that provides a mechanism for wireless clients to retrieve packets buffered by an Access Point. U-APSD reduces the amount of signaling frames sent from a client to retrieve buffered data from an Access Point. U-APSD also allows Access Points to deliver buffered data frames as *bursts*, without backing-off between data frames. These improvements are useful for voice clients, as they provide improved battery life and call quality.

The Wi-Fi alliance has created *Wireless Multimedia* (WMM) and *WMM Power Save* (WMM-PS) certification programs to ensure interoperability between 802.11e WLAN infrastructure implementations and wireless clients. A WiNG wireless network supports both WMM and WMM-Power Save techniques. WMM and WMM-PS (U-APSD) are enabled by default in each WLAN profile.

Enabling WMM support on a WLAN just advertises the WLAN's WMM capability and radio configuration to wireless clients. The wireless clients must be also able to support WMM and use the values correctly while accessing the WLAN.

WMM includes advanced parameters (CWMin, CWMax, AIFSN and TXOP) specifying back-off duration and inter-frame spacing when accessing the network. These parameters are relevant to both connected Access Point radios and their wireless clients. Parameters impacting Access Point transmissions to their clients are controlled using per radio WMM settings, while parameters used by wireless clients are controlled by a WLAN's WMM settings.

WiNG wireless devices include a *Session Initiation Protocol* (SIP), *Skinny Call Control Protocol* (SCCP) and *Application Layer Gateway* (ALGs) enabling devices to identify voice streams and dynamically set voice call bandwidth. Controllers and service platforms use the data to provide prioritization and admission control to these devices without requiring TSPEC or WMM client support.

WiNG wireless devices support static QoS mechanisms per WLAN to provide prioritization of WLAN traffic when legacy (non WMM) clients are deployed. When enabled on a WLAN, traffic forwarded to a client is prioritized and forwarded based on the WLAN's WMM access control setting.

NOTE: Statically setting a WLAN WMM access category value only prioritizes traffic from the to the client, not from the client.

Rate limits can be applied to WLANs using groups defined locally or externally from a RADIUS server using *Vendor Specific Attributes* (VSAs). Rate limits can be applied to authenticating users using 802.1X, captive portal authentication and MAC authentication.

6.3.1 Configuring Radio QoS Policies

Radio QoS Policy

To configure a radio's QoS policy:

1 Select **Configuration** > **Wireless** > **Radio QoS Policy** to display existing Radio QoS policies.

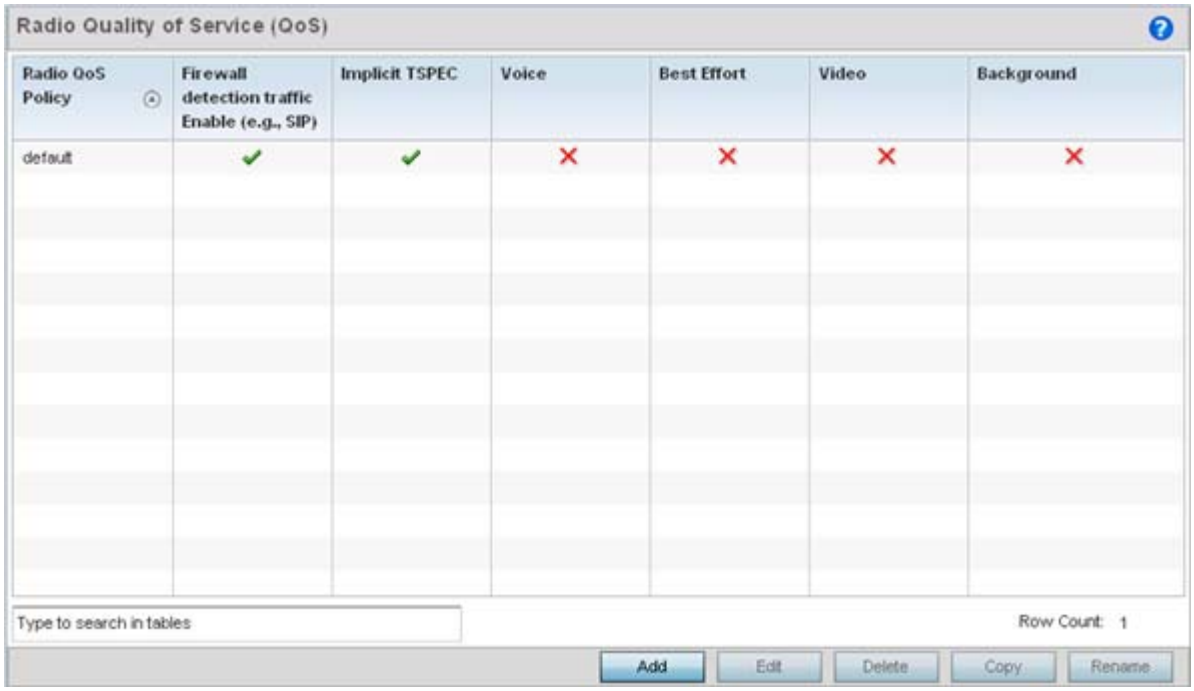


Figure 6-35 *Radio QoS Policy screen*

The Radio QoS Policy screen lists those radio QoS policies created thus far. Any of these policies can be selected and applied.

2 Refer to the following information listed for each existing Radio QoS policy:

Radio QoS Policy	Displays the name of each Radio QoS policy. This is the name set for each listed policy when it was created and cannot be modified as part of the policy edit process.
Firewall detection traffic Enable (e.g., SIP)	A green check mark defines the policy as applying radio QoS settings to traffic detected by the Firewall. A red "X" defines the policy as having Firewall detection disabled. When enabled, the Firewall simulates the reception of frames for voice traffic when the voice traffic was originated via SIP or SCCP control traffic. If a client exceeds configured values, the call is stopped and/or received voice frames are forwarded at the next non admission controlled traffic class priority. This applies to clients that do not send TSPEC frames only.

Implicit TSPEC	A green check mark defines the policy as requiring wireless clients to send their traffic specifications to a controller or service platform managed Access Point before they can transmit or receive data. If enabled, this setting applies to just this radio's QoS policy. When enabled, the Access Point simulates the reception of frames for any traffic class by looking at the amount of traffic the client is receiving and sending. If the client sends more traffic than has been configured for an admission controlled traffic class, the traffic is forwarded at the priority of the next non admission controlled traffic class. This applies to clients that do not send TSPEC frames only.
Voice	A green check mark indicates that Voice prioritization QoS is enabled on the radio. A red X indicates *Voice* prioritization QoS is disabled on the radio.
Best Effort	A green check mark indicates that Best Effort QoS is enabled on the radio. A red X indicates *Best Effort* QoS is disabled on the radio.
Video	A green check mark indicates that Video prioritization QoS is enabled on the radio. A red X indicates *Video* prioritization QoS is disabled on the radio.
Background	A green check mark indicates that Background prioritization QoS is enabled on the radio. A red X indicates *Background* prioritization QoS is disabled on the radio.

3 Either select **Add** to create a new radio QoS policy, or select one of the existing policies listed and select the **Edit** button to modify its configuration. Optionally **Copy** or **Rename** QoS policies as needed.

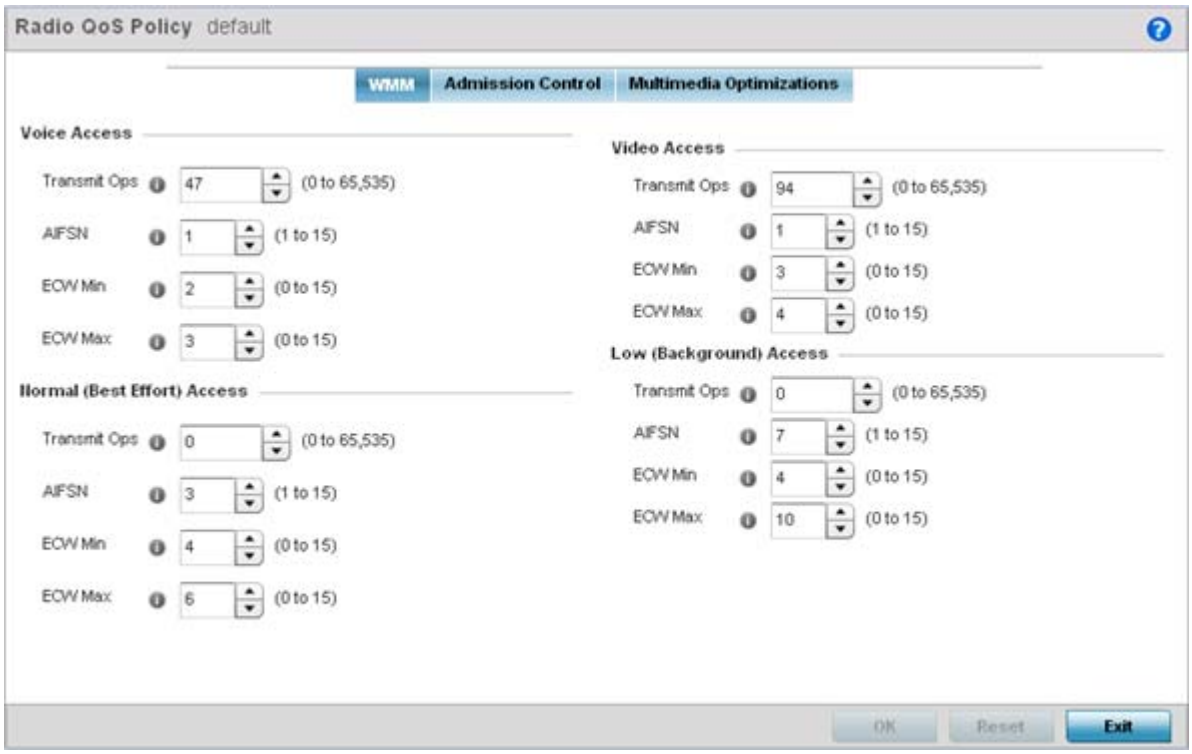


Figure 6-36 *Radio QoS Policy WMM screen*

The Radio QoS Policy screen displays the **WMM** tab by default. Use the WMM tab to define the access category configuration (*CWMin*, *CWMax*, *AIFSN* and *TXOP* values) in respect to the type of wireless data planned for this new or updated WLAN radio QoS policy.

4 Set the following **Voice Access** settings for the Radio QoS policy:

Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. When resources are shared between a *Voice over IP* (VoIP) call and a low priority file transfer, bandwidth is normally exploited by the file transfer, thus reducing call quality or even causing the call to disconnect. With voice QoS, a VoIP call (a real-time session), receives priority, maintaining a high level of voice quality. For higher-priority traffic categories (like voice), the Transmit Ops value should be set to a low number. The default value is 47.
AIFSN	Set the current AIFSN between 1-15. Higher-priority traffic voice categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 1.
ECW Min	The ECW Min is combined with the ECW Max to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 2.
ECW Max	The ECW Max is combined with the ECW Min to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic. The available range is from 0-15. The default value is 3.

5 Set the following **Normal (Best Effort) Access** settings for the radio QoS policy:

Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number. The default value is 0.
AIFSN	Set the current AIFSN between1-15. Lower priority traffic categories should have higher AIFSNs than higher priority traffic categories. This will cause lower priority traffic to wait longer before attempting access. The default value is 3.
ECW Min	The ECW Min is combined with the ECW Max to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Normal). The available range is from 0-15. The default value is 4.
ECW Max	The ECW Max is combined with the ECW Min to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Normal). The available range is from 0-15. The default value is 6.

6 Set the following **Video Access** settings for the Radio QoS policy:

Transmit Ops	Use the spinner control to set the maximum duration a radio can transmit after obtaining a transmit opportunity. For higher-priority traffic categories (like video), this value should be set to a low number. The default value is 94.

AIFSN	Set the current AIFSN between 1-15. Higher-priority traffic categories should have lower AIFSNs than lower-priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 1.
ECW Min	The ECW Min is combined with the ECW Max to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 3.
ECW Max	The ECW Max is combined with the ECW Min to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 4.

7 Set the following **Low (Background) Access** settings for the radio QoS policy:

Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number. The default value is 0.
AIFSN	Set the current AIFSN between 1-15. Lower priority traffic categories should have higher AIFSNs than higher priority traffic categories. This will cause lower priority traffic to wait longer before attempting access. The default value is 7.
ECW Min	The ECW Min is combined with the ECW Max to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Higher values are used for lower priority traffic (like Low). The available range is from 0-15. The default value is 4.
ECW Max	The ECW Max is combined with the ECW Min to create a contention value in the form of a numerical range. From this range, a random number is selected for the back off mechanism. Lower values are used for higher priority traffic (like video). The available range is from 0-15. The default value is 10.

8 Select **OK** when completed to update the radio QoS settings for this policy. Select **Reset** to revert the WMM screen back to its last saved configuration.

9 Select the **Admission Control** tab to configure an admission control configuration for selected radio QoS policy. Admission control requires clients send their *traffic specifications* (TSPEC) to a controller or service platform managed Access Point before they can transmit or receive data.

The name of the Radio QoS policy for which the admission control settings apply displays in the banner of the QoS Policy screen.

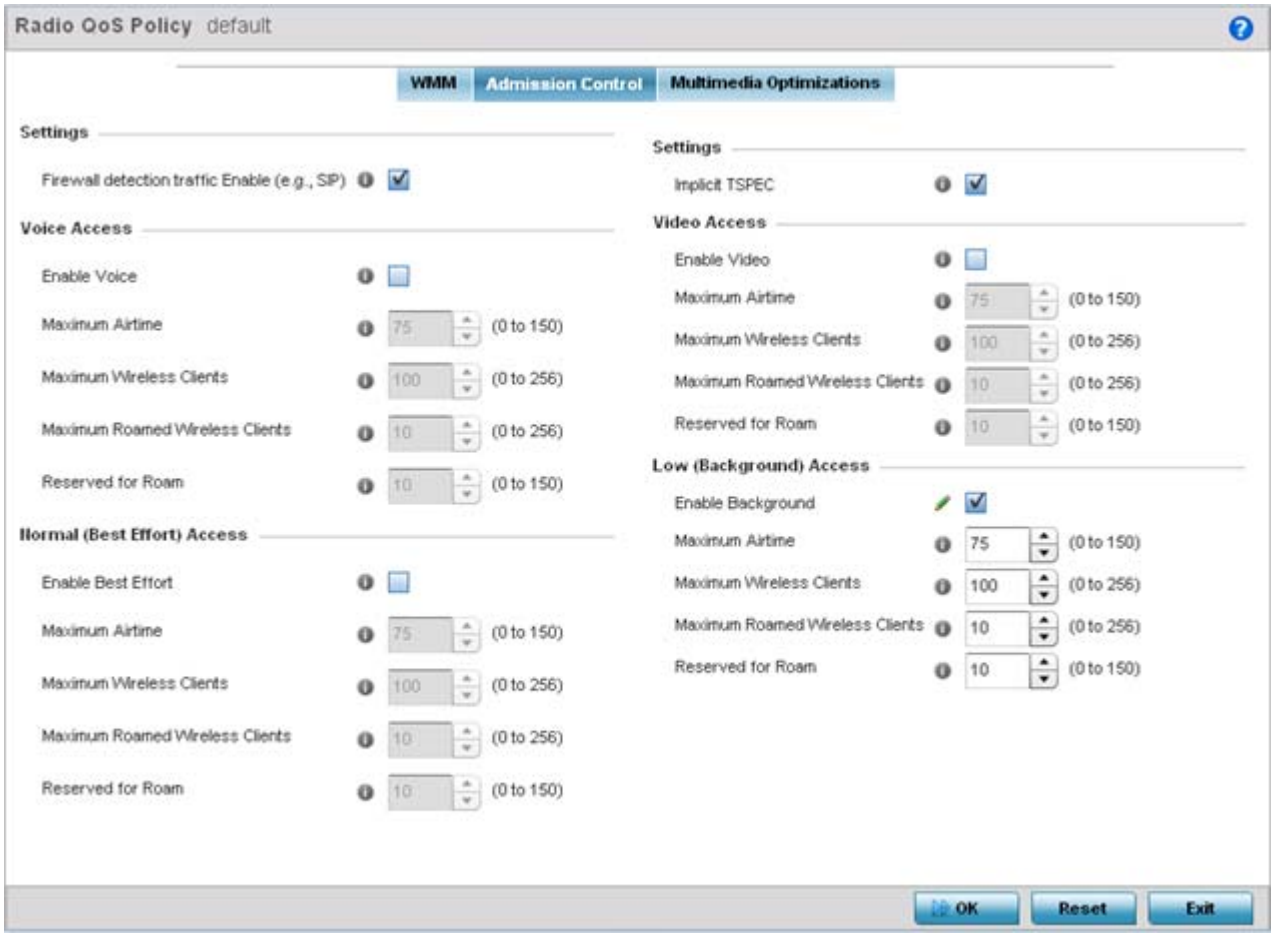


Figure 6-37 *Radio QoS Policy Admission Control screen*

10 Select the **Firewall detection traffic Enable (e.g, SIP)** check box to force admission control to traffic whose access category is detected by the firewall. This feature is enabled by default.

11 Select the **Implicit TSPEC** check box to require wireless clients to send their traffic specifications to a controller or service platform managed Access Point before they can transmit or receive data. If enabled, this setting applies to just this radio's QoS policy. This feature is enabled by default.

12 Set the following **Voice Access** admission control settings for this radio QoS policy:

Enable Voice	Select the check box to enable admission control for this policy's voice traffic. Only voice traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured).
Maximum Airtime	Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported client traffic. The available percentage range is from 0-150%, with 150% being available to account for over-subscription. This value ensures the radio's bandwidth is available for high bandwidth voice traffic (if anticipated on the wireless medium) or other access category traffic if voice support is not prioritized. Voice traffic requires longer radio airtime to process, so set a longer airtime value if this radio QoS policy is intended to support voice. The default value is 75%.

Maximum Wireless Clients	Set the number of voice supported wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from an available range of 0-256 clients. Consider setting this value proportionally to the number of other QoS policies supporting the voice access category, as wireless clients supporting voice use a greater proportion of resources than lower bandwidth traffic (like low and best effort categories). The default value is 100 clients.
Maximum Roamed Wireless Clients	Set the number of voice supported wireless clients allowed to roam to a different radio. Select from a range of 0-256 clients. The default value is 10 roamed clients.
Reserved for Roam	Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for voice supported clients who have roamed to a different radio. The available percentage range is from 0-150%, with 150% available to account for over-subscription. The default value is 10%.

13 Set the following **Normal (Best Effort) Access** admission control settings for this radio QoS policy

Enable Best Effort	Select the check box to enable admission control for this policy's video traffic. Only normal background traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured). This feature is disabled by default.
Maximum Airtime	Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal background client traffic. The available percentage range is from 0-150%, with 150% being available to account for over-subscription. This value helps ensure the radio's bandwidth is available for lower bandwidth normal traffic (if anticipated to proliferate the wireless medium). Normal background traffic only needs a short radio airtime to process, so set an intermediate airtime value if this radio QoS policy is reserved for background data support. The default value is 75%.
Maximum Wireless Clients	Set the number of wireless clients supporting background traffic allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from an available range of 0-256 clients. The default value is 100 clients.
Maximum Roamed Wireless Clients	Set the number of voice supported wireless clients allowed to roam to a different radio. Select from a range of 0-256 clients. The default value is 10 roamed clients.
Reserved for Roam	Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal background supported clients who have roamed to a different radio. The available percentage range is from 0-150%, with 150% available to account for over-subscription. The default value is 10%.

14 Set the following **Video Access** admission control settings for this radio QoS policy:

Enable Video	Select the check box to enable admission control for this policy's video traffic. Only video traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured). This feature is disabled by default.

Maximum Airtime	Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for video supported client traffic. The available percentage range is from 0-150%, with 150% being available to account for over-subscription. This value helps ensure the radio's bandwidth is available for high bandwidth video traffic (if anticipated on the wireless medium) or other access category traffic if video support is not prioritized. Video traffic requires longer radio airtime to process, so set a longer airtime value if this radio QoS policy is intended to support video. The default value is 75%.
Maximum Wireless Clients	Set the number of wireless clients supporting background traffic allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from an available range of 0-256 clients. The default value is 100 clients.
Maximum Roamed Wireless Clients	Set the number of video supported wireless clients allowed to roam to a different radio. Select from a range of 0-256 clients. The default value is 10 roamed clients.
Reserved for Roam	Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for video supported clients who have roamed to a different radio. The available percentage range is from 0-150%, with 150% accounting for over-subscription. The default value is 10%.

15 Set the following **Low (Background) Access** admission control settings for this radio QoS policy:

Enable Background	Select the check box to enable admission control for this policy's lower priority best effort traffic. Only low best effort traffic admission control is enabled, not any of the other access categories (each access category must be separately enabled and configured).
Maximum Airtime	Set the maximum airtime (in the form of a percentage of the radio's bandwidth) allotted to admission control for low, best effort, client traffic. The available percentage range is from 0-150%, with 150% being available to account for over-subscription. Best effort traffic only needs a short radio airtime to process, so set an intermediate airtime value if this radio QoS policy is reserved to support background data. The default value is 75%.
Maximum Wireless Clients	Set the number of low and best effort supported wireless clients allowed to exist (and consume bandwidth) within the radio's QoS policy. Select from an available range of 0-256 clients. The default value is 100 clients.
Maximum Roamed Wireless Clients	Set the number of low and best effort supported wireless clients allowed to roam to a different radio. Select from a range of 0-256 clients. The default value is 10 roamed clients.
Reserved for Roam	Set the roam utilization (in the form of a percentage of the radio's bandwidth) allotted to admission control for normal background supported clients who have roamed to a different radio. The available percentage range is from 0-150%, with 150% available to account for over-subscription. The default value is 10%.

16 Select the **Multimedia Optimizations** tab to set the advanced multimedia QoS and Smart Aggregation configuration for selected radio QoS policy.

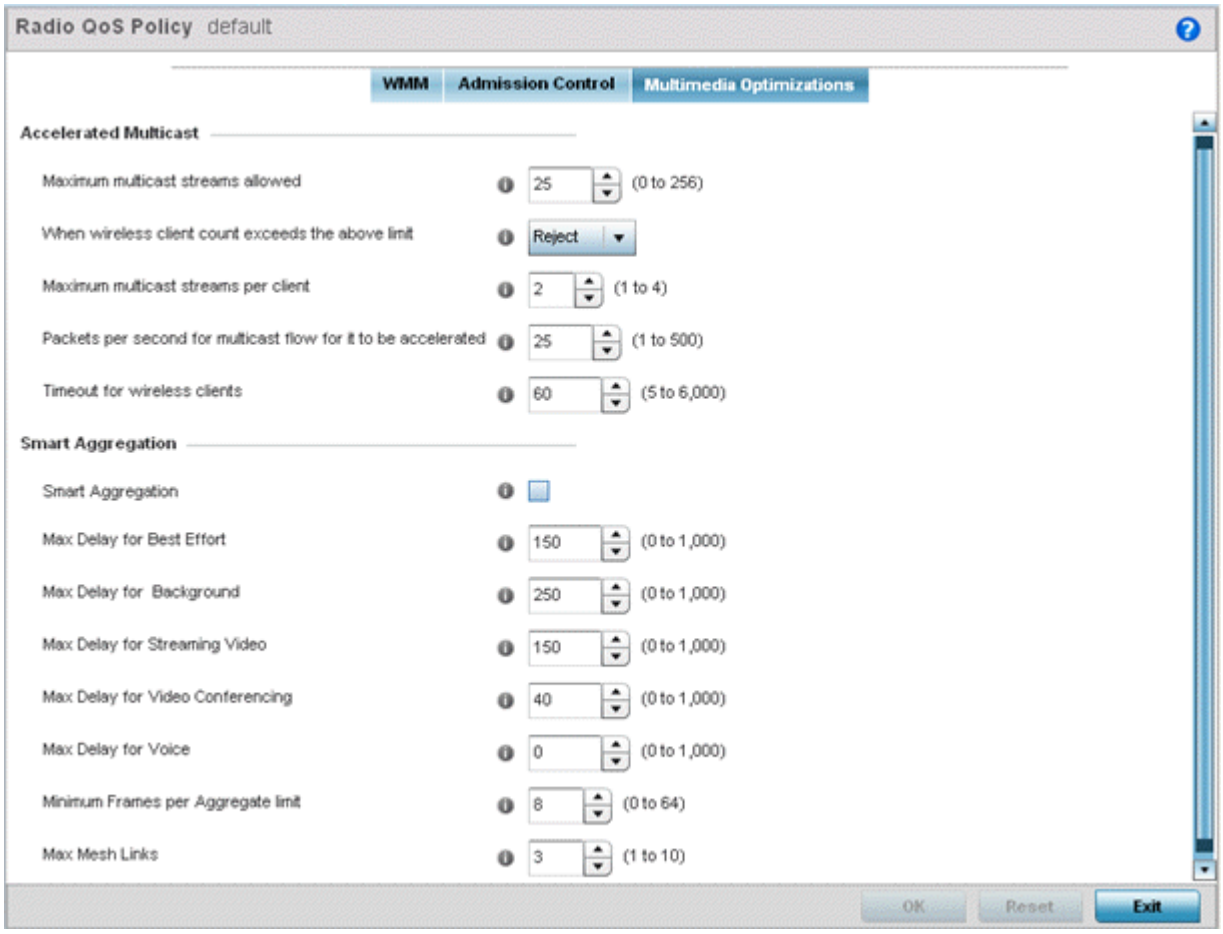


Figure 6-38 *Radio QoS Policy Multimedia Optimizations screen*

17 Set the following **Accelerated Multicast** settings for this radio QoS policy:

Maximum multicast streams allowed	Specify the maximum number of multicast streams (between 0 and 256) permitted to use accelerated multicast. The default value is 25.
When wireless client count exceeds the above limit	When the wireless client count using accelerated multicast exceeds the maximum number, set the radio to either *Reject* new wireless clients or *Revert* existing clients to a non-accelerated state.
Maximum multicast streams per client	Specify the maximum number of multicast streams (between 1 and 4) wireless clients can use. The default value is 2.
Packets per second for multicast flow for it to be accelerated	Specify the threshold of multicast packets per second (between 1 and 500) that triggers acceleration for wireless clients. The default value is 25.
Timeout for wireless clients	Specify a timeout value in seconds (between 5 and 6,000) for wireless clients to revert back to a non-accelerated state. The default value is 60.

18 Define the following **Smart Aggregation** settings:

Smart Aggregation enhances frame aggregation by dynamically selecting the time when the aggregated frame is transmitted. In a frame's typical aggregation, an aggregated frame is sent when it meets one of these conditions:

- When a preconfigured number of aggregated frames is reached

- When an administrator defined interval has elapsed since the first frame (of a set of frames to be aggregated) was received
- When an administrator defined interval has elapsed since the last frame (not necessarily the final frame) of a set of frames to be aggregated was received

With this enhancement, an aggregation delay is set uniquely for each traffic class. For example, voice traffic might not be aggregated, but sent immediately. Whereas, background data traffic is set a delay for aggregating frames, and these aggregated frames are sent.

Smart Aggregation	Select to enable smart aggregation and dynamically define when an aggregated frame is transmitted. Smart aggregation is disabled by default.
Max Delay for Best Effort	Set the maximum time (in milliseconds) to delay best effort traffic. The default setting is 150 milliseconds.
Max Delay for Background	Set the maximum time (in milliseconds) to delay background traffic. The default setting is 250 milliseconds.
Max Delay for Streaming Video	Set the maximum time (in milliseconds) to delay streaming video traffic. The default setting is 150 milliseconds.
Max Delay for Video Conferencing	Set the maximum time (in milliseconds) to delay video conferencing traffic. The default setting is 40 milliseconds.
Max Delay for Voice	Set the maximum time (in milliseconds) to delay voice traffic. The default setting is 0 milliseconds.
Minimum frames per Aggregate limit	Set the minimum number of frames to aggregate in a frame before it is transmitted. The default setting is 8 frames.
Max Mesh Links	Set the maximum number of mesh hops for smart aggregation. The default setting is 3.

Select **OK** to update the radio QoS settings for this policy. Select **Reset** to revert to the last saved configuration.

6.3.2 Radio QoS Configuration and Deployment Considerations

Radio QoS Policy

- Before defining a radio QoS policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:
- To support QoS, each multimedia application, wireless client and WLAN is required to support WMM.
- WMM enabled clients can co-exist with non-WMM clients on the same WLAN. Non-WMM clients are always assigned a Best Effort access category.
- Default WMM values should be used for all deployments. Changing these values can lead to unexpected traffic blockages, and the blockages might be difficult to diagnose.
- Overloading an Access Point radio with too much high priority traffic (especially voice) degrades overall service quality for all users.
- TSPEC admission control is only available with newer voice over WLAN phones. Many legacy voice devices do not support TSPEC or even support WMM traffic prioritization.

6.4 Association ACL

An association ACL is a policy-based ACL that either prevents or allows wireless clients from connecting to a WLAN.

An association ACL affords a system administrator the ability to grant or restrict client access by specifying a wireless client MAC address or range of MAC addresses to either include or exclude from connectivity.

Association ACLs are applied to WLANs as an additional access control mechanism. They can be applied to WLANs from within a WLAN Policy's Advanced configuration screen. For more information on applying an existing Association ACL to a WLAN, see *Configuring Advanced WLAN Settings*.

To define an association ACL deployable with a WLAN:

1 Select **Configuration** > **Wireless** > **Association ACL** to display existing Association ACLs.

The **Association Access Control List (ACL)** screen lists those Association ACL policies created thus far. Any of these policies can be selected and applied.

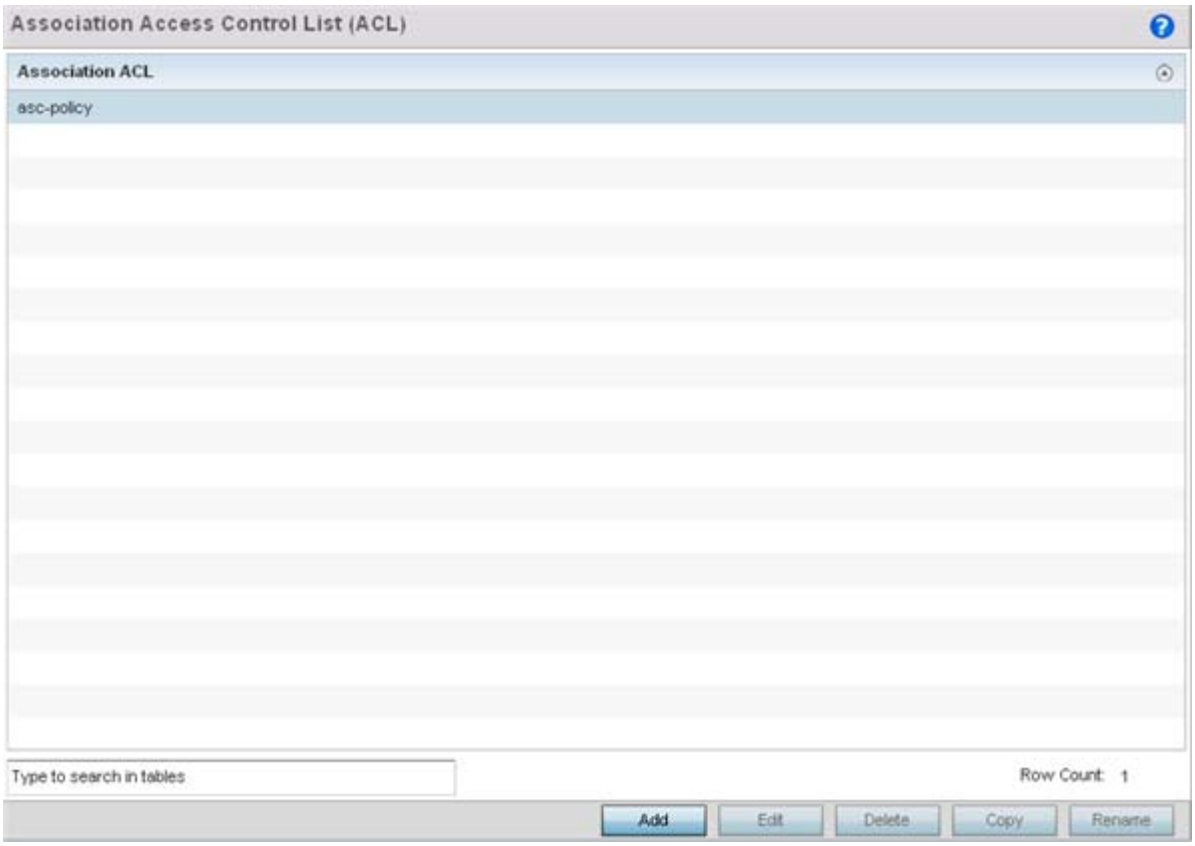


Figure 6-39 *Association Access Control List (ACL) screen*

2 Select **Add** to define a new ACL configuration, **Edit** to modify an existing ACL configuration or **Delete** to remove one. Optionally **Copy** or **Rename** a list as needed.

A unique Association ACL screen displays for defining the new ACL or modifying a selected ACL.

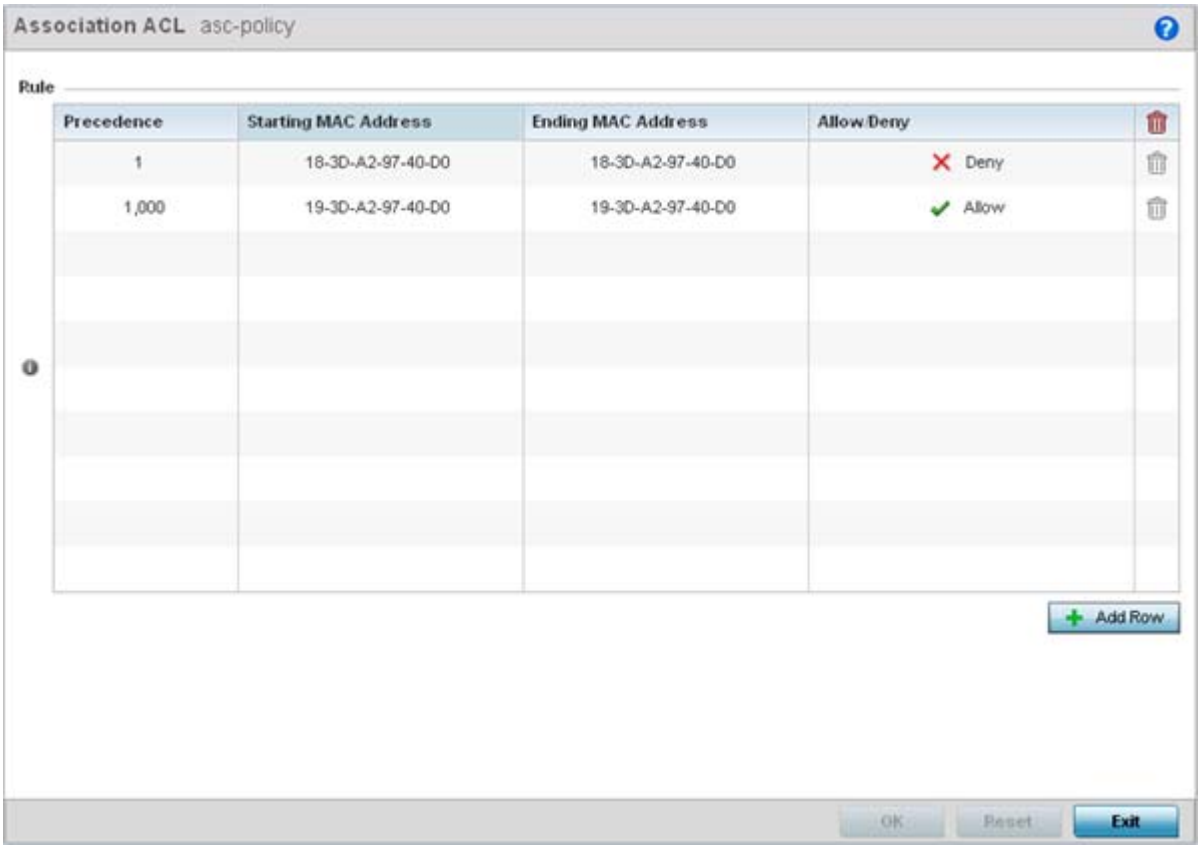


Figure 6-40 *Association Access Control List (ACL) screen*

3 Select the **+ Add Row** button to add an association ACL template.

4 Set the following parameters for the creation or modification of the Association ACL:

Association ACL	If creating an new association ACL, provide a name specific to its function. Avoid naming it after the WLAN it may support. The name cannot exceed 32 characters.
Precedence	The rules within a WLAN's ACL are applied to packets based on their precedence values. Every rule has a unique sequential precedence value you define. You cannot add two rules's with the same precedence. The default precedence is 1, so be careful to prioritize ACLs accordingly as they are added.
Starting MAC Address	Provide a starting MAC range address for clients requesting association.
Ending MAC Address	Provide an ending MAC range address for clients requesting association.
Allow/Deny	Use the drop-down menu to either *Allow* or *Deny* access if a MAC address matches this rule.

5 Select the **+ Add Row** button to add MAC address ranges and allow/deny designations.

6 Select **OK** to update the Association ACL settings. Select **Reset** to revert to the last saved configuration.

6.4.1 Association ACL Deployment Considerations

Association ACL

Before defining an Association ACL configuration and applying it to a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Use the Association ACL screen strategically to name and configure ACL policies meeting the requirements of the particular WLANs they may map to. However, be careful not to name ACLs after specific WLANs, as individual ACL policies can be used by more than one WLAN.
- You cannot apply more than one MAC based ACL to a Layer 2 interface. If a MAC ACL is already configured on a Layer 2 interface, and a new MAC ACL is applied to the interface, the new ACL replaces the previously configured one.

6.5 Smart RF Policy

Self Monitoring At Run Time RF Management (Smart RF) is a WiNG innovation designed to simplify RF configurations for new deployments, while (over time) providing on-going deployment optimization radio performance improvements.

A Smart RF policy can reduce deployment costs by scanning the RF environment to determine the best channel and transmit power configuration for each radio. Smart RF policies can be applied to specific RF Domains, to apply site specific deployment configurations and self-healing values to groups of devices within pre-defined physical RF coverage areas.

Smart RF centralizes the decision process and makes intelligent RF configuration decisions using information obtained from the RF environment. Smart RF helps reduce ongoing management and maintenance costs by constantly monitoring the network for external interference, neighbor interference, non-WiFi interference and client connectivity. Smart RF then intelligently applies various algorithms to arrive at the optimal channel and power selection for all Access Points in the network and constantly reacts to changes in the RF environment.

Smart RF also provides self-healing functions by monitoring the network in real-time and provides automatic mitigation from potentially problematic events such as radio interference, non-WiFi interference (noise), external WiFi interference, coverage holes and radio failures. Smart RF employs self-healing to enable a WLAN to better maintain wireless client performance and site coverage during dynamic RF environment changes, which typically require manual reconfiguration to resolve.

Smart RF is supported on any RF Domain manager. In standalone environments, individual controllers, service platforms or Access Points manage the calibration and monitoring phases. In clustered environments, a single controller or service platform is elected a Smart RF master and the remaining cluster members operate as Smart RF clients. In cluster operation, the Smart RF master co-ordinates the calibration and configuration and during the monitoring phase receives information from the Smart RF clients.

If a Smart RF managed radio is operating in WLAN mode on a channel requiring DFS, it will switch channels if radar is detected.

- If Smart RF is enabled, the radio picks a channel defined in the Smart RF policy.
- If Smart RF is disabled, but a Smart RF policy is mapped, the radio picks a channels specified in the Smart RF policy
- If no SMART RF policy is mapped, the radio selects a random channel

If the radio is a dedicated sensor, it stops termination on that channel if a neighboring Access Points detects radar. The Access Point attempts to come back to its original channel (statically configured or selected by Smart RF) after the channel evacuation period has expired.

Change this behavior using a no dfs-rehome command from the controller or service platform CLI. This keeps the radio on the newly selected channel and prevents the radio from coming back to the original channel, even after the channel evacuation period.

NOTE: RF planning must be performed to ensure overlapping coverage exists at a deployment site for Smart RF to be a viable network performance tool. Smart RF can only provide recovery when Access Points are deployed appropriately. Smart RF is not a solution, it's a temporary measure. Administrators need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist.

To define a Smart RF policy:

1 Select **Configuration** > **Wireless** > **Smart RF Policy** to display existing Smart RF policies.

The Smart RF screen lists those Smart RF policies created thus far. Any of these policies can be selected and applied.

The user has the option of displaying the configurations of each Smart RF Policy defined thus far, or referring to the **Smart RF Browser** and either selecting individual Smart RF polices or selecting existing RF Domains to review which Smart RF policies have been applied. For more information on how RF Domains function, and how to apply a Smart RF policy, see *About RF Domains* and *Managing RF Domains*.

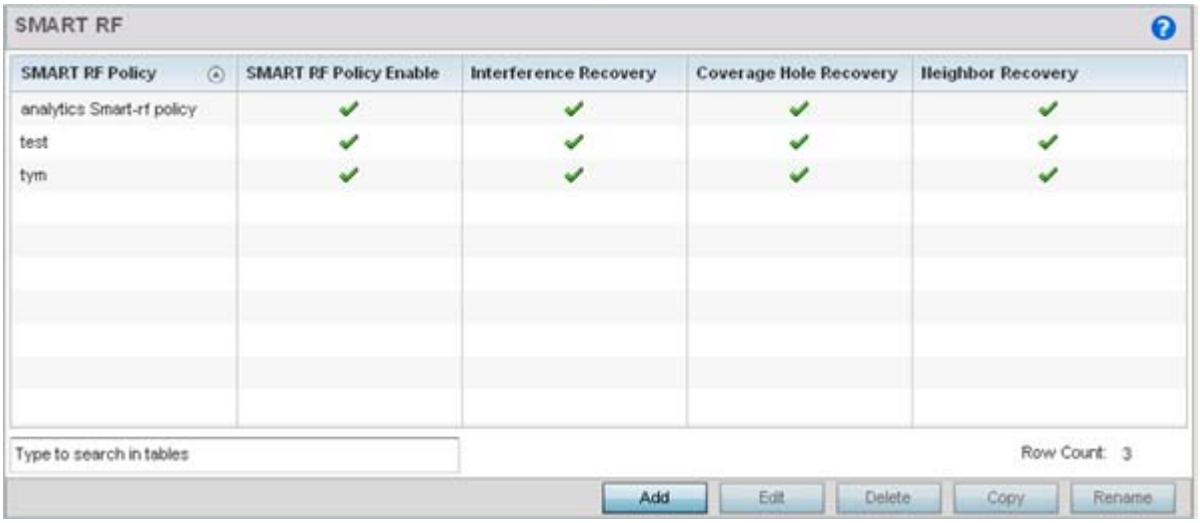


Figure 6-41 *Smart RF Policy screen*

2 Refer to the following configuration data for existing Smart RF policies:

Smart RF Policy	Displays the name assigned to the Smart RF policy when it was initially created. The name cannot be modified as part of the edit process.
Smart RF Policy Enable	Displays a green check mark if Smart RF has been enabled for the listed policy. A red "X" designates the policy as being disabled.
Interference Recovery	Displays a green check mark if interference recovery has been enabled for the listed policy. A red "X" designates interference recovery being disabled.

Coverage Hole Recovery	Displays a green check mark if coverage hole recovery has been enabled for the listed policy. A red “X” designates coverage hole recovery being disabled.
Neighbor Recovery	Displays a green check mark if neighbor recovery has been enabled for the listed policy. A red “X” designates neighbor recovery being disabled.

3 Select **Add** to create a new Smart RF policy, **Edit** to modify the attributes of a existing policy or **Delete** to remove obsolete policies from the list of those available. Optionally **Copy** or **Rename** a list as needed.

The **Basic Configuration** screen displays by default for the new or modified Smart RF policy.

Figure 6-42 *Smart RF Basic Configuration screen*

4 Refer to the **Basic Settings** field to enable a Smart RF policy and define its sensitivity and detector status.

Sensitivity	Select a radio button corresponding to the desired Smart RF sensitivity. Options include *Low*, *Medium*, *High* and *Custom*. Medium, is the default setting. The Custom option allows an administrator to adjust the parameters and thresholds for Interference Recovery, Coverage Hole Recovery and Neighbor Recovery. Using the Low, Medium (recommended) and High settings still allow these features to be utilized.
SMART RF Policy Enable	Select the *Smart RF Policy Enable* check box to enable this Smart RF policy for immediate support or inclusion with a RF Domain. Smart RF is enabled by default.

Interference Recovery	Select the check box to enable Interference Recovery from neighboring radios and other sources of WiFi and non-WiFi interference when excess noise and interference is detected within the Smart RF supported radio coverage area. Smart RF provides mitigation from interference sources by monitoring the noise levels and other RF parameters on an Access Point radio's current channel. When a noise threshold is exceeded, Smart RF can select an alternative channel with less interference. To avoid channel flapping, a hold timer is defined which disables interference avoidance for a specific period of time upon detection. Interference Recovery is enabled by default.
Coverage Hole Recovery	Select the check box to enable Coverage Hole Recovery when a radio coverage hole is detected within the Smart RF supported radio coverage area. When coverage hole is detected, Smart RF first determines the power increase needed based on the signal to noise ratio for a client as seen by the Access Point radio. If a client's signal to noise value is above the threshold, the transmit power is increased until the signal to noise rate falls below the threshold.
Neighbor Recovery	Select the check box to enable Neighbor Recovery when a failed radio is detected within the Smart RF supported radio coverage area. Smart RF can provide automatic recovery by instructing neighboring APs to increase their transmit power to compensate for the coverage loss. Neighbor recovery is enabled by default when the sensitivity setting is medium.

5 Refer to the **Calibration Assignment** field to define whether Smart RF Calibration and radio grouping is conducted by area or floor. Both options are disabled by default.

6 Select **OK** to update the Smart RF Basic Configuration settings for this policy. Select **Reset** to revert to the last saved configuration.

7 Select **Channel and Power**.

Use the Channel and Power screen to refine Smart RF power settings over both 5 and 2.4 GHz radios and select channel settings in respect to the device channel usage.

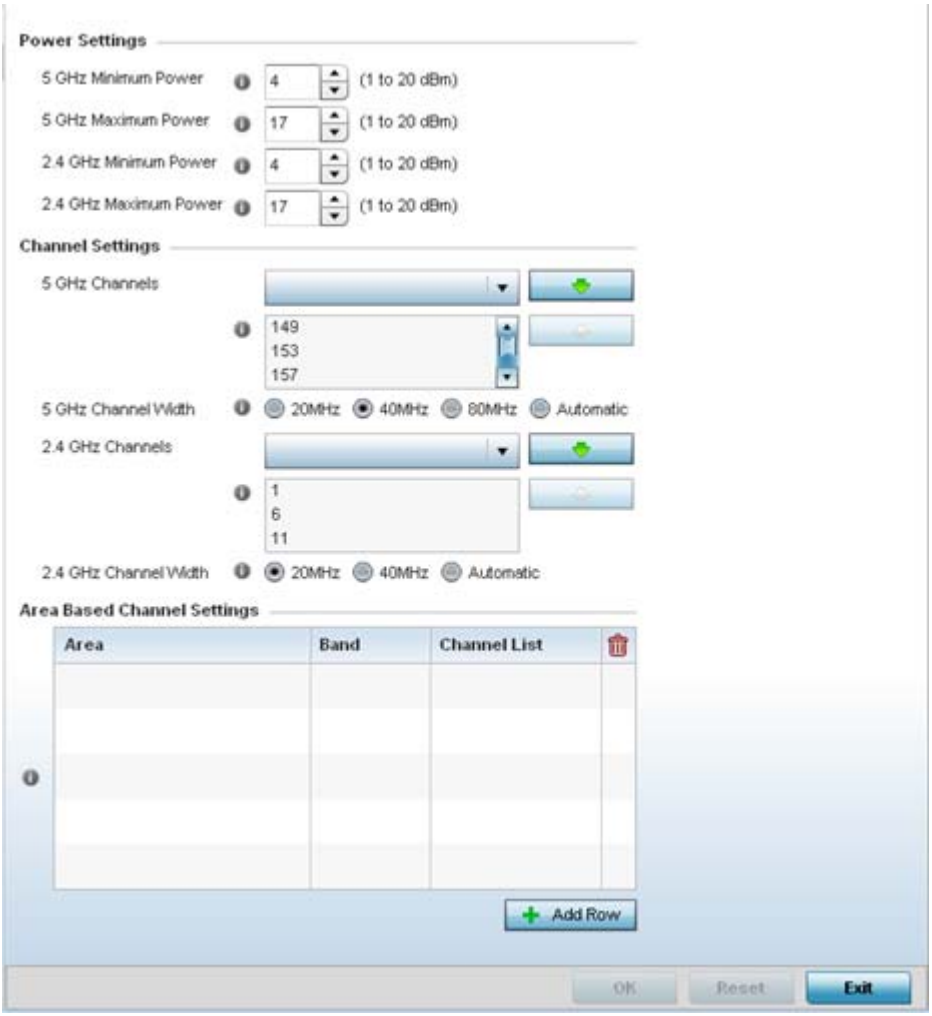


Figure 6-43 *Smart RF Channel and Power screen*

NOTE: The Power Settings and Channel Settings parameters are only enabled when Custom or Medium is selected as the Sensitivity setting from the Basic Configuration screen.

8 Refer to the **Power Settings** field to define Smart RF recovery settings for either the selected 5.0 GHz (802.11a) or 2.4 GHz (802.11bg) radio.

5 GHz Minimum Power	Use the spinner control to select a 1 - 20 dBm minimum power level for Smart RF to assign to a radio in the 5 GHz band. 4 dBm is the default setting.
5 GHz Maximum Power	Use the spinner control to select a 1 - 20 dBm maximum power level Smart RF can assign a radio in the 5 GHz band. 17 dBm is the default setting.
2.4 GHz Minimum Power	Use the spinner control to select a 1 - 20 dBm minimum power level Smart RF can assign a radio in the 2.4 GHz band. 4 dBm is the default setting.
2.4 GHz Maximum Power	Use the spinner control to select a 1 - 20 dBm maximum power level Smart RF can assign a radio in the 2.4 GHz band. 17 dBm is the default setting.

9 Set the following **Channel Settings** for the 5.0 GHz and 2.4 GHz radios:

5 GHz Channels	Use the *Select* drop-down menu to define the 5 GHz channels used for Smart RF assignments.
5 GHz Channel Width	20 and 40 MHz channel widths are supported by the 802.11a radio. 20/40 MHz operation (the default setting for the 5 GHz radio) allows the Access Point to receive packets from clients using 20 MHz of bandwidth while transmitting a packet using 40 MHz bandwidth. This mode is supported for 11n users on both the 2.4 and 5 GHz radios. If an 11n user selects two channels (a Primary and Secondary channel), the system is configured for dynamic 20/40 operation. When 20/40 is selected, clients can take advantage of wider channels. 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select *Automatic* to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources. 40MHz is the default setting. If deploying an 802.11ac supported Access Point, 80MHz channel width options are available as well.
2.4 GHz Channels	Set the 2.4 GHz channels used in Smart RF scans.
2.4 GHz Channel Width	20 and 40 MHz channel widths are supported by the 802.11a radio. 20 MHz is the default setting for 2.4 GHz radios. 20/40 MHz operation (the default setting for the 5 GHz radio) allows the Access Point to receive packets from clients using 20 MHz of bandwidth while transmitting a packet using 40 MHz bandwidth. This mode is supported for 11n users on both the 2.4 and 5 GHz radios. If an 11n user selects two channels (a Primary and Secondary channel), the system is configured for dynamic 20/40 operation. When 20/40 is selected, clients can take advantage of *wider channels*. 802.11n clients experience improved throughput using 40 MHz while legacy clients (either 802.11a or 802.11b/g depending on the radio selected) can still be serviced without interruption using 20 MHz. Select *Automatic* to enable automatic assignment of channels to working radios to avoid channel overlap and avoid interference from external RF sources. 20MHz is the default setting.

10 Select **+ Add Row** and set the following **Area Based Channel Settings** for the Smart RF policy:

Area	Specify the deployment area assigned to the listed policy when deployed a means of identifying the devices physical locations.
Band	Specify the radio band, either 2.4 GHz or 5 GHz, for the Smart RF policy assigned to the specified area.
Channel List	Specify the channels associated with the Smart RF policy for the specified area and band.

11 Select **OK** to update the Smart RF Channel and Power settings for this policy. Select **Reset** to revert to the last saved configuration.

12 Select the **Scanning Configuration** tab.

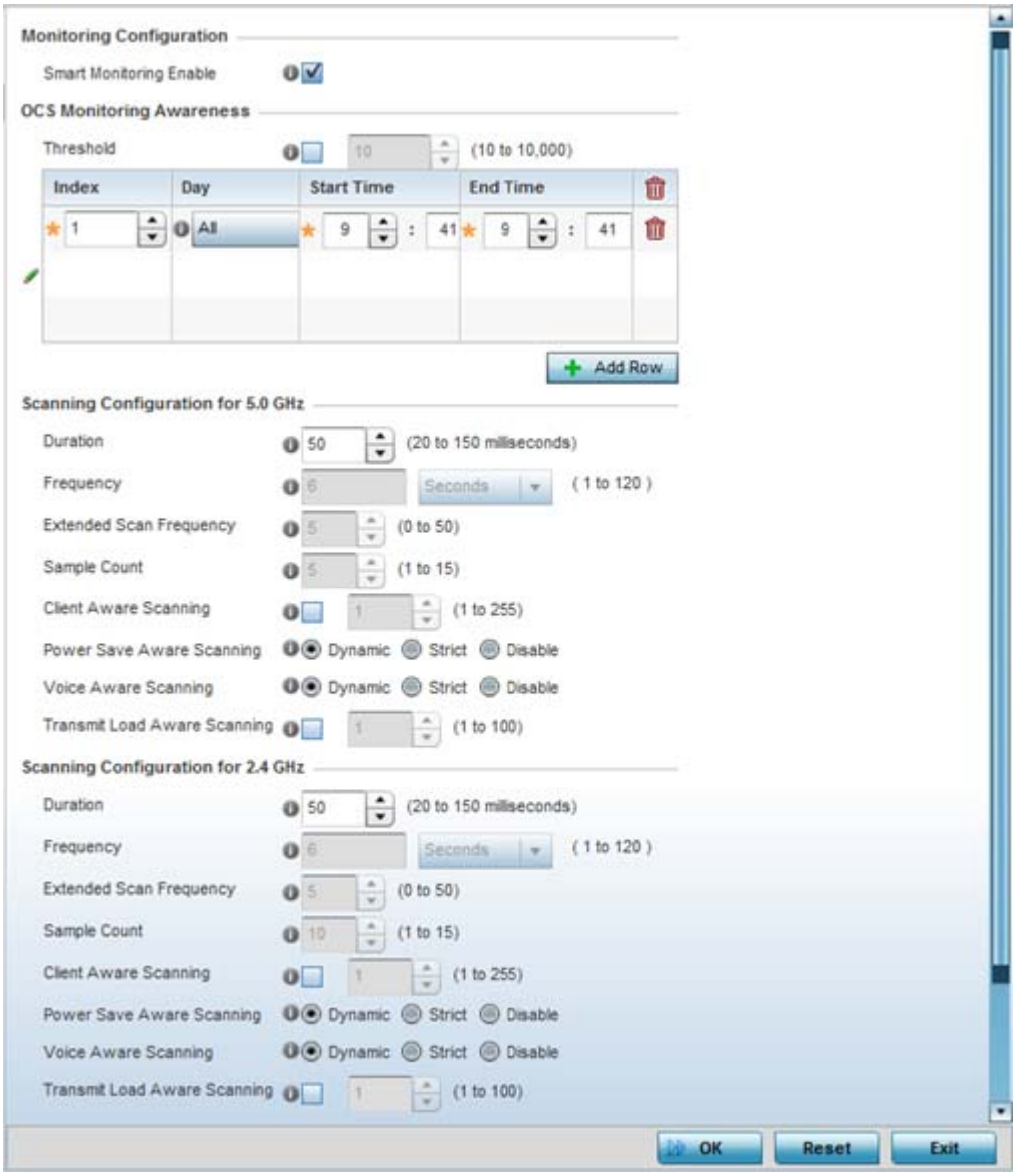


Figure 6-44 *Smart RF Scanning Configuration screen*

NOTE: The monitoring and scanning parameters within the Scanning Configuration screen are only enabled when *Custom* is selected as the Sensitivity setting from the Basic Configuration screen.

13 *Enable* or *disable* **Smart Monitoring Enable**. The feature is enabled by default.

When enabled, detector radios monitor their coverage areas for potential failed peers or coverage area holes requiring transmission adjustments for coverage compensation.

14 Select **+ Add Row** and set **OCS Monitoring Awareness Settings** for the Smart RF policy:

Threshold	Select this option and specify a threshold from 10 - 10,000. When the threshold is reached awareness settings are overridden with the values specified in the table.

Index	Select an Index value from 1 - 3 for awareness overrides. The overrides are executed based on index, with the lowest index being executed first.
Day	Use the drop-down menu to select a day of the week to apply the override. Selecting All will apply the policy every day. Selecting weekends will apply the policy on Saturdays and Sundays only. Selecting weekdays will apply the policy on Monday, Tuesday, Wednesday, Thursday and Friday. Selecting individual days of the week will apply the policy only on the selected day.
Start Time	This value sets the starting time of day(s) that the overrides will be activated. Use the spinner controls to select the hour and minute, in 12h time format. Then use the radio button to choose AM or PM.
End Time	This value sets the ending time of day(s) that the overrides will be disabled. Use the spinner controls to select the hour and minute, in 12h time format. Then use the radio button to choose AM or PM.

15 Set the following **Scanning Configurations** for both the **2.4** and **5.0** GHz radio bands:

Duration	Set a channel scan duration (from 20 - 150 milliseconds) Access Point radios use to monitor devices within the network and, if necessary, perform self healing and neighbor recovery to compensate for coverage area losses within a RF Domain. The default setting is 50 milliseconds for both the 2.4 and 5 GHz bands.
Frequency	Set the scan frequency using the drop-down menu. Set a scan frequency in either *Seconds* (1 - 120) or *Minutes* (0 - 2). The default setting is 6 seconds for both the 5 and 2.4 GHz bands.
Extended Scan Frequency	Use the spinner control to set an extended scan frequency between 0 - 50. This is the frequency radios scan channels on other than their peer radios. The default setting is 5 for both the 5 and 2.4 GHz bands.
Sample Count	Use the spinner control to set a sample scan count value between 1 - 15. This is the number of RF readings radios gather before they send the data to the Smart RF master. The default setting is 5 for both the 5 and 2.4 GHz bands
Client Aware Scanning	Set a client awareness count (number of clients from 1 - 255) for off channel scans of either the 5 GHz or 2.4 GHz band.
Power Save Aware Scanning	Select either the *Dynamic*, *Strict* or *Disable* radio button to define how power save scanning is set for Smart RF. Strict disables smart monitoring as long as a power save capable client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a power save client at the radio. The default setting is Dynamic for both the 5 and 2.4 GHz bands.
Voice Aware Scanning	Select either the *Dynamic*, *Strict* or *Disable* radio button to define how voice aware recognition is set for Smart RF. Strict disables smart monitoring as long as a voice client is associated to a radio. Dynamic disables smart monitoring as long as there is data buffered for a voice client at the radio. The default setting is Dynamic for both the 5 and 2.4 GHz bands.
Transmit Load Aware Scanning	Select this option to set a transmit load percentage from 1 - 100 serving as a threshold before scanning is avoided for an Access Point's 2.4 GHz radio.

16 Select **OK** to update the Smart RF Scanning Configuration settings for this policy. Select **Reset** to revert to the last saved configuration.

17 Select **Recovery**.

> **NOTE:** The recovery parameters within the Neighbor Recovery, Interference and Coverage Hole Recovery tabs are only enabled when *Custom* is selected as the Sensitivity setting from the Basic Configuration screen.

The **Neighbor Recovery** tab displays by default. Use the *Neighbor*, *Interference* and *Coverage Hole* recovery tabs to define how 5 and 2.4 GHz radios compensate for failed neighbor radios, interference impacting the Smart RF supported network and detected coverage holes requiring neighbor radio intervention.

18 Set the **Hold Time** for the Smart RF configuration.

Power Hold Time	Defines the minimum time between two radio power changes during neighbor recovery. Set the time in either *Seconds* (0 - 3,600), *Minutes* (0 - 60) or *Hours* (0 - 1). The default setting is 0 seconds.

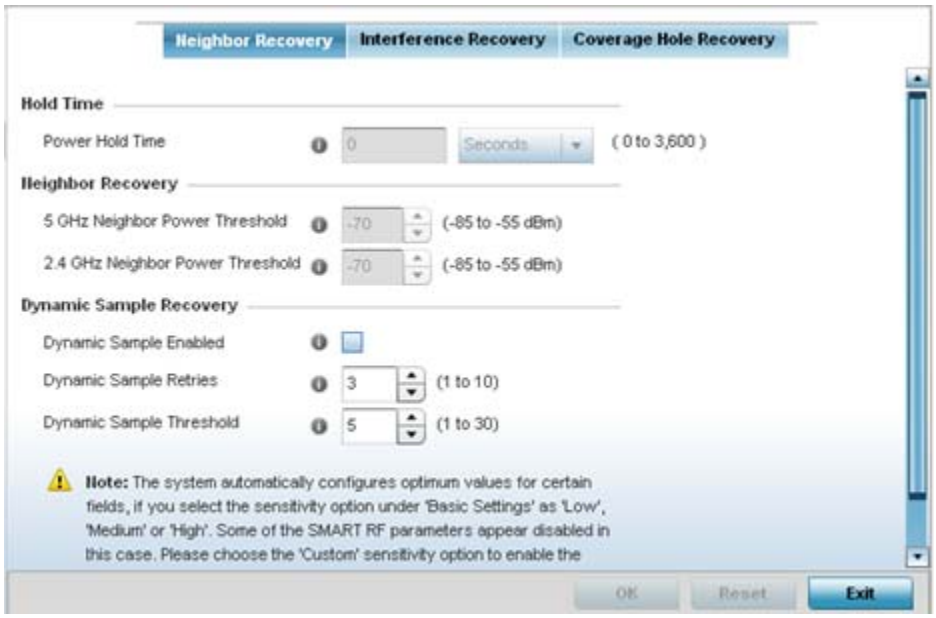


Figure 6-45 *Smart RF Advanced Configuration screen - Neighbor Recovery tab*

19 Set the following **Neighbor Recovery** parameters:

5 GHz Neighbor Power Threshold	Use the spinner control to set a value between -85 to -55 dBm the 5.0 GHz radio uses as a maximum power increase threshold if the radio is required to increase its output power to compensate for a failed radio within its wireless radio coverage area. The default value is -70 dBm.
2.4 GHz Neighbor Power Threshold	Use the spinner control to set a value between -85 to -55 dBm the 2.4 GHz radio uses as a maximum power increase threshold if the radio is required to increase its output power to compensate for a failed radio within its wireless radio coverage area. The default value is -70 dBm.

20 Set the following **Dynamic Sample Recovery** parameters:

Dynamic Sample Enabled	Select this option to enable dynamic sampling. Dynamic sampling enables an administrator to define how Smart RF adjustments are triggered by locking retry and threshold values. This setting is disabled by default.
Dynamic Sample Retries	Set the number of retries (from 1 - 10) attempted before a power level adjustment is implemented to compensate for a potential coverage hole. The default setting is 3.
Dynamic Sample Threshold	Set the minimum number of sample reports (from 1- 30) before a Smart RF power compensation requires dynamic sampling. The default setting is 5.

21 Select **OK** to update the Smart RF Neighbor Recovery settings for this policy. Select **Reset** to revert to the last saved configuration.

22 Select the **Interference Recovery** tab.

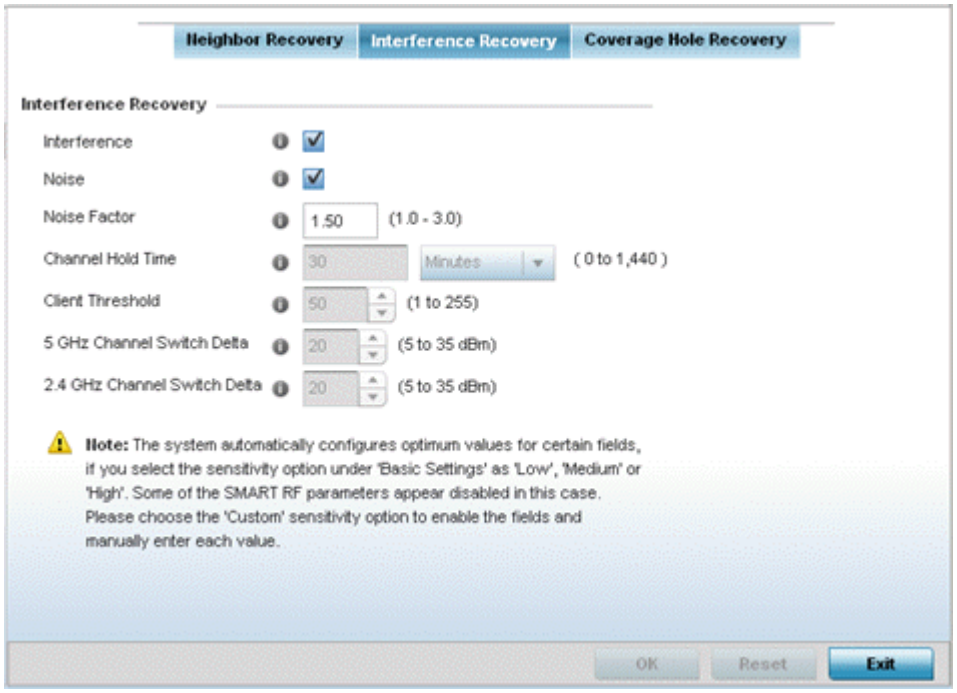


Figure 6-46 *Smart RF Advanced Configuration screen - Interference Recovery tab*

23 Set the following **Interference Recovery** parameters:

Interference	Select the check box to allow the Smart RF policy to scan for excess interference from supported radio devices. WLANs are susceptible to sources of interference, such as neighboring radios, cordless phones, microwave ovens and Bluetooth devices. When interference for WiFi sources is detected, Smart RF supported devices can change the channel and move to a cleaner channel. This feature is enabled by default.
Noise	Select the check box to allow the Smart RF policy to scan for excess noise from WiFi devices. When detected, Smart RF supported devices can change their channel and move to a cleaner channel. This feature is enabled by default.

Noise Factor	Define the *noise factor* (level of network interference detected) taken into account by Smart RF during interference recovery calculations. The default setting is 1.50.
Channel Hold Time	Defines the minimum time between channel changes during neighbor recovery. Set the time in either *Seconds* (0 - 86,400), *Minutes* (0 - 1,440) or *Hours* (0 - 24) or *Days* (0 - 1). The default setting is 30 minutes.
Client Threshold	Use the spinner to set a client threshold for the Smart RF policy between 1 - 255. If the set threshold number of clients are connected to a radio, it does not change its channel even though it requires one, based on the interference recovery determination made by the smart master. The default is 50.
5 GHz Channel Switch Delta	Use the spinner to set a channel interference delta (between 5 - 35 dBm) for the 5.0 GHz radio. This parameter is the difference between interference levels on the current channel and a prospective channel. If the difference is below the configured threshold, the channel will not change. The default setting is 20 dBm.
2.4 GHz Channel Switch Delta	Use the spinner to set a channel interference delta (between 5 - 35 dBm) for the 2.4 GHz radio. This parameter is the difference between interference levels on the current channel and a prospective channel. If the difference is below the configured threshold, the channel will not change. The default setting is 20 dBm.

24 Select **OK** to update the Smart RF Interference Recovery settings for this policy. Select **Reset** to revert to the last saved configuration.

25 Select the **Coverage Hole Recovery** tab.

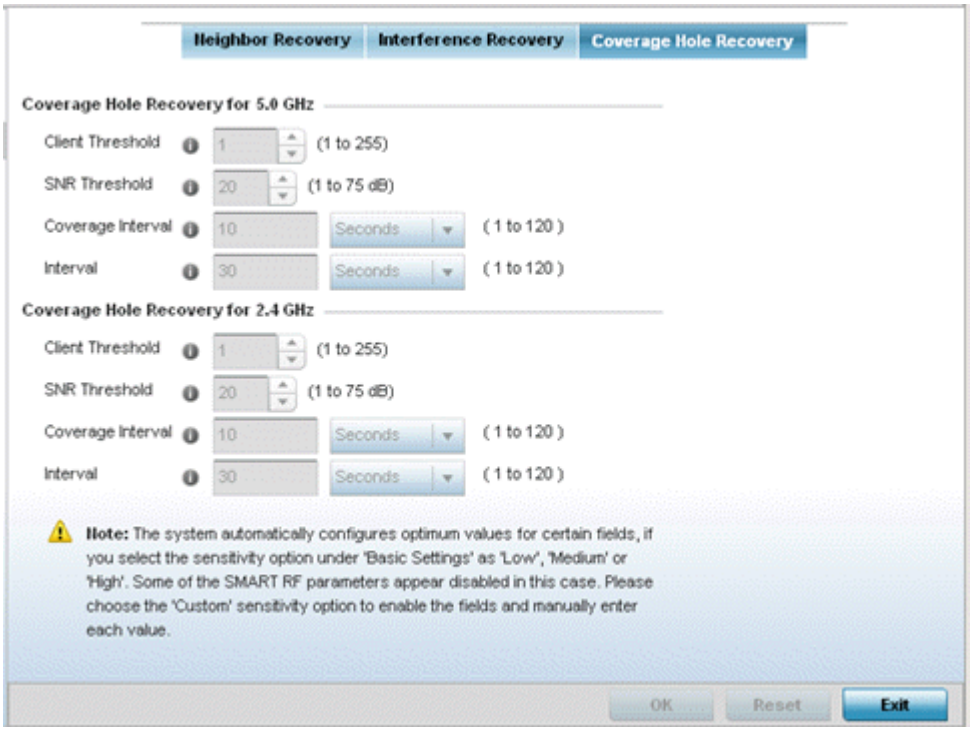


Figure 6-47 *Smart RF Advanced Configuration screen - Coverage Hole Recovery tab*

26 Set the following **Coverage Hole Recovery for 2.4 GHz** and **5.0 GHz** parameters:

Client Threshold	Use the spinner to set a client threshold for the Smart RF policy between 1 - 255. This is the minimum number of clients a radio should have associated in order for coverage hole recovery to trigger. The default setting is 1.
SNR Threshold	Use the spinner control to set a signal to noise threshold (between 1 - 75 dB). This is the signal to noise threshold for an associated client as seen by its associated Access Point radio. When exceeded, the radio increases its transmit power in order to increase coverage for the associated client. The default value is 20 dB.
Coverage Interval	Define the interval coverage hole recovery should be initiated after a coverage hole is detected. The default is 10 seconds for both the 2.4 and 5.0 GHz radios.
Interval	Define the interval coverage hole recovery should be conducted before a coverage hole is detected. The default is 30 seconds for both the 2.4 and 5.0 GHz radios.

27 Select **OK** to update the Smart RF coverage hole recovery settings for this policy. Select **Reset** to revert to the last saved configuration.

6.5.1 Smart RF Configuration and Deployment Considerations

Smart RF Policy

Before defining a Smart RF policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- The Smart RF calibration process impacts associated users and should not be run during business or production hours. The calibration process should be performed during scheduled maintenance intervals or non-business hours.
- For Smart RF to provide effective recovery, RF planning must be performed to ensure overlapping coverage exists at the deployment site. Smart RF can only provide recovery when Access Points are deployed appropriately. Smart RF is not a solution, it's a temporary measure. Administrators need to determine the root cause of RF deterioration and fix it. Smart RF history/events can assist.

If a Smart RF managed radio is operating in WLAN mode on a channel requiring DFS, it will switch channels if radar is detected.

- If Smart RF is enabled, the radio picks a channel defined in the Smart RF policy
- If Smart RF is disabled, but a Smart RF policy is mapped, the radio picks a channels specified in the Smart RF policy
- If no SMART RF policy is mapped, the radio selects a random channel

If the radio is a dedicated sensor, it stops termination on that channel if a neighboring Access Points detects radar. The Access Point attempts to come back to its original channel (statically configured or selected by Smart RF) after the channel evacuation period has expired.

Change this behavior using a no dfs-rehome command from the controller or service platform CLI. This keeps the radio on the newly selected channel and prevents the radio from coming back to the original channel, even after the channel evacuation period.

6.6 MeshConnex Policy

MeshConnex is a mesh networking technology that is comparable to the 802.11s mesh networking specification. MeshConnex meshing uses a hybrid proactive/on-demand path selection protocol, similar to *Ad hoc On Demand Distance Vector* (AODV) routing protocols. This allows it to form efficient paths using multiple attachment points to a distribution WAN, or form purely ad-hoc peer-to-peer mesh networks in the absence of a WAN. Each device in the MeshConnex mesh proactively manages its own path to the distribution WAN, but can also form peer-to-peer paths on demand to improve forwarding efficiency. MeshConnex is not compatible with MiNT Based meshing, though the two technologies can be enabled simultaneously in certain circumstances.

MeshConnex is designed for large-scale, high-mobility outdoor mesh deployments. MeshConnex continually gathers data from beacons and transmission attempts to estimate the efficiency and throughput of each MP-to-MP link. MeshConnex uses this data to dynamically form and continually maintain paths for forwarding network frames.

In MeshConnex systems, a *mesh point* (MP) is a virtual mesh networking instance on a device, similar to a WLAN AP. On each device, up to 4 MPs can be created and 2 can be created per radio. MPs can be configured to use one or both radios in the device. If the MP is configured to use both radios, the path selection protocols will continually select the best radio to reach each destination. Each MP participates in a single Mesh Network, defined by the MeshID. The MeshID is typically a descriptive network name, similar to the SSID of a WLAN. All MPs configured to use the same MeshID attempt to form a mesh and interoperate. The MeshID allows overlapping mesh networks to discriminate and disregard MPs belonging to different networks.

To define a MeshConnex policy:

1 Select **Configuration** > **Wireless** > **MeshConnex Policy** to display existing MeshConnex policies.

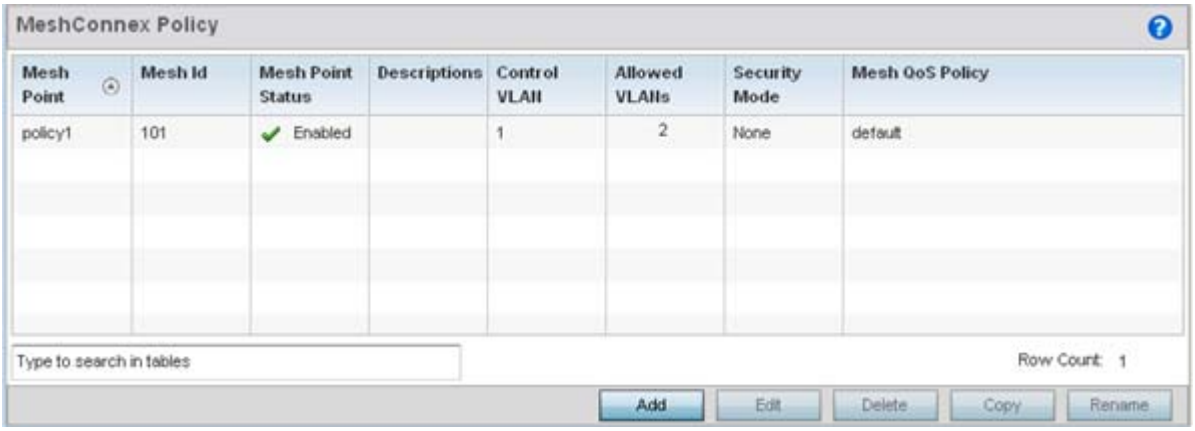


Figure 6-48 *MeshConnex Policy screen*

2 Refer to the following configuration data for existing MeshConnex policies:

Mesh Point Name	Displays the administrator assigned name of each listed mesh point.
Mesh ID	Displays the IDs (mesh identifiers) assigned to mesh points.
Mesh Point Status	Specified the status of each configured mesh point (either *Enabled* or *Disabled*).
Descriptions	Displays any descriptive text provided by the administrator for each configured mesh point.

Control VLAN	Displays the VLAN (virtual interface ID) for the control VLAN on each of the configured mesh points.
Allowed VLANs	Displays the list of VLANs allowed on each configured mesh point.
Security Mode	Displays the security assigned to each configured mesh point. The field displays *None* for no security or *PSK* for pre-shared key authentication.
Mesh QoS Policy	Displays the mesh Quality of Service policy associated to each configured mesh point.

3 Select **Add** to create a new MeshConnex policy, **Edit** to modify the attributes of a existing policy or **Delete** to remove obsolete policies from the list of those available. Optionally **Copy** or **Rename** a policy as needed.

The **Configuration** screen displays by default for the new or modified MeshConnex policy.

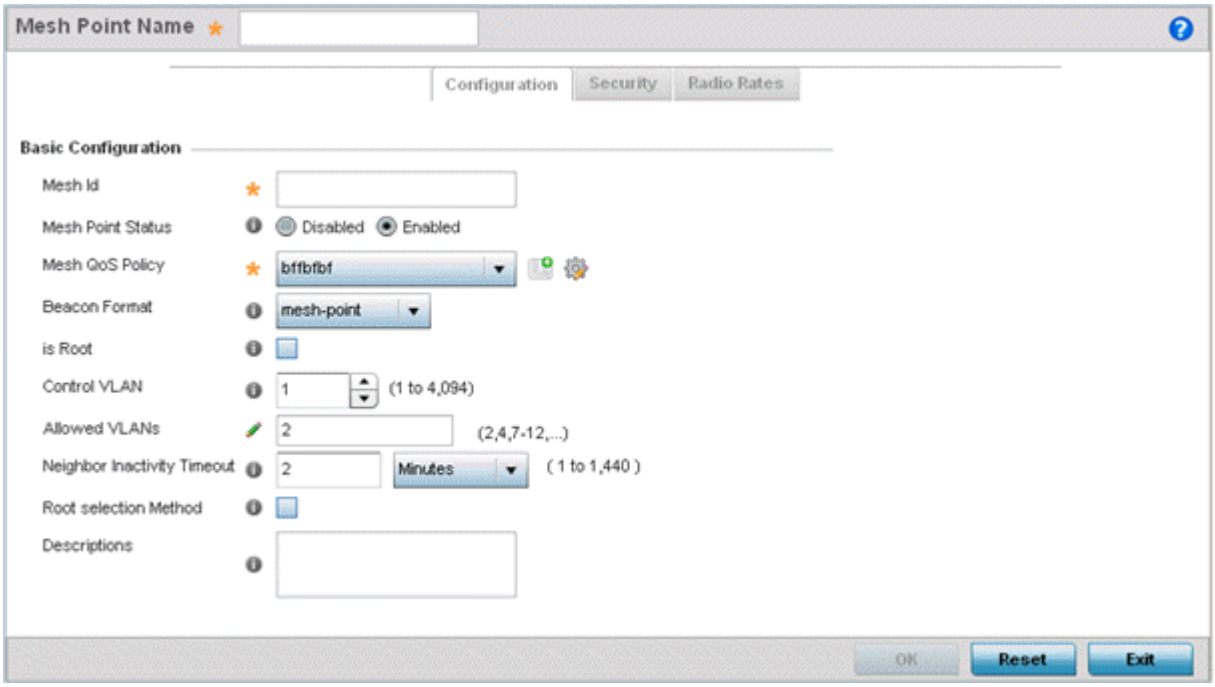


Figure 6-49 *MeshConnex Configuration screen*

4 Refer to the **Basic Configuration** field to define a MeshConnex configuration.

Mesh Point Name	Specify a name for the new mesh point. The name should be descriptive to easily differentiate it from other mesh points. This field is mandatory.
Mesh Id	Specify a 32 character maximum mesh identifier for this mesh point. This field is optional.
Mesh Point Status	To enable this mesh point, click the *Enabled* radio button. To disable the mesh point click the Disabled button.The default value is enabled.
Mesh QoS Policy	Use the drop-down menu to specify the mesh Quality of Service policy to use on this mesh point. This value is mandatory. If no suitable Mesh QoS policies exist, click the create icon to create a new Mesh QoS policy.
Beacon Format	Use the drop-down menu to specify the format for beacon transmissions. To use Access Point style beacons, select *access-point* from the drop-down menu. To use mesh point style beacons, select *mesh-point*. The default value is mesh-point.

Is Root	Select this option to specify the mesh point as a root in the mesh topology.
Control VLAN	Use the spinner control to specify a VLAN to carry meshpoint control traffic. The valid range for control VLAN is between 1 and 4094. The default value is VLAN 1.
Allowed VLANs	Specify the VLANs allowed to pass traffic on the mesh point. Separate all VLANs with a comma. To specify a range of allowed VLANs separate the starting VLAN and the ending VLAN with a hyphen.
Neighbor Inactivity Timeout	Specify a timeout in *seconds*, *minutes*, *hours* or *days,* up to a maximum of 1 day. This represents the allowed interval between frames received from a neighbor before their client privileges are revoked. The default value is 2 minutes.
Description	Enter a 64 character maximum description about the mesh point configuration.

5 Select **OK** to update the MeshConnex Configuration settings for this policy. Select **Reset** to revert to the last saved configuration.

6 Select the **Security** tab.

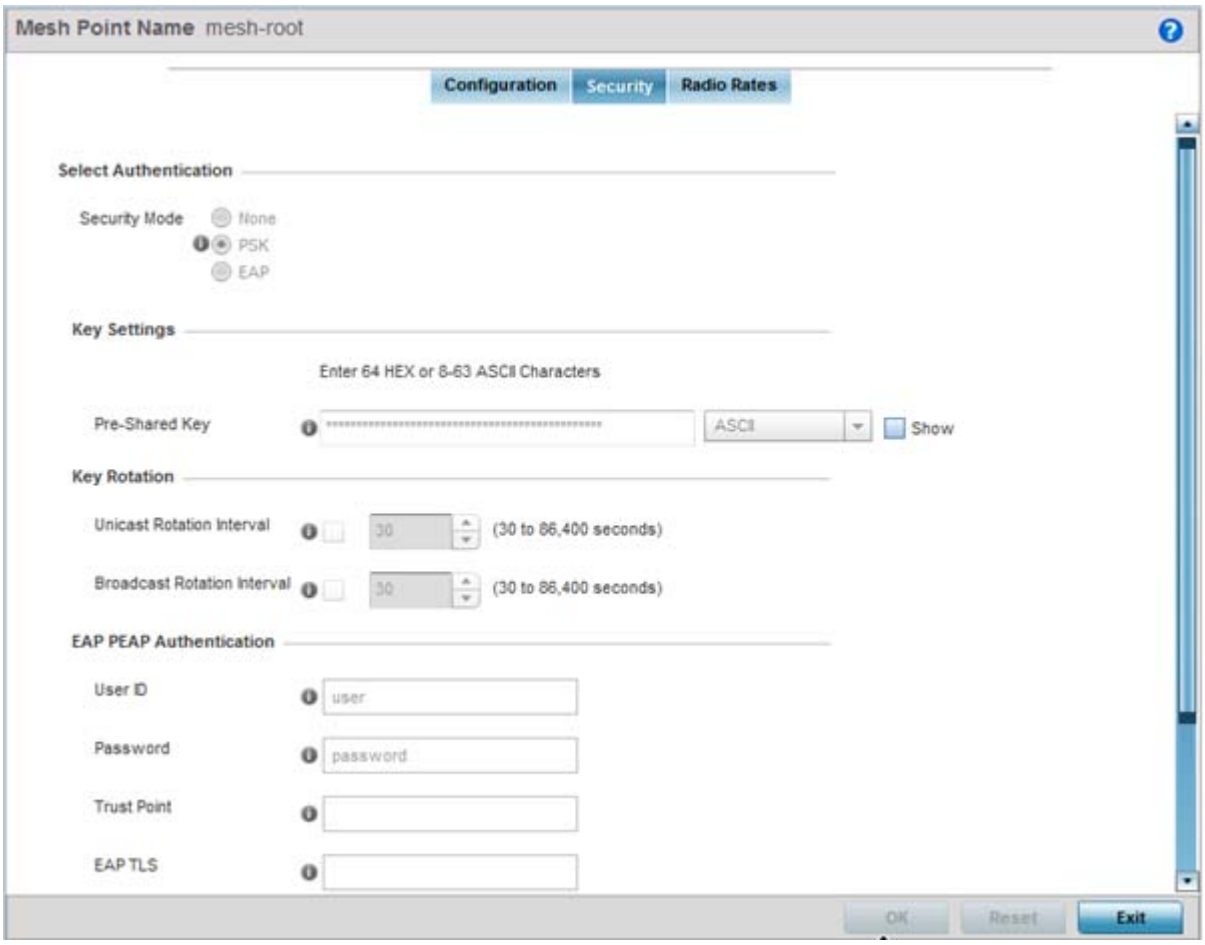


Figure 6-50 *MeshConnex Security screen*

7 Refer to the **Select Authentication** field to define an authentication method for the mesh policy.

Security Mode	Select a security authentication mode for the mesh point. Select *None* to have no authentication for the mesh point. Select *EAP* to use a secured credential exchange, dynamic keying and strong encryption. If selecting EAP, refer to the *EAP PEAP Authentication* field at the bottom of the screen and define the credentials of an EAP user and trustpoint. Select *PSK* to set a pre-shared key as the authentication for the mesh-point. If PSK is selected, enter a pre-shared key in the *Key Settings* field.

8 Set the following **Key Settings** for the mesh point:

Pre-Shared Key	When the security mode is set as PSK, enter a 64 character HEX or an 8-63 ASCII character passphrase used for authentication on the mesh point.

9 Set the following **Key Rotation** for the mesh point:

Unicast Rotation Interval	Define an interval for unicast key transmission (30 -86,400 seconds).
Broadcast Rotation Interval	When enabled, the key indices used for encrypting/decrypting broadcast traffic is alternatively rotated based on the defined interval. Define an interval for broadcast key transmission in seconds (30-86,400). Key rotation enhances the broadcast traffic security on the WLAN.

10 Set the following **EAP PEAP Authentication** settings if using EAP to secure the mesh point:

User ID	Create a 32 character maximum user name for a peap-mschapv2 authentication credential exchange.
Password	Define a 32 character maximum password for the EAP PEAP username created above.
Trust Point	Provide the 64 character maximum name of the trustpoint used for installing the CA certificate and validating the server certificate.
EAP TLS	Provide the 64 character maximum name of the trustpoint used for installing the client certificate, client private key and CA certificate.
Type	Use the drop-down menu to select the EAP authentication method used by the supplicant. The default EAP type is PEAP-MS-CHAPv2.
EAP Identity	Enter the 32 character maximum identity string used during phase 1 authentication. This string does not need to represent the identity of the user, rather an anonymous identity string.
AAA Policy	Select an existing AAA Policy from the drop-down menu to apply to this user's mesh point EAP configuration. *Authentication, authorization,* and *accounting* (AAA) is a framework for intelligently controlling access to the network, enforcing user authorization policies and auditing and tracking usage. These combined processes are central for securing wireless client resources and wireless network data flows.

11 Select **OK** to save the changes made to the configuration. Select **Reset** to revert to the last saved configuration.

12 Select the **Radio Rates** tab.

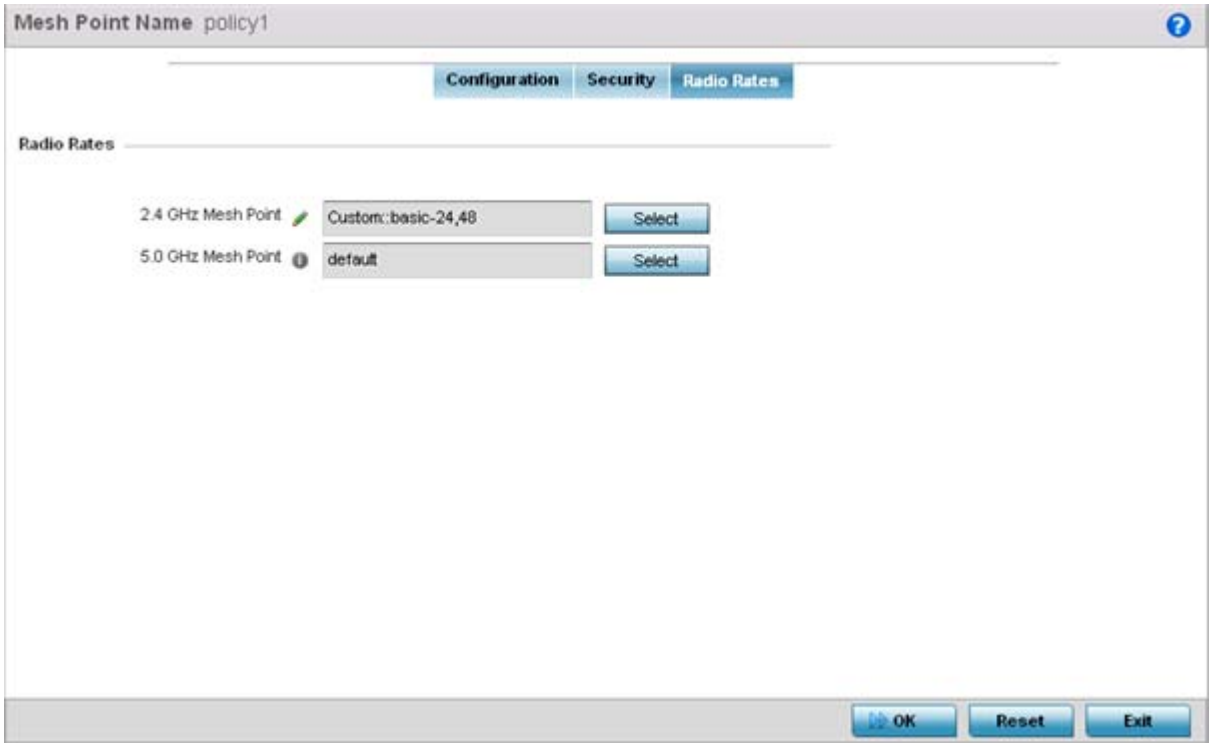


Figure 6-51 *Radio Rate Settings*

13 Set the following **Radio Rates** for both the 2.4 and 5 GHz radio bands:

2.4 GHz Mesh Point	Click the *Select* button to configure radio rates for the 2.4 GHz band. Define both minimum Basic and optimal Supported rates as required for the 802.11b rates, 802.11g rates and 802.11n rates supported by the 2.4 GHz band. These are the rates wireless client traffic is supported within this mesh point. If supporting 802.11n, select a Supported MCS index. Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Mesh points can communicate as long as they support the same basic MCS (as well as non-11n basic rates). The selected rates apply to associated client traffic within this mesh point only.
5.0 GHz Mesh Point	Click the *Select* button to configure radio rates for the 5.0 GHz band. Define both minimum Basic and optimal Supported rates as required for 802.11a and 802.11n rates supported by the 5.0 GHz radio band. These are the rates wireless client traffic is supported within this mesh point. If supporting 802.11n, select a Supported MCS index. Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Mesh points can communicate as long as they support the same basic MCS (as well as non-11n basic rates). The selected rates apply to associated client traffic within this mesh point only.

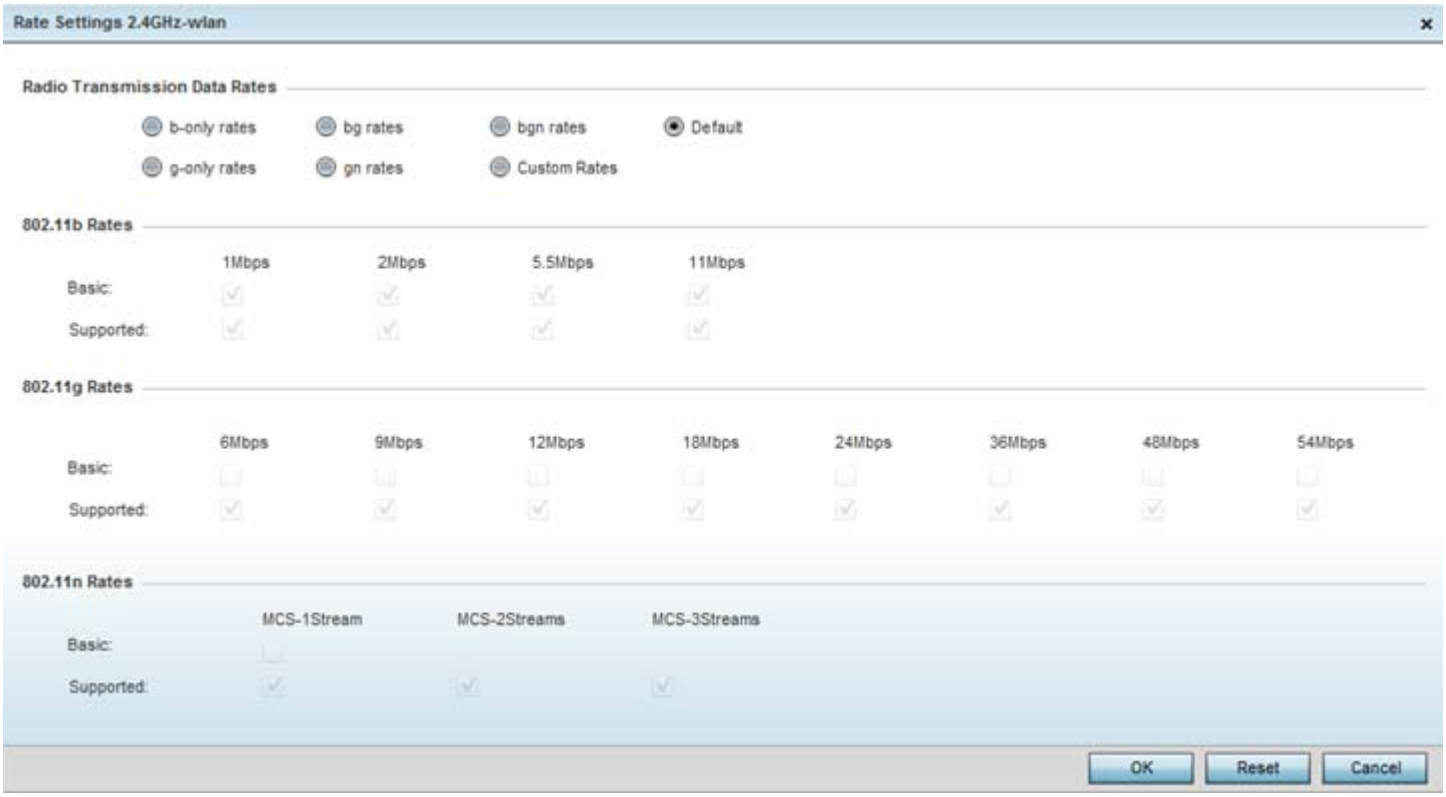


Figure 6-52 *Advanced Rate Settings 2.4 GHz screen*

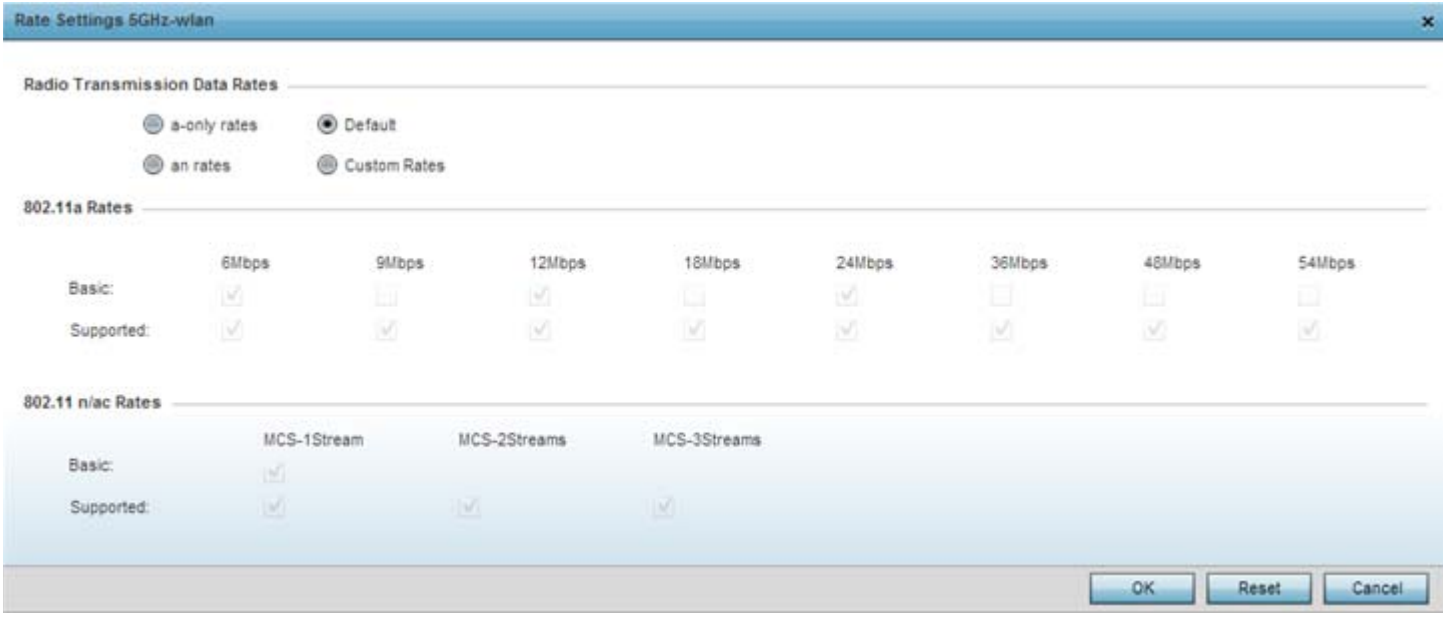


Figure 6-53 *Advanced Rate Settings 5 GHz screen*

Define both minimum *Basic* and optimal *Supported* rates as required for the 802.11b rates, 802.11g rates and 802.11n rates supported by the 2.4 GHz band and 802.11a and 802.11n rates supported by the 5.0 GHz radio band. These are the rates wireless client traffic is supported within this mesh point.

If supporting 802.11n, select a Supported MCS index. Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal

combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).

14 Select **OK** to save the changes made to the configuration. Select **Reset** to revert to the last saved configuration.

6.7 Mesh QoS Policy

Mesh *Quality of Service* (QoS) provides a data traffic prioritization scheme. QoS reduces congestion from excessive traffic. If there is enough bandwidth for all users and applications (unlikely because excessive bandwidth comes at a very high cost), then applying QoS has very little value. QoS provides policy enforcement for mission-critical applications and/or users that have critical bandwidth requirements when bandwidth is shared by different users and applications.

Mesh QoS helps ensure each mesh point on the mesh network receives a fair share of the overall bandwidth, either equally or as per the proportion configured. Packets directed towards clients are classified into categories such as video, voice and data. packets within each category are processed based on the weights defined for each mesh point.

The Quality of Service screen displays a list of Mesh QoS policies available to mesh points. Each mesh QoS policy can be selected to edit its properties. If none of the exiting Mesh QoS policies supports an ideal QoS configuration for the intended data traffic of this mesh point, select the Add button to create new policy. Select an existing mesh QoS policy and select **Edit** to change the properties of the Mesh QoS policy.

To define a Mesh QoS policy:

1 Select **Configuration** > **Wireless** > **Mesh QoS Policy** to display existing Mesh QoS policies.

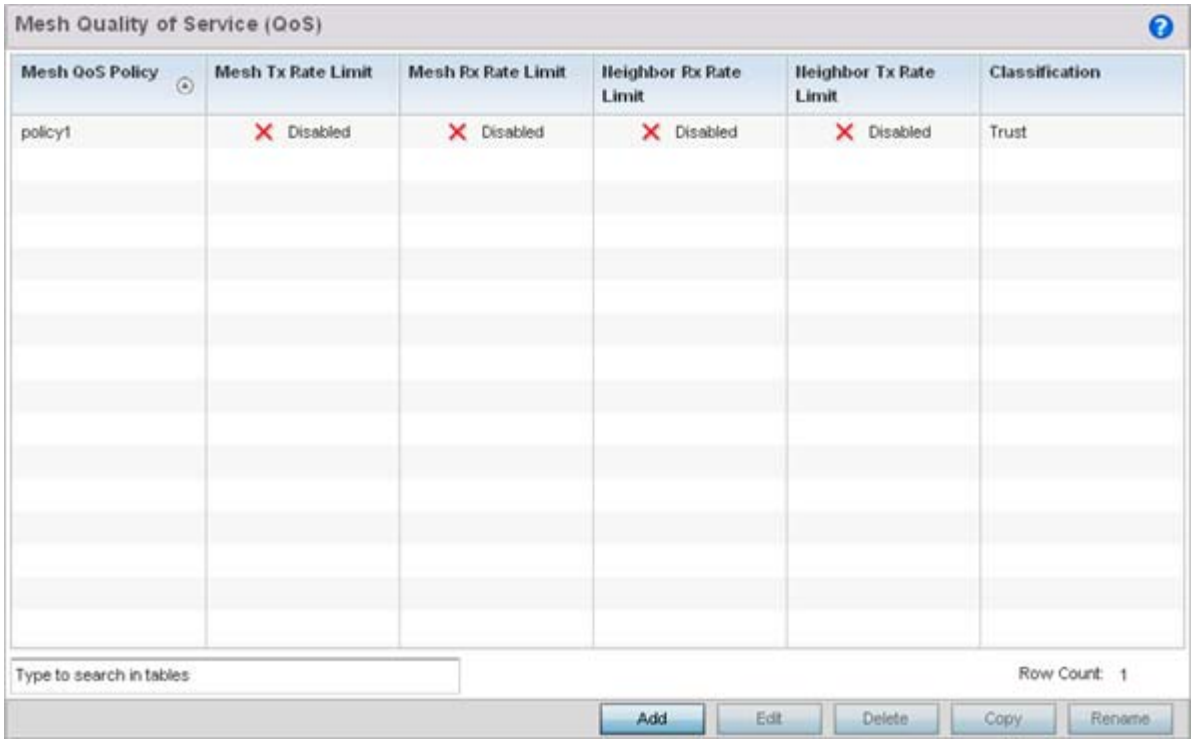


Figure 6-54 *Mesh QoS Policy screen*

2 Refer to the following configuration data for existing Smart RF policies:

Mesh QoS Policy	Displays the administrator assigned name of each mesh QoS policy.
Mesh Tx Rate Limit	Displays whether or not a *Mesh Tx Rate Limit* is enabled for each Mesh QoS policy. When the rate limit is enabled a green check mark is displayed, when it is disabled a red X is displayed.
Mesh Rx Rate Limit	Displays whether or not a *Mesh Rx Rate Limit* is enabled for each Mesh QoS policy. When the rate limit is enabled a green check mark is displayed, when it is disabled a red X is displayed.
Neighbor Rx Rate Limit	Displays whether or not a *Neighbor Rx Rate Limit* is enabled for each Mesh QoS policy. When the rate limit is enabled a green check mark is displayed, when it is disabled a red X is displayed.
Neighbor Tx Rate Limit	Displays whether or not a *Neighbor Tx Rate Limit* is enabled for each Mesh QoS policy. When the rate limit is enabled a green check mark is displayed, when it is disabled a red X is displayed.
Classification	Displays the forwarding QoS classification for each Mesh QoS policy. Classification types are *Trust*, *Voice, Video, Best Effort* and *Background*.

3 Select the **Add** button to define a new Mesh QoS policy, or select an existing Mesh QoS policy and select **Edit** to modify its existing configuration. Existing QoS policies can be selected and deleted as needed. Optionally **Copy** or **Rename** a policy as needed.

The **Rate Limit** screen displays by default for the new or modified QoS policy.

Excessive traffic can cause performance issues or bring down the network entirely. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that has infected on one or more devices at the branch. Rate limiting limits the maximum rate sent to or received from the wireless network (and mesh point) per neighbor. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. An administrator can set separate QoS rate limit configurations for data transmitted from the network and data transmitted from a mesh point's neighbor back to their associated Access Point radios and managing controller or service platform.

Before defining rate limit thresholds for mesh point transmit and receive traffic, define the normal number of ARP, broadcast, multicast and unknown unicast packets that typically transmit and receive from each supported WMM access category. If thresholds are defined too low, normal network traffic (required by end-user devices) is dropped, resulting in intermittent outages and performance problems.

A connected neighbor can also have QoS rate limit settings defined in both the *transmit* and *receive* direction.

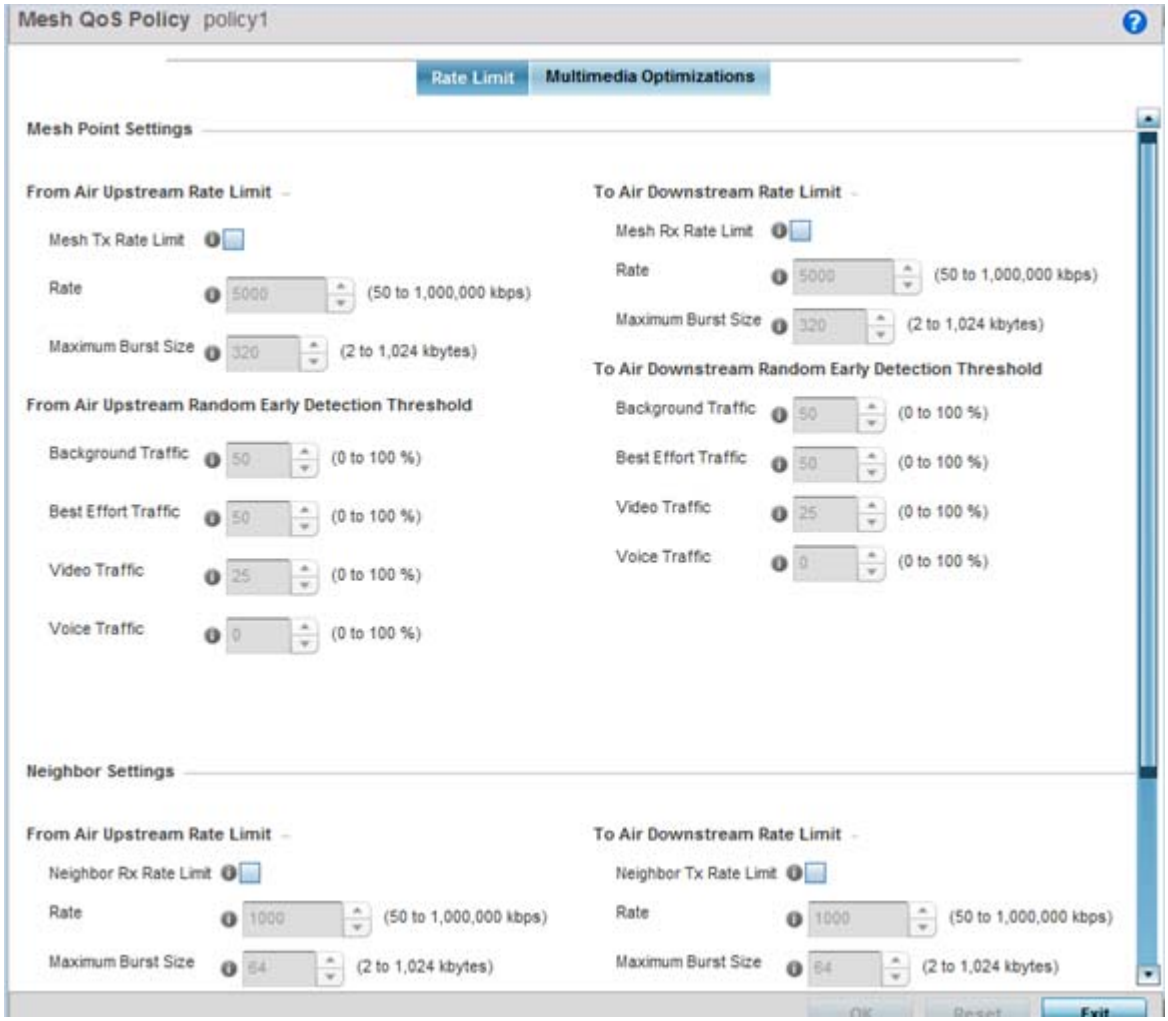


Figure 6-55 *Mesh QoS Policy Rate Limit screen*

4 Configure the following parameters in respect to the intended **From Air Upstream Rate Limit,** or traffic from the controller to associated Access Point radios and their associated neighbor:

Mesh Tx Rate Limit	Select the check box to enable rate limiting for all data received from any mesh point in the mesh network. This feature is disabled by default.
Rate	Define a receive rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the mesh point (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.
Maximum Burst Size	Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the transmit packet transmission will result in congestion for the mesh point's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a 10% margin (minimally) to allow for traffic bursts at the site. The default burst size is 320 kbytes.

5 Set the following **From Air Upstream Random Early Detection Threshold** settings for each access category. An early random drop is done when a traffic stream falls below the set threshold.

Background Traffic	Set a percentage value for background traffic in the transmit direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
Best Effort Traffic	Set a percentage value for best effort traffic in the transmit direction. This is a percentage of the maximum burst size for normal priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
Video Traffic	Set a percentage value for video traffic in the transmit direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.
Voice Traffic	Set a percentage value for voice traffic in the transmit direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%.

6 Configure the following parameters in respect to the intended **To Air Downstream Rate Limit,** or traffic from neighbors to associated Access Point radios and the controller or service platform:

Mesh Rx Rate Limit	Select the check box to enable rate limiting for all data transmitted by the device to any mesh point in the mesh. This feature is disabled by default.
Rate	Define an transmit rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the mesh point (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.
Maximum Burst Size	Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the receive packet transmission will result in congestion for the mesh points wireless client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should then add a minimum of a 10% margin to allow for traffic bursts at the site. The default burst size is 320 kbytes.

7 Set the following **To Air Downstream Random Early Detection Threshold** settings for each access category. An early random drop occurs when the amount of tokens for a traffic stream falls below the set threshold.

Background Traffic	Set a percentage value for background traffic in the receive direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped and a log message is generated. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general receive rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
Best Effort Traffic	Set a percentage value for best effort traffic in the receive direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general receive rate is known by the network administrator (using a time trend analysis). The default threshold is 50%.
Video Traffic	Set a percentage value for video traffic in the receive direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped and a log message is generated. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general receive rate is known by the network administrator (using a time trend analysis). The default threshold is 25%.
Voice Traffic	Set a percentage value for voice traffic in the receive direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped and a log message is generated. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general transmit rate is known by the network administrator (using a time trend analysis). The default threshold is 0%. 0% means no early random drops will occur.

8 Configure the following parameters in respect to the intended Neighbor Settings **From Air Upstream Rate Limit**:

Neighbor Rx Rate Limit	Select the radio button to enable rate limiting for data transmitted from the client to its associated Access Point radio and connected controller or service platform. Enabling this option does not invoke client rate limiting for data traffic in the receive direction. This feature is disabled by default.
Rate	Define an transmit rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped by the client and a log message is generated. The default rate is 1,000 kbps.
Maximum Burst Size	Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the transmit packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.

9 Set the following Neighbor Settings **From Air Upstream Random Early Detection Threshold** for each access category:

Background Traffic	Set a percentage value for background traffic in the transmit direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.
Best Effort Traffic	Set a percentage value for best effort traffic in the transmit direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 50%.
Video Traffic	Set a percentage value for video traffic in the transmit direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 25%.
Voice Traffic	Set a percentage value for voice traffic in the receive direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 0%.0% implies no early random drops will occur.

10 Configure the following parameters in respect to the intended Neighbor **To Air Downstream Rate Limit,** or traffic from a controller or service platform to associated Access Point radios and the wireless client:

Neighbor Tx Rate Limit	Select the radio button to enable rate limiting for data transmitted from connected wireless clients. Enabling this option does not invoke rate limiting for data traffic in the transmit direction. This feature is disabled by default.
Rate	Define a receive rate limit between 50 - 1,000,000 kbps.This limit constitutes a threshold for the maximum the number of packets transmitted or received by the client. Traffic that exceeds the defined rate is dropped and a log message is generated. The default rate is 1,000 kbytes.
Maximum Burst Size	Set a maximum burst size between 2 - 64 kbytes. The smaller the burst, the less likely the receive packet transmission will result in congestion for the wireless client. The default burst size is 64 kbytes.

11 Set the following **To Air Downstream Random Early Detection** settings for each access category:

Background Traffic	Set a percentage value for background traffic in the receive direction. This is a percentage of the maximum burst size for low priority traffic. Background traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default is 50%.
Best Effort Traffic	Set a percentage value for best effort traffic in the receive direction. This is a percentage of the maximum burst size for normal traffic. Best effort traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default is 50%.
Video Traffic	Set a percentage value for video traffic in the receive direction. This is a percentage of the maximum burst size for video traffic. Video traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default is 25%.

Voice Traffic	Set a percentage value for voice traffic in the receive direction. This is a percentage of the maximum burst size for voice traffic. Voice traffic exceeding the defined threshold is dropped by the client and a log message is generated. The default threshold is 0%.0% means no early random drops occur.

12 Select **OK** when completed to update this Mesh QoS rate limit settings. Select **Reset** to revert the screen back to its last saved configuration.

13 Select the **Multimedia Optimizations** tab.

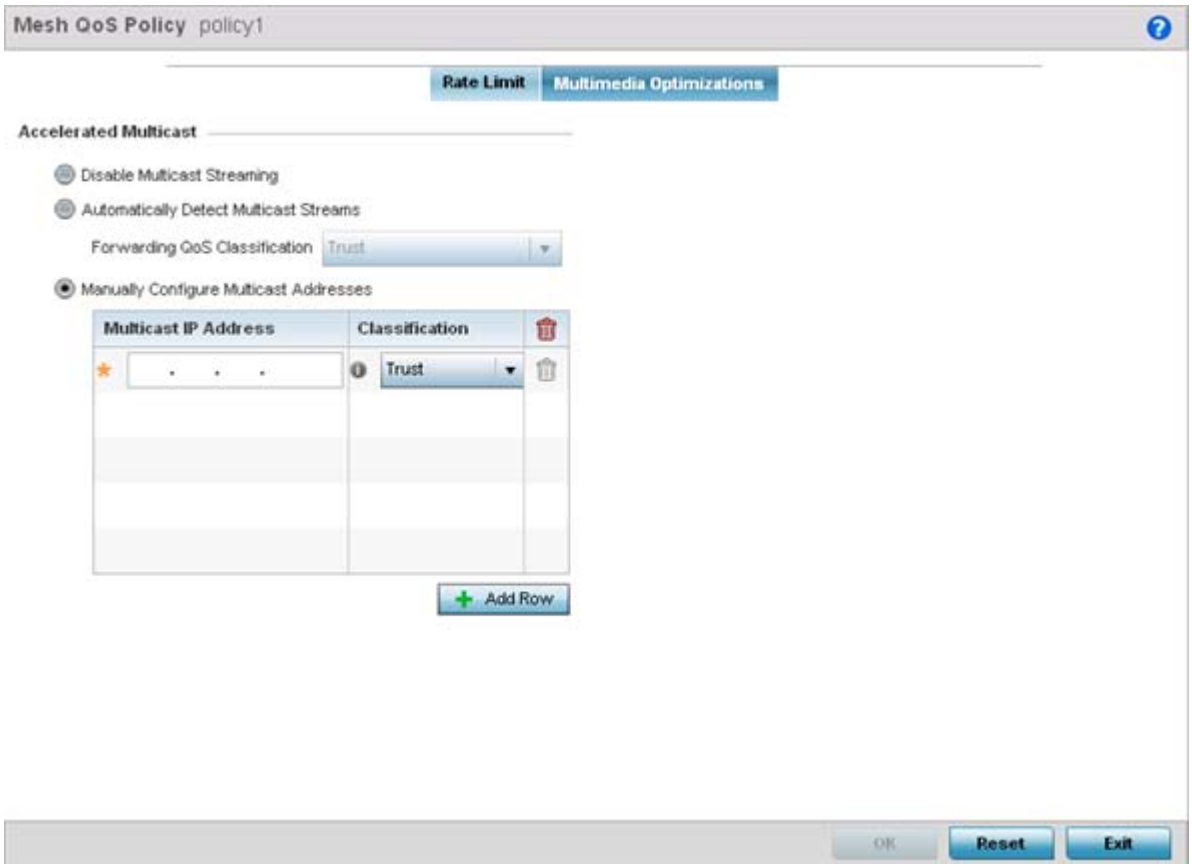


Figure 6-56 *Mesh QoS Policy Multimedia Optimizations screen*

14 Set the following **Accelerated Multicast** settings:

Disable Multicast Streaming	Select this option to disable all Multicast Streaming on the mesh point.
Automatically Detect Multicast Streams	Select this option to allow the administrator to have multicast packets that are being bridged converted to unicast to provide better overall airtime utilization and performance. The administrator can either have the system automatically detect multicast streams and convert all detected multicast streams to unicast, or specify which multicast streams are to be converted to unicast. When the stream is converted and being queued up for transmission, there are a number of classification mechanisms that can be applied to the stream and the administrator can select what type of classification they would want. Classification types are *Trust, Voice*, *Video*, *Best Effort*, and *Background*.

Manually Configure Multicast Addresses	Select *+ Add Row* and specify a list of multicast addresses and classifications. Packets are accelerated when the destination addresses matches.

15 Select **OK** when completed to update the Mesh Multimedia Optimizations settings. Select **Reset** to revert the screen back to its last saved configuration.

6.8 Passpoint Policy

A *passpoint* policy provides an interoperable platform for streamlining Wi-Fi access to Access Points deployed as public hotspots. Passpoint is supported across a wide range of wireless network deployment scenarios and client devices.

Passpoint makes connecting to Wi-Fi networks easier by authenticating the user with an account based on an existing relationship, such as the user's mobile carrier or broadband ISP.

The Passpoint Policy screen displays a list of passpoint polices for network hotspots. Each passpoint policy can be selected to edit its properties. If no exiting passpoint policies supports the required deployment, select Add to create a new policy.

To administrate and manage existing passpoint policies:

1 Select **Configuration** > **Wireless** > **Passpoint Policy** to display existing policies.

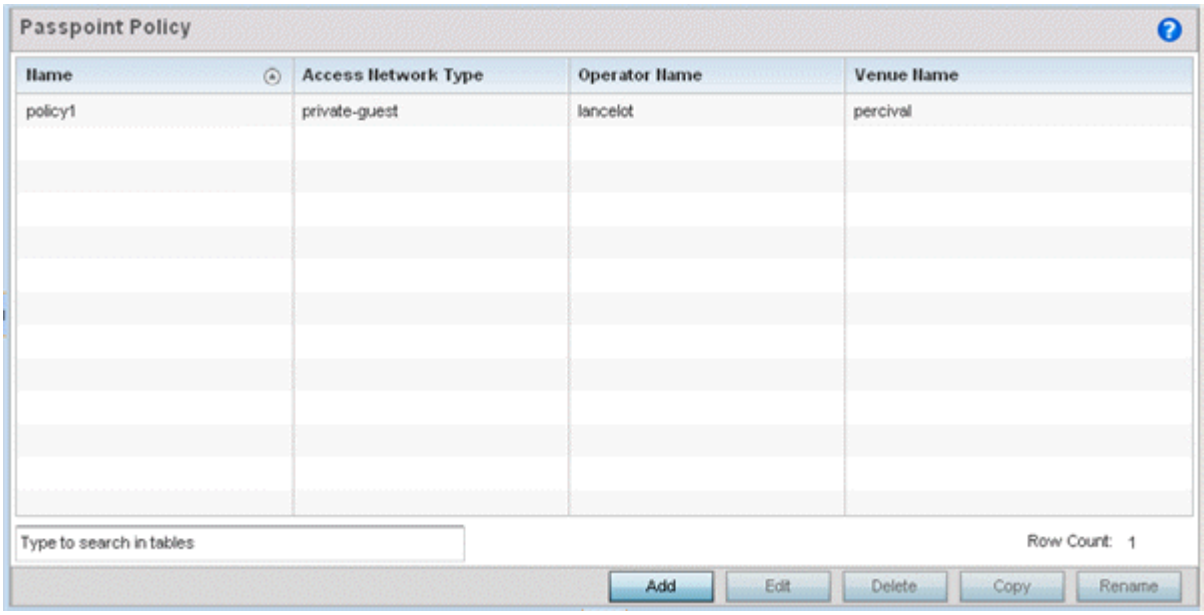


Figure 6-57 *Passpoint Policy screen*

2 Refer to the following configuration data for existing passpoint policies:

Name	Displays the administrator assigned name of each passpoint policy.
Access Network Type	Displays the network access permissions the administrator has set for the passpoint policy.
Operator Name	Displays the unique name assigned to the administrator or operator responsible for the configuration and operation of the Access Point managed hotspot.

Venue Name	Displays the administrator assigned name of the venue (or physical location) of the deployed Access Point hotspot.

3 Select **Add** to define a new passpoint policy, or select an existing policy and select **Edit** to modify its configuration. Existing policies can be selected and deleted, copied, or renamed as needed. Optionally **Copy** or **Rename** a policy as needed.

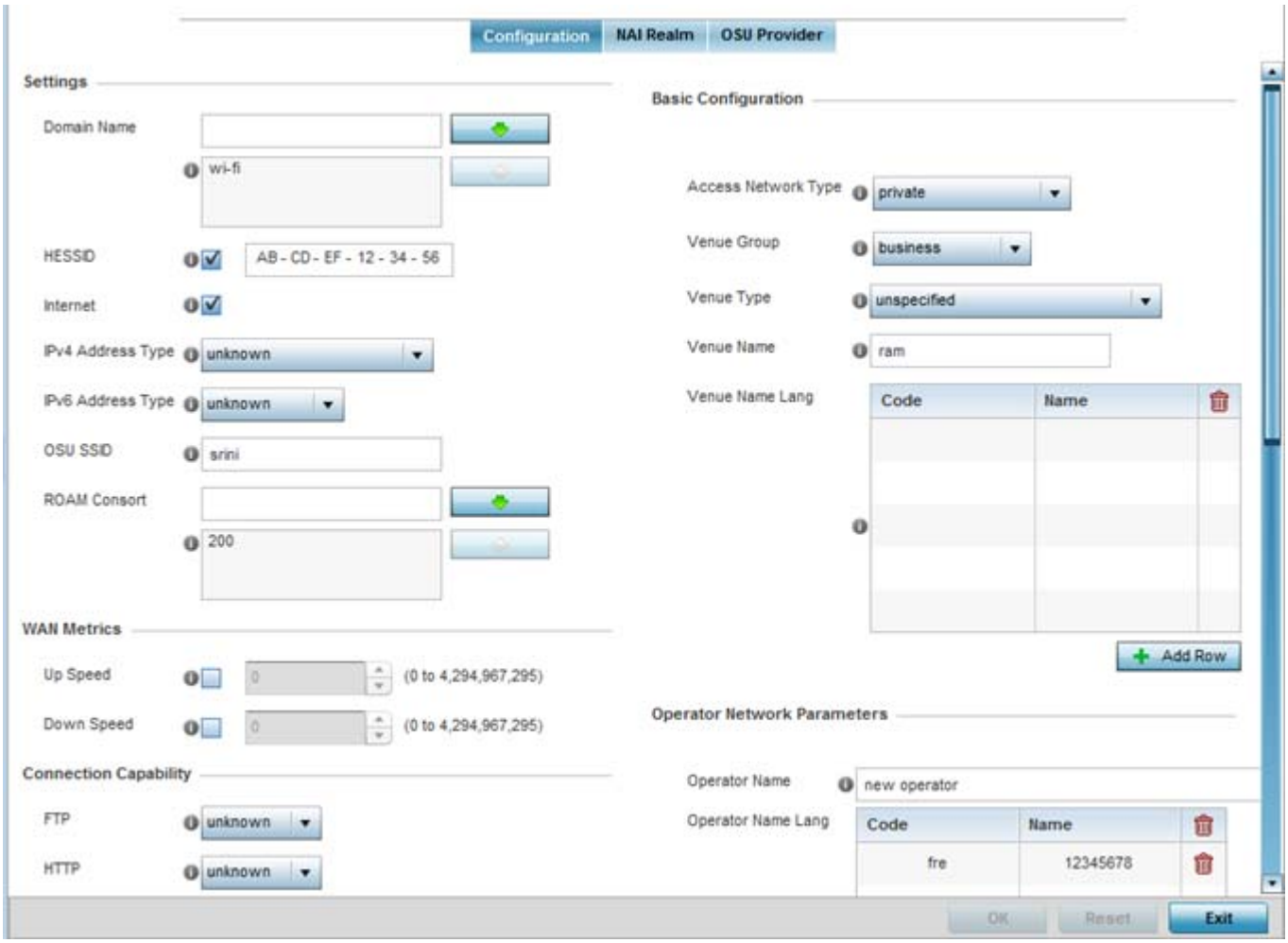


Figure 6-58 *Passpoint Policy - Configuration screen*

4 Refer to the following **Settings** to define an Internet connection medium for the passpoint policy:

Domain Name	Optionally add a 255 character maximum domain name to the pool available to the passpoint policy.
HESSID	Select this option to apply a homogenous ESS ID. Leaving this option blank applies the BSSID instead. This option is disabled by default.
Internet	Select this option to enable Internet access to users of the passpoint hotspot. Internet access is enabled by default.

IPv4 Address Type	Use the drop-down menu to select the IPv4 formatted address type for this passpoint policy. IPv4 is a connectionless protocol operating on a best effort delivery model. IPv4 does not guarantee delivery or assures proper sequencing or avoidance of duplicate delivery (unlike TCP). Options include, *not available, public, port-restricted, port-restricted-double-nat, single-nat, double-nat, port-restricted-single-nat* and *unknown*.
IPv6 Address Type	Use the drop-down menu to select the IPv4 formatted address type for this passpoint policy. IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. Options include, *available, unavailable* and *unknown*.
OSU SSID	Optionally define a 32 character maximum sign-on ID that must be correctly provided to access the passpoint policy's hotspot resources.
ROAM Consort	Provide a 0 - 255 character roaming consortium number. A roaming consort ID is sent as roaming consortium information in a hotspot query response.

5 Set the following **WAN Metrics** for upstream and downstream bandwidth:

Up Speed	Enable this option to estimate the maximum upstream bandwidth from 0 - 4,294,967,295 Kbps.
Down Speed	Enable this option to estimate the maximum downstream bandwidth from 0 - 4,294,967,295 Kbps.

6 Set the following **Connection Capability** for passpoint policy's **FTP, HTTP, ICMP, IPSec VPN, PPTP VPN, SIP, SSH** and **TLS VPN** interfaces:

7 Use the drop-down menu to define these interfaces as **open, closed** or **unknown** for this passpoint policy configuration. Disabling unused interfaces is recommended to close unnecessary security holes.

8 Select **+ Add Row** to set a **Connection Capability Variable** to make specific virtual ports **open** or **closed** for Wi-Fi connection attempts, set rules for how the user is to connect with routing preference using this passpoint policy.

9 Select **+ Add Row** and set a **Network Authentication Type** to select how Wi-Fi connection attempts are authenticated and validated using a dedicated redirection URL resource.

10 Refer to the **Basic Configuration** field to set the following:

Access Network Type	Use the drop-down menu to select the network access method for this passpoint policy. Access network types include: *private* – General access to a private network hotspot (default setting) *private-guest* – Access to a private network hotspot with guest services *chargeable-public* – Access to a public hotspot with billable services *personal-device* – Access to a hotspot for personal devices such as wireless routers *emergency services* – Dedicated network hotspot access for emergency services only

Venue Group	Passpoint is supported across a wide range of wireless network deployment scenarios and client devices. Select the group type best suited to the majority of hotspot requestors utilizing the passpoint policy's unique configuration.
Venue Type	Select the venue type best suited to the actual location passpoint requestors are located. If an adequate option cannot be applied, a numeric venue type can be utilized.
Venue Name	Enter the *Venue Name* and address. The operator can configure an Access Point to describe the location of the hotspot. This information typically includes the name and address of the deployment location where the hotspot is located. Enter the name and address configured for the Access Point hotspot. The name cannot exceed 252 characters.
Venue Name Lang	Hotspot operators can list venue names in multiple languages. Select the *+ Add Row* button to add venue name languages. Enter the two or three character ISO-14962-1997 encoded string that defines the language used in the *Code* field. Enter the name of the venue in the *Name* field. The name cannot exceed 252 characters.

11 Refer to the **Operator Network Parameters** field to define the following:

Operator Name	Provide the unique name (in English) of the administrator or operator responsible for the configuration and management or the hotspot. The name cannot exceed 64 characters.
Operator Name Lang	Operator names can be listed in multiple languages. Select *+ Add Row* to add operator name languages. Enter the two or three character ISO-14962-1997 encoded string defining the language used in the *Code* field. Enter the name of the operator in the *Name* field. The name cannot exceed 252 characters.
PLMNID	Operators providing mobile and Wi-Fi hotspot services have a unique *Public Land Mobile Network* (PLMN) ID. Select the *+ Add Row* button to add PLMN information for operators responsible for the configuration and operation of the hotspot. Provide a Description for the PLMN not exceeding 64 characters. Enter a three digit *Mobile Country Code* (MCC) and two digit *Mobile Network Code* (MNC) for the PLMN ID. The MCC identifies the region and country where the hotspot is deployed. The MNC identifies the operator responsible for the configuration and management of the hotspot by PLMN ID and country. Both the MCC and MNC fields are mandatory.

12 Select **OK** when completed to update the passpoint policy settings. Select **Reset** to revert the screen back to the last saved configuration.

13 Select the **NAI Realm** tab.

The *Network Access Identifier* (NAI) is the user identity submitted by the hotspot requesting client during authentication. The standard syntax is *user@realm*. NAI is frequently used when roaming, to identify the user and assist in routing an authentication request to the user's authentication server. The realm name is often the domain name of the service provider.

The NAI realm screen displays those realms created thus far for utilization with a passpoint policy.

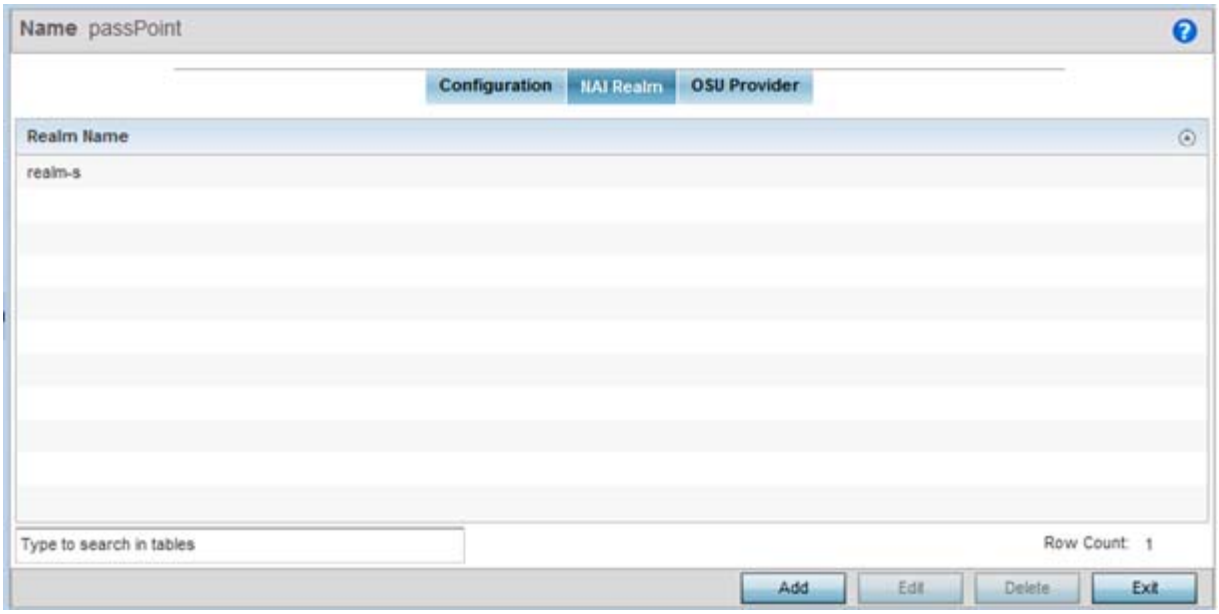


Figure 6-59 *Passpoint Policy - NAI Realm screen*

Either select **Add** to create a new NAI realm configuration for passpoint hotspot utilization, **Edit** to modify the attributes on an existing selected configuration or **Delete** to remove a selected configuration from those available. Provide a **Realm Name** or names (32 characters maximum) delimited by a semi colon. Select **+ Add Row** to create a **EAP Method** configuration for the NAI realm.

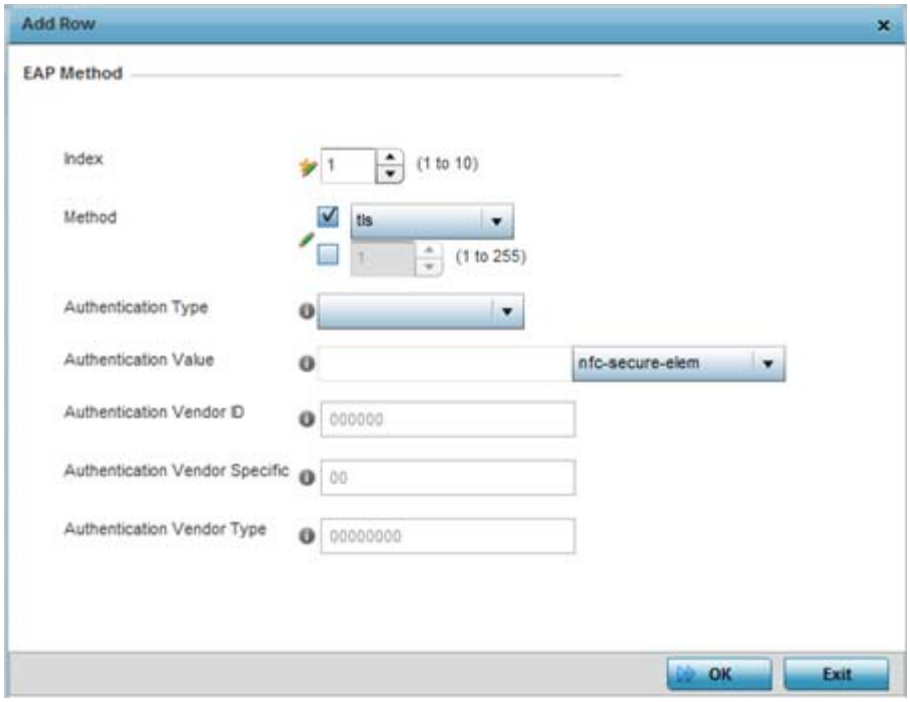


Figure 6-60 *Passpoint Policy - NAI Realm Add/Edit screen*

14 Set the following **EAP Method** attributes to secure the NAI realm used by the passpoint policy:

Index	Select an EAP instance index from 1 - 10 to apply to this hotspot's EAP credential exchange and verification session. NAIs are often user identifiers in the EAP authentication protocol.
Method	Set an EAP method for the NAI realm. Options include *identity, otp, gtc, rsa-public-key, tls, sim, ttls, peap, ms-auth, ms-authv2, fast, psk* and *ikev2*.
Authentication Type	Use the drop-menu to specify the EAP method authentication type. Options include *expanded-eap, non-eap-inner, inner-eap, expanded-inner-eap*, *credential*, *tunn-eap-credential* and *vendor*.
Authentication Value	If setting the authentication type to either *non-eap-inner, inner-eap, credential* or *tunnel-eap-credential* define an authentication value that must be shared with the EAP credential validation server resource.
Authentication Vendor ID	If the authentication type is set to either, *expanded-eap* or *expanded-inner-eap*, set a 6 character authentication vendor ID that must match the one utilized by the EAP server resource.
Authentication Vendor Specific	If required, add 2 - 510 character vendor specific authentication data required for the selected authentication type. Enter the value is an *a-FA -F0-9* format.
Authentication Vendor Type	Set a 8 character authentication vendor type used exclusively for the *expanded-eap* or *expanded-inner-eap* authentication types.

15 Select **OK** to save the updates to the NAI realm.

16 Select the **OSU Provider** tab.

WiNG managed clients can use Online Sign-Up (OSU) for registration and credential provisioning to obtain hotspot network access. Service providers have an OSU AAA server and certificate authority (CA). For a client and hotspot to trust one another, the OSU server holds a certificate signed by a CA whose root certificate is issued by a CA authorized by the Wi-Fi Alliance, and CA certificates are installed on the client device. A CA performs four functions:

- Issues certificates (creates and signs)
- Maintains certificate status information and issues *certificate revocation lists* (CRLs)
- Publishes current (non-expired) certificates and CRLs
- Maintains status archives for the expired or revoked certificates it has issued

Passpoint certificates are governed by the Hotspot 2.0 OSU Certificate Policy Specification. An OSU server certificate should be obtained from any of the CAs authorized by the Wi-Fi Alliance. Once an OSU provider is selected, the client connects to the OSU WLAN. It then triggers an HTTPS connection to the OSU server, which was received with the OSU providers list. The client validates the server certificate to ensure it's a trusted OSU server. The client is prompted to complete an online registration through their browser. When the client has a valid credential for the hotspot 2.0 WLAN, it disassociates from the OSU WLAN and connects to the hotspot 2.0 WLAN.

The OSU Provider screen displays those provider configurations created thus far for utilization with a passpoint policy.

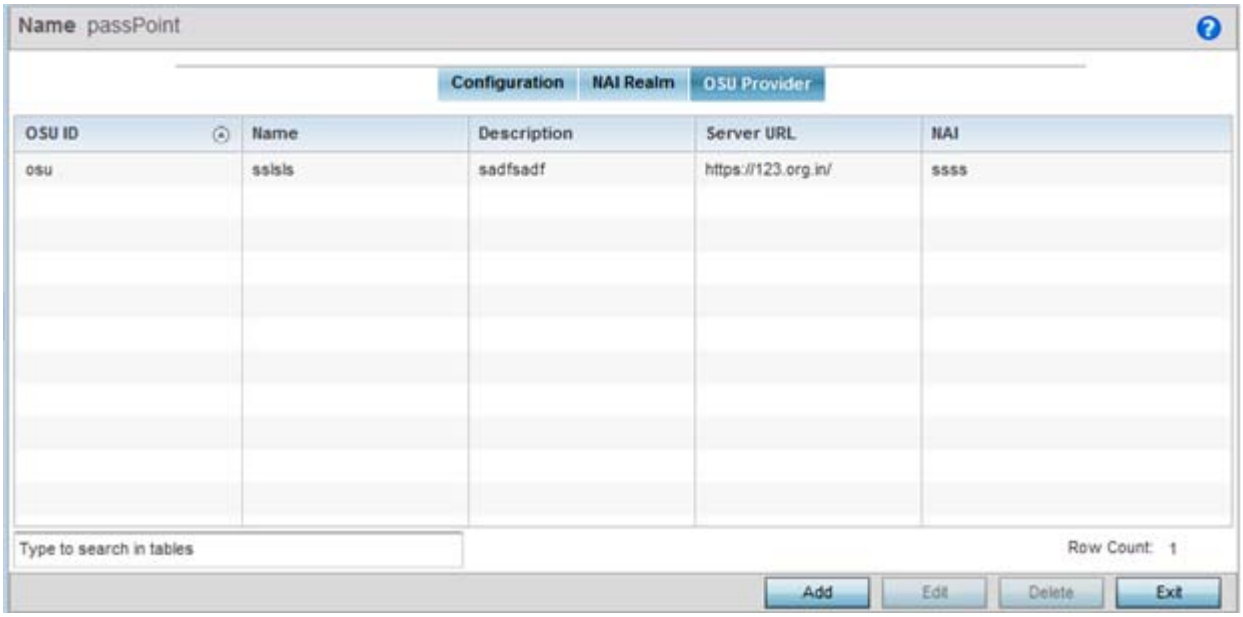


Figure 6-61 *Passpoint Policy - OSU Provider screen*

Either select **Add** to create a new OSU provider configuration for passpoint hotspot utilization, **Edit** to modify the attributes on an existing selected configuration or **Delete** to remove a selected configuration from those available.

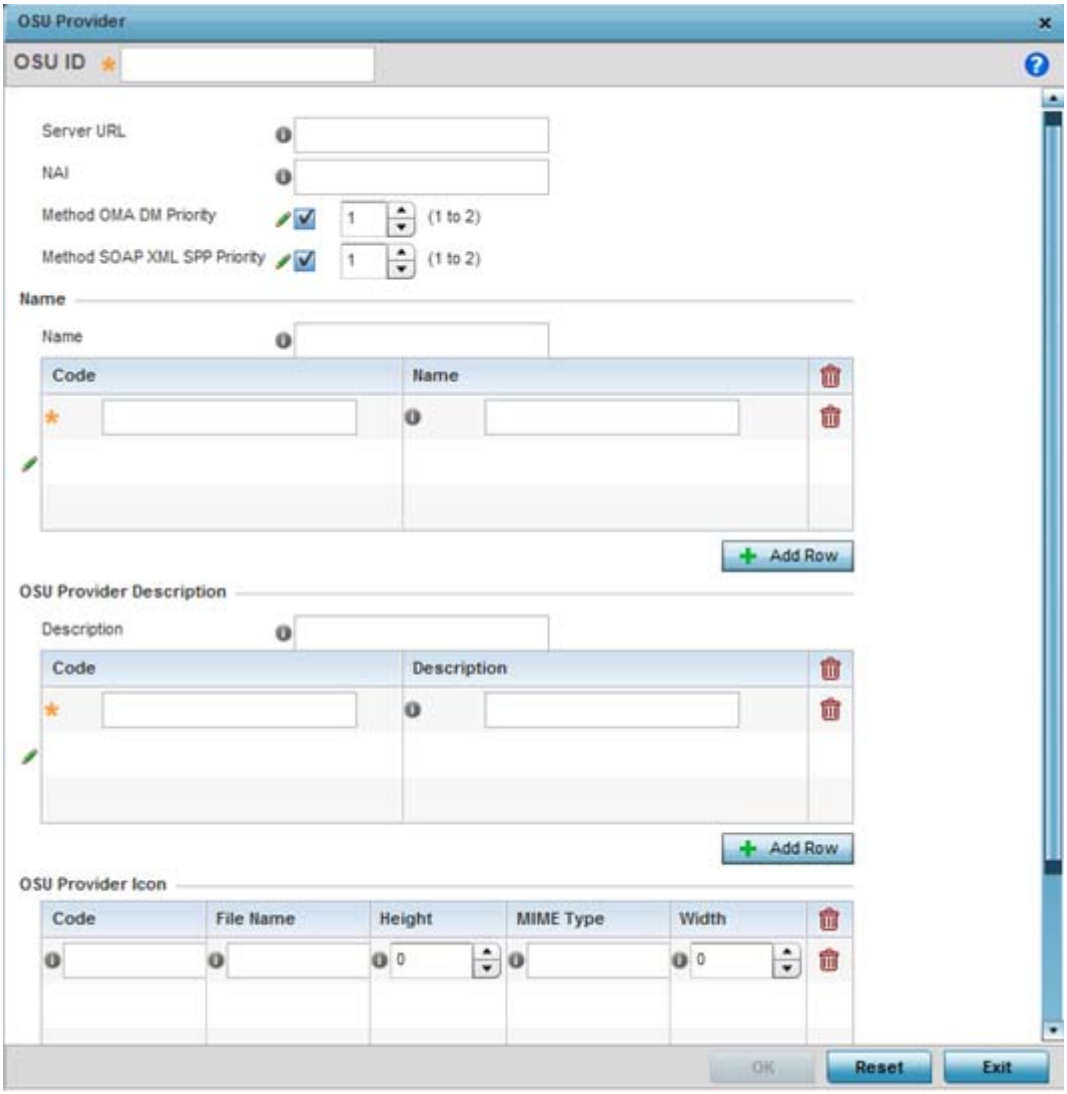


Figure 6-62 *Passpoint Policy - OSU Provider Add/Edit screen*

17 If creating a new OSU provider configuration, provide it a 32 character maximum **OSU ID** serving as an online sign up identifier.

18 Set the following attributes to secure the NAI realm used by the passpoint policy:

Server URL	Provide a 255 character maximum sign up server URL for the OSU provider.
NAI	Enter a 255 character maximum *Network Access Identifier* (NAI) to identify the user and assist in routing an authentication request to the authentication server. The realm name is often the domain name of the service provider
Method OMA DM Priority	Select this option to provide *open mobile alliance* (OMA) device management priority. The OMA is a standards body developing open standards for mobile clients. OMA is relevant to service providers working across countries (with different languages), operators and mobile terminals. Adherence to OMA is strictly voluntary. Use the drop-menu to specify the priority as 1 or 2.

Method SOAP XML SPP Priority	Select this option to apply a SOAP-XML subscription provisioning protocol priority of either 1 or 2. The *simple object access protocol* (SOAP) is a protocol for exchanging structured information in Web services. SOAP uses XML as its message format, and relies on other application layer protocols, like HTTP or SMTP for message negotiation and transmission.

19 Refer to the **Name** field to optionally set a 252 character English language sign up name, then provide a 3 character maximum ISO-639 language **Code** to apply the sign up name in a language other then English. Apply a 252 character maximum hexadecimal online sign up **Name** to encode in the ISO-639 language code applied to the sign up name.

20 Refer to the **OSU Provider Description** field to set an online sign up description in a language other then English.

Select **+ Add Row** and provide a 3 character maximum ISO-639 language **Code** to apply the sign up name in a language other then English. Apply a 252 character maximum hexadecimal online sign up **Description** to encode in the ISO-639 language code applied to the sign up name.

21 Optionally provide an **OSU Provider Icon** by selecting **+ Add Row**. Apply the following configuration attributes to the icon.

Code	Enter a 3 character maximum ISO-639 language *Code* to define the language used in the OSU provider icon.
File Name	Provide a 255 character maximum icon name and directory path location to the icon file.
Height	Provide the icon height size in pixels from 0 - 65,535. The default setting is 0.
MIME Type	Set the icon MIME file type from 0 - 64. The MIME associates filename extensions with a MIME type. A MIME enables a fallback on an extension and are frequently used by Web servers.
Width	Provide the icon width size in pixels from 0 - 65,535. The default setting is 0.

22 Select **OK** to save the updates to the OSU provider configuration. Select **Reset** to revert to the last saved configuration.

6.9 Sensor Policy

In addition to WIPS support, sensor functionality has now been added for Extreme Networks' MPact locationing system. The MPact system for Wi-Fi locationing includes WiNG controllers and Access Points functioning as sensors. Within the MPact architecture, sensors scan for RSSI data on an administrator defined interval and send to a dedicated MPact Server resource, as opposed to an ADSP server. The MPact Server collects the RSSI data from WiNG sensor devices, and calculates the location of Wi-Fi devices for MPact administrators.

To administrate and manage existing sensor policies:

1 Select **Configuration** > **Wireless** > **Sensor Policy** to display existing policies.

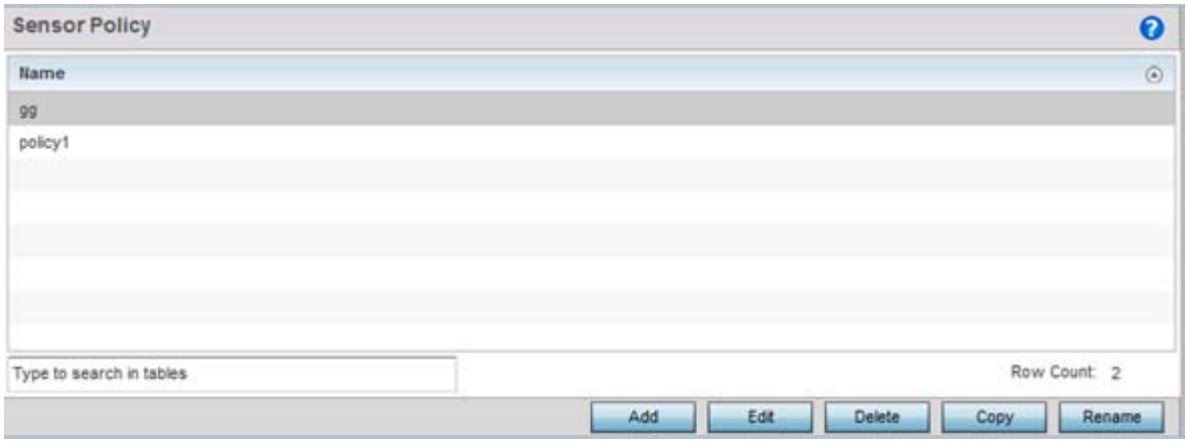


Figure 6-63 *Sensor Policy screen*

2 Select **Add** to define a new sensor policy, or select an existing policy and select **Edit** to modify its configuration. Existing sensor policies can be selected and deleted, copied, or renamed as needed.

NOTE: If a dedicated sensor is utilized with WIPS for rogue detection, any sensor policy selected from the Sensor Policy drop-down menu is discarded and not utilized by the sensor. To avoid this situation, use ADSP channel settings exclusively to configure the sensor and not the WiNG interface.

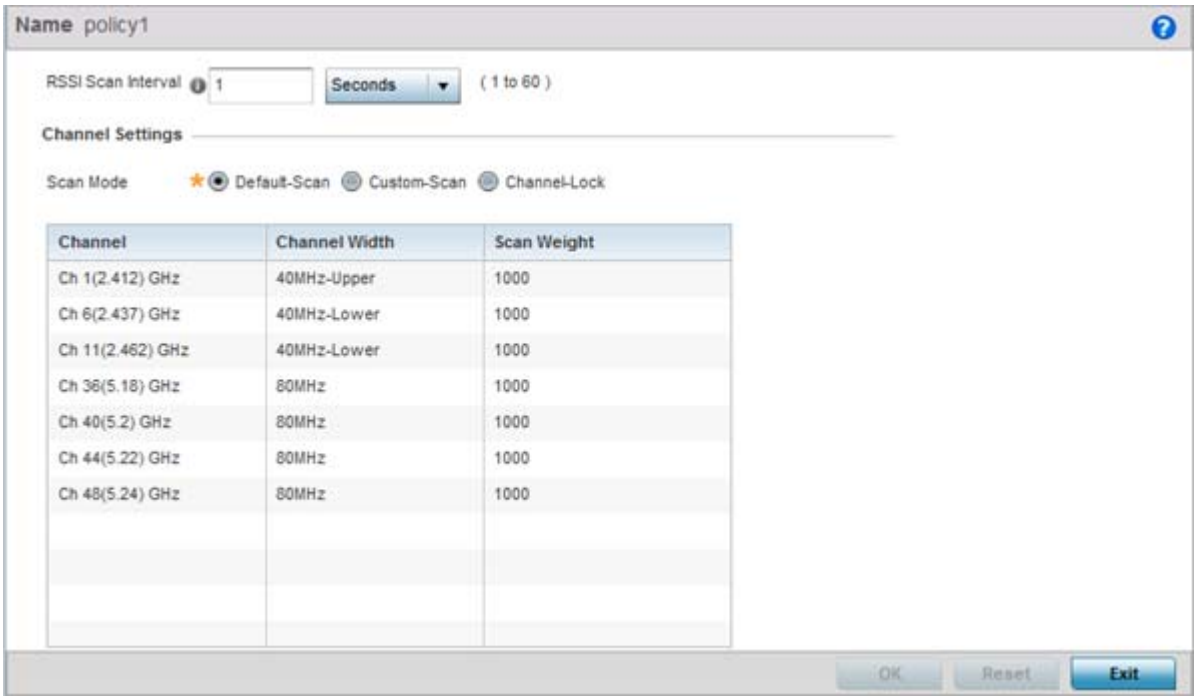


Figure 6-64 *Sensor Policy - Configuration screen*

3 Select **Add** to define a new sensor policy, or select an existing policy and select **Edit** to modify its configuration. Existing sensor policies can be selected and deleted, copied, or renamed as needed.

4 If creating a new sensor policy, assign it a **Name** up to 32 characters. No character spaces are permitted within the name. Define a name unique to the policy's channel and scan mode configuration to help differentiate it from other policies. If adding a new sensor policy, the Name must be provided and **Continue** selected to enable the remaining configuration parameters.

   Use the **RSSI Scan Interval** drop-down menu to set a scan interval from 1 - 60 seconds. This is the scan period dedicated sensors (Access Point radios) utilize for RSSI (signal strength) assessments. Once obtained, the sensor sends the RSSI data to a specified MPact server resource (not an ADSP server) for the calculation of Wi-Fi device locations. The default is 1 second.

5 Set the following **Scan Mode** values depending on whether *Default-Scan, Custom Scan* or *Channel Lock* has been selected as the mode of scan operation:

Channel	*Default-Scan* - The list of available scan channels is fixed and defaulted in a spread pattern of 1, 6, 11, 36, 40, 44 and 48. No alternations to this channel pattern are available to the administrator. *Custom-Scan* - A list of unique channels in the 2.4, 4.9, 5 and 6 GHz band can be collectively or individually enabled for customized channel scans and RSSI reporting. *Channel-Lock* - Once selected, the existing Channel, Channel Width and Scan Weight table items are replaced by a Lock Frequency drop-down menu. Use this menu to lock the RSSI scan to one specific channel.
Channel Width	*Default-Scan* - Each channel's width is fixed and defaulted to either 40MHz-Upper (Ch 1), 40MHz-Lower (Ch 6 and CH 11) or 80MHz (CH 36, CH 40, CH 44 and CH 48). *Custom-Scan* - When custom channels are selected for RSSI scans, each selected channel can have its own width defined. Numerous channels have their width fixed at 20MHz, 802.11a radios support 20 and 40 MHz channel widths. *Channel-Lock* - If a specific channel is selected and locked for an RSSI scan, there's no ability to refine the width between adjacent channels, as only one channel is locked.
Scan Weight	*Default-Scan* - Each default channel's scan is of equal duration (1000) within the defined RSSI scan interval. No one channel receives scan priority within the defined RSSI scan interval. *Custom-Scan* - Each selected channel can have its weight prioritized in respect to the amount of time a scan is permitted within the defined RSSI scan interval. *Channel-Lock* - If a specific channel is selected and locked for an RSSI scan, there's no ability to refine the scan weightage in respect to all the remaining unlocked channels.

6 Select **OK** when completed to update the sensor policy settings. Select **Reset** to revert the screen back to the last saved configuration.

7 Network Configuration

Controllers, service platforms and Access Points allow packet routing customizations and unique network resources for deployment specific routing configurations.

For more information on the options available, refer to the following:

- *Policy Based Routing*
- *L2TP V3 Configuration*
- *Crypto CMP Policy*
- *AAA Policy*
- *AAA TACACS Policy*
- *IPv6 Router Advertisement Policy*
- *BGP*
- *Alias*
- *Application Policy*
- *Application*
- *Application Group*
- *Schedule Policy*
- *URL Filtering*
- *Web Filtering*
- *EX3500 QoS Class*
- *EX3500 QoS Policy Map*
- *Network Deployment Considerations*

7.1 Policy Based Routing

Define a *policy based routing* (PBR) configuration to direct packets to selective paths. PBR can optionally mark traffic for preferential services. PBR minimally provides the following:

- A means to use source address, protocol, application and traffic class as traffic routing criteria
- The ability to load balance multiple WAN uplinks
- A means to selectively mark traffic for QoS optimization

Since PBR is applied to incoming routed packets, a route-map is created containing a set of filters and associated actions. Based on the actions defined in the route-map, packets are forwarded to the next relevant hop. Route-maps are configurable under a global policy called routing-policy, and applied to profiles and devices.

Route-maps contain a set of filters which select traffic (match clauses) and associated actions (set clauses) for routing. A routemap consists of multiple entries, each carrying a precedence value. An incoming packet is matched against the route-map with the highest precedence (lowest numerical value). If it matches, the routing decision is based on this route-map. If the packet does not match the route-map, the route-map entry with next highest precedence is matched. If the incoming packet does not match any of the route-map entries, it's subjected to typical destination based routing. Each route-map entry can optionally enable/disable logging.

The following criteria can optionally be used as traffic selection segregation criteria:

- *IP Access List* - A typical IP ACL can be used for traffic permissions. The mark and log actions in ACL rules however are neglected. Route-map entries have separate logging. Only one ACL can be configured per route map entry.

- *IP DSCP* - Packet filtering can be performed by traffic class, as determined from the IP DSCP field. One DSCP value is configurable per route map entry. If IP ACLs on a WLAN, ports or SVI mark the packet, the new/marked DSCP value is used for matching.
- *Incoming WLAN* - Packets can be filtered by the incoming WLAN. There are two ways to match the WLAN:
  - If the device doing policy based routing has an onboard radio and a packet is received on a local WLAN, then this WLAN is used for selection.
  - If the device doing policy based routing does not have an onboard radio and a packet is received from an extended VLAN, then the device which received the packet passes the WLAN information in the MINT packet for the PBR router to use as match criteria.
- *Client role* - The client role can be used as match criteria, similar to a WLAN. Each device has to agree on a unique identifier for role definition and pass the same MINT tunneled packets.
- *Incoming SVI* - A source IP address qualifier in an ACL typically satisfies filter requirements. But if the host originating the packet is multiple hops away, the incoming SVI can be used as match criteria. In this context the SVI refers to the device interface performing policy based routing, and not the originating connected device.

Each route map entry has a set of match and set (action) clauses. ACL rules configured under route map entries merge to create a single ACL. Route map precedence values determine the prioritization of the rules in this merged ACL. An IP DSCP value is also added to the ACL rules.

Set (or action) clauses determine the routing function when a packet satisfies match criteria. If no set clauses are defined, the default is to fallback to destination based routing for packets satisfying the match criteria. If no set clause is configured and fallback to destination based routing is disabled, then the packet is dropped. The following can be defined within set clauses:

- *Next hop* - The IP address of the next hop or the outgoing interface through which the packet should be routed. Up to two next hops can be specified. The outgoing interface should be a PPP, a tunnel interface or a SVI which has DHCP client configured. The first reachable hop should be used, but if all the next hops aren't reachable, typical destination based route lookup is performed.
- *Default next hop* - If a packet subjected to PBR does not have an explicit route to the destination, the configured default next hop is used. This can be either the IP address of the next hop or the outgoing interface. Only one default next hop can be defined. The difference between the next hop and the default next-hop is in case of former, PBR occurs first, then destination based routing. In case of the latter, the order is reversed. With both cases:
  a If a defined next hop is reachable, it's used. If fallback is configured refer to (b).
  b Do normal destination based route lookup. If a next hop is found its used, if not refer to (c).
  c If default next hop is configured and reachable, it's used. If not, drop the packet.
- *Fallback* - Fallback to destination based routing if none of the configured next hops are reachable (or not configured). This is enabled by default.
- *Mark IP DSCP* - Set IP DSCP bits for QoS using an ACL. The mark action of the route maps takes precedence over the mark action of an ACL.

NOTE: A packet should optimally satisfy all the match criteria, if no match clause is defined in a route-map, it would match everything. Packets not conforming to any of the match clauses are subjected to normal destination based routing.

To define a PBR configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Network.**

3 Select **Policy Based Routing**. The Policy Based Routing screen displays by default.

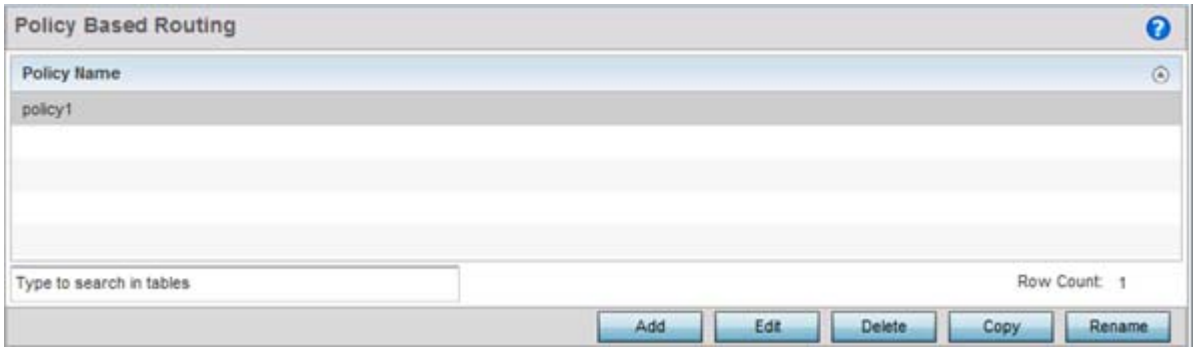


Figure 7-1 *Policy Based Routing screen*

4 Either select **Add** to create a new PBR configuration, **Edit** to modify the attributes of an existing PBR configuration or **Delete** to remove a selected PBR configuration.

5 If creating a new PBR policy assign it a **Policy Name** up to 32 characters to distinguish this route map configuration from others with similar attributes. Select **Continue** to proceed to the Policy Name screen where route map configurations can be added, modified or removed. Select **Exit** to exit without creating a PBR policy.

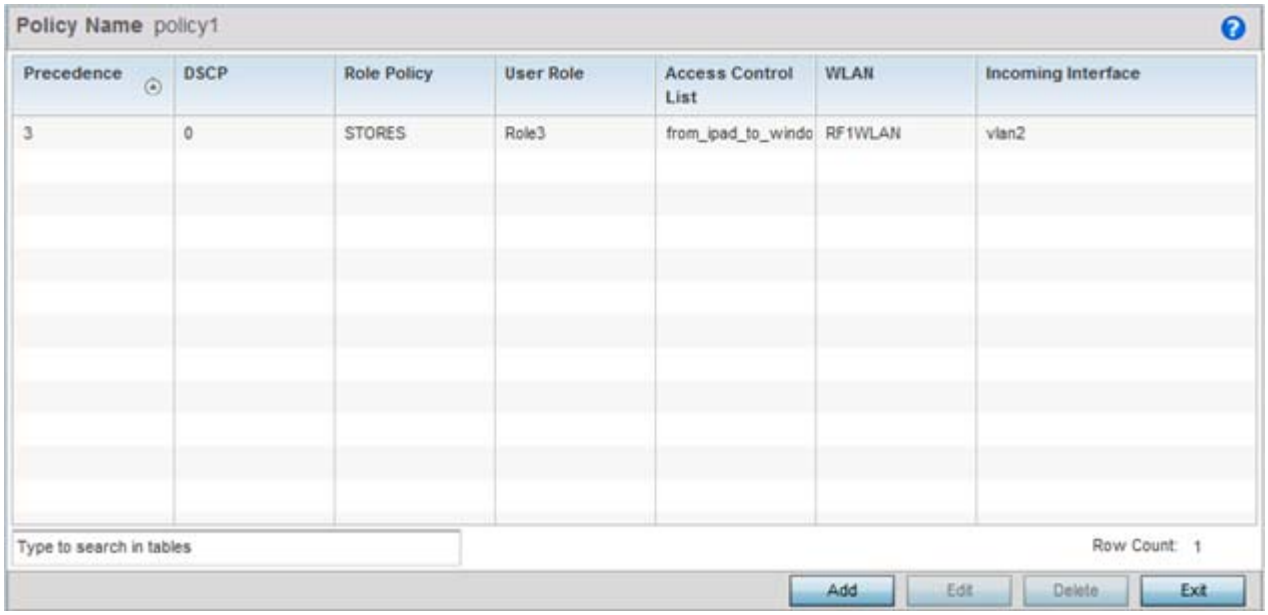


Figure 7-2 *Policy Based Routing, Policy Name screen*

6 Refer to the following to determine whether a new route-map configuration requires creation or an existing route-map requires modification or removal:

Precedence	Lists the numeric precedence (priority) assigned to each listed PBR configuration. A routemap consists of multiple entries, each carrying a precedence value. An incoming packet is matched against the route-map with the highest precedence (lowest numerical value).
DSCP	Displays each policy's DSCP value used as matching criteria for the route map. DSCP is the *Differentiated Services Code Point* field in an IP header and is for packet classification. Packets are filtered based on the traffic class defined in the IP DSCP field. One DSCP value can be configured per route map entry.

Role Policy	Lists each policy's role policy used as matching criteria.
User Role	Lists the user role defined in the Role Policy.
Access Control List	Displays each policy's IP ACL used as an access/deny filter criteria for the route map.
WLAN	Displays each policy's WLAN used as an access/deny filter for the route map.
Incoming Interface	Display the name of the Access Point WWAN or VLAN interface on which the packet is received for the listed PBR policy.

7 Select **Add** or **Edit** to create or modify a route-map configuration. Configurations can optionally be removed by selecting **Delete**.

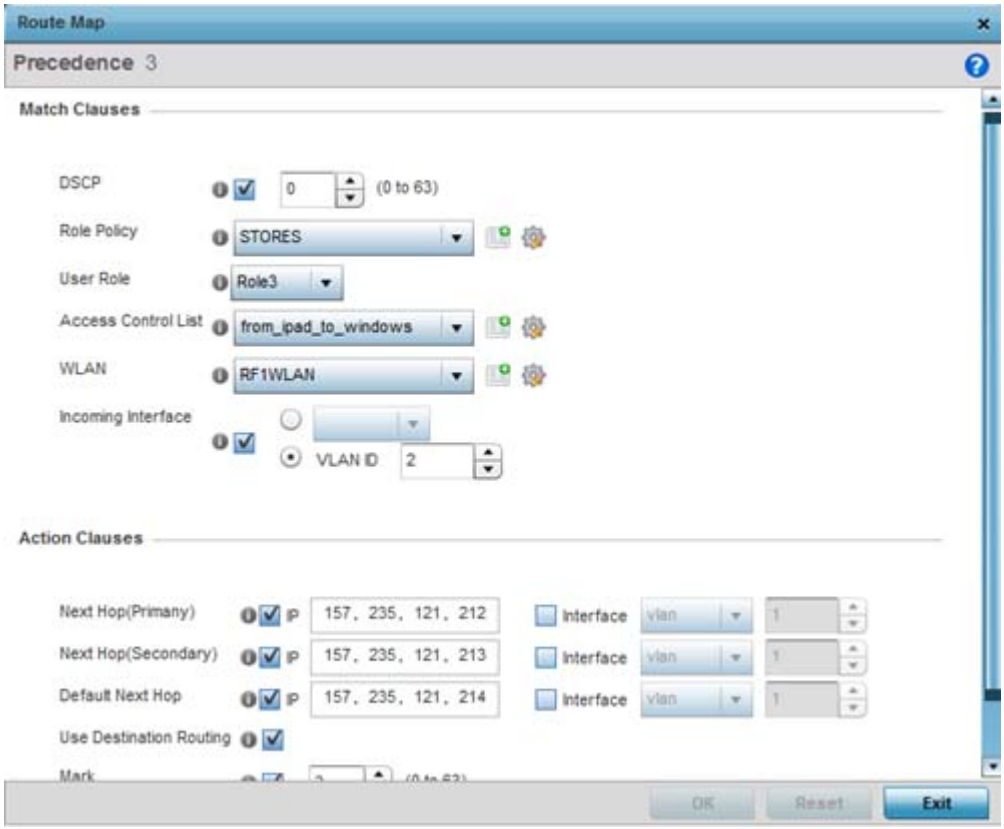


Figure 7-3 *Policy Based Routing screen - Add a Route Map*

8 If adding a route map, use the spinner control to set a numeric **Precedence** (priority) for this route-map. An incoming packet is matched against the route-map with the highest precedence (lowest numerical value).

9 Refer to the **Match Clauses** field to define the following matching criteria for the route-map configuration:

DSCP	Select this option to enable a spinner control to define the DSCP value used as matching criteria for the route map. DSCP is the *Differentiated Services Code Point* field in an IP header and is for packet classification. Packets are filtered based on the traffic class defined in the IP DSCP field. One DSCP value can be configured per route map entry.

Role Policy	Use the drop-down to select a Role Policy to use with this route-map. Click the *Create* icon to create a new Role Policy. To view and modify an existing policy, click the *Edit* icon.
User Role	Use the drop-down menu to select a role defined in the selected Role Policy. This user role is used while deciding the routing.
Access Control List	Use the drop-down menu to select an IP based ACL used as matching criteria for this route-map. Click the *Create* icon to create a new ACL. To view and modify an existing ACL, click the *Edit* icon.
WLAN	Use the drop-down menu to select the Access Point WLAN used as matching criteria for this route-map. Click the *Create* icon to create a new WLAN. To view and modify an existing WLAN, click the *Edit* icon.
Incoming Interface	Select this option to enable radio buttons used to define the interfaces required to receive route-map packets. Use the drop-down menu to define either the Access Point's wwan1 or pppoe1 interface. Neither is selected by default. Or, select the VLAN ID option to define the Access Point VLAN to receive route-map-packets.

10 Set the following **Action Clauses** to determine the routing function performed when a packet satisfies match criteria. Optionally fallback to destination based routing if no hop resource is available.

Next Hop (Primary)	Define a first hop priority request. Set either the *IP* address of the virtual resource or select the Interface option and define either a *wwan1, pppoe1* or a *VLAN* interface. In the simplest terms, if this primary hop resource is available, its used with no additional considerations.
Next Hop (Secondary)	If the primary hop request were unavailable, a second resource can be defined. Set either the *IP* address of the virtual resource or select the Interface option and define either a *wwan1, pppoe1* or a *VLAN* interface.
Default Next Hop	If a packet subjected to PBR does not have an explicit route to the destination, the configured default next hop is used. This value is set as either the IP address of the next hop or the outgoing interface. Only one default next hop can be defined. The difference between the next hop and the default next-hop is in case of former, PBR occurs first, then destination based routing. In case of the latter, the order is reverse. Set either the next hop IP address or define either a *wwan1, pppoe1* or a *VLAN* interface.
Use Destination Routing	It may be a good idea to select this option to default back to destination based routing if none of the defined hop resources are reachable. Packets are dropped if a next hop resource is unavailable and fallback to destination routing is disabled. This option is enabled by default.
Mark	Select this option and use the spinner control to set IP DSCP bits for QoS using an ACL. The mark action of the route maps takes precedence over the mark action of an ACL.

11 Select **OK** to save the updates to the route-map configuration. Select **Reset** to revert to the last saved configuration.

7.2 L2TP V3 Configuration

L2TP V3 is an IETF standard used for transporting different types of layer 2 frames in an IP network. L2TP V3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes.

Use L2TP V3 to create tunnels for transporting layer 2 frames. L2TP V3 enables WiNG managed wireless devices to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TP V3 tunnels can be defined between WiNG devices and other vendor devices supporting the L2TP V3 protocol.

Multiple pseudowires can be created within an L2TP V3 tunnel. WiNG Access Points support an Ethernet VLAN pseudowire type exclusively.

NOTE: A pseudowire is an emulation of a layer 2 point-to-point connection over a *packet-switching network* (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TP V3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TP V3 sessions. Each tunnel session corresponds to one pseudowire. An L2TP V3 control connection (a L2TP V3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TP V3 session originator and responder need to know the psuedowire type and identifier. These two parameters are communicated during L2TP V3 session establishment. An L2TP V3 session created within an L2TP V3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.

The working status of a pseudowire is reflected by the state of the L2TP V3 session. If a L2TP V3 session is down, the pseudowire associated with it must be shut down. The L2TP V3 control connection keep-alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.

NOTE: If connecting an Ethernet port to another Ethernet port, the pseudowire type must be Ethernet port, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be Ethernet VLAN.

To define an L2TP V3 tunnel configuration:

1 Select **Configuration** > **Network** > **L2TPv3**.

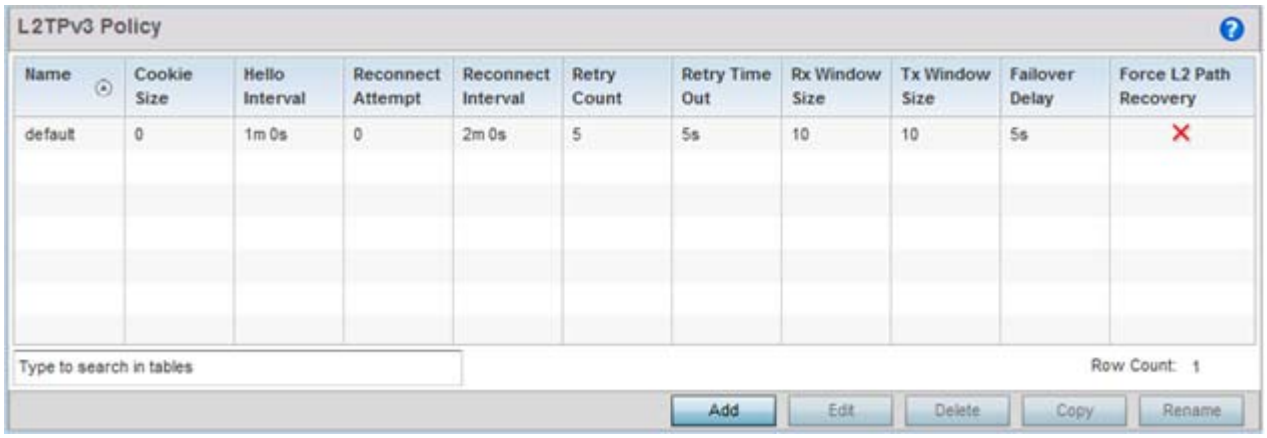


Figure 7-4 *L2TP v3 Policy screen*

The L2TP V3 screen lists the policy configurations defined thus far.

2 Refer to the following to determine whether a new L2TP V3 requires creation or modification:

Name	Lists the 31 character maximum name assigned to each listed L2TP V3 policy, designated upon creation.
Cookie size	Displays the size of each policy's cookie field present within each L2TP V3 data packet. L2TP V3 data packets contain a session cookie which identifies the session (pseudowire) corresponding to it. If using the CLI, cookie size can't be configured per session, and are the same size for all sessions within a tunnel.
Hello Interval	Displays each policy's interval between L2TP V3 hello keep alive messages exchanged within the L2TP V3 connection.
Reconnect Attempt	Lists each policy's maximum number of reconnection attempts available to reestablish the tunnel if the connection is lost.
Reconnect Interval	Displays the duration set for each listed policy between two successive reconnection attempts.
Retry Count	Lists the number of retransmission attempts set for each listed policy before a target tunnel peer is defined as not reachable.
Retry Time Out	Lists the interval the interval (in seconds) set for each listed policy before the retransmission of a L2TP V3 signaling message.
Rx Window Size	Displays the number of packets that can be received without sending an acknowledgement.
Tx Window Size	Displays the number of packets that can be transmitted without receiving an acknowledgement.
Failover Delay	Lists the time (in either seconds or minutes) for establishing a tunnel after a failover (VRRP/RF Domain/Cluster).
Force L2 Path Recovery	Lists whether force L2 path recovery is enabled (as defined by a green checkmark) or disabled (as defined by a red X). Once a tunnel is established, enabling this setting forces server and gateway learning behind the L2TPv3 tunnel.

3 Select **Add** to create a new L2TP V3 policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available. Existing policies can be copied or deleted as needed.

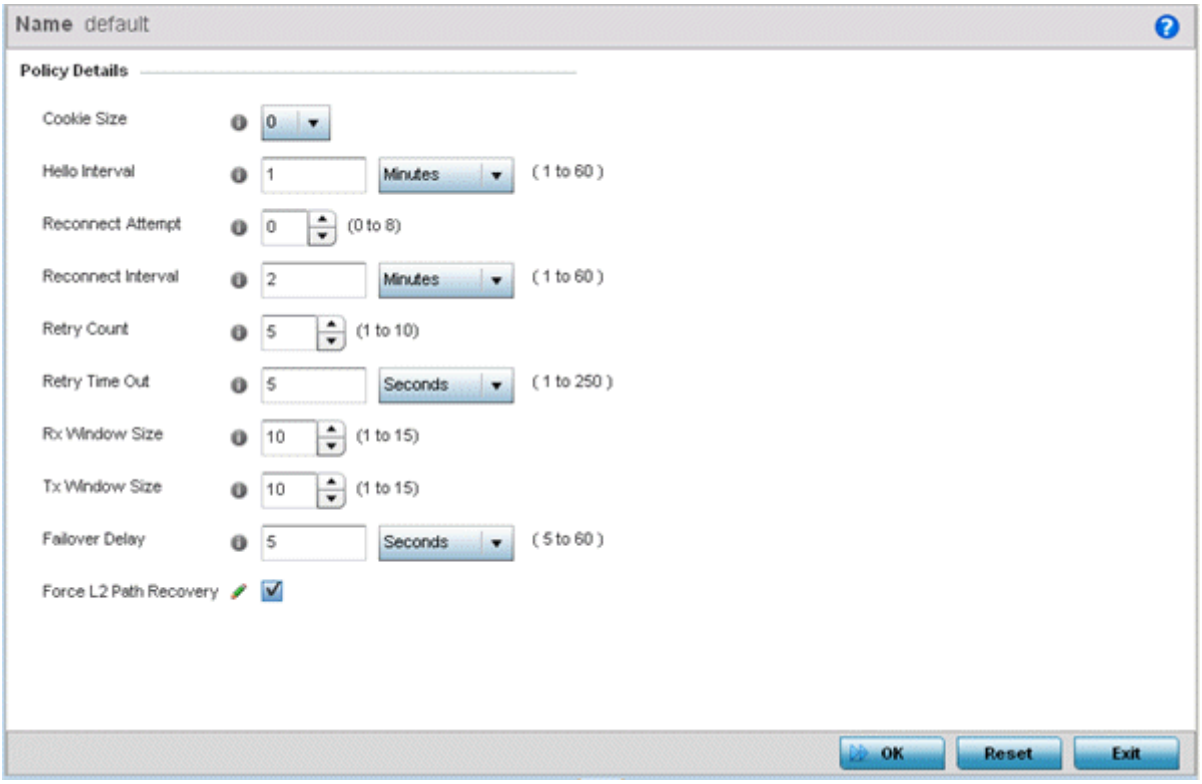


Figure 7-5 *L2TP V3 Policy Creation screen*

4 If creating a new L2TP V3 policy assign it a **Name** up to 31 characters. Remember, a single L2TP V3 policy can be used by numerous L2TP V3 tunnels.

5 Define the following **Policy Details** to add a device to a list of devices sanctioned for network operation:

Cookie size	L2TP V3 data packets contain a session cookie which identifies the session (pseudowire) corresponding to it. Use the spinner control to set the size of the cookie field present within each L2TP V3 data packet. Options include 0, 4 and 8. the default setting is 0. If using the CLI, the cookie size can't be configured per session, and are the same size for all sessions within a tunnel.
Hello Interval	Define an interval in either *Seconds* (1 - 3,600), *Minutes* (1 -60) or *Hours* (1) between L2TP V3 hello keep alive messages exchanged within the L2TP V3 control connection. The default setting is 1 minute.
Reconnect Attempt	Use the spinner control to set a value (from 0 - 8) representing the maximum number of reconnection attempts initiated to reestablish the tunnel. The default interval is 0.
Reconnect Interval	Define an interval in either *Seconds* (1 - 3,600), *Minutes* (1 -60) or *Hours* (1) between two successive reconnection attempts. The default setting is 2 minutes.
Retry Count	Use the spinner control to define how many retransmission attempts are made before determining a target tunnel peer is not reachable. The available range is from 1 - 10, with a default value of 5.
Retry Time Out	Use the spinner control to define the interval (in seconds) before initiating a retransmission of a L2TP V3 signaling message. The available range is from 1 - 250, with a default value of 5.

Rx Window Size	Specify the number of packets that can be received without sending an acknowledgement. The available range is from 1 - 15, with a default setting of 10.
Tx Window Size	Specify the number of packets that can be transmitted without receiving an acknowledgement. The available range is from 1 - 15, with a default setting of 10.
Failover Delay	Set the time in *Seconds* (5 - 60) or *Minutes* (1) for establishing a tunnel after a failover (VRRP/RF Domain/Cluster). The default setting is 5 seconds.
Force L2 Path Recovery	Determine whether force L2 path recovery is *enabled* or *disabled.* Once a tunnel is established, enabling this setting forces server and gateway learning behind the L2TPv3 tunnel. The default setting is disabled.

6 Select **OK** to save the updates to the L2TP V3 policy. Select **Reset** to revert to the last saved configuration.

7.3 Crypto CMP Policy

Certificate Management Protocol (CMP) is an Internet protocol to obtain and manage digital certificates in a *Public Key Infrastructure* (PKI) network. A *Certificate Authority* (CA) issues the certificates using the defined CMP.

Using CMP, a device can communicate to a CMP supported CA server, initiate a certificate request and download the required certificates from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting the certificates from the server. It can also auto update the certificates which are about to expire.

The CMP client on the controller, service platform or Access Point triggers a request for the configured CMS CA server. Once the certificate is validated and confirmed from the CA server it is saved on the device and becomes part of the trustpoint. During the creation of the CMP policy the trustpoint is assigned a name and client information. An administrator can use a manually created trustpoint for one service (like HTTPs) and use the CMP generated trustpoint for RADIUS EAP certificate based authentication.

To review, create or edit a Crypto CMP policy:

1 Select **Configuration** > **Network** > **Crypto CMP Policy**.

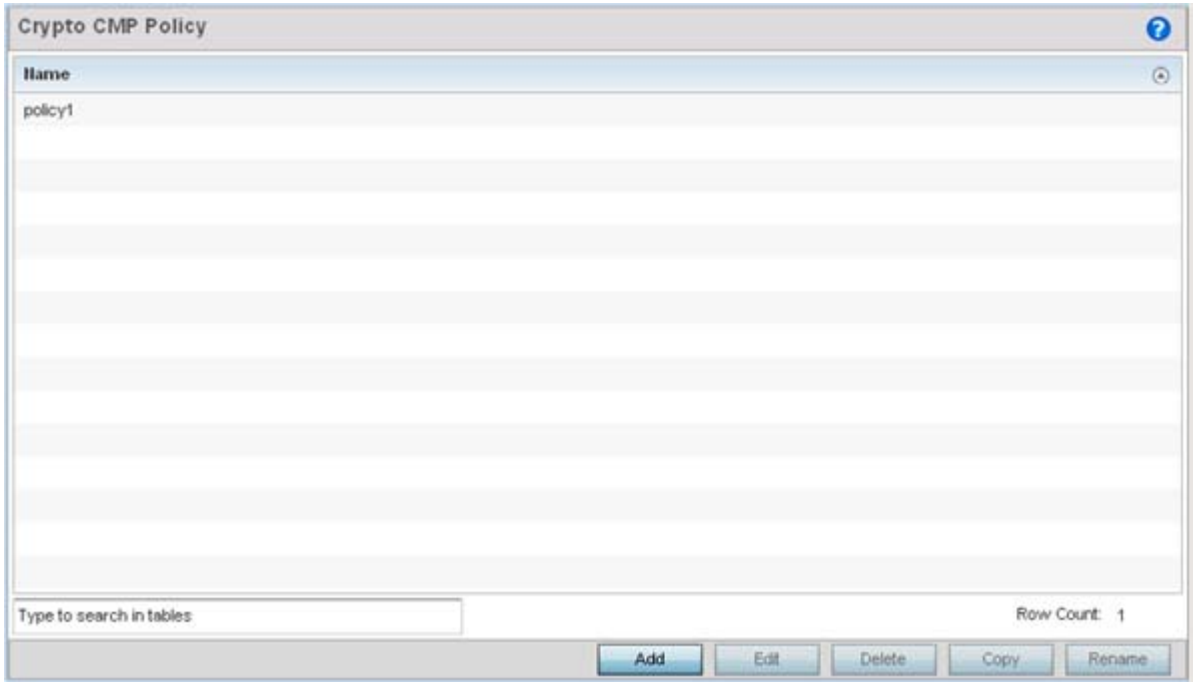


Figure 7-6 *Crypto CMP Policy screen*

The **Crypto CMP Policy** screen lists the policy configurations defined thus far.

2 Select **Add** to create a new Crypto CMP policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available. Existing policies can be copied or renamed as needed.

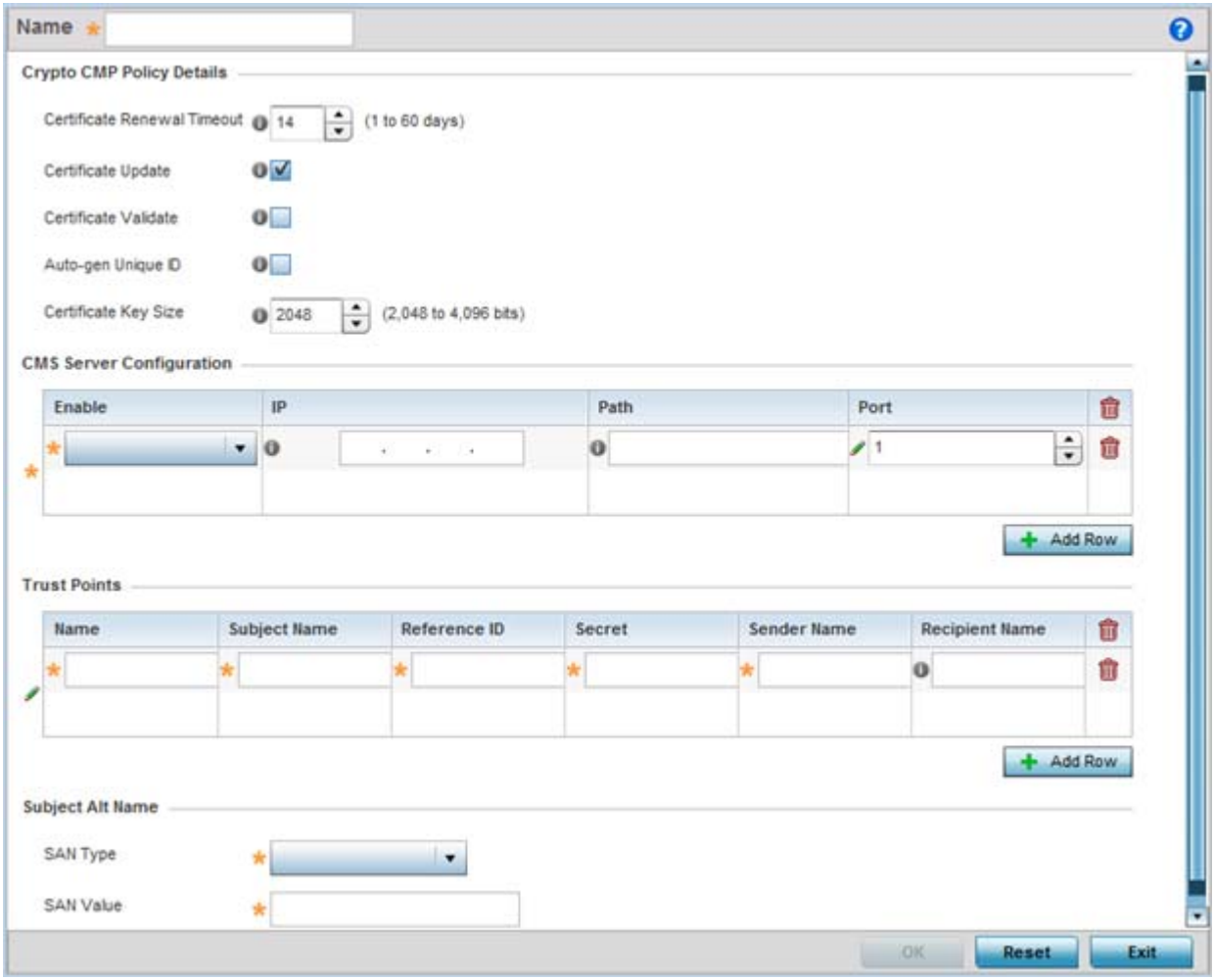


Figure 7-7 *Crypto CMP Policy Creation screen*

3 If creating a new Crypto CMP policy assign it a **Name** up to 31 characters to help distinguish it.

4 Set the **Certificate Renewal Timeout** period to trigger a new certificate renewal request with the dedicated CMP server resource. The range is 1-60 days. The default is 14 days.

The expiration of the certificate is checked once a day. When a certificate is about to expire a certificate renewal is initiated with the server via an existing IPsec tunnel. If the tunnel is not established, the CMP renewal request is not sent. If a renewal succeeds the newly obtained certificate overwrites an existing certificate. If the renewal fails, an error is logged.

5 Select **Certificate Update** to update the renewal data of the certificate. This setting is enabled by default.

6 Select **Certificate Validate** to validate the cross-certificate when enabled. This setting is disabled by default.

7 Select **Auto-gen Unique ID** to add (prepend) an autogenerated ID in both the subject and sender fields. This setting is disabled by default.

8 Use the **Certificate Key Size** spinner control to set a key size (from 2,048 - 4096 bits) for the certificate request. The default key size is 2,048.

9 Select **+ Add Row** and define the following **CMS Server Configuration** settings for the server resource:

Enable	Use the drop-down menu to set the CMS server as either the *Primary* (first choice) or *Secondary* (secondary option) CMP server resource.
IP	Define the IP address for the CMP CA server managing digital certificate requests. CMP certificates are encrypted with CA's public key and transmitted to the defined IP destination over a typical HTTP or TLS session.
Path	Provide a complete path to the CMP CA's trustpoint.
Port	Provide a CMP CA port number.

10 Set the following **Trust Points** settings.The trustpoint is used for various services as specifically set the controller, service platform or Access Point.

Name	Enter the 32 character maximum name assigned to the target trustpoint. A trustpoint represents a CA/identity pair containing the identity of the CA, CA specific configuration parameters, and an association with an enrolled identity certificate. This field is mandatory.
Subject Name	Provide a subject name of up to 512 characters for the certificate template example. This field is mandatory.
Reference ID	Set the user reference value for the CMP CA trust point message. The range is 0-256. This field is mandatory.
Secret	Specify the secret used for trustpoint authentication over the designated CMP server resource.
Sender Name	Enter a sender name up to 512 characters for the trustpoint request. This field is mandatory.
Recipient Name	Enter a recipient name value of up to 512 characters for the trustpoint request.

11 Use the **SAN Type** drop-down menu to provide an alternative name (disguise) for the subject. Options include *email, IP Address, Distinguished Name, FQDN* and *string*.

12 Use the **SAN Value** field to enter a 128 character maximum alternative value for the subject.

13 Select **OK** to save the updates to the CMP Crypto policy, **Reset** to revert to the last saved configuration, or **Exit** to close the screen.

7.4 AAA Policy

Authentication, Authorization, and Accounting (AAA) provides the mechanism by which network administrators define access control within the network.

Controllers, service platforms and Access Points can interoperate with external RADIUS and LDAP Servers (AAA Servers) to provide user database information and user authentication data. Each WLAN can maintain its own unique AAA configuration.

AAA provides a modular way of performing the following services:

Authentication — Authentication provides a means for identifying users, including login and password dialog, challenge and response, messaging support and (depending on the security protocol), encryption. Authentication is the technique by which a user is identified before allowed access to the network. Configure AAA authentication by defining a list of authentication methods, and then applying the list to various interfaces. The list defines the authentication schemes performed and their sequence. The list must be applied to an interface before the defined authentication technique is conducted.

Authorization — Authorization occurs immediately after authentication. Authorization is a method for remote access control, including authorization for services and individual user accounts and profiles. Authorization functions through the assembly of attribute sets describing what the user is authorized to perform. These attributes are compared to information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database could be located locally or be hosted remotely on a RADIUS server. Remote RADIUS servers authorize users by associating *attribute-value* (AV) pairs with the appropriate user. Each authorization method must be defined through AAA. When AAA authorization is enabled it's applied equally to all interfaces.

Accounting — Accounting is the method for collecting and sending security server information for billing, auditing, and reporting user data; such as start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables wireless network administrators to track the services users are accessing and the network resources they are consuming. When accounting is enabled, the network access server reports user activity to a RADIUS security server in the form of accounting records. Each accounting record is comprised of AV pairs and is stored on the access control server. The data can be analyzed for network management, client billing, and/or auditing. Accounting methods must be defined through AAA. When AAA accounting is activated, it's applied equally to all interfaces on the access servers.

To define unique WLAN AAA configurations:

1 Select **Configuration** > **Network** > **AAA Policy** to display existing AAA policies.

The **Authentication, Authorization, and Accounting (AAA)** screen lists those AAA policies created thus far. Any of these policies can be selected and applied.

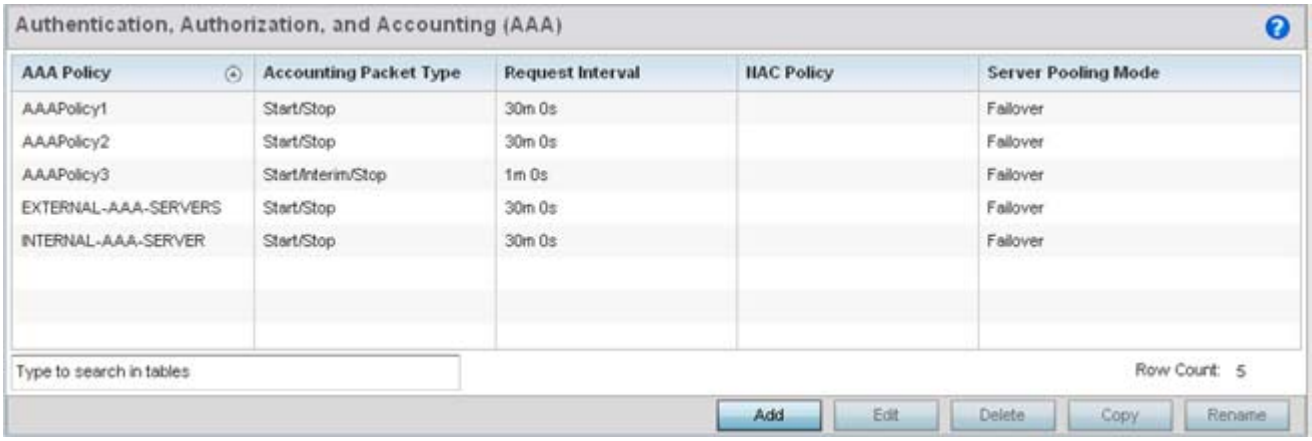


Figure 7-8 *Authentication, Authorization, and Accounting (AAA) screen*

2 Refer to the following information listed for each existing AAA policy:

AAA Policy	Displays the name assigned to the AAA TACACS policy when it was initially created. The name cannot be edited within a listed profile.

Accounting Packet Type	Displays the accounting type set for the AAA policy. Options include: *Start Only* - Sends a start accounting notice to initiate user accounting. *Start/Stop* - Sends a start accounting notice at the beginning of a process and a stop notice at the end of a process. The start accounting record is sent in the background. The requested process begins regardless of whether the start accounting notice is received by the accounting server. *Start/Interim/Stop* - Sends a start accounting notice at the beginning of a process and a stop notice at the end of a process. A notice is also sent at the completion of each interim packet transmission during the process.
Request Interval	Lists each AAA policy's interval used to send a RADIUS accounting request to the RADIUS server.
NAC Policy	Lists the name *Network Access Control* (NAC) filter used to either *include* or *exclude* clients from access.
Server Pooling Mode	The server pooling mode controls how requests are transmitted across RADIUS servers. Selecting *Failover* results in working down the list of servers if a server is unresponsive or unavailable. *Load Balanced* uses all available servers transmitting requests in round robin.

3 To configure a new AAA policy, click the **Add** button. To modify an existing policy, select it from amongst those available and select the **Edit** button. Optionally **Copy** or **Rename** the AAA policy as needed.

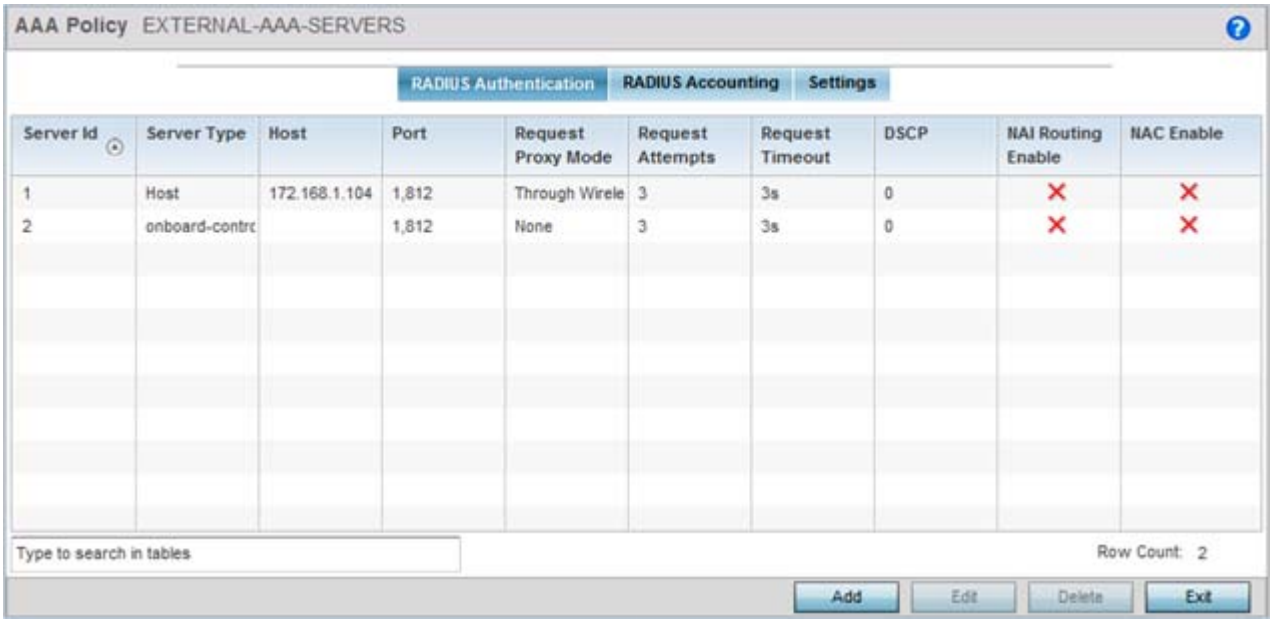


Figure 7-9 *AAA Policy - RADIUS Authentication screen*

4 Refer to the following AAA authentication policy data:

Server ID	Displays the numerical server index (1-6) for the accounting server when added to the list available.
Server Type	Displays the type of AAA server in use either *Host*, *onboard-self*, or *onboard-controller*.
Host	Displays the IP address or hostname of the RADIUS authentication server.

Port	Displays the port on which the RADIUS server listens to traffic within the network. The port range is 1 to 65,535. The default port is 1812.
Request Proxy Mode	Displays whether a request is transmitted directly through the server or proxied through the Access Point or RF Domain manager.
Request Attempts	Displays the number of attempts a client can retransmit a missed frame to the RADIUS server before it times out of the authentication session. The available range is between 1 and 10 attempts. The default is 3 attempts.
Request Timeout	Displays the time (from 1 - 60) seconds for the re-transmission of request packets. The default is 3 seconds. If this time is exceeded, the authentication session is terminated.
DSCP	Displays the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification. The valid range is from 0 - 63 with a default of 46.
NAI Routing Enable	Displays NAI routing status. AAA servers identify clients using the NAI. The NAI is a character string in the format of an e-mail address as either user or user@ but it need not be a valid e-mail address or a fully qualified domain name. The NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. The generic form allows all users to be configured on a single command line. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of the NAI was to support roaming between dialup ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each.
NAC Enable	A green check defines NAC as enabled, while a Red X defines NAC disabled with this AAA policy.

5 Select a configuration from the table and select **Edit,** or select **Add** to create a new RADIUS authentication policy. Optionally **Delete** a policy as they become obsolete.

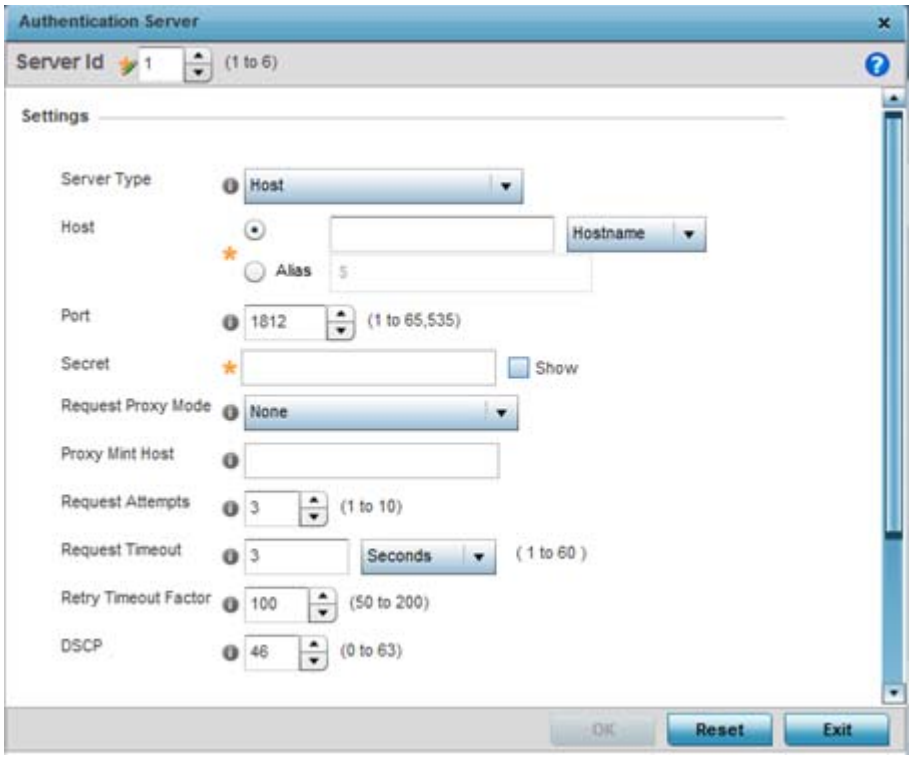


Figure 7-10 *AAA Policy - Add RADIUS Authentication Server*

6 Define the following **Settings** to add or modify a AAA RADIUS authentication server configuration:

Server ID	If adding a server, define the numerical server index (1-6) for the authentication server when added to the list available.
Server Type	Select the type of AAA server in use either *Host*, *onboard-self*, *onboard-controller* or *onboard-centralized-controller*.
Host	Specify the IP address or hostname of the RADIUS authentication server. Hostnames cannot include an underscore character.
Port	Define or edit the port on which the RADIUS server listens to traffic within the network. The port range is 1 to 65,535. The default port is 1812.
Secret	Specify the secret used for authentication on the selected RADIUS server. By default the secret will be displayed as asterisks. To show the secret in plain text, check the Show box.
Request Proxy Mode	Select the method of proxy that browsers communicate with the RADIUS authentication server. The mode could either be *None, Through Wireless Controller*, *through-centralized-controller*, *Through RF Domain Manager*, or *Through Mint Host*.
Request Mint Host	Specify a 64 character maximum hostname (or Mint ID) of the Mint device used for proxying requests. Hostnames cannot include an underscore character.
Request Attempts	Specify the number of attempts a client can retransmit a missed frame to the RADIUS server before it times out of the authentication session. The available range is between 1 and 10 attempts. The default is 3 attempts.

Request Timeout	Specify the time between 1 and 60 seconds for the re-transmission of request packets. The default is 5 seconds. If this time is exceeded, the authentication session is terminated.
Request Timeout Factor	Specify the amount of time between 50 and 200 seconds between retry timeouts for the re-transmission of request packets. The default is 100.
DSCP	Specify the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification. The valid range is between 0 and 63 with a default value of 46.

7 Set the following **Network Access Identifier Routing** values:

NAI Routing Enable	Check to enable NAI routing. AAA servers identify clients using the NAI. The NAI is a character string in the format of an e-mail address as either user or user@ but it need not be a valid e-mail address or a fully qualified domain name. The NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. The generic form allows users to be configured on a single command line. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of the NAI was to support roaming between dialup ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each.
Realm	Enter the realm name in the field. The name cannot exceed 50 characters. When the RADIUS server receives a request for a user name the server references a table of usernames. If the user name is known, the server proxies the request to the RADIUS server.
Realm Type	Specify whether the *Prefix* or *Suffix* of the username is matched to the realm.
Strip Realm	Check strip to remove information from the packet when NAI routing is enabled.

8 Select the **RADIUS Accounting** tab.

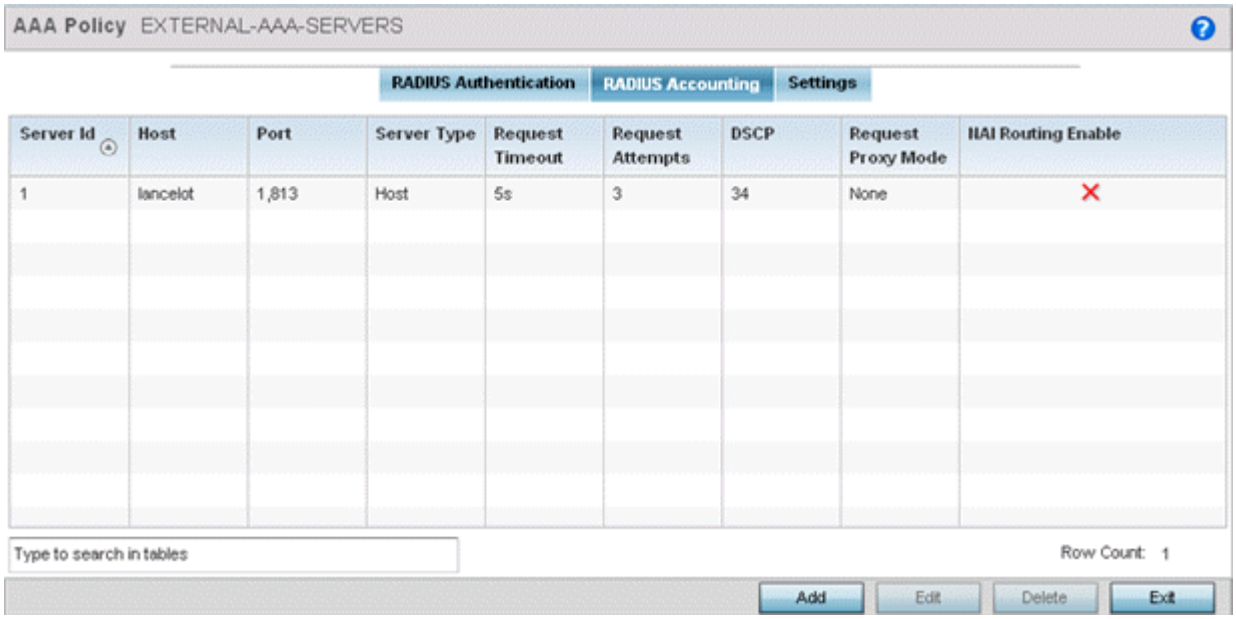


Figure 7-11 *AAA Policy - RADIUS Accounting screen*

9 Refer to the following information for each existing AAA server policy to determine whether new RADIUS accounting policies require creation or existing policies require modification:

Server ID	Displays the numerical server index (1-6) for the accounting server assigned when added to the WiNG operating system.
Host	Displays the IP address or hostname of the RADIUS authentication server. Hostnames cannot include an underscore character.
Port	Displays the port on which the RADIUS server listens to traffic within the network. The port range is 1 to 65,535. The default port is 1813.
Server Type	Displays the type of AAA server in use either *Host, onboard-self*, or *onboard-controller.*
Request Timeout	Displays the time between 1 and 60 seconds for the wireless controller's re-transmission of request packets. If this time is exceeded, the authentication session is terminated.
Request Attempts	Displays the number of attempts a client can retransmit a missed frame to the RADIUS server before it times out of the authentication session. The available range is between 1 and 10 attempts. The default is 3 attempts.
DSCP	Displays the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification. The valid range is between 0 and 63 with a default value of 34.
Request Proxy Mode	Displays the method of proxy that browsers communicate with the RADIUS authentication server. The mode could either be *None, Through Wireless Controller*, or *Through RF Domain Manager.*

NAI Routing Enable	Displays NAI routing status. AAA servers identify clients using the NAI. The NAI is a character string in the format of an e-mail address as either user or user@ but it need not be a valid e-mail address or a fully qualified domain name. The NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. The generic form allows all users to be configured on a single command line. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of the NAI was to support roaming between dialup ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS servers can proxy requests to remote servers for each.

10 To edit an existing accounting profile, select the profile then **Edit**. To add a new policy select **Add**. Optionally **Delete** a policy as they become obsolete.

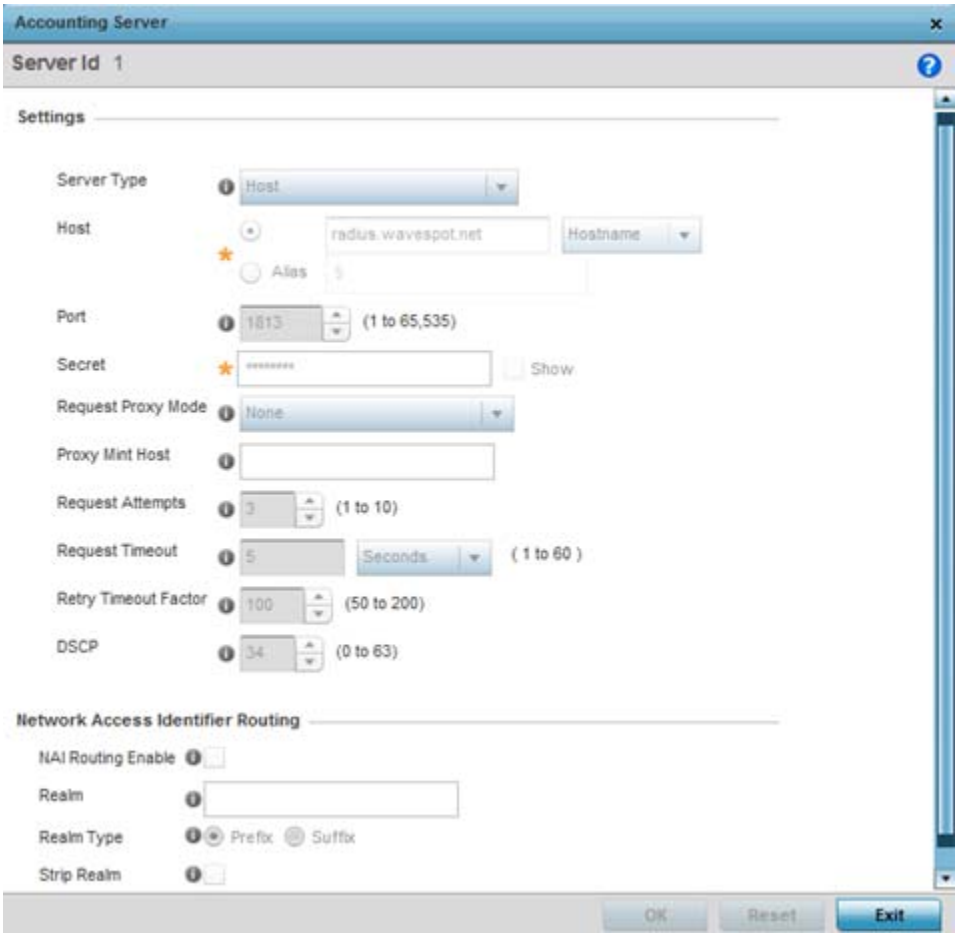


Figure 7-12 *AAA Policy - Add RADIUS Accounting Server*

11 If creating a new AAA Accounting Server configuration as a user database and user authentication resource, assign it a **Server ID** from 1 - 6.

12 Define the following **Settings** to add or modify AAA RADIUS accounting server configuration.

Server Type	Select the type of AAA server as either *Host, onboard-self*, *onboard-controller* or *onboard-centralized-controller.*

Host	Specify the IP address or hostname of the RADIUS accounting server. Hostnames cannot include an underscore character. Select *Alias* to define the hostname alias once and use the alias character set across different configuration items.
Port	Define or edit the port on which the RADIUS accounting server listens to traffic within the network. The port range is 1 to 65,535. The default port is 1813.
Secret	Specify the secret (password) used for authentication on the selected RADIUS server. By default the secret is displayed as asterisks. To show the secret in plain text, select *Show*.
Request Proxy Mode	Select the method of proxy that browsers communicate with the RADIUS authentication server. The mode could either be *None, Through Wireless Controller*, *through-centralized-controller, Through RF Domain Manager* or *Through Mint Host.*
Request Mint Host	Specify a 64 character maximum hostname or the Mint ID of the Mint device used for proxying requests. Hostnames cannot include an underscore character.
Request Attempts	Displays the number of attempts a client can retransmit a missed frame to the RADIUS accounting server before it times out of the authentication session. The available range is 1 - 10 attempts. The default is 3 attempts.
Request Timeout	Specify the time from 1 - 60 seconds for the re-transmission of request packets. The default is 5 seconds. If this time is exceeded, the authentication session is terminated.
Retry Timeout Factor	Specify the amount of time from 50 - 200 seconds between retry timeouts for the re-transmission of request packets. The default is 100.
DSCP	Displays the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification. The valid range is between 0 and 63 with a default value of 34.

13 Set the following **Network Access Identifier routing** values for the accounting server:

NAI Routing Enable	Check to enable NAI routing. AAA servers identify clients using the NAI. The NAI is a character string in the format of an e-mail address as either user or user@ but it need not be a valid e-mail address or a fully qualified domain name. The NAI can be used either in a specific or generic form. The specific form, which must contain the user portion and may contain the @ portion, identifies a single user. The generic form allows all users in a given or without a to be configured on a single command line. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of the NAI was to support roaming between dialup ISPs. Using NAI, each ISP need not have all the accounts for all of its roaming partners in a single RADIUS database. RADIUS accounting servers can proxy requests to remote servers for each.
Realm	Enter the realm name in the field. The name cannot exceed 50 characters. When the RADIUS server receives a request for a user name the server references a table of usernames. If the user name is known, the server proxies the request to the RADIUS server.
Realm Type	Specify whether the *Prefix* or *Suffix* of the username is matched to the realm.

Strip Realm	Check strip to remove information from the packet when NAI routing is enabled.

14 Select the **Settings** tab.

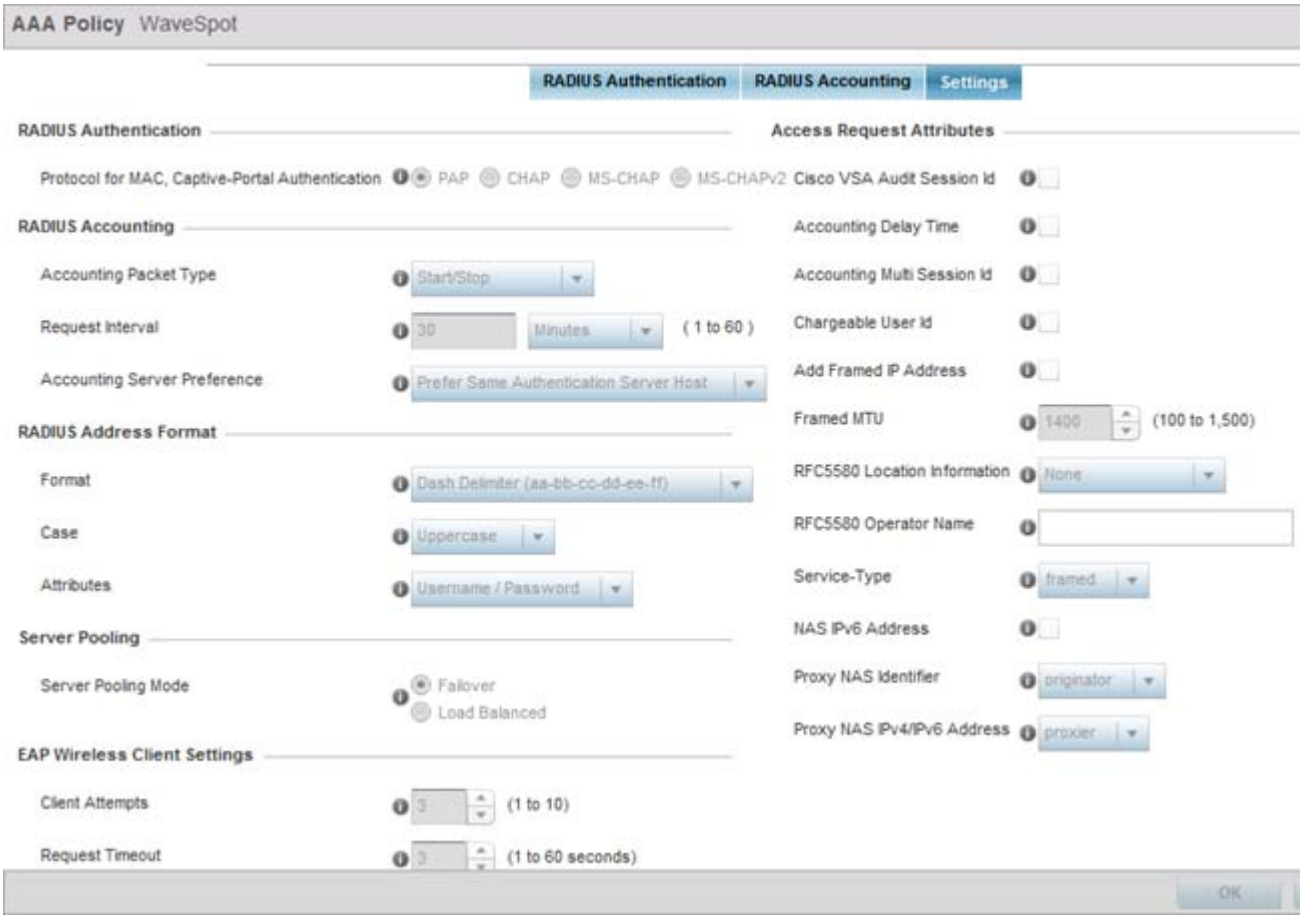


Figure 7-13 *AAA Policy - Settings screen*

15 Set the **Protocol for MAC, Captive-Portal Authentication**.

The authentication protocol *Password Authentication Protocol* (PAP), *Challenge Handshake Authentication Protocol* (CHAP) MS-CHAP or MS-CHAPv2 when the server is used for any non-EAP authentication. PAP is the default setting.

16 Set the following **RADIUS Accounting** settings:

Accounting Packet Type	Set the RADIUS Accounting request packet type. Options include *Stop Only*, *Start/Stop* and *Start/Interim/Stop*. Start/Stop is the default setting.
Request Interval	Set the periodicity of the interim accounting requests to 1 hour, 1 - 60 minutes or 60 - 3600 seconds. The default is 30 minutes.

Accounting Server Preference	Select the server preference for RADIUS accounting. The options include: *Prefer Same Authentication Server Host* - Uses the authentication server host name as the host used for RADIUS accounting. This is the default setting. *Prefer Same Authentication Server Index* - Uses the same index as the authentication server for RADIUS accounting. *Select Accounting Server Independently* - Allows users to specify a RADIUS accounting server separate from the RADIUS authentication server.

17 Set the following **RADIUS Address Format** settings:

Format	Select the format of the MAC address used in the RADIUS accounting packets.
Case	Select whether the MAC address is sent using uppercase or lowercase characters. The default setting is uppercase.
Attributes	Select whether the format specified applies only to the username/password in MAC Auth requests or for all attributes including a MAC address, such as *calling-station-id* or *called-station-id.*

18 Set the **Server Pooling Mode:**

Server Pooling Mode	Control how requests are transmitted across RADIUS servers. *Failover* implies traversing the list of servers if any server is unresponsive. *Load Balanced* means using all servers in a round-robin fashion. The default setting is Failover.

19 Set the following **EAP Wireless Client Settings**:

Client Attempts	Defines the number of times (1 - 10) an EAP request is transmitted to a client before giving up. The default setting is 3.
Request Timeout	Set the amount of time after which an EAP request to a client is retried. The default setting is 3 seconds.
ID Request Timeout	Define the amount of time (1 - 60 seconds) after which an EAP ID Request to a client is retried. The default setting is 30 seconds.
Retransmission Scale Factor	Set the scaling of the retransmission attempts. Timeout at each attempt is a function of the request timeout factor and client attempts number. 100 (default setting) implies a constant timeout at each retry; smaller values indicate more aggressive (shorter) timeouts, larger numbers set more conservative (longer) timeouts on each successive attempt.

20 Set **Access Request Attributes**.

Cisco VSA Audit Session Id	Set a *vendor specific attribute* (VSA) to allow CISCO's *Identity Services Engine* (ISE) to validate a requesting client's network compliance, such as the validity of virus definition files (antivirus software or definition files for an anti-spyware software application). This setting is disabled by default.
Accounting Delay Time	Select this option to enable the support of an accounting delay time attribute within accounting requests. This setting is disabled by default.

Accounting Multi Session Id	Select this option to enable the support of an accounting multi session ID attribute. This setting is disabled by default.
Chargeable User Id	Select this option to enable the support of chargeable user identity. This setting is disabled by default.
Add Framed IP Address	Select this option to add an IP address attribute to access requests. This setting is disabled by default.
Framed MTU	Set the framed MTU attribute (from 100 - 1500) used in access requests. The default setting is 1400.
RFC5580 Location Information	Select a support option for the RFC5580 location attribute. Options include *None*, *include-always* and *server-requested.* The default setting is None.
RFC5580 Operator Name	Provide a 63 character maximum RFC5580 operator name.
Service-Type	Set the service type attribute value. Options include *framed* (default setting) and *login*.
NAS IPv6 Address	Select this option to provide support for NAS IPv6 formatted addresses when not proxying. This setting is disabled by default.
Proxy NAS Identifier	Select a RADIUS attribute NAS identifier when proxying through the controller or RF Domain manager. Options include *originator* (default setting) or *proxier*.
Proxy NAS IPv6 Address	Sets the RADIUS attribute NAS IP address and NAS IPv4 address behavior when proxying through the controller or RF Domain manager. Options include *None* and *proxier* (default setting).

21 Select **OK** to save the updates to the AAA configuration. Select **Reset** to revert to the last saved configuration.

7.5 AAA TACACS Policy

Terminal Access Controller Access - Control System+ (TACACS) is a protocol created by CISCO Systems which provides access control to network devices (routers, network access servers and other networked computing devices) using one or more centralized servers. TACACS provides separate authentication, authorization, and accounting services running on different servers.

TACACS controls user access to devices and network resources while providing separate accounting, authentication, and authorization services. Some of the services provided by TACACS are:

- Authorizing each command with the TACACS server before execution
- Accounting each session's logon and log off event
- Authenticating each user with the TACACS server before enabling access to network resources.

To define a unique AAA TACACS configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Network.**

3 Select **AAA TACACS Policy** to display a high level display of existing AAA policies.

The **Authentication, Authorization, and Accounting (AAA) TACACS** screen lists existing AAA policies. Any of these policies can be selected and applied to a controller, service platform or Access Point.

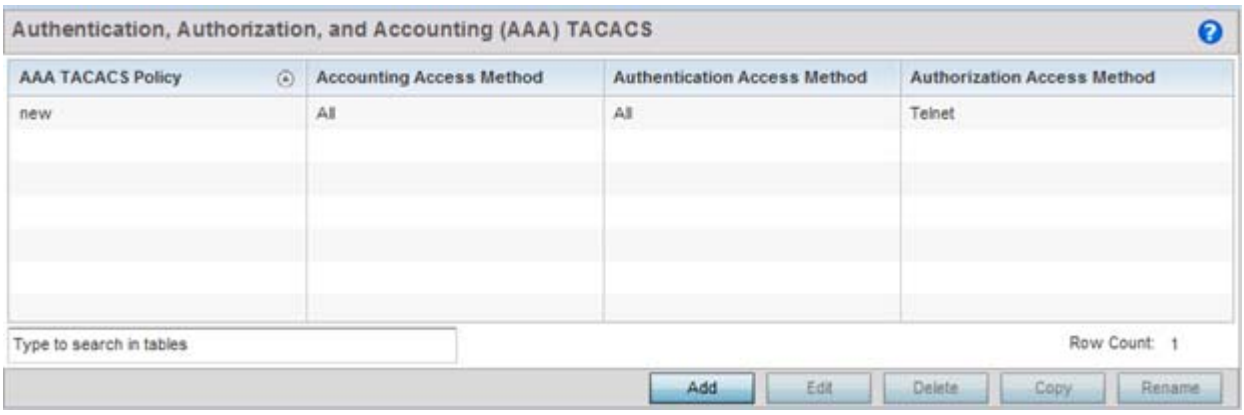


Figure 7-14 *Authentication, Authorization, and Accounting (AAA) TACACS screen*

4 Refer to the following information for each existing AAA TACACS policy to determine whether new policies require creation or existing policies require modification:

AAA TACACS Policy	Displays the name assigned to the AAA TACACS policy when it was initially created. The name cannot be edited within a listed profile.
Accounting Access Method	Displays the connection method used to access the AAA TACACS accounting server. Options include *All, SSH, Console,* or *Telnet.*
Authentication Access Method	Displays the method used to access the AAA TACACS authentication server. Options include *All, SSH, Console, Telnet,* or *Web.*
Authorization Access Method	Displays the method used to access the AAA TACACS authorization server. Options include *All, SSH, Console,* or *Telnet.*

5 Select **Add** to configure a new AAA TACACS policy. Optionally **Copy** or **Rename** a policy as needed.

6 Provide a 32 character maximum name for the policy in the **AAA TACACS Policy** field. Select **OK** to proceed. The **Server Info** tab displays by default.

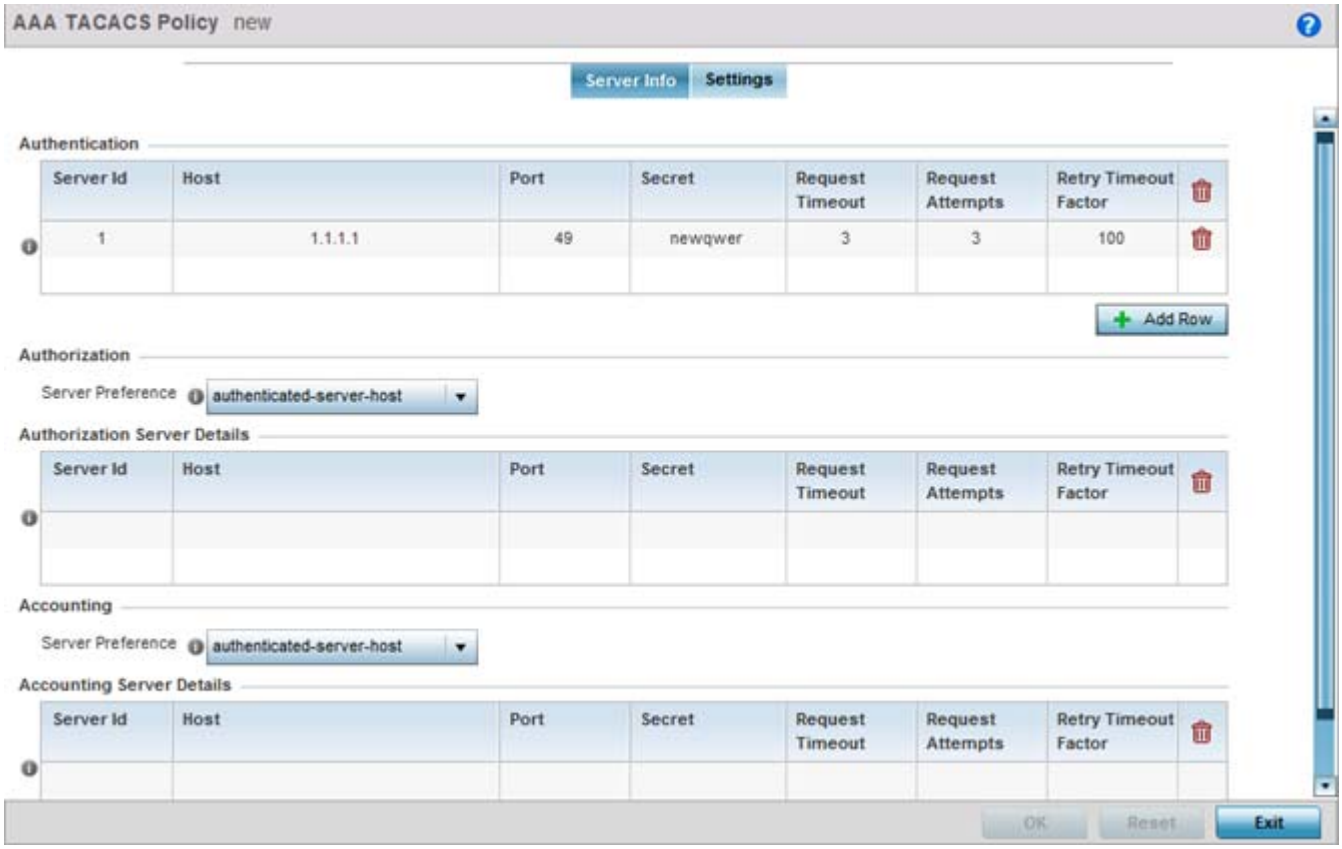


Figure 7-15 *AAA TACACS Policy - Server Info*

7 Under the **Authentication** table, select **+ Add Row**.

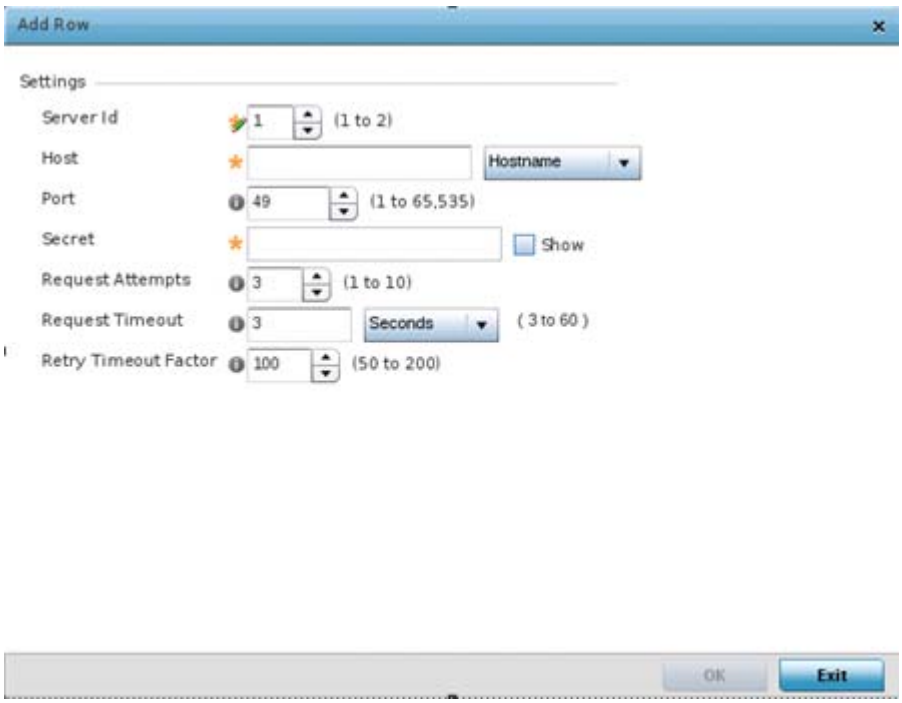


Figure 7-16 *AAA TACACS Policy - Authentication Server - Add Row*

8 Set the following Authentication settings:

Server Id	Set numerical server index (1-2) for the authentication server when added to the list of available TACACS authentication server resources.
Host	Specify the IP address or hostname of the AAA TACACS server. Hostnames cannot include an underscore character.
Port	Define or edit the port on which the AAA TACACS server listens to traffic. The port range is 1 - 65,535. The default port is 49.
Secret	Specify (and confirm) the secret (password) used for authentication between the selected AAA TACACS server and the controller, service platform or Access Point. By default the secret is displayed as asterisk. To show the secret in plain text, select *Show*.
Request Attempts	Set the number of connection request attempts to the TACACS server before it times out of the authentication session. The available range is from 1 - 10. The default is 3.
Request Timeout	Specify the time for the re-transmission of request packets after an unsuccessful attempt. The default is 3 seconds. If the set time is exceeded, the authentication session is terminated.
Retry Timeout Factor	Set the scaling of retransmission attempts from 50 - 200 seconds. The timeout at each attempt is the function of the retry timeout factor and the attempt number. 100 (the default value) implies a constant timeout on each retry. Smaller values indicate more aggressive (shorter) timeouts. Larger numbers define more conservative (larger) timeouts on each successive attempt. The default is 100.

9 Select **OK** to save the changes or **Exit** to close the screen.

10 Set the **Server Preference,** within the **Authorization** field, to specify which server, in the pool of servers, is selected to receice authorization requests. Options include *None*, *authenticated-server-host*, and *authenticated-server-number*. If selecting None or authenticated-server-number select **+ Add Row** and set the server's ID, host, port, password and connection attempt parameters.

11 Set the following **Authorization Server Details**:

Server Id	Lists the numerical server index (1-2) for each authentication server when added to the list available to the controller, service platform or Access Point.
Host	Displays the IP address or hostname set for the AAA TACACS authentication server.
Port	Displays the port the TACACS authentication server listens to traffic. The port range is 1 - 65,535. The default port is 49.
Secret	Specify (and confirm) the secret (password) used for authentication between the selected AAA TACACS server and the controller, service platform or Access Point. By default the secret is displayed as asterisks. To show the secret in plain text, select *Show.*
Request Attempts	Displays the number of connection attempts before the controller, service platform or Access Point times out of the authentication session. The available range is from 1 - 10. The default is 3.
Request Timeout	Specify the time for the re-transmission of request packets after an unsuccessful attempt. The default is 3 seconds. If the set time is exceeded, the authentication session is terminated.

Retry Timeout Factor	Set the scaling of retransmission attempts from 50 - 200 seconds. The timeout at each attempt is the function of the retry timeout factor and the attempt number. 100 (the default value) implies a constant timeout on each retry. Smaller values indicate more aggressive (shorter) timeouts. Larger numbers define more conservative (larger) timeouts on each successive attempt. The default is 100.

12 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

13 Set the **Server Preference,** within the **Accounting** field, to select the accounting server, from the pool of servers, to receive accounting requests. Options inlcude *None, authenticated-server-host*, *authenticated-server-number*, *authorized-server-host* and *authorized-server-number*. The default is authenticated-server-host. If selecting *None, authenticated-server-number* or *authorized-server-number* select **+ Add Row** and set the server's ID, host, port, password and connection attempt parameters.

14 Set the following **Accounting Server Details**:

Server Id	Lists the numerical server index (1-2) for each authentication server when added to the list available to the controller, service platform or Access Point.
Host	Displays the IP address or hostname set for the AAA TACACS authentication server.
Port	Displays the port the TACACS authentication server listens to traffic. The port range is 1 - 65,535. The default port is 49.
Secret	Specify (and confirm) the secret (password) used for authentication between the selected AAA TACACS server and the controller, service platform or Access Point. By default the secret is displayed as asterisks. To show the secret in plain text, select *Show*.
Request Attempts	Displays the number of connection attempts before the controller, service platform or Access Point times out of the authentication session. The available range is from 1 - 10. The default is 3.
Request Timeout	Specify the time for the re-transmission of request packets after an unsuccessful attempt. The default is 3 seconds. If the set time is exceeded, the authentication session is terminated.
Retry Timeout Factor	Set the scaling of retransmission attempts from 50 - 200 seconds. The timeout at each attempt is the function of the retry timeout factor and the attempt number. 100 (the default value) implies a constant timeout on each retry. Smaller values indicate more aggressive (shorter) timeouts. Larger numbers define more conservative (larger) timeouts on each successive attempt. The default is 100.

15 Select **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

16 Select the **Settings** tab.

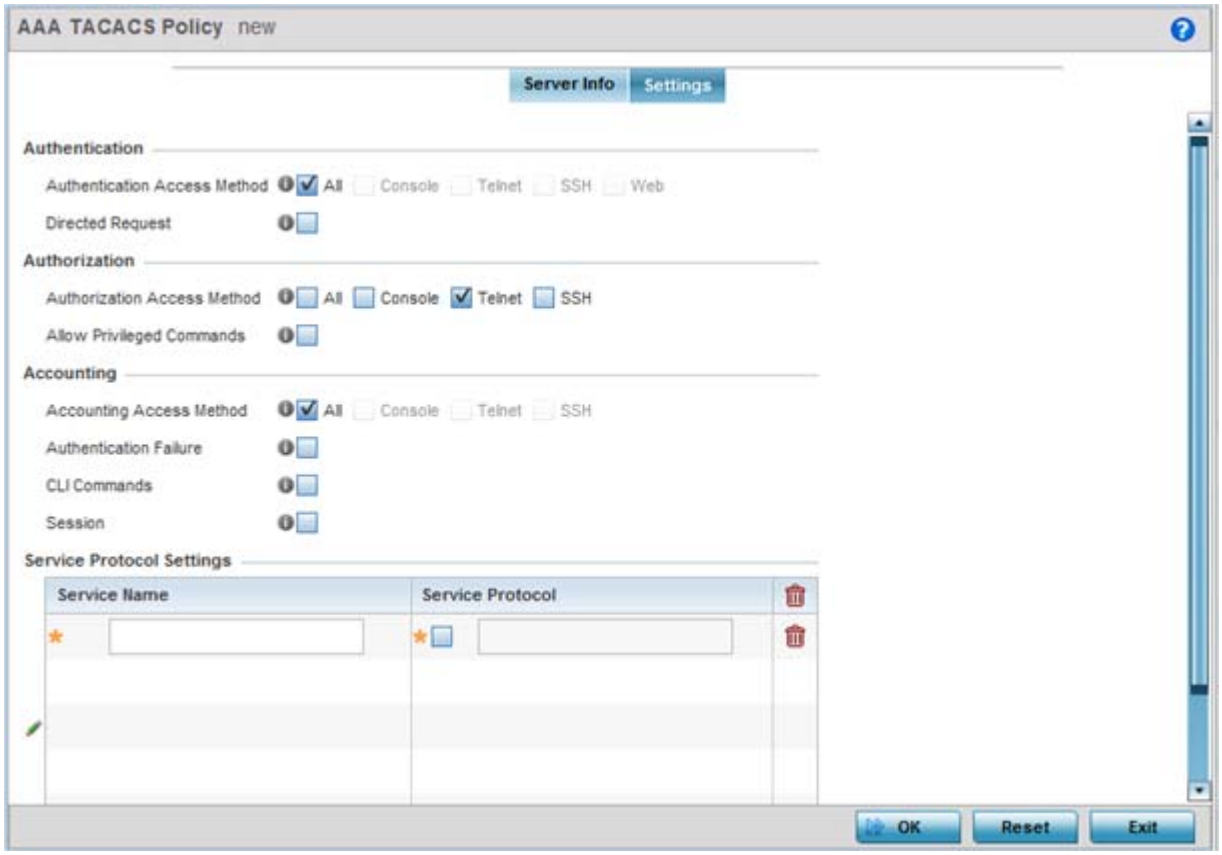


Figure 7-17 *AAA TACACS Policy - Settings screen*

17 Set the following AAA TACACS **Authentication** server configuration parameters:

Authentication Access Method	Specify the connection method(s) for authentication requests. • *All* – Authentication is performed for all types of access without prioritization. • *Console* – Authentication is performed only for console access. • *Telnet* – Authentication is performed only for access through Telnet. • *SSH* – Authentication is performed only for access through SSH. • *Web* – Authentication is performed only for access through the Web interface.
Directed Request	Select to enable the AAA TACACS authentication server to be used with the '@<server name>' nomenclature. The specified server must be present in the list of defined Authentication servers.

18 Set the following AAA TACACS **Authorization** server configuration parameters:

Authorization Access Method	Specify the connection methods for authorization requests: • *All* – Authorization is performed for all types of access without prioritization. • *Console* – Authorization is performed only for console access. • *Telnet* – Authorization is performed only for access through Telnet. • *SSH* – Authorization is performed only for access through SSH.

Allow Privileged Commands	Select this option to enable privileged commands executed without command authorization. Privileged commands are commands that can alter/change the authorization server configuration.

19 Set the following AAA TACACS **Accounting** server configuration parameters:

Accounting Access Method	Specify access methods for accounting server connections. • *All* – Accounting is performed for all types of access with none given priority. • *Console* – Accounting is performed for console access only. • *Telnet* – Accounting is performed only for access through Telnet. • *SSH* – Accounting is performed only for access through SSH.
Authentication Failure	Select the option to enable accounting upon authentication failures. This setting is disabled by default.
CLI Commands	Select this option to enable accounting for CLI commands. This setting is disabled by default.
Session	Select this option to enable accounting for session start and session stop events. This setting is disabled by default.

20 Select **+ Add Row** and set the following **Service Protocol Settings** parameters:

Service Name	Provide a 30 character maximum shell service for user authorization.
Service Protocol	Enter a protocol for user authentication using the service.

NOTE: A maximum or 5 entries can be made in the **Service Protocol Settings** table.

21 Select **OK** to save the updates to the AAA TACACS policy. Select **Reset** to revert to the last saved configuration.

7.6 IPv6 Router Advertisement Policy

An IPv6 router policy allows routers to advertise their presence in response to solicitation messages. After receiving a neighbor solicitation message, the destination node sends an advertisement message. which includes the link layer address of the source node. After receiving the advertisement, the destination device replies with a neighbor advertisement message on the local link. After the source receives the advertisement it can communicate with other devices.

Advertisement messages are also sent to indicate a change in link layer address for a node on the local link. With such a change, the multicast address becomes the destination address for advertisement messages.

To define a IPv6 router advertisement policy:

1 Select **Configuration** > **Network** > **IPv6 Router Advertisement Policy**.

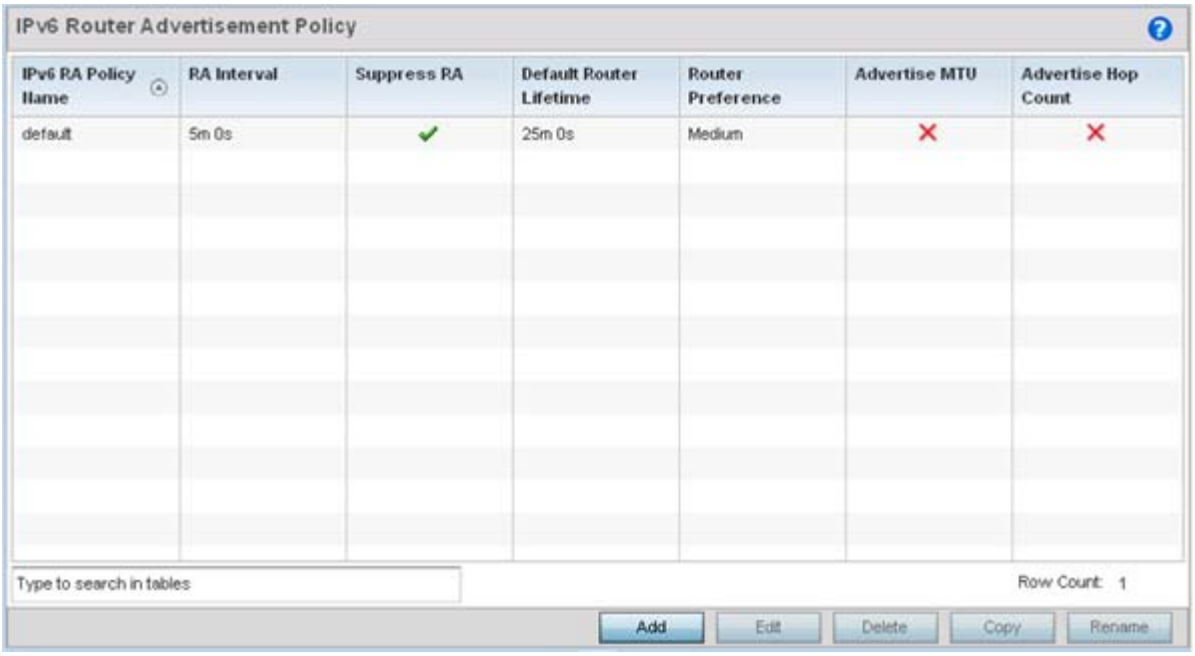


Figure 7-18 *Network IPv6 Router Advertisement Policy screen*

2 Select **Add** to create a new IPv6 router advertisement policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available. Existing policies can be copied or renamed as needed.

Provide a 32 character maximum name for the policy in the **IPv6 RA Policy Name** field. Select **OK** to proceed.

The **IPv6 RA Policy Name** screen displays.

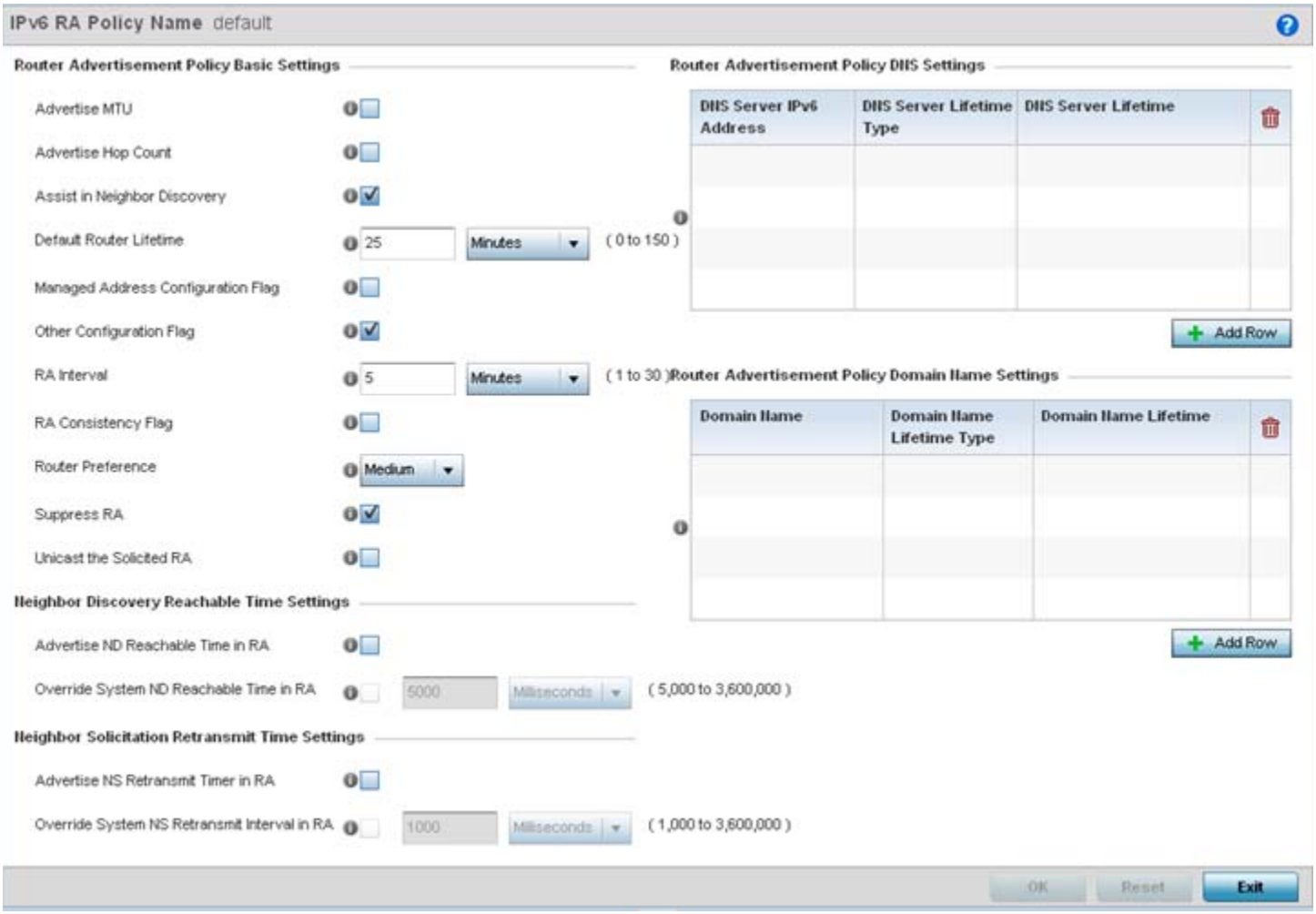


Figure 7-19 *Network IPv6 RA Policy Name screen*

3 Set the following **Router Advertisement Policy Basic Settings**:

Advertise MTU	Select this option to include the *Maximum Transmission Unit* (MTU) in the router advertisements. The default setting is disabled.
Advertise Hop Count	Select this option to include the hop count in the header of outgoing IPv6 packets. The default setting is disabled.
Assist in Neighbor Discovery	Select this option to send the source link layer address in a router advertisement to assist in neighbor discovery. The default setting is enabled.
Default Router Lifetime	Set the default router lifetime availability for IPv6 router advertisements. A lifetime of 0 indicates that the router is not a default router. The router advertisement interval range is 0 - 9000 *Seconds*, 0 - 150 *Minutes*, or 0 - 2.5 *Hours*. The default is 30 minutes.
Managed Address Configuration Flag	Select this option to send the managed address configuration flag in router advertisements. When set, the flag indicates that the addresses are available via DHCP v6. The default setting is disabled.

Other Configuration Flag	Select this option to send the other configuration flag in router advertisements. When set, the flag indicates other configuration information (DNS related information, information on other servers within the network) is available via DHCP v6. The default setting is disabled.
RA Interval	Set the interval for unsolicited IPv6 router assignments. The router advertisement interval range is 3 - 1800 seconds or 0 - 150 minutes. The default is 5 minutes.
RA Consistency Flag	Select this option to check if parameters advertised by other routers on the local link are in conflict with those router advertisements by this controller, service platform or Access Point. This option is disabled by default.
Router Preference	Set a *High*, *Medium* or *Low* preference designation on this router versus other router resource that may be available to the controller, service platform or Access Point. The default setting is medium.
Suppress RA	Use this setting to enable or diable the transmission of a router advertisement within the IPv6 packet. This setting is enabled by default.
Unicast Solicited RA	Select this option to enable the unicast (single destination) transmission of a router advertisement within the IPv6 packet. This setting is disabled by default.

4 Set the following **Neighbor Discovery Reachable Time Settings**:

Advertise ND Reachable Time in RA	Select this option *not* specify the neighbor reachable time in the router advertisements. When unspecified, the neighbor reachable time configured for the system is advertised. The default setting is disabled.
Override System ND Reachable Time in RA	Set the period for sending neighbor reachable time in the router advertisements. When unspecified, the neighbor reachable time configured for the system is advertised. The interval range is from 5,000 - 3,600,000 milliseconds. The default is 5000 milliseconds.

5 Set the following **Neighbor Solicitation Retransmit Time Settings**:

Advertise NS Retransmit Timer in RA	Select this option to *not* specify the neighbor solicitation retransmit timer value in router advertisements. The default setting is disabled.
Override System NS Retransmit Interval in RA	Set the period for sending the neighbor solicitation retransmit timer in router advertisements. When unspecified, the setting configured for the system is advertised. The interval range is from 1000 - 3,600,000 milliseconds. The default is 1000 milliseconds.

6 Select **+ Add Row** under the **Router Advertisement Policy DNS Settings** table and set the following:

DNS Server IPv6 Address	Use a DNS server to resolve host names to IPv6 addresses. When an IPv6 host is configured with the address of a DNS server, the host sends DNS name queries to the server for resolution. This field is mandatory
DNS Server Lifetime Type	Set the lifetime afforded to the DNS server resource. Options include *expired*, *External* (fixed), and *infinite*. The default is External (fixed).
DNS Server Lifetime	Set the maximum time the DNS server is available for name resolution. The interval range is from 1000 - 3,600,000 milliseconds. The default is 10 minutes.

7 Select **+ Add Row** under the **Router Advertisement Policy Domain Name Settings** table and define the following settings:

Domain Name	Enter a *fully qualified domain name* (FQDN) is an unambiguous domain name available a router advertisement resource. To distinguish an FQDN from a regular domain name, a trailing period is added. For example, somehost.example.com. This field is mandatory
Domain Name Lifetime Type	Set the DNS Server Lifetime Type. Options include *expired*, *External* (fixed), and *infinite.* The default is External (fixed).
Domain Name Lifetime	Set the maximum time the DNS domain name is available as a name resolution resource. The default is 10 minutes.

8 Select **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

7.7 BGP

Border Gateway Protocol (BGP) is an inter-ISP routing protocol for establishing routes between ISPs. ISPs use BGP to exchange routing and reachability information between *Autonomous Systems* (AS) on the Internet. BGP makes routing decisions based on paths, network policies and/or rules set by network administrators. The primary role of a BGP system is to exchange network reachability information with other BGP peers. This includes AS information the reachability information traverses. This information is sufficient to create a graph of AS connectivity from which routing decisions are created and rules enforced.

An *Autonomous System* (AS) is a set of routers under the same administration using *Interior Gateway Protocol* (IGP) and common metrics to define how to route packets. AS uses inter-AS routing to route packets to other ASs. For an external AS, an AS appears as a single coherent interior routing plan and presents a consistent picture of reachable destinations.

Routing information exchanged through BGP supports only destination based forwarding (it assumes that a router forwards packets based on the destination address carried in the IP header of the packet).

BGP uses TCP as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgment, and sequencing. BGP listens on TCP port 179. The error notification mechanism used in BGP assumes TCP supports a *graceful* close (all outstanding data is delivered before the connection is closed).

Refer to the following to configure access lists, path lists, IP prefix lists, community lists and external community lists for BGP:

- *IP Access List*
- *AS Path List*
- *IP Prefix List*
- *Community List*
- *External Community List*

To review existing BGP configurations or potentially create new ones:

1 Select the **Configuration** > **Network** > **BGP**.
Expand the BGP menu to display its submenu options.

2 Select **Route Map**.

In a BGP implementation, a route map is a method to control and modify routing information. The control and modification of routing information occurs using route redistribution rules.

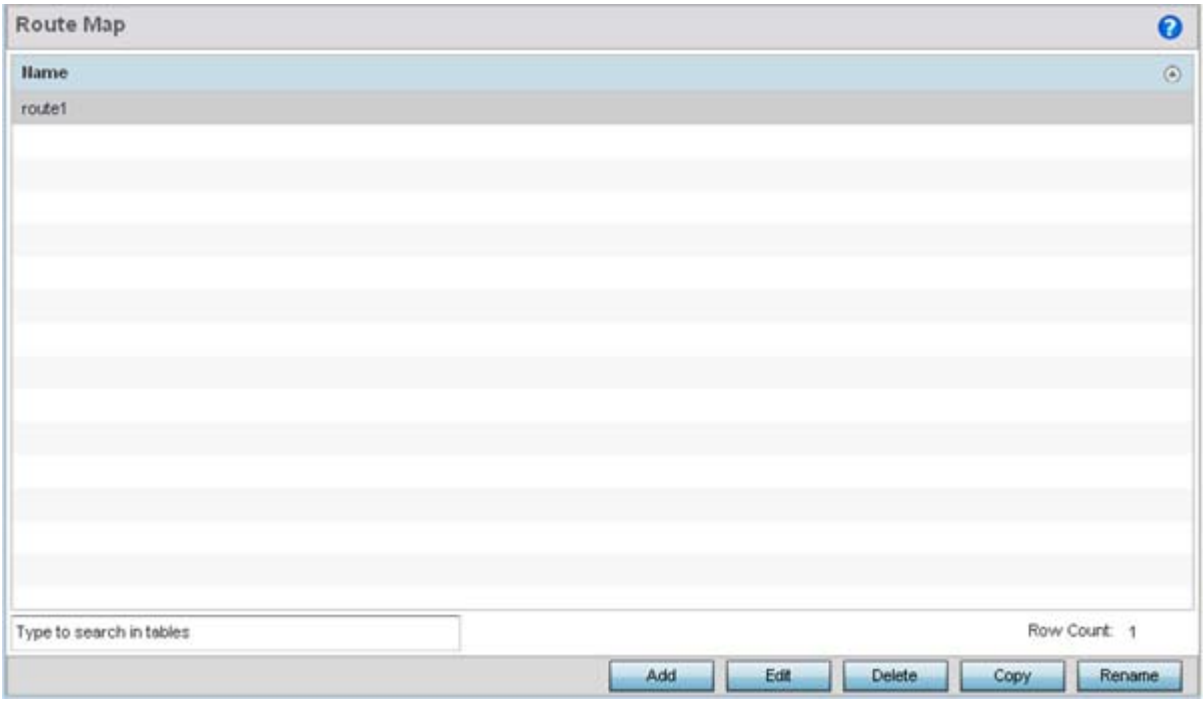


Figure 7-20 *Network BGP Route Map screen*

3 Select **Add** to create a new route map, **Edit** to modify the attributes of a selected route. Existing route map configurations can be copied or renamed as needed.

The **Route Map Rule** screen lists existing rules and their access permissions.

The **General** tab is displayed by default when adding or editing route maps.

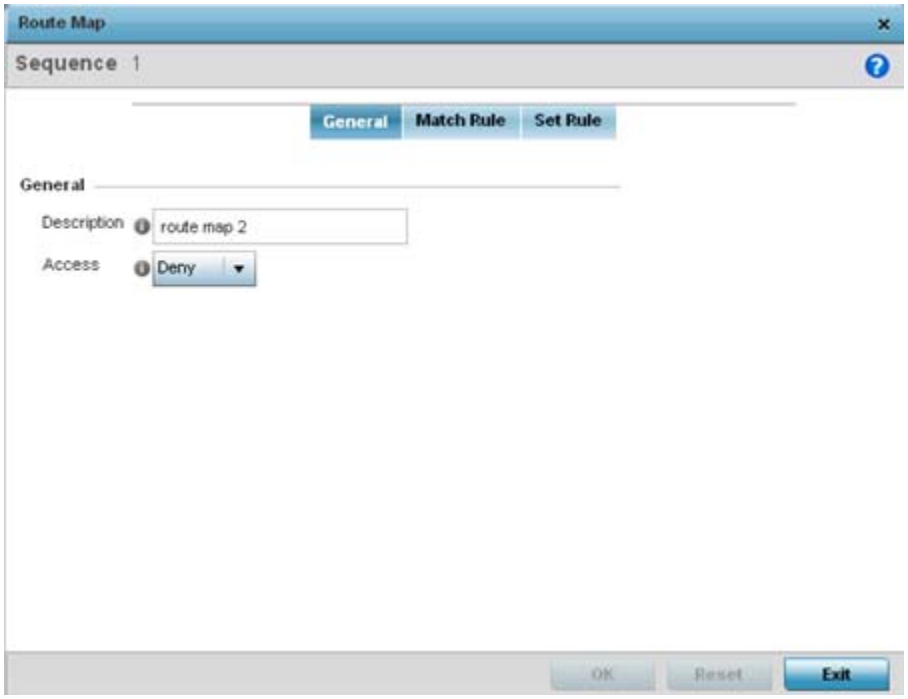


Figure 7-21 *Network Route Map Name - General screen*

4 Set the following **General** settings:

Description	Provide a 64 character maximum description to help distinguish this route map from others with similar access permissions.
Access	Set the *permit* or *deny* access designation for the route map. The default setting is deny.

5 Select the **Match Rule** tab.

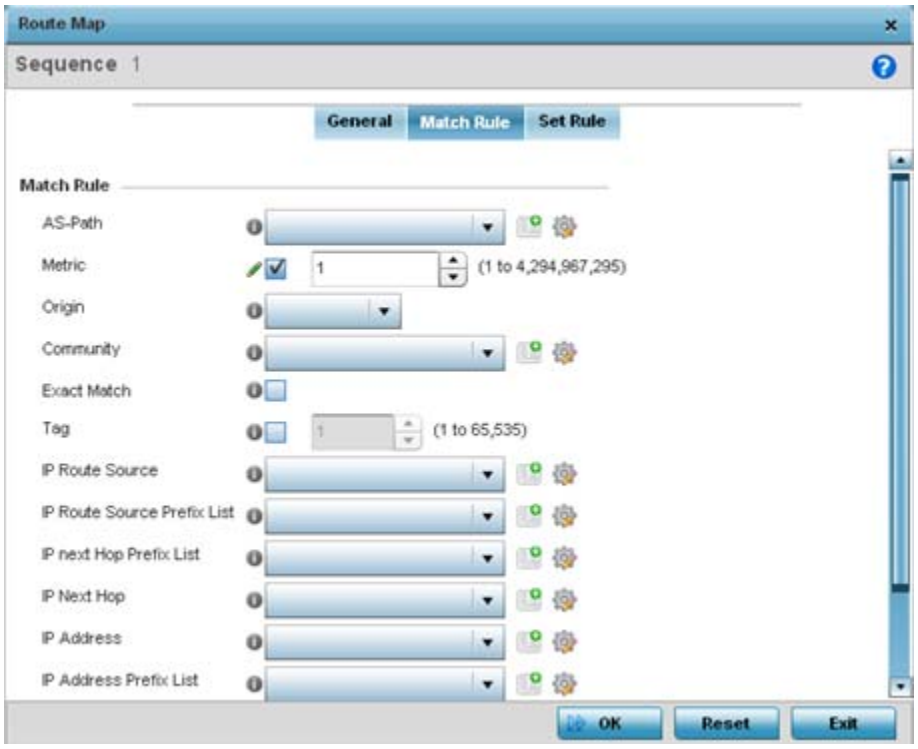


Figure 7-22 *Network Route Map Name - Match Rule screen*

6 Set the following **Match Rule** settings:

AS-Path	An AS path is a list of *Autonomous Systems* (AS) a packet traverses to reach its destination. From the drop-down menu, select a pre-configured AS-Path list. Use the *Create* icon to create an AS-Path list or select an existing one and use the *Edit* icon.
Metric	Select this option to define the exterior metric (1 - 4,294,967,295) used for route map distribution. BGP uses a route table managed by the external defined. Setting a metric provides a dynamic way to load balance between routes of equal cost.
Origin	Use the drop-down menu to set the source of the BGP route. Options include: *egp* - Matches if the origin of the route is from the *exterior gateway protocol* (eBGP). eBGP exchanges routing table information between hosts outside an autonomous system. *igp* - Matches if the origin of the route is from the *interior gateway protocol* (iBGP). iBGP exchanges routing table information between routers within an autonomous system. *incomplete* - Matches if the origin of the route is not identifiable.

Community	Use the drop-down menu to set the autonomous system community. A new community can be defined by selecting the *Create* icon, or an existing autonomous system community can be modified by selecting the *Edit* icon. Options include: *internet* - Advertises this route to the Internet. This is a global community. *local-AS* - Prevents the transmit of packets outside the local AS. *no-advertise* - Do not advertise this route to any peer, either internal or external. *no-export* - Do not advertise to BGP peers, keeping this route within an AS. *aa:nn* - The first part (aa) represents the AS number. The second part (nn) represents a 2-byte number.
Exact Match	When matching the *Community*, use exact matching. The default setting is disabled.
Tag	The *Tag* is a way to preserve a route's AS path information for routers in iBGP. The default setting is disabled.
IP Route Source	The *IP Route Source* is a list of IP addresses used to filter routes based on the advertised IP address of the source. Use the drop-down menu to set the IP route source. A new route source can be defined by selecting the *Create* icon, or an existing one can be modified by selecting the *Edit* icon.
IP Route Source Prefix List	The *IP Route Source Prefix List* is a list of prefixes used to filter routes based on the prefix list used for the source. Use the drop-down menu to set the IP route source prefix list. A new list can be defined by selecting the *Create* icon, or an existing AS-Path can be modified by selecting the *Edit* icon.
IP Next Hop Prefix List	The *IP Next Hop Prefix List* is a list of prefixes for the route's next hop determining how the route is filtered. Use the drop-down menu to set the IP next hop prefix list. A new list can be defined by selecting the *Create* icon, or an existing IP next hop prefix list can be modified by selecting the *Edit* icon.
IP Next Hop	The *IP Next Hop* is a list of IP addresses used to filter routes based on the IP address of the next hop in the route. Use the drop-down menu to set an IP next hop. A new next hop can be defined by selecting the *Create* icon, or an existing IP next hop can be modified by selecting the *Edit* icon.
IP Address	The *IP Address* parameter is a list of IP addresses in the route used to filter the route. Use the drop-down menu to set the IP address. A new address can be defined by selecting the *Create* icon, or an existing IP address can be modified by selecting the *Edit* icon.
IP Address Prefix List	The *IP Address Prefix List* is a list of prefixes in the route used to filter the route. Use the drop-down menu to set the IP address prefix list. A new community can be defined by selecting the *Create* icon, or an existing IP address prefix list can be modified by selecting the *Edit* icon.

7 Use the drop-down menu to set the **Math Rule Experimental Feature** External Community setting. A new External Community setting can be defined by selecting the **Create** icon, or an existing External Community setting can be modified by selecting the **Edit** icon.

8 Select the **Set Rule** tab.

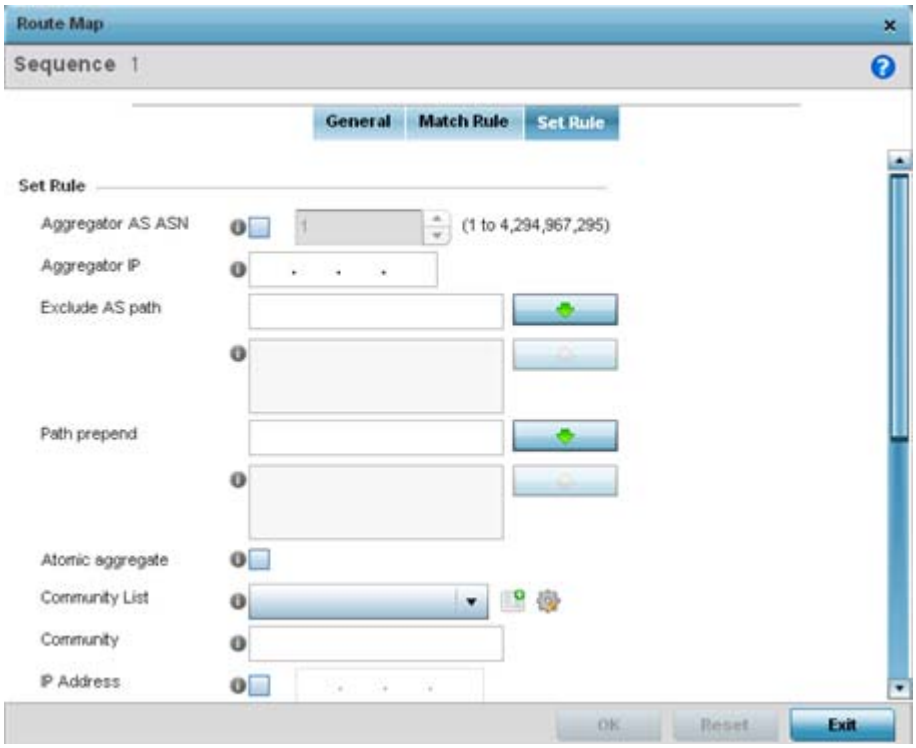


Figure 7-23 *Network Route Map Name - Set Rule screen*

9 Define the following **Set Rule** parameters:

Aggregator AS ASN	Select the *Autonomous System Number* (ASN) for the BGP aggregator. Aggregates minimize the size of routing tables. Aggregation combines the characteristics of multiple routes and advertises them as a single route. Select the ASN for this aggregator. Set a value from 1 - 4,294,967,295. This setting is disabled by default.
Aggregator IP	Provide the IP address of the route aggregator. BGP allows the aggregation of specific routes into one route using an aggregate IP address.
Exclude AS path	Enter an AS, or a list of ASs, excluded from the AS path.
Path prepend	Enter an AS, or a list of ASs, prepended to the AS path.
Atomic Aggregate	When a BGP enabled wireless controller or service platforms receives a set of overlapping routes from a peer, or if the set of routes selects a less specific route, then the local device must set this value when propagating the route to its neighbors. This setting is disabled by default.
Community List	The *Community List* is a list of communities added to the route. A BGP community is a group of routes sharing a common attribute.
Community	The *Community* is the community attribute set to this route.
IP Address	Set the IP address for this route.
Enable (Next hop peer)	Select this option to enable the identification of the next hop address for peer devices. This setting is disabled by default.
Local Preference	Select this option to enable the communication of preferred routes out of the AS between peers. This setting is disabled by default.

Metric	BGP uses a route table managed by the external metric defined. Setting a metric provides a dynamic way to load balance between routes of equal cost. Set a metric value for this route from 1 - 4,294,967,295.
Origin	Select the origin code for this BGP route. • *egp* - Sets the origin of the route to eBGP. • *igp* - Sets the origin of the route to iBGP. • *incomplete* - Sets the origin of the route as not identifiable. Set this if the route is from a source other than eBGP or iBGP.
Originator ID	Set the IP address of the originator of this route map.
Source ID	Set the IP address of the source of this route map.
Tag	The *Tag* is a way to preserve a route's AS path information for routers in iBGP. Set a tag value from 1 - 65535.
Weight	Select this option to enable the assignment of a weighted priority to the aggregate route. The range is 1 - 4,294,967,295.

10 Set the following **Set Rule Experimental Feature** settings:

Route Target Community	Enter a 254 character maximum route target community name.
Site of Origin Community	Enter a 254 character maximum origin community associated with the route reflector.

11 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

7.7.1 IP Access List

BGP peers and route maps can reference a single IP based access list. Apply IP access lists to both inbound and outbound route updates. Every route update is passed through the access list. BGP applies each rule in the access list in the order it appears in the list. When a route matches a rule, the decision to permit or deny the route is applied. No additional rules are processed.

To define a IP access list:

1 Select the **Configuration** > **Network** > **BGP**.
Expand the BGP menu to display its submenu options.

2 Select **IP Access List**.

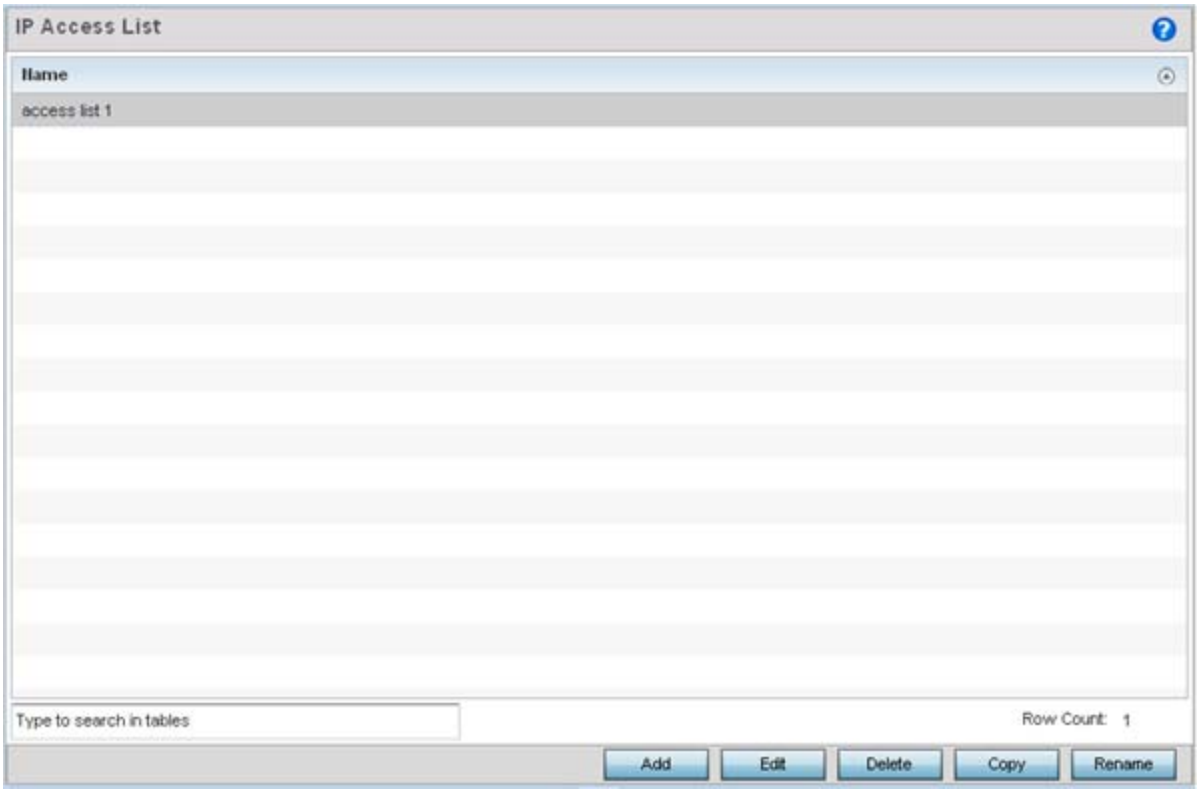


Figure 7-24 *Network BGP IP Access List screen*

3 Select **Add** to create a new IP access list, **Edit** to modify the attributes of a selected list or **Delete** to remove an obsolete list. Existing policies can be copied or renamed as needed.

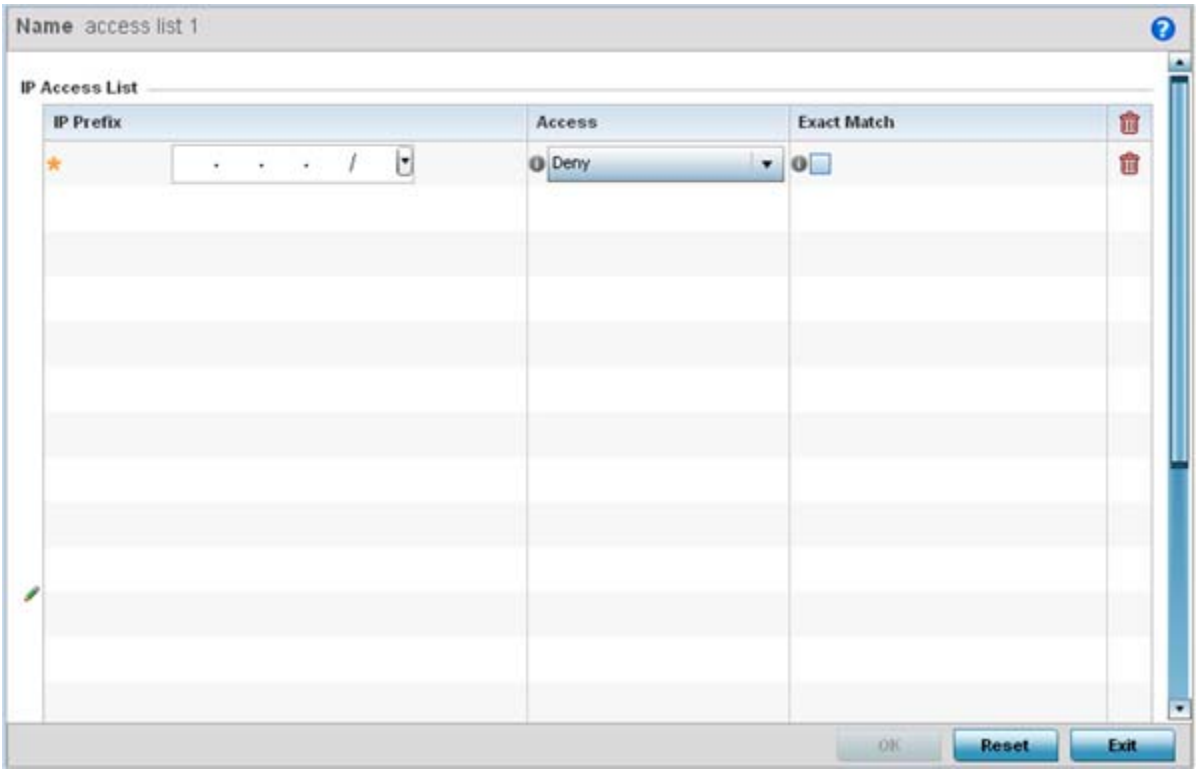


Figure 7-25 *Network BGP IP Access List Name screen*

4 Set the following **IP Access List** settings:

IP Prefix	Provide the IP address used to define the prefix list rule.
Access	Use the drop-down menu to *Permit* or *Deny* requests for network access originating from IP addresses with the IP prefix. The default setting is deny.
Exact Match	Check to require an exact match for the IP prefix before access is granted. Permit and deny apply only when there is an exact match between the regular expression and the autonomous system path.This setting is disabled by default.

5 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

7.7.2 AS Path List

BGP uses a routing algorithm to exchange network reachability information with other BGP supported devices. Network availability ad reachability information is exchanged between BGP peers in routing updates. This information contains a network number, path specific attributes and the list of autonomous system numbers a route transits to reach a destination. This list is contained in the *AS path*. BGP prevents routing loops by rejecting any routing update that contains a local autonomous system number, as this indicates the route has already traveled through that autonomous system and a loop would be created. BGP's routing algorithm is a combination of a distance vector routing algorithm and AS path loop detection.

The AS path contains a set of numbers for passing routing information. A BGP supported device adds its own autonomous system number to the list when it forwards an update message to external peers.

To define an AS path list:

1 Select the **Configuration** > **Network** > **BGP**.
Expand the BGP menu to display its submenu options.

2 Select **AS Path List**.

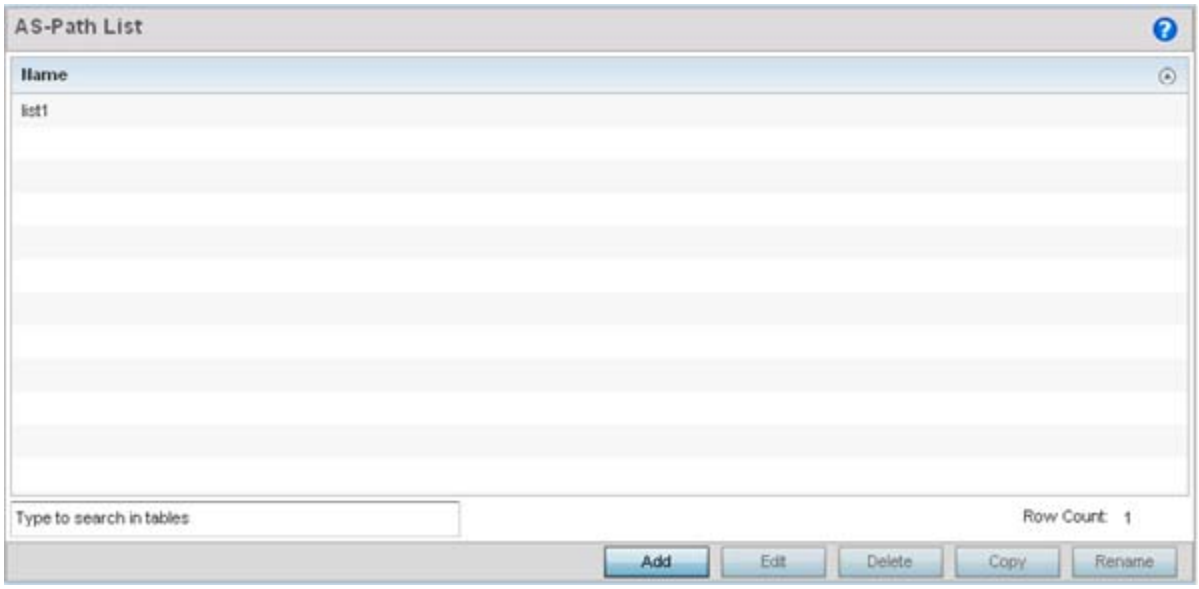


Figure 7-26 *Network BGP AS Path List screen*

3 Select **Add** to create a new AS path list or **Edit** to modify the attributes of a selected path list. Existing policies can be copied or renamed as needed.

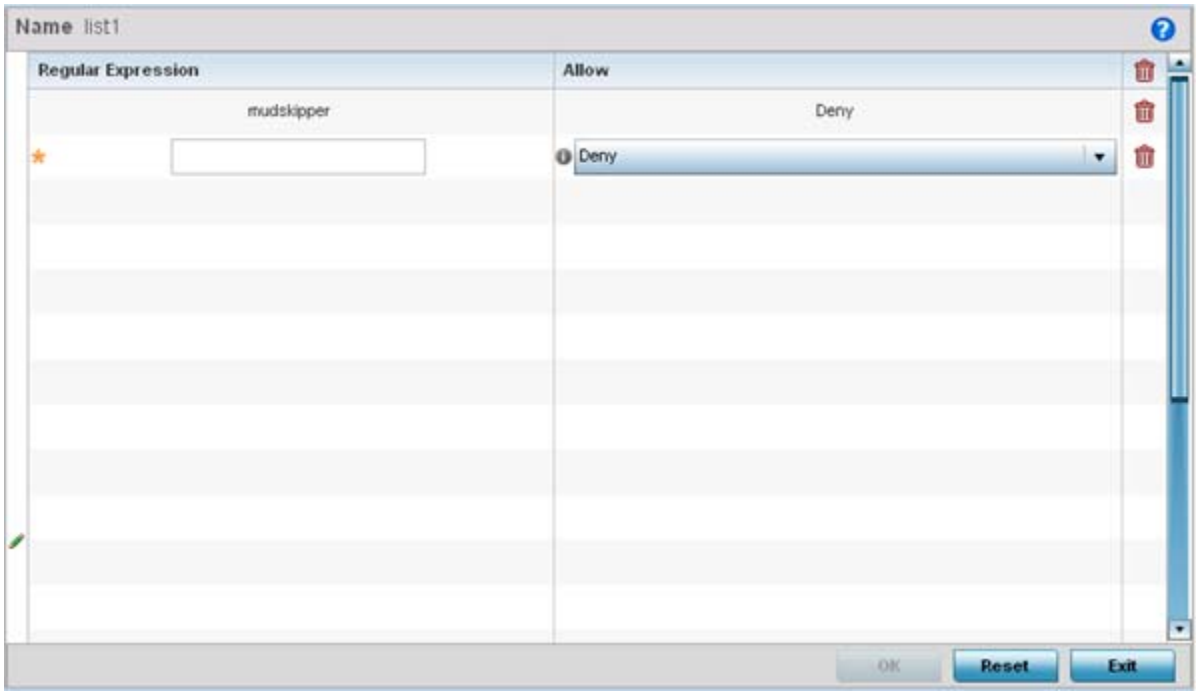


Figure 7-27 *Network BGP AS Path List Name screen*

4 Set the following **AS Path List** settings:

Regular Expression	Provide a 64 character maximum regular expression unique to the AS path list rule. Regular expressions are used to specify patterns to match community attributes.
Allow	Use the drop-down menu to *Permit* or *Deny* requests for network access using the defined AS path list. The default setting is deny.

5 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

7.7.3 IP Prefix List

IP prefix lists are a convenient way to filter networks in BGP supported networks. IP prefix lists work similarly to access lists. A prefix list contains ordered entries processed sequentially. Like access lists, the evaluation of a prefix against a prefix list ends as soon as a match is found.

To restrict the routing information advertised, use filters consisting of an IP prefix list applied to updates both to and from neighbors.

To define an IP prefix list:

1 Select the **Configuration** > **Network** > **BGP**.
Expand the BGP menu to display its submenu options.

2 Select **IP Prefix List**.

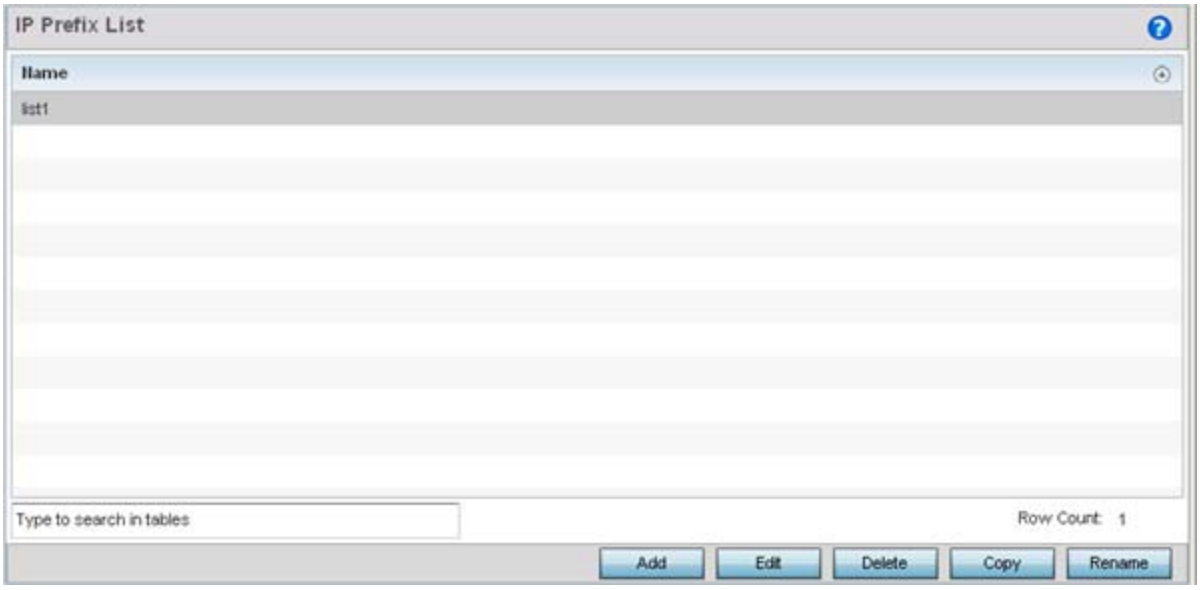


Figure 7-28 *Network BGP IP Profile List screen*

3 Select **Add** to create a new IP prefix list or **Edit** to modify the attributes of a selected list. Existing policies can be copied or renamed as needed.

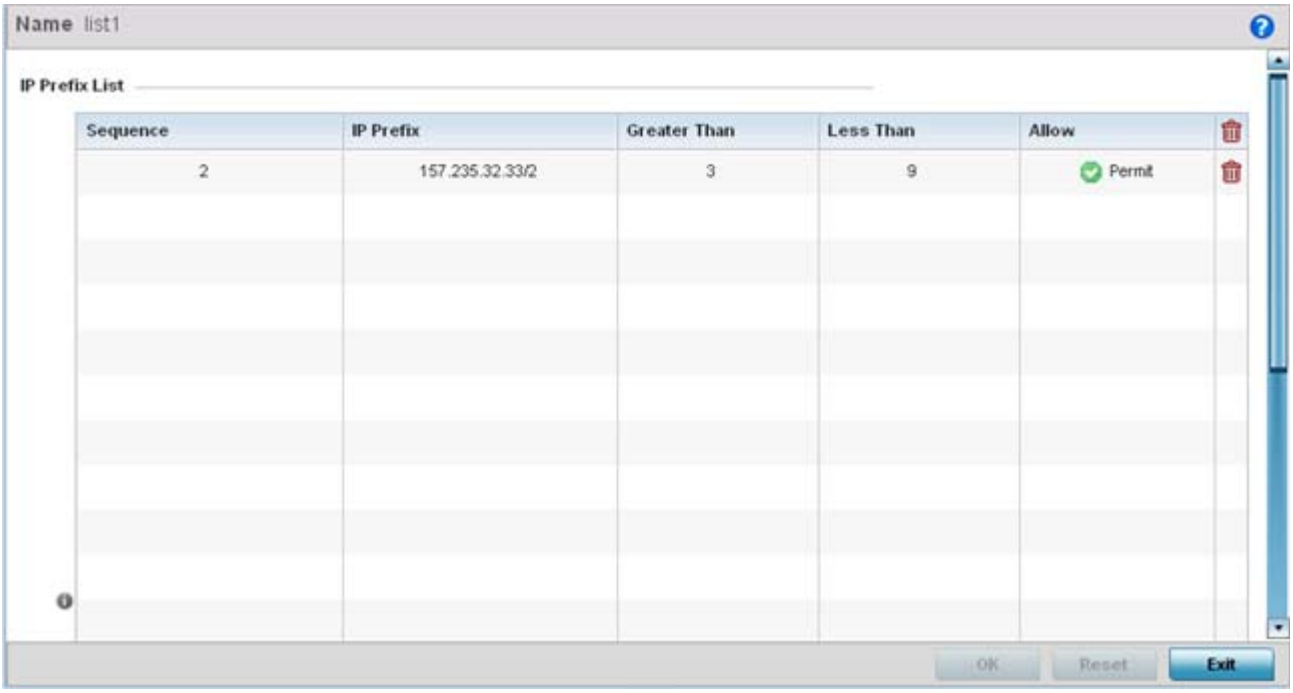


Figure 7-29 *Network BGP IP Prefix List Name screen*

4 Define the following **IP Prefix List** settings:

Sequence	Supply a sequence number to determine the prefix utilization order for existing lists.
IP Prefix	Set the IP prefix used as an prefix list rule.
Greater Than	Specify a greater than or equal to value for an IP prefix range.
Less Than	Specify a less than or equal to value for an IP prefix range.
Allow	Use the drop-down menu to set a *Permit* or *Deny* designation to the rule configuration.

5 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

7.7.4 Community List

A BGP community is a group of routes sharing a common attribute. The BGP list enables an administrator to assign names to community lists and increase the number of community lists configurable. A community list can be configured with regular expressions and numbered community lists. All the rules in numbered communities apply to named community lists, except there is no limitation in the number of community attributes configurable for a named community list.

To define a BGP community list:

1 Select the **Configuration** > **Network** > **BGP**.
Expand the BGP menu to display its submenu options.

2 Select **Community List**.

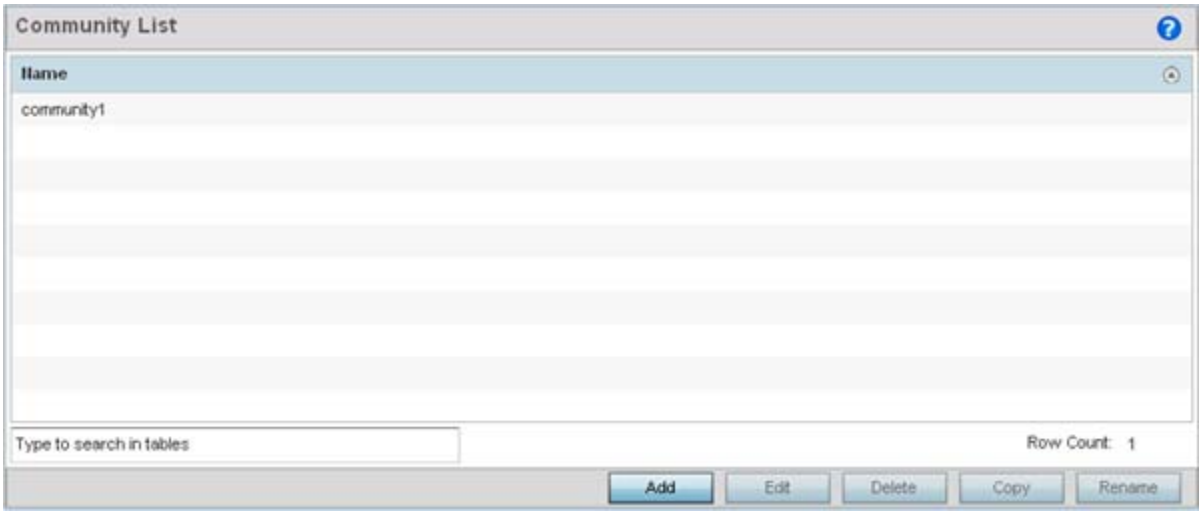


Figure 7-30 *Network BGP Community List screen*

3 Select **Add** to create a new community list or **Edit** to modify the attributes of a selected list. Existing lists can be copied or renamed as needed.

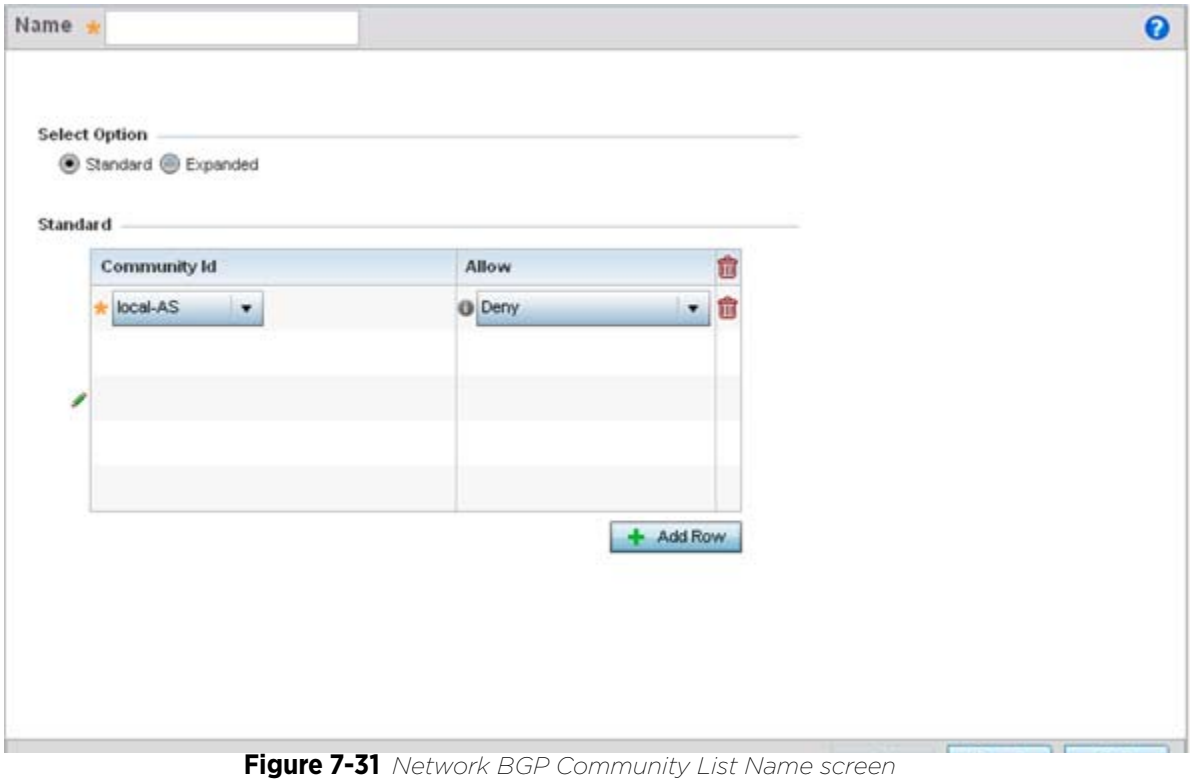


Figure 7-31 *Network BGP Community List Name screen*

4 Define whether the list is **Standard** or **Expanded.**

Standard community lists specify known communities and community numbers. *Expanded* community lists filter communities using a regular expression that specifies patterns to match the attributes of different communities.

5 Set the following Community List settings:

Community Id	Provide a community ID unique to this particular rule. The following are available: *internet* - Advertises this route to the Internet. This is a global community. *local-AS* - Prevents the transmit of packets outside the local AS. *no-advertise* - Do not advertise this route to any peer, either internal or external. *no-export* - Do not advertise to BGP peers (keeping) this route within an AS. *aa:nn* - The first part (aa) represents the AS number. The second part (nn) represents a 2-byte number.
Allow	Use the drop-down menu to *Permit* or *Deny* requests for the community ID. The default setting is deny.

6 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

7.7.5 External Community List

A BGP external community is a group of routes sharing a common attribute, regardless of their network or physical boundary. By using a BGP community attribute, routing policies can implement *inbound* or *outbound* route filters based on a community tag, rather than a long list of individual permit or deny rules. A BGP community list is used to create groups of communities to use in a match clause of a route map. An external community list can be used to control which routes are accepted, preferred, distributed, or advertised.

To define a BGP external community list:

1 Select the **Configuration** > **Network** > **BGP**.
Expand the BGP menu to display its submenu options.

2 Select **External Community List**.

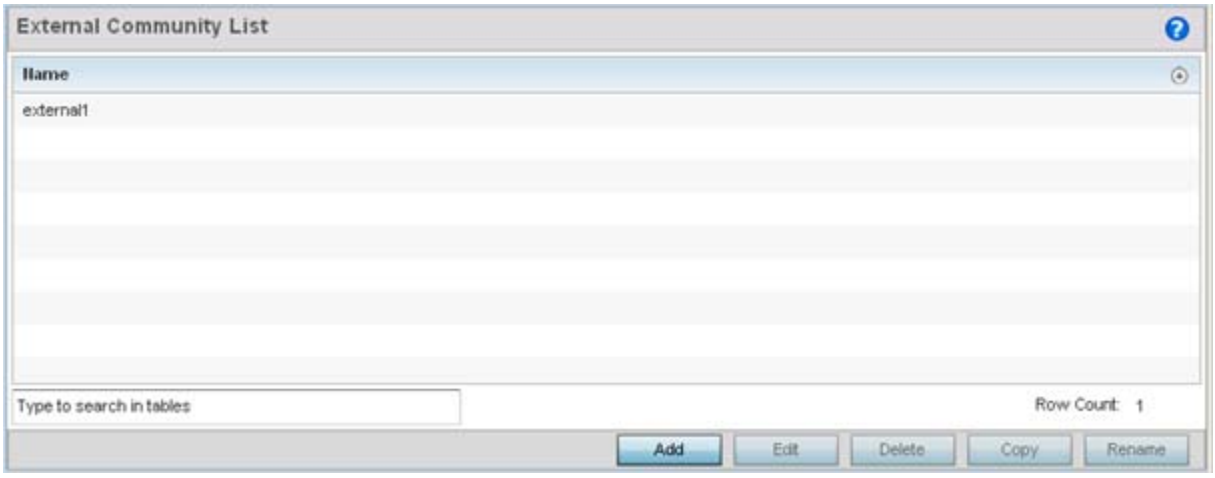


Figure 7-32 *Network BGP External Community List screen*

3 Select **Add** to create a new external community list, **Edit** to modify the attributes of a selected list or **Delete** to remove an obsolete list from those available. Existing lists can be copied or renamed as needed.

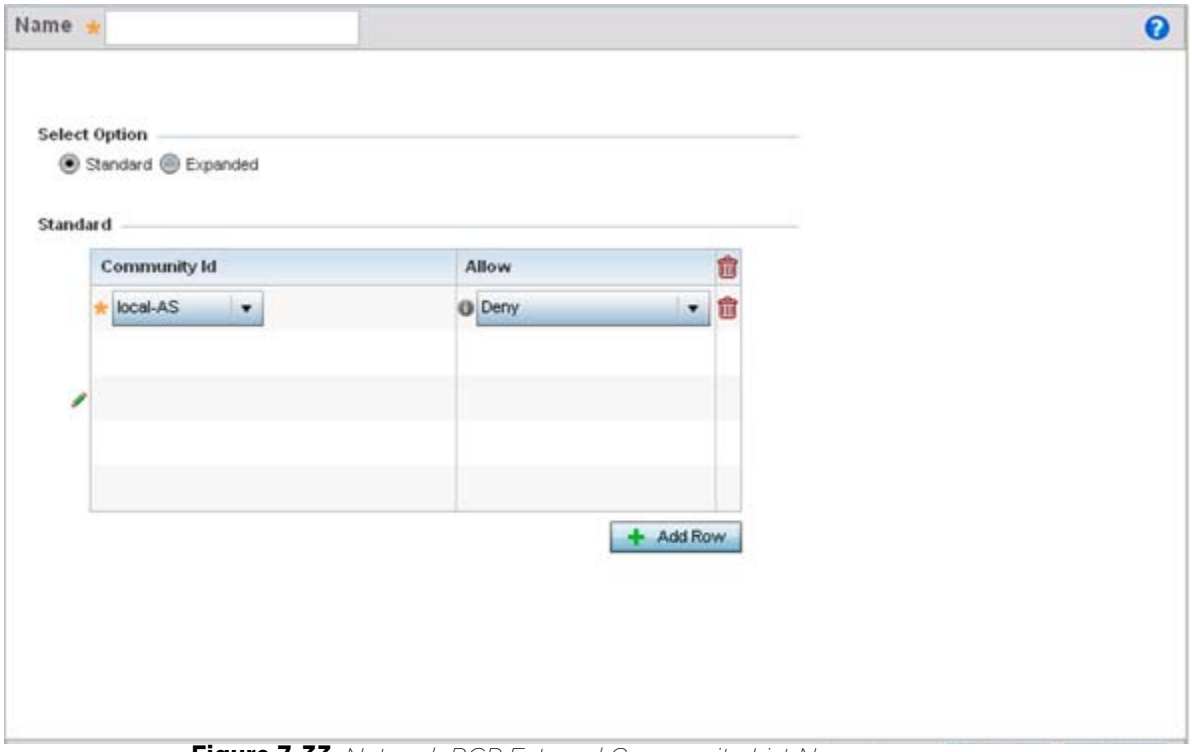


Figure 7-33 *Network BGP External Community List Name screen*

4 Define whether the list is **Standard** or **Expanded.**

Standard community lists specify known communities and community numbers. *Expanded* community lists filter communities using a regular expression that specifies patterns to match the attributes of different communities.

5 Set the following based on the Standard or Extended option selected:

Community Id	If selecting *Standard*, enter a numeric community ID unique to this particular rule. If selecting *Extended*, enter a regular expression unique to this particular rule.
Allow	Use the drop-down menu to *Permit* or *Deny* requests for the external community ID. The default setting is deny.

6 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

7.8 Alias

With large deployments, the configuration of remote sites utilizes a set of shared attributes, of which a small set of attributes are unique for each location. For such deployments, maintaining separate configuration (WLANs, profiles, policies and ACLs) for each remote site is complex. Migrating any global change to a particular configuration item to all the remote sites is a complex and time consuming operation.

Also, this practice does not scale gracefully for quick growing deployments.

An alias enables an administrator to define a configuration item, such as a hostname, as an alias once and use the defined alias across different configuration items such as multiple ACLs.

Once a configuration item, such as an ACL, is utilized across remote locations, the Alias used in the configuration item (ACL) is modified to meet local deployment requirement. Any other ACL or other configuration items using the modified alias also get modified, simplifying maintenance at the remote deployment.

Aliases have scope depending on where the Alias is defined. Alias are defined with the following scopes:

- *Global aliases* are defined from the **Configuration** > **Network** > **Alias** screen. Global aliases are available for use globally across all devices, profiles and RF Domains in the system.
- *Profiles aliases* are defined from the **Configuration** > **Devices** > **System Profile** > **Network** > **Alias** screen. Profile aliases are available for use to a specific group of wireless controllers or Access Points. Alias values defined in a profile override the alias values defined within global aliases.
- *RF Domain aliases* are defined from the **Configuration** > **Devices** > **RF Domain** > **Alias** screen. RF Domain aliases are available for use for a site as a RF Domain is site specific. RF Domain alias values override alias values defined in a global alias or a profile alias configuration.
- *Device aliases* are defined from the **Configuration** > **Devices** > **Device Overrides** > **Network** > **Alias** screen. Device aliases are utilized by a singular device only. Device alias values override global, profile or RF Domain alias configurations.

Using an alias, configuration changes made at a remote location override any updates at the management center. For example, if an network alias defines a network range as 192.168.10.0/24 for the entire network, and at a remote deployment location, the local network range is 172.16.10.0/24, the network alias can be overridden at the deployment location to suit the local requirement. For the remote deployment location, the network alias work with the 172.16.10.0/24 network. Existing ACLs using this network alias need not be modified and will work with the local network for the deployment location. This simplifies ACL definition and management while taking care of specific local deployment requirements.

For more information, refer to the following:

- *Network Basic Alias*
- *Network Group Alias*
- *Network Service Alias*

7.8.1 Network Basic Alias

A *basic alias* is a set of configurations consisting of *VLAN*, *Host*, *Network* and *Address Range* alias configurations. A VLAN alias is a configuration for optimal VLAN re-use and management for local and remote deployments. A host alias configuration is for a particular host device's IP address. A network alias configuration is utilized for an IP address on a particular network. An address range alias is a configuration for a range of IP addresses.

To set a network basic alias configuration:

1 Select **Configuration** > **Network** from the Web UI.

2 Select **Alias** from the Network menu options on the left-hand side of the UI.
The Alias screen displays with the Basic Alias tab displayed by default.

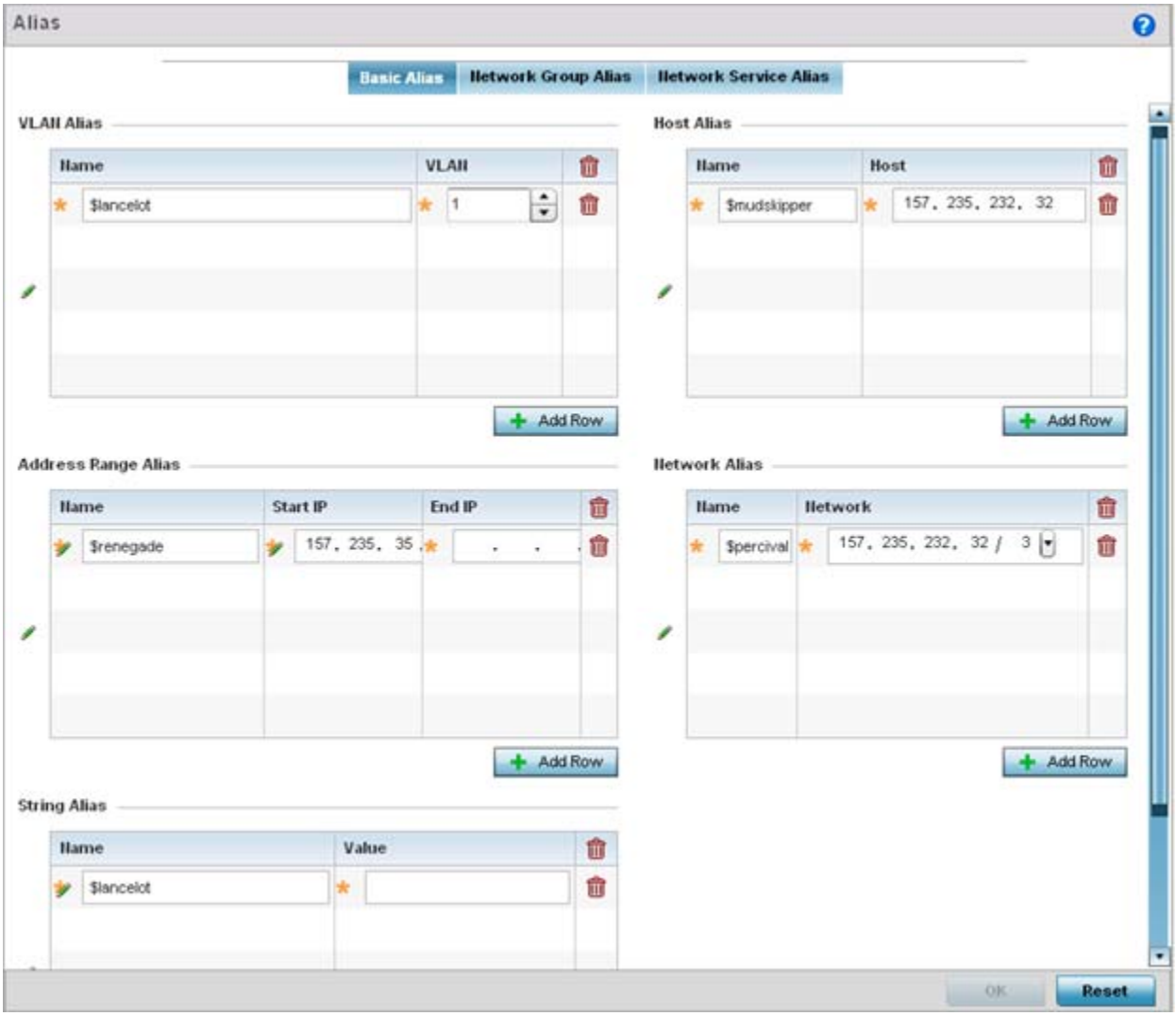


Figure 7-34 *Basic Alias screen*

3 Select **+ Add Row** to define **VLAN Alias** settings:

Use the **Vlan Alias** field to create unique aliases for VLANs that can be utilized at different deployments. For example, if a VLAN ID is set as 10 for the central network, and the VLAN is set as 26 at a remote location, the VLAN can be overridden at the remote location using an alias. At the remote location, the network is functional with an ID of 26, but utilizes the name defined at the central local network. A new VLAN need not be created specifically at the remote location.

Name	If adding a new *VLAN Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Vlan	Use the spinner control to set a numeric VLAN from 1 - 4094.

4 Select **+ Add Row** to define **Address Range Alias** settings:

Use the **Address Range Alias** field to create aliases for IP address ranges that can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110,

the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.

Name	If adding a new *Address Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Start IP	Set a starting IP address used with a range of addresses utilized with the address range alias.
End IP	Set an ending IP address used with a range of addresses utilized with the address range alias.

5 Select **+ Add Row** to define **String Alias** settings:

Use the **String Alias** field to create aliases for hosts that can be utilized at different deployments. For example, if the main domain at a remote location is called loc1.domain.com and at another deployment location it is called loc2.domain.com, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the loc1.domain.com domain and at the other with the loc2.domain.com domain.

Name	If adding a new *String Alias,* provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Value	Provide a string value to use in the alias.

6 Select **+ Add Row** to define **Host Alias** settings:

Use the **Host Alias** field to create aliases for hosts that can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.

Name	If adding a new *Host Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Host	Set the IP address of the host machine.

7 Select **+ Add Row** to define **Network Alias** settings:

Use the **Network Alias** field to create aliases for IP networks that can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

Name	If adding a new *Network Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Network	Provide a network address in the form of *host/mask*.

8 Select **OK** when completed to update the set of basic alias rules. Select **Reset** to revert the screen back to its last saved configuration.

7.8.2 Network Group Alias

A *network group alias* is a set of configurations consisting of host and network configurations. Network configurations are complete networks in the form of 192.168.10.0/24 or an IP address range in the form of 192.168.10.10-192.168.10.20. Host configurations are in the form of a single IP address, 192.168.10.23.

A network group alias can contain multiple definitions for a host, network, and IP address range. A maximum of eight (8) Host entries, eight (8) network entries and eight (8) IP addresses range entries can be configured inside a network group alias. A maximum of 32 network group alias entries can be created.

To set a network group alias configuration:

1 Select **Configuration** > **Network** from the Web UI.

2 Select **Alias** from the Network menu options on the left-hand side of the UI.

3 Select the **Network Group Alias** tab. The screen displays existing network group alias configurations.

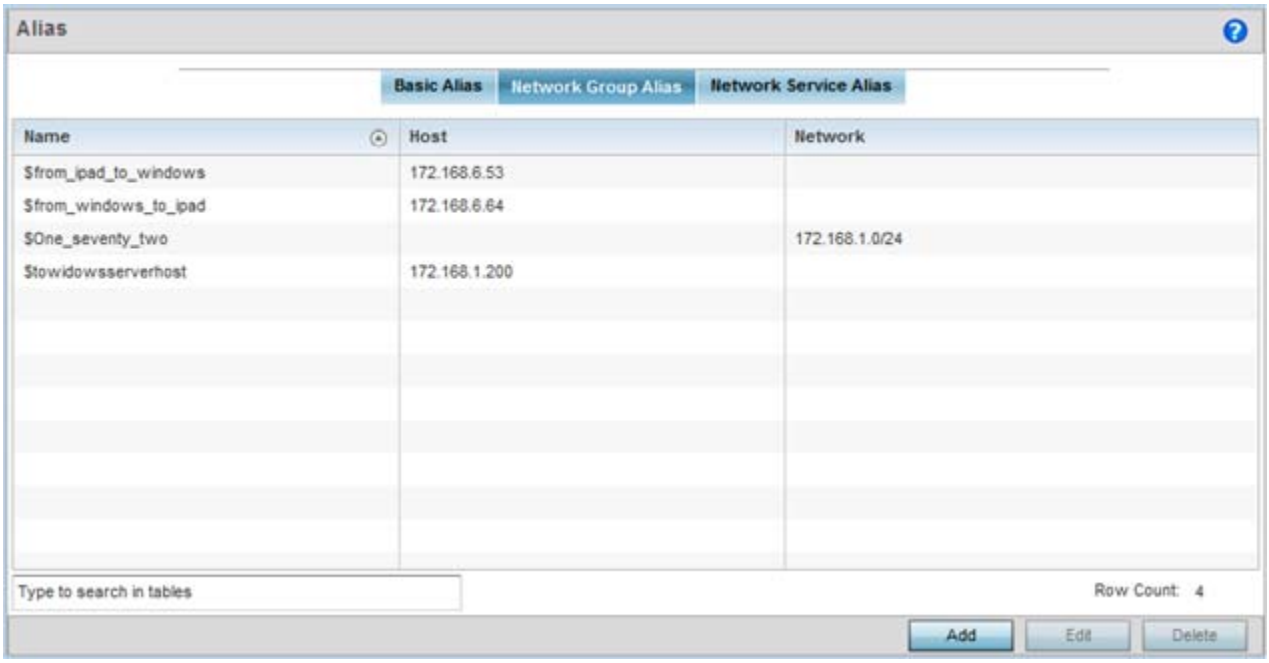


Figure 7-35 *Network Group Alias screen*

Name	Displays the administrator assigned name used with the network group alias.
Host	Displays all the host aliases configured in the listed network group alias. Displays a blank column if no host alias is defined.
Network	Displays all network aliases configured in the listed network group alias. Displays a blank column if no network alias is defined.

4 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies.

5 Select the added row to expand it into configurable parameters for defining the network alias rule.

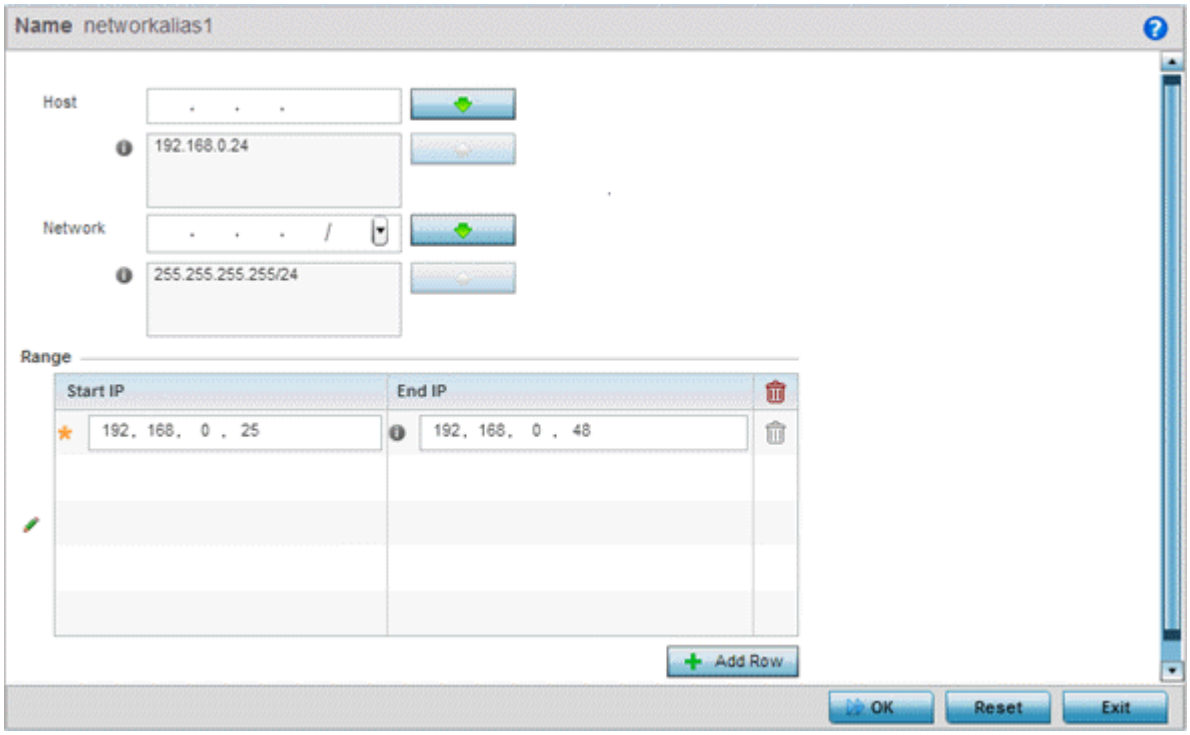


Figure 7-36 *Network Group Alias Add screen*

6 If adding a new **Network Alias Rule,** provide it a name up to 32 characters. The network group alias name always starts with a dollar sign ($).

7 Define the following network alias parameters:

Host	Specify the Host IP address for up to eight IP addresses supporting network aliasing. Select the down arrow to add the IP address to the table.
Network	Specify the netmask for up to eight IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Select the down arrow to add the mask to the table.

8 Within the **Range** table, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the alias range or double-click on an existing an alias range entry to edit it.

9 Select **OK** when completed to update the network alias rules. Select **Reset** to revert the screen back to its last saved configuration.

7.8.3 Network Service Alias

A *Network service alias* is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per network service alias.

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

To define a service alias configuration:

1 Select **Configuration** > **Network** from the Web UI.

2 Select **Alias** from the Network menu options on the left-hand side of the UI.

3 Select the **Network Service Alias** tab. The screen displays existing network service alias configurations.

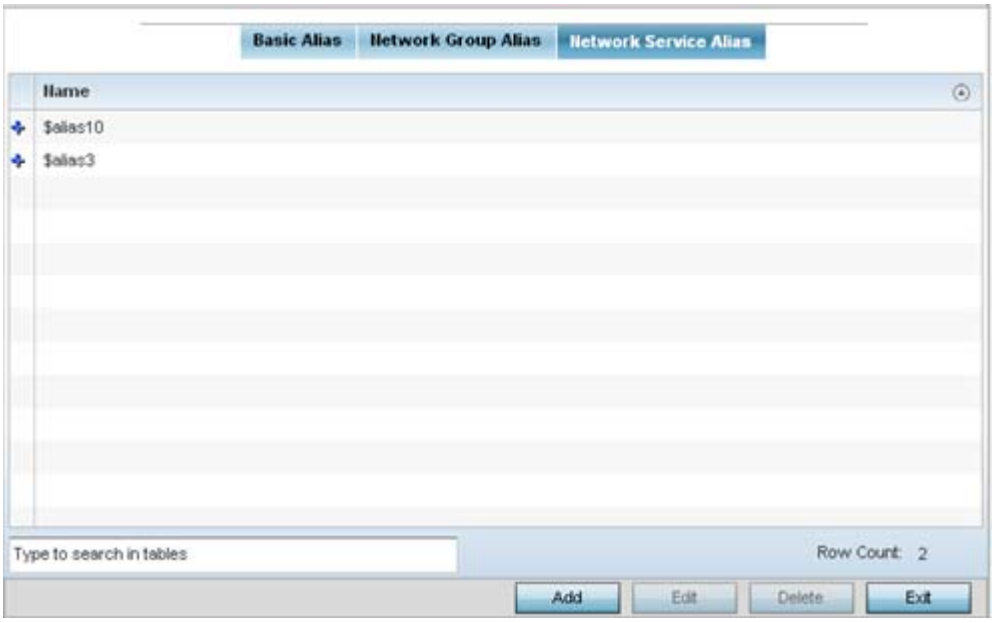


Figure 7-37 *Network Service Alias screen*

4 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies.

5 Select the added row to expand it into configurable parameters for defining the service alias rule.

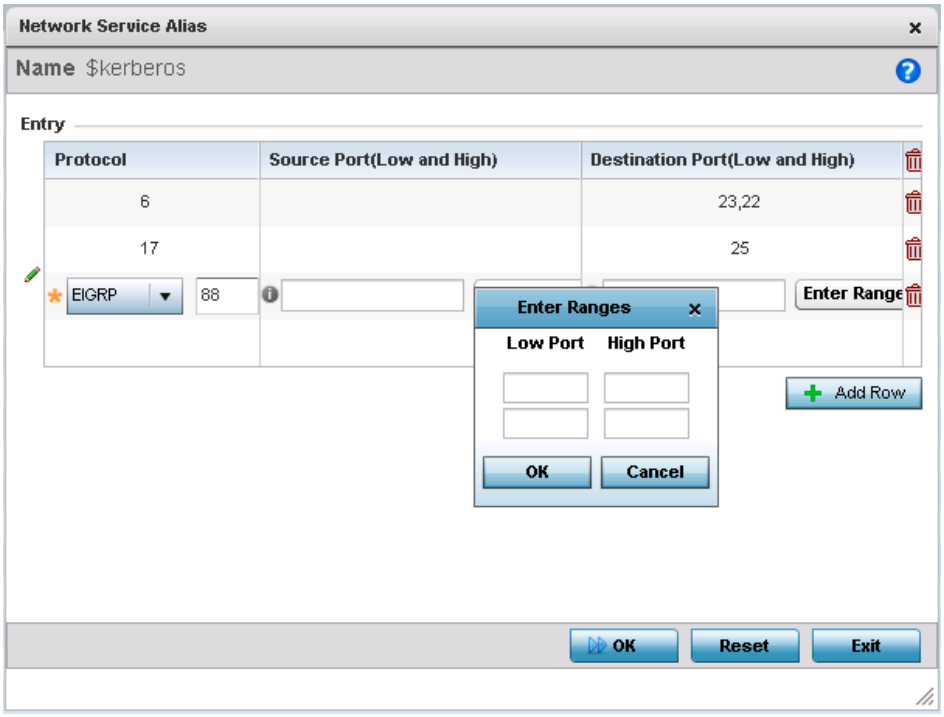


Figure 7-38 *Network Service Alias Add screen*

6 If adding a new **Service Alias Rule,** provide it a name up to 32 characters. Ensure a $ precedes the name.

7 Select **+ Add Row** and provide the following configuration parameters:

Protocol	Specify the protocol for which the alias has to be created. Use the drop down to select the protocol from *eigrp, gre, icmp, igmp, ip, vrrp, igp, ospf, tcp* and *udp.* Select *other* if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected.
Source Port (Low and High)	This field is only relevant if the protocol is either *tcp* or *udp.* Specify the source ports for this protocol entry. A range of ports can be specified. Select the *Enter Ranges* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.
Destination Port (Low and High)	This field is only relevant if the protocol is either *tcp* or *udp*. Specify the destination ports for this protocol entry. A range of ports can be specified. Select the *Enter Ranges* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

8 Within the **Range** field, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the service alias range or double-click on an existing service alias range entry to edit it.

9 Select **OK** when completed to update the service alias rules. Select **Reset** to revert the screen back to its last saved configuration.

7.9 Application Policy

When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that specific application. An application policy defines the rules or actions executed on recognized applications (for example, Facebook) or application-categories (for example, social-networking). The following are the rules/actions that can be applied in an application policy:

- *Allow* - Allow packets for a specific application or application category
- *Deny* - Deny packets for a a specific application or application category
- *Mark* - Mark packets with DSCP/8021p value for a specific application or application category
- *Rate-limit* - Rate limit packets from specific application types.

For each rule defined, a precedence is assigned to resolve conflicting rules for applications and categories. A *deny* rule is exclusive, as no other action can be combined with a deny. An *allow* rule is redundant with other actions, since the default action is allow. An allow rule is useful when wanting to deny packets for a category, but wanting to allow a few applications in the same category to proceed. In such a cases, add an allow rule for applications with a higher precedence then a deny rule for that category.

Mark actions mark packets for a recognized application and category with DSCP/8021p values used for QoS. *Rate-limits* create a rate-limiter applied to packets recognized for an application and category. Ingress and egress rates need to be specified for the rate-limiter, but both are not required. Mark and rate-limit are the only two actions that can be combined for an application and category. All other combinations are invalid.

To define an application policy configuration:

1 Select **Configuration** > **Network** > **Application Policy**.

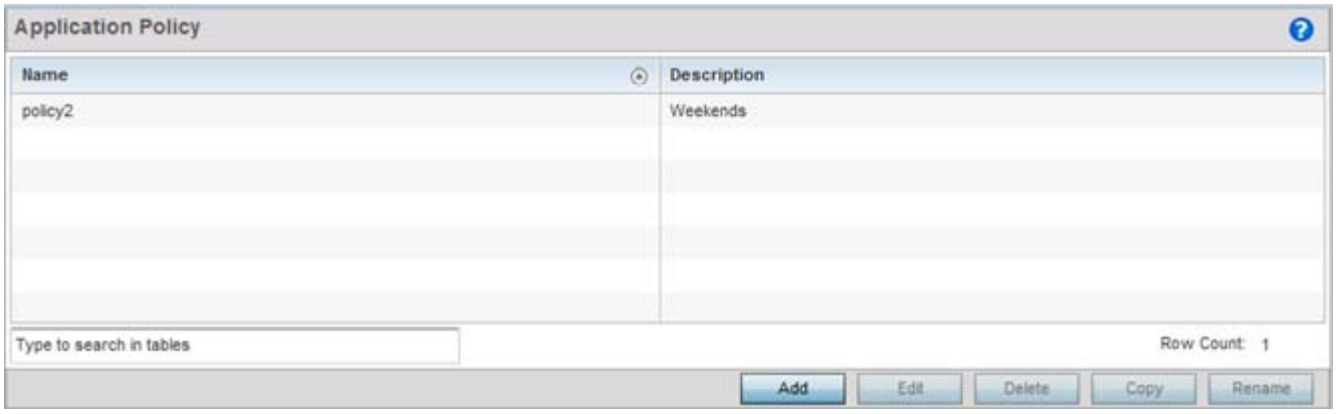


Figure 7-39 *Application Policy screen*

The screen lists the application policy configurations defined thus far.

2 Refer to the following to determine whether a new application policy requires creation, modification or deletion:-

Name	Lists the 32 character maximum name assigned to each listed application policy, designated upon creation.
Description	Displays the 80 character maximum description assigned to each listed application policy, as a means of further distinguishing policies with similar configurations.

3 Select **Add** to create a new application policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available. Existing policies can be copied or renamed as needed.

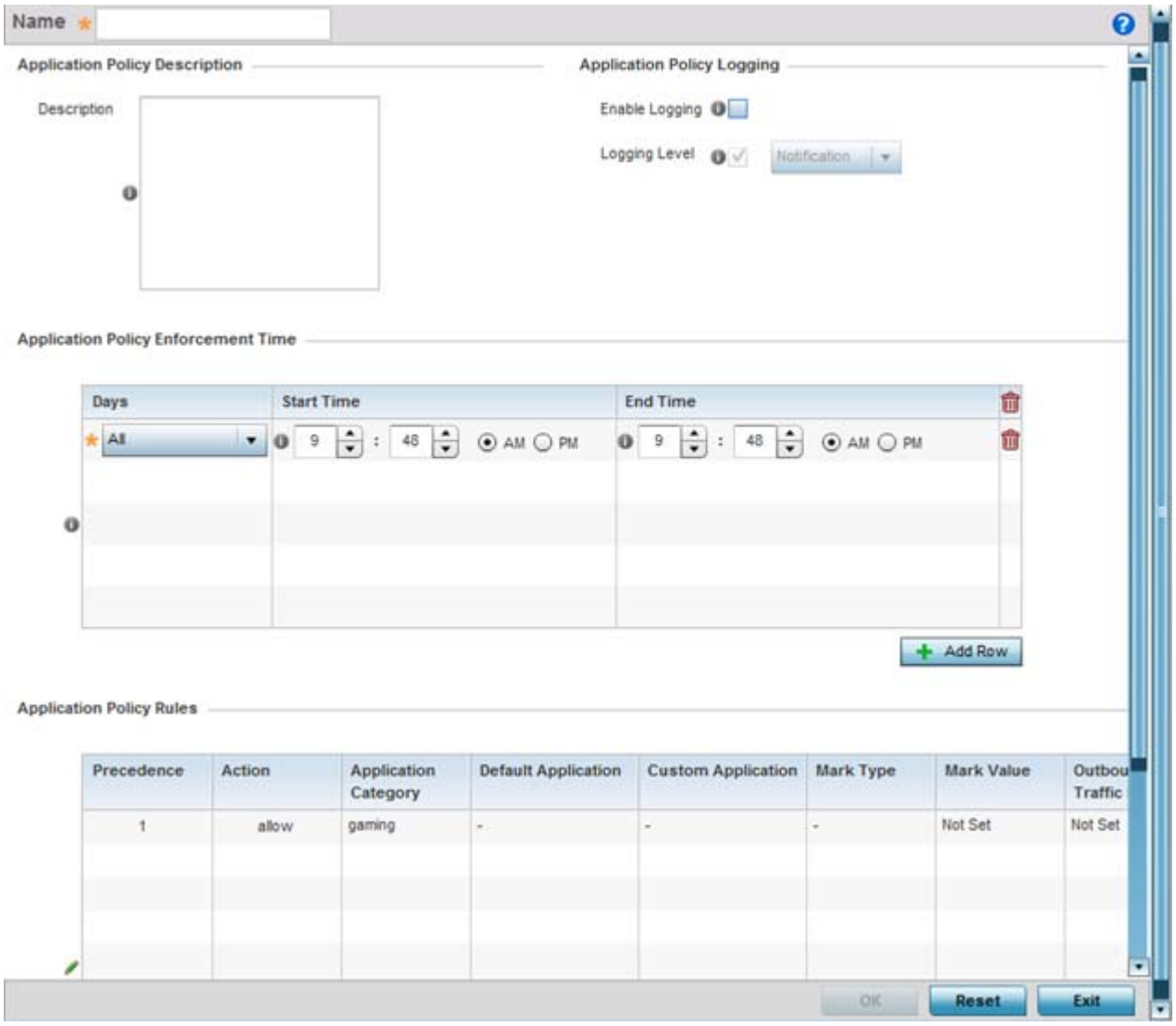


Figure 7-40 *Application Policy Add/Edit screen*

4 If creating a new application policy, assign it a **Name** up to 32 characters.

5 Provide this application policy an 80 character maximum **Description** to highlight its application and category filters and differentiate it from other policies with similar configurations.

6 Define the following **Application Policy Logging** options to enable and filter logging for application specific packet flows:

Enable Logging	Enables the log functionality, where each new flow is shown with the corresponding matched application, the action taken and the policy name. When enabled, logging just shows what applications are getting recognized.
Logging Level	Select this option to log application events by severity. Severity levels include *Emergency*, *Alert, Critical, Errors, Warning, Notification, Information* and *Debug*. The default logging level is Notification.

7 Refer to the **Application Policy Enforcement Time** table configure time periods for policy activation for each policy.

Select **+ Add Row** to populate the table with an enforcement time configuration to activate application policies based on the current local time. The option to configure a time activation period is applicable for a single application policy. Configure the days and time period when the application policy is enforced. If no time enforcement configuration is set, the policy is continually in effect without restriction.

8 Refer to the **Application Policy Rules** table assess existing policy rules, their precedence (implementation priority), their actions (allow, deny etc.), application category and schedule policy enforcement restrictions.

9 Select **+ Add Row** launch a screen to create a new policy rule.

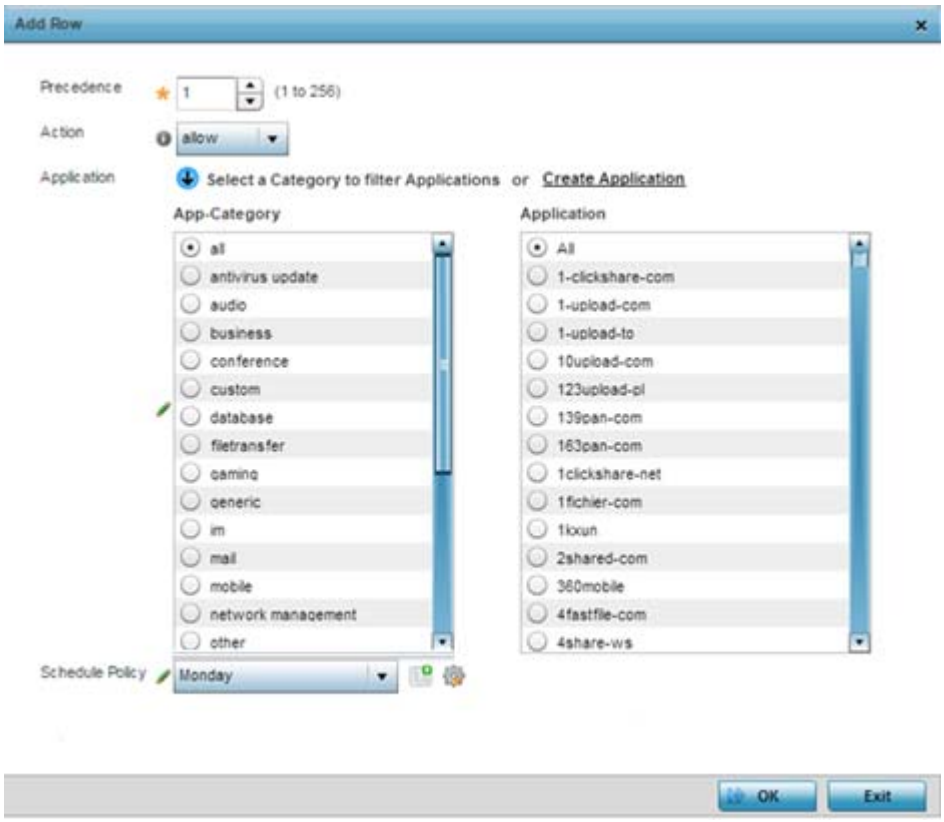


Figure 7-41 *Application Policy, Add Rule screen*

10 Assign the following attributes to the new application rule policy:

Precedence	Set the priority (from 1 - 256) for the application policy rule. The lower the value, the higher the priority assigned to this rule's enforcement action and the category and application assigned. A precedence also helps resolve conflicting rules for applications and categories.
Action	Set the action executed on the selected application category and application. The default setting is Allow.
Application	From the *App-Category* table, select the category for which the application rule applies. Selecting All auto-selects All within the Application table. Select *All* from the *Application* table to list all application category statistics, or specify a particular category name to display its statistics only.

11 Use the **Schedule Policy** drop-down menu to select an existing schedule policy to strategically enforce application filter policy rules for specific intervals. This provides stricter, time and schedule based, access or restriction to specific applications and their parent categories. If an existing policy does not meet requirements, either select the **Create** icon to configure a new policy or the **Edit** icon to modify an existing policy. For more information on configuring schedule policies, see *Schedule Policy on page 7-62*.

Select **OK** to save the updates to the application policy. Select **Reset** to revert to the last saved configuration.

7.10 Application

Use the **Application** screen to create custom application configurations.

To create a user-defined application:

1 Select **Configuration** > **Network** > **Application**.

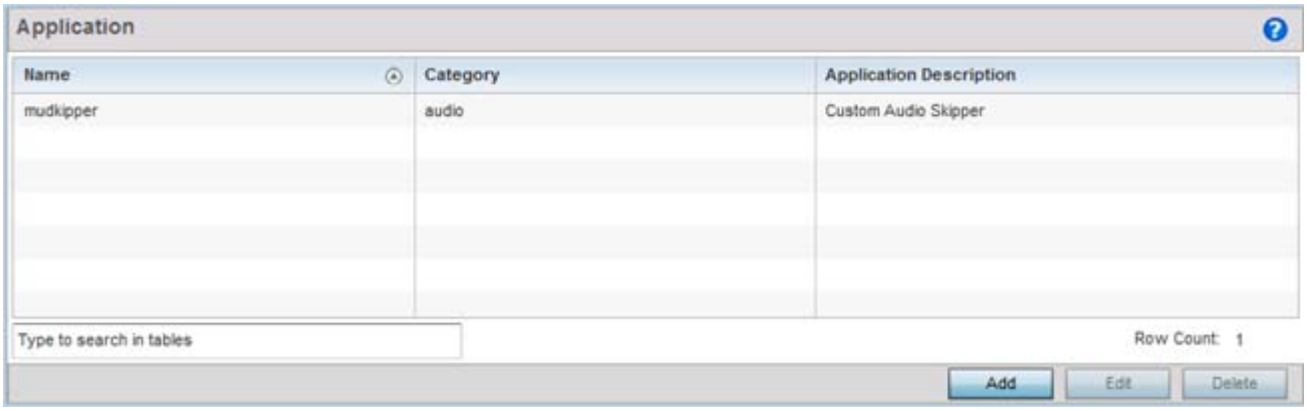


Figure 7-42 *Application screen*

The screen lists the application configurations defined thus far.

2 Refer to the following to determine whether a application requires creation, modification or deletion:

Name	Displays the name of each user-defined application created using this application interface.
Category	Lists the category to which each listed user-defined application belongs.
Application Description	Lists the 80 character maximum description administratively assigned to each listed user-defined application.

3 Select **Add** to create a new application configuration, **Edit** to modify the attributes of a selected application or **Delete** to remove obsolete applications from the list of those available.

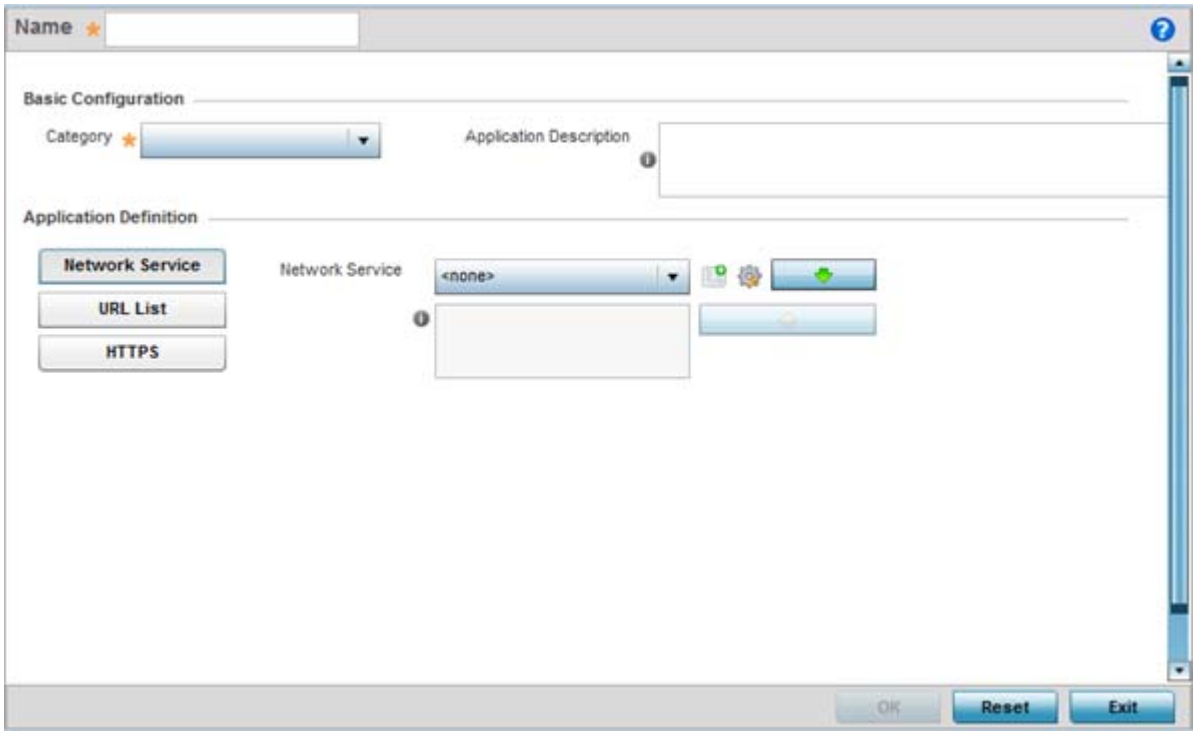


Figure 7-43 *Application Policy Add screen*

4 If creating a new user-defined application type, assign it a **Name** up to 32 characters. Ensure you do create confusion by naming a user-defined application with the same name as an existing application appearing the Application Policy screen.

5 Provide an 80 character maximum **Application Description** to each new user-defined application to further differentiate it from existing applications.

6 Refer to the **Application Definition** field to assign either a network service alias, pre-defined URL list or set of HTTPS parameters to the user-defined application.

Network Service	Use the drop-down menu to select an existing network service alias for the user-defined application. If there's no existing network service alias suited to this new user-defined application, select the *Create* icon to define a new alias or the *Edit* icon to modify an existing one. Provide or modify a 32 character maximum name, along with a protocol type or number and source and destination port value. Up to four service aliases can be supported.
URL List	Use the drop-down menu to select a pre-defined URL list to apply to the user-defined application. URL lists are utilized for whitelisting and blacklisting Web application URLs from being launched and consuming bandwidth within the WiNG managed network. If there's no URL list suited to this new user-defined application, select the *Create* icon to define a new list or the *Edit* icon to modify an existing URL list.
HTTPS	Select the *+ Add Row* button to populate the table with configurable rows for HTTPS parameter type, attribute type, match criteria for the HTTPS server name and 64 character maximum server name attribute used in the HTTPS server message exchange.

7 Select **OK** to save the updates to the user-defined application configuration. Select **Reset** to revert to the last saved configuration.

7.11 Application Group

An application group is a heterogeneous, user-defined collection of system-provided and/or user-defined applications and application categories. It consists of multiple applications grouped together to form a collection. Use this option to review/edit existing application groups and create new application groups.

To review an application group:

1 Select **Configuration** > **Network** > **Application Group**.

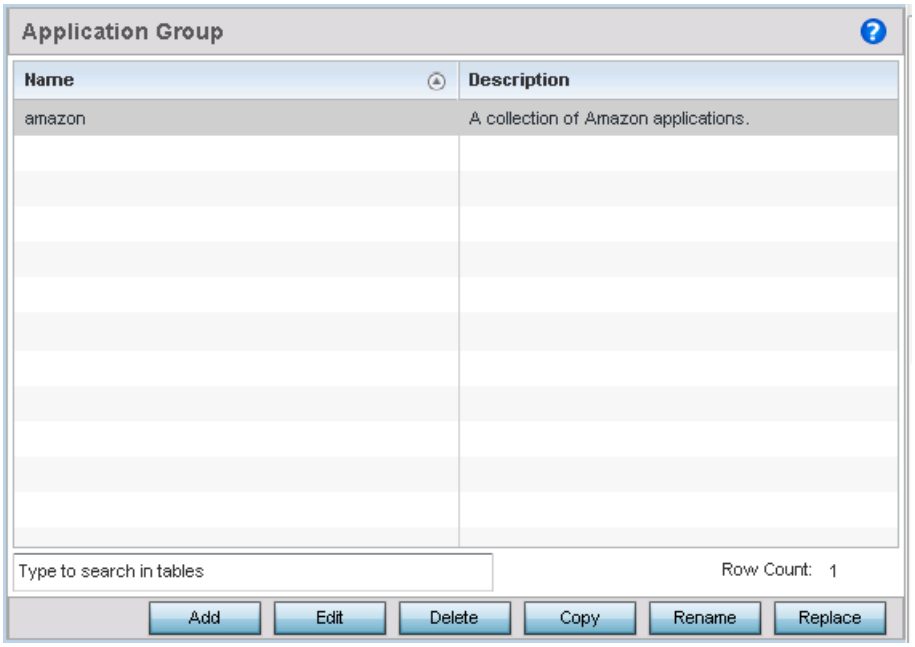


Figure 7-44 *Application Group screen*

The screen lists the existing application group configurations. You can edit and existing application group or create a new application group.

2 Refer to the following to determine whether an application group requires creation, modification or deletion:

Name	Displays the name of each user-defined application group
Description	Displays the description assigned to each listed user-defined application group.

3 Select **Add** to create a new application group configuration, **Edit** to modify the attributes of a selected application group or **Delete** to remove obsolete application groups from the list of those available.

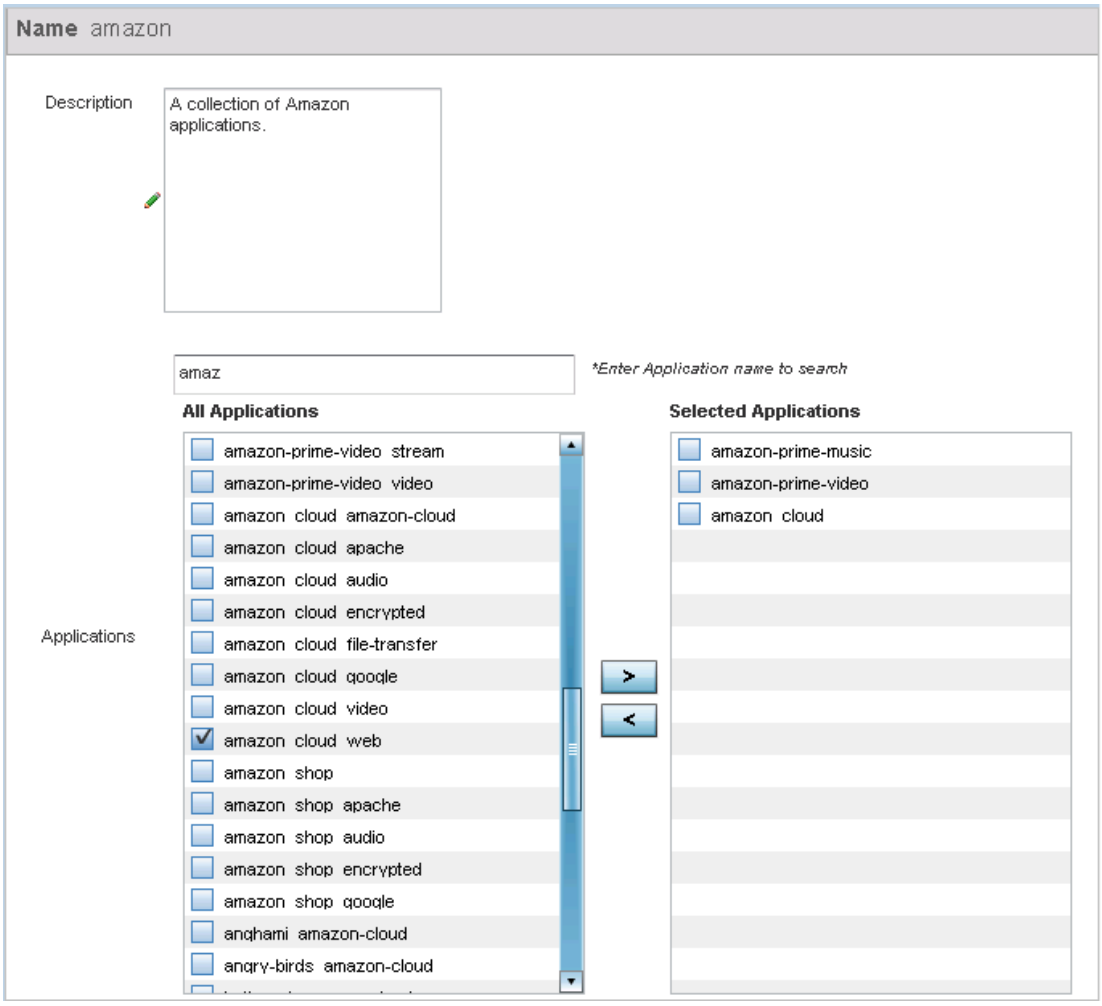


Figure 7-45 *Application Group Add screen*

4 If creating a new application group, assign a Name not exceeding 32 characters in length. Ensure that the name uniquely differentiates it from existing application groups.

5 Provide an 80 character maximum Description to further differentiate the new group from existing application groups

6 Refer to the All Applications field. This field lists available applications - system-provided and user-defined.

The WiNG software has 299 built-in applications, in addition to the user-defined ones. To facilitate your search, enter a string value in the ***Enter Application name to search** field. Based on the search string provided, the ***All Applications*** list is updated to display applications containing the specified string.

7 Select the applications to be included in the application group and move to the **Selected Applications** list.

8 Select **OK** to save the updates to the application group configuration. Select **Reset** to revert to the last saved configuration.

7.12 Schedule Policy

Define schedule policies to strategically enforce application filter policy rules for specific intervals. This provides stricter, time and schedule based, access or restriction to specific applications and their parent categories.

To review existing schedule policies and assess whether new ones require creation or modification:

1 Select **Configuration** > **Network** > **Schedule Policy**.

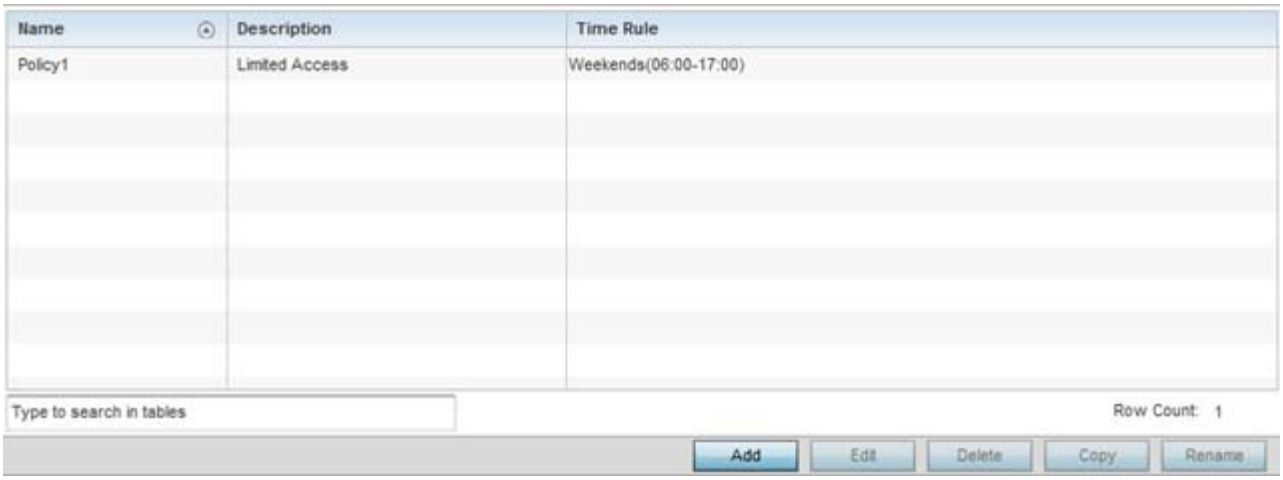


Figure 7-46 *Schedule Policy screen*

2 Select **Add** to create a new schedule policy time rule, or select an existing policy then **Edit** to modify the duration of an existing time rule. Schedule policies can be **Deleted** as they become obsolete. **Copy** or **Rename** a schedule policy as needed.

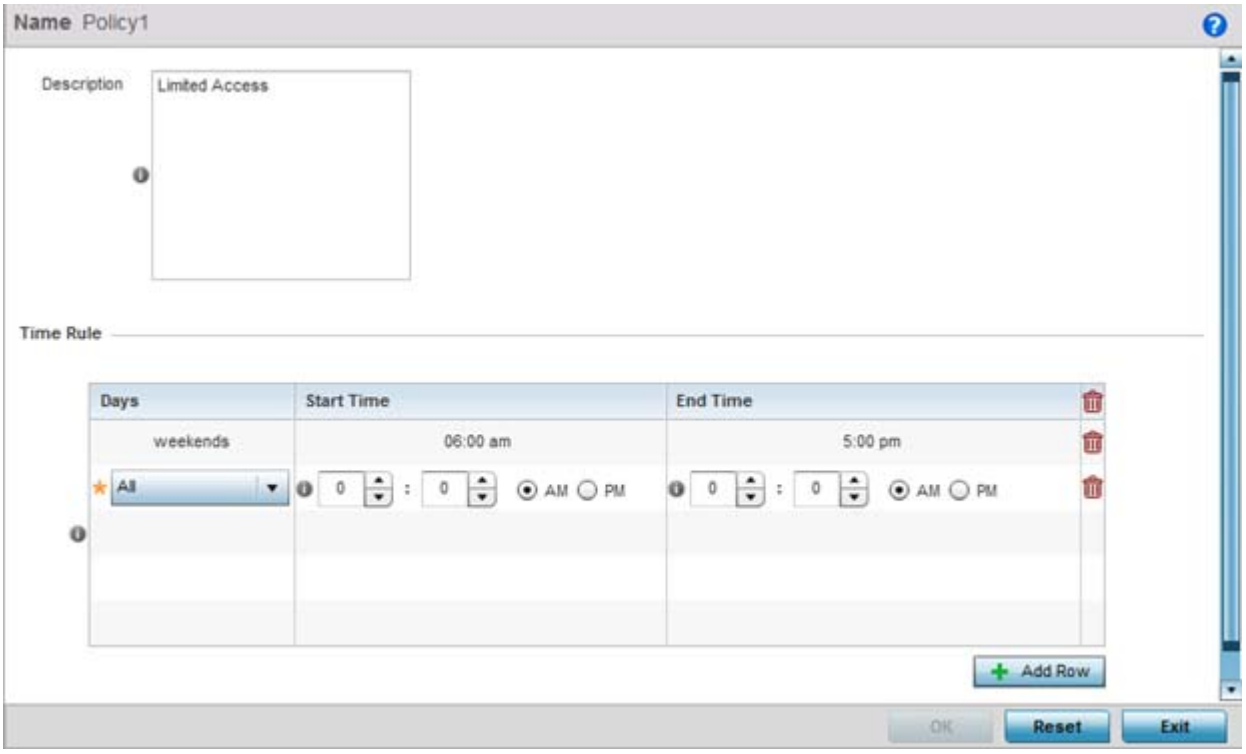


Figure 7-47 *Schedule Policy Add/Edit screen*

3 If creating a new schedule policy time rule configuration, enter a 32 character maximum **Name** relevant to its specific permissions objective.

4 Provide this schedule policy an 80 character maximum **Description** to differentiate it from other policies with similar time rule configurations.

5 Define the following **Time Rule** settings:

Days	Use the drop-down menu to select a day of the week to apply this schedule policy time rule. Selecting *All* applies the schedule policy every day (no enforcement rule restrictions). Selecting *weekends* applies the policy on Saturdays and Sundays only. Selecting *weekdays* applies the policy on Monday, Tuesday, Wednesday, Thursday and Friday only. Selecting individual days of the week applies the policy only on just selected day.
Start Time	Set the start when the schedule policy time rule applies. Use the spinner controls to select the hour and minute, in a 12h time format. Then use the radio button to choose *AM* or *PM*.
End Time	Set the ending time when the time rule is no longer enforced. Use the spinner controls to select the hour and minute, in a 12h time format. Then use the radio button to choose *AM* or *PM*.

6 Select **OK** to save the updates to the schedule policy time rule configuration. Select **Reset** to revert to the last saved configuration.

7.13 URL Filtering

A URL filter is Web content filter. A URL filter is comprised of several filter rules. To construct a filter rule, either whitelist or blacklist a filter level, category type, category or a custom category. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.

To review existing URL filter rules and assess whether new ones require creation or modification:

1 Select **Configuration** > **Network** > **URL Filter**.

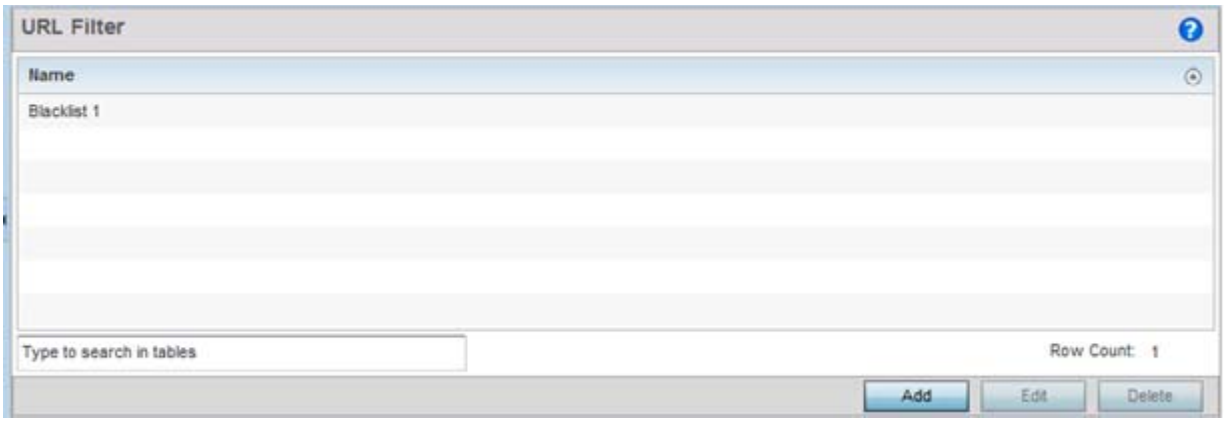


Figure 7-48 *URL Filter screen*

2 Select **Add** to create a new URL filter rule configuration, or select an exiting configuration then **Edit** to modify the attributes of an existing rule. Obsolete rules can be selected and **Deleted** as required.

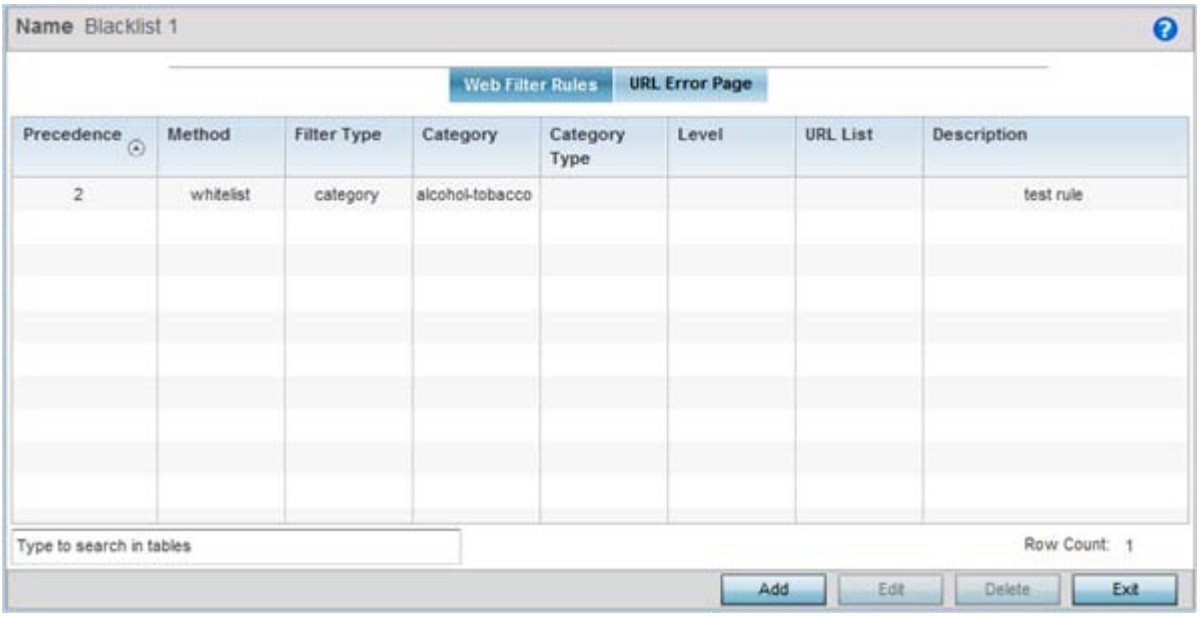


Figure 7-49 *URL Filter - Web Filter Rules tab*

3 If creating a new URL filter rule, enter a 32 character maximum **Name** relevant to its filtering objective and select **Continue**.

4 Select **Add** to create a new Web filter rule configuration, or select an exiting configuration then **Edit** to modify the attributes of an existing Web filter rule.

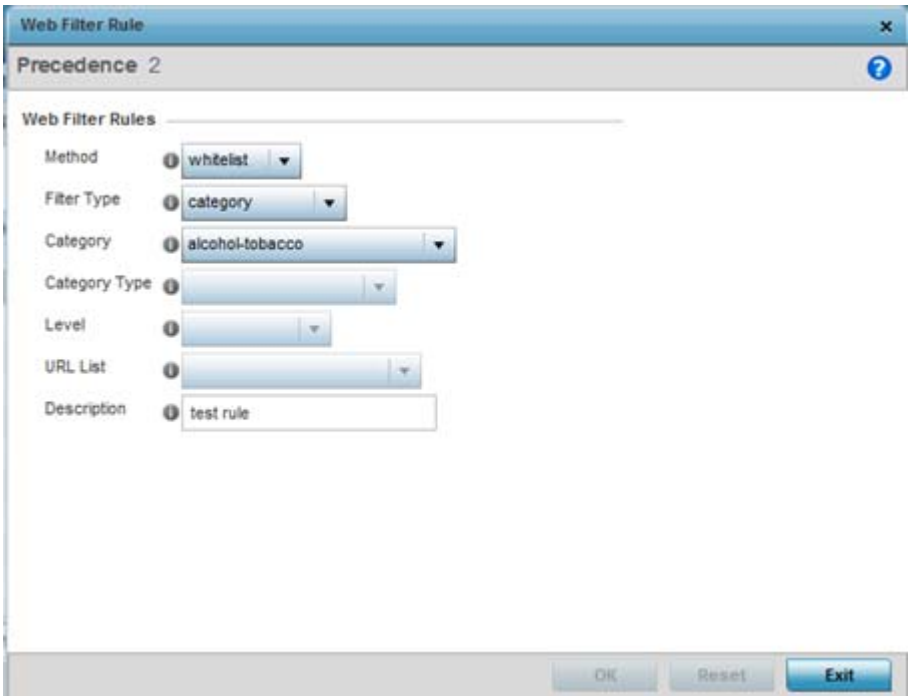


Figure 7-50 *URL Filter - Add/Edit Web Filter Rules*

5 Define the following **Web Filter Rule** settings:

Precedence	Set a precedence (priority) from 1 - 500 for the filter rule's utilization versus other Web filter rules. 1 is the highest priority and 500 the lowest.

Method	Select either *whitelist* or *Blacklist* to specify whether the rule is for inclusion or exclusion. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.
Filter Type	If the *Filter Type* is set to category, use the drop down menu to select from a list of predefined categories to align with the whitelist or blacklist *Method* designation and the precedence assigned.
Category	A category is a pre-defined URL list available in the WiNG software. If *category* is selected as the *Filter Type*, the *Category* drop-down menu becomes enabled for the selection of an existing URL type or whitelist or blacklist. Categories are based on an external database, and cannot be modified or removed. Custom categories can be created with the *URL List* and added to the database.
Category Type	When *category_type* is selected as the Filter Type, select an existing category type (adult-content, security-risk etc.) and either blacklist or whitelist the URLs in that category type. There are 12 category types available.
Level	*Basic, Low, Medium, medium-high* and *High* filter levels are available. Each level is pre-configured to use a set of category types. The user cannot change the categories in the category types used for these pre-configured filter-level settings, and add/modify/remove the category types mapped to the filter-level setting.
URL List	URL lists are customized categories included in the custom filter-level setting. URL lists enable an administrator to blacklist or whitelist URLs in addition to the built-in categories.
Description	Enter a 80 character maximum description for this Web filter rule to help differentiate it from others with similar category include or exclude rule configurations.

6 Select **OK** to save the changes to the Web Filter Rule. Select **Exit** to close the screen without saving the updates.

7 Select the **URL Error Page** tab to define the configuration and layout of a URL error page launched when a Web filter rule is invoked and an error page needs to be displayed to a user instead of they're expected Web page.

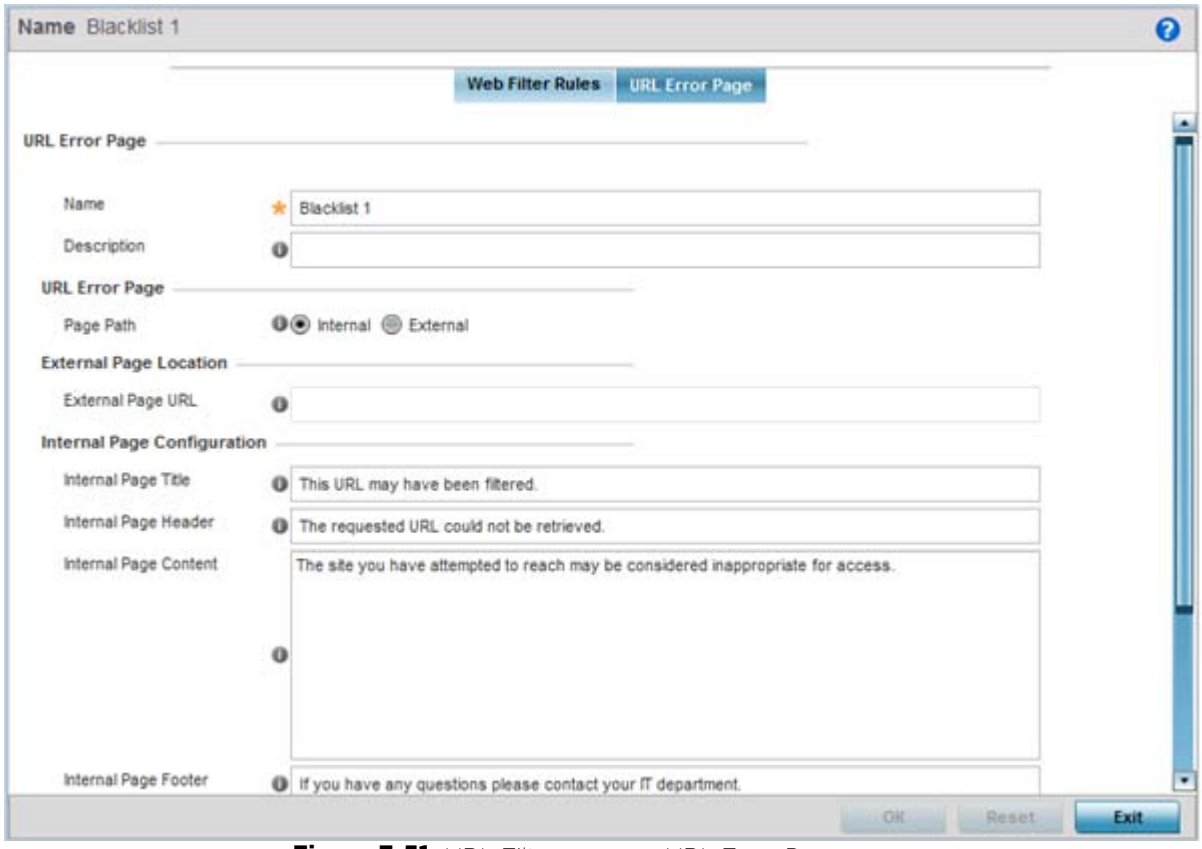


Figure 7-51 *URL Filter screen - URL Error Page*

8 Set the following **URL Error Page** display properties:

Name	Provide a 32 character maximum name for the title of the blocking page. The name should help convey that this page is launched to prevent the client's requested page from displaying.
Description	Provide a 80 character maximum description of the page to help differentiate it from other pages with similar page restriction properties.
Page Path	Set the path to the page sent back to the client browser explaining the reason for blocking the client's requested URL. It can be generated internally at the time the page is sent, or be a URL to an *External* Web server if the administrator chooses to utilize a customized page. The default setting is Internal, requiring the administrator to define the page configuration within the fields in the *Internal Page Configuration* portion of the screen.
External Page URL	If *External* is selected as the Page Path, provide a 511 character maximum External Page URL used as the Web link designation of the externally hosted blocking page.
Internal Page Title	Either enter a 255 character maximum title for the URL blocking page or use the existing default text (*This URL may have been filtered*).
Internal Page Header	Either enter a 255 character maximum header for the top of the URL blocking page or use the existing default text (*The requested URL could not be retrieved*).

Internal Page Content	Enter a 255 character maximum set of text used as the main body (middle portion) of the blocking page. Optionally use the default message (*The site you have attempted to reach may be considered inappropriate for access*).
Internal Page Footer	Either enter a 255 character maximum footer for the bottom of the URL blocking page or use the existing default text (*If you have any questions contact your IT department*).
Internal Page Org Name	Enter a 255 character maximum organizational name responsible for the URL blocking page. The default organizational name (*Your Organizational Name*) is not very practical, and is just a guideline for customization.
Internal Page Org Structure	Enter a 255 character maximum organizational signature responsible for the URL blocking page. The default organizational signature (Your Organizational Name, All Rights Reserved) is not very practical, and is just a guideline for customization.
Internal Page Logo 1	Provide the location and filename of a small graphic image displayed in the blocking page.
Internal Page Logo 2	Provide the location and filename of a main graphic image displayed in the blocking page.

9 Select **OK** to save the updates to the URL filter configuration. Select **Reset** to revert to the last saved configuration.

7.14 Web Filtering

A Web filter policy is means of managing the number of records and time cached URLs are retained. A policy also determines whether to filter access to a cached URL when a categorization server is unreachable or unable to classify request types.

To review existing Web filter policies and assess whether new ones require creation, modification or deletion:

1 Select **Configuration** > **Network** > **Web Filter**.

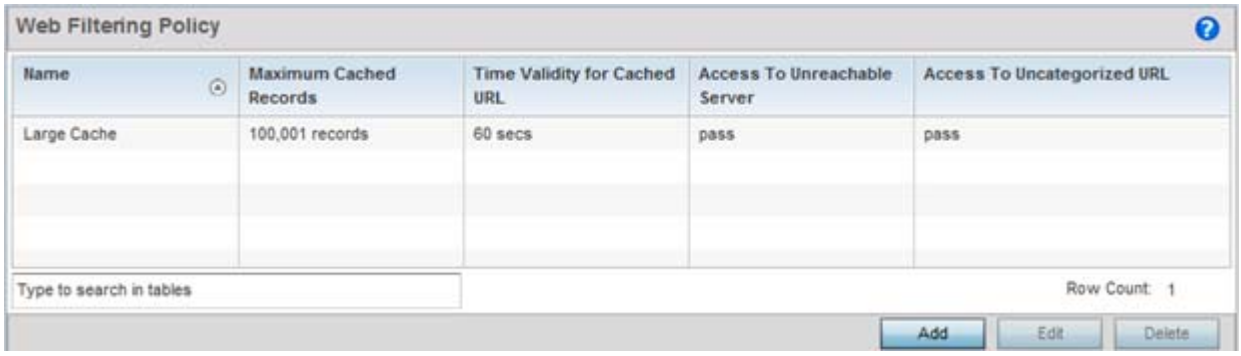


Figure 7-52 *Web Filter Policy screen*

2 Select **Add** to create a new Web filter policy, or select an existing policy and **Edit** to modify its attributes. Obsolete policies can be selected and **Deleted** as needed.

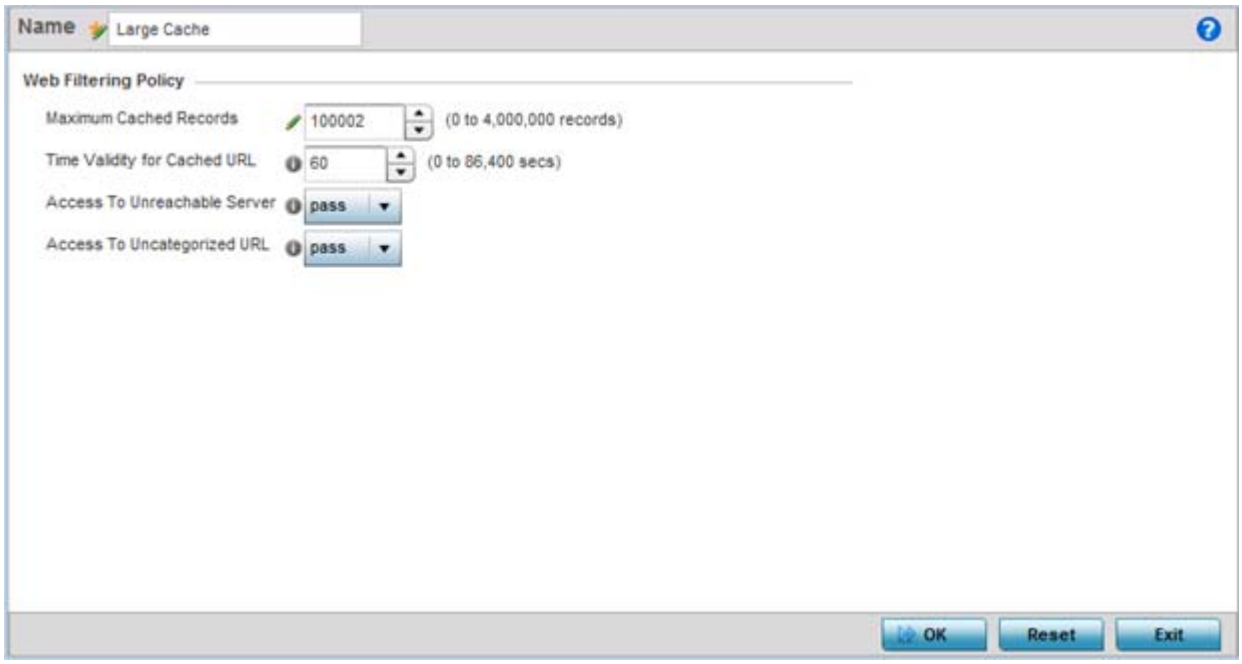


Figure 7-53 *Web Filter - Add/Edit*

3 If creating a Web URL filter, enter a 32 character maximum **Name** relevant to its filtering objective and cache considerations, then select **Continue**.

4 Define the following **Web Filtering Policy** settings.

Maximum Cached Records	Set the maximum number of records (from 0 - 4,000,000) for Web content cached locally on this controller or service platform. The default setting is 100,000 records.
Time Validity for Cached URL	Set the maximum amount of a time, from 0 - 86,400 seconds, a URL is valid in the controller or service platform cache. Consider the bandwidth depletion if caching a large number of records over the maximum permissible time validity.
Access to Unreachable Server	Either *pass* or *block* (filter) access to a cached URL when the categorization server is unreachable. Access is allowed by default.
Access to Uncategorized URL	Either *pass* or *block* (filter) access to a cached URL when the categorization server fails to classify a request type. Access is allowed by default.

5 Select **OK** to save the changes to the Web filter policy. Select **Exit** to close the screen without saving the updates.

7.15 EX3500 QoS Class

An EX3500 switch can have its own QoS class policy applied as specific interoperability requirements dictate between an EX3500 switch and its connected devices. The QoS class configuration specifies permitted and excluded MAC and IP addresses and the precedence upon which filter rules are applied to EX3500 switch traffic.

To review existing EX3500 QoS policies and assess whether new ones require creation, modification or deletion:

1 Select **Configuration** > **Network** > **EX3500 QoS Class**.

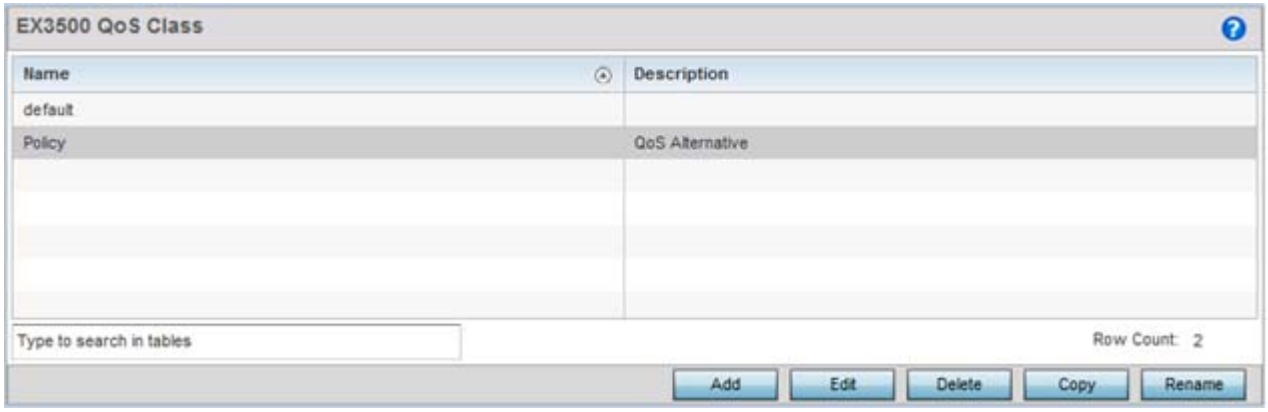


Figure 7-54 *EX3500 QoS Class screen*

2 Select **Add** to create a new EX3500 QoS policy, or select an existing policy and **Edit** to modify its attributes. Obsolete policies can be selected and **Deleted** as needed. **Copy** a policy to duplicate an existing QoS policy or **Rename** them as needed.

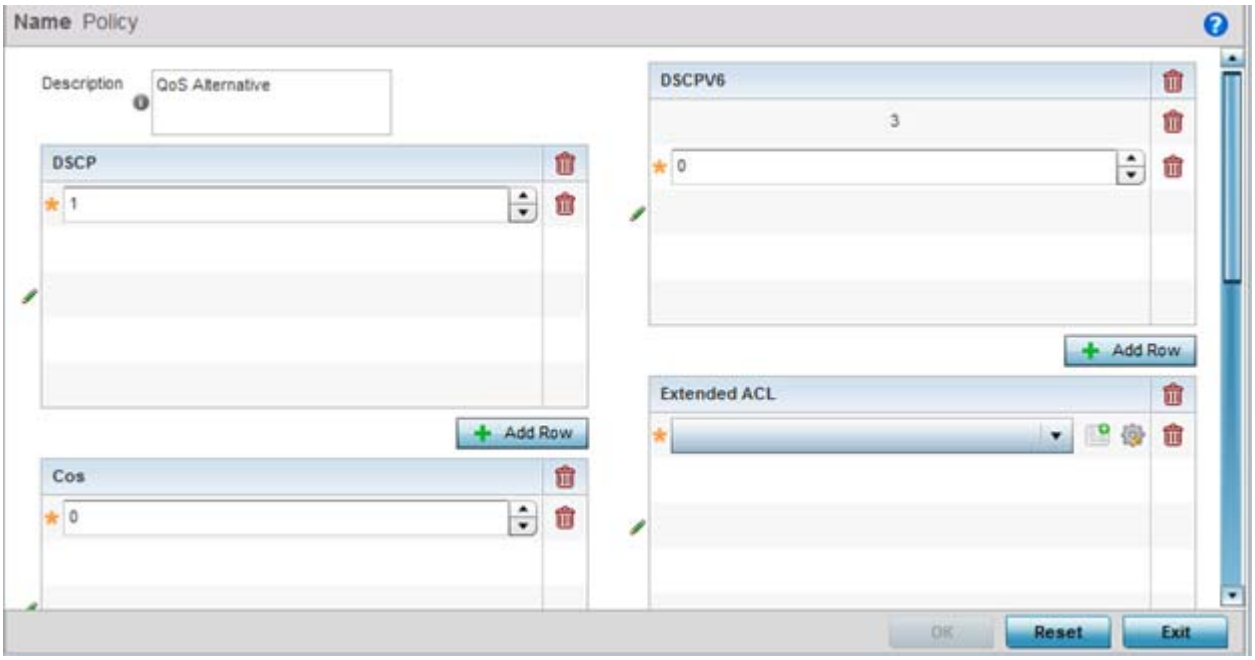


Figure 7-55 *EX3500 QoS Class screen - Add/Edit*

3 If creating a EX3500 QoS policy, enter a 64 character maximum **Description** to help differentiate this policy's EX3500 traffic prioritization scheme.

4 Refer to the **DSCP** field to set the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification. The range is 0 to 63 like DSCPv6.

The screen maps the 6-bit *Differentiated Service Code Point* (DSCP) code points to the older 3-bit IP Precedent field located in the Type of Service byte of an IP header. DSCP is a protocol for specifying and controlling network traffic by class so that certain traffic types get precedence. DSCP specifies a specific per-hop behavior that is applied to a packet. This QoS assignment can be overridden as needed, but removes the device configuration from the profile that may be shared with other similar device models.

5 Use the **Cos** field to Assign a 802.1p priority (0 - 7) as a 3-bit IP precedence value of the IP header used to set the user priority. The valid values for this field are 0 – *Best Effort,* 1 – *Background*, 2 – *Spare*, 3 – *Excellent Effort*, 4 – *Controlled Load*, 5 – *Video*, 6 – *Voice*, 7 – *Network Control*.

6 Optionally apply **MAC ACL** rules to EX3500 packet traffic. Use the drop-down menu to select an existing MAC ACL, select the **Create** icon to add a new MAC ACL rule, or select an existing MAC ACL and the **Edit** icon to modify its configuration. For information on creating MAC ACLs, refer to *Configuring MAC Firewall Rules on page 10-15*.

Administrators can filter Layer 2 EX3500 traffic on a physical Layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical *allow*, *deny* or *mark* designation to WLAN packet traffic.

7 Optionally apply IP based **Standard ACL** rules to EX3500 packet traffic. A standard ACL for an EX3500 is a policy-based ACL that either prevents or allows specific clients from using the device. Select the **Create** icon to add a new ACL rule, or select an existing ACL and the **Edit** icon to modify its configuration. If creating a new standard ACL, provide a name up to 32 characters to help differentiate this rule from others with similar configurations. Select **+ Add Row**. For more information on creating a standard ACL, see *EX3500 ACL Standard on page 10-29*.

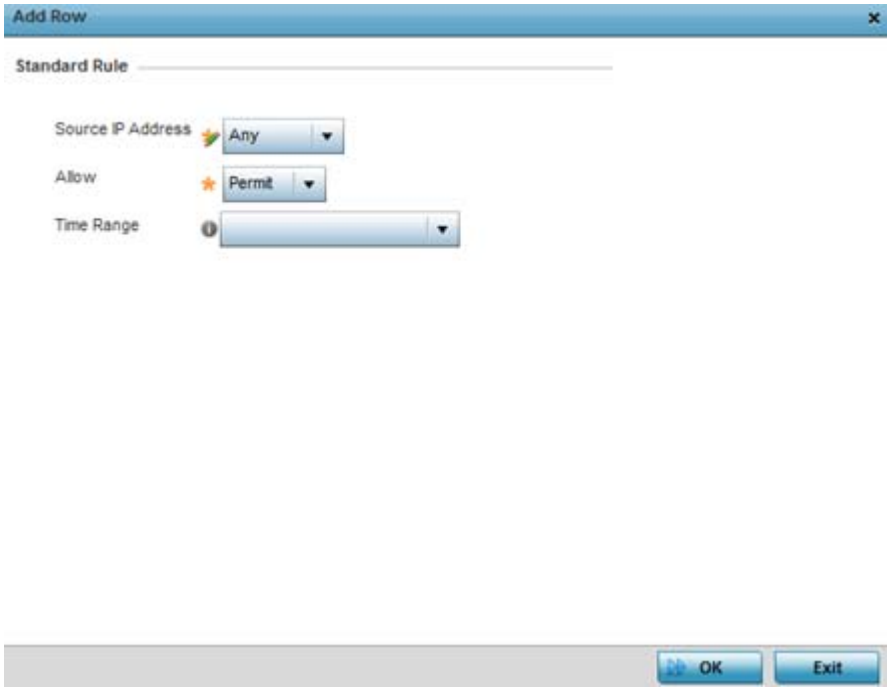


Figure 7-56 *EX3500 QoS Class screen - Add/Edit*

8 Set the following standard ACL attributes:

Source IP Address	Set whether the permit or deny rules assigned to this ACL are applied to a *Host* IP address, *Network* IP address and mask or *Any* address.
Allow	Set the *Permit* or *Deny* action on IP packet traffic with the EX3500 switch. The default is Permit.
Time Range	Defines the period when the permit or deny are applied to EX3500 IP traffic.

9 Refer to the **DSCPV6** field and select **+ Add Row** to specify a DSCPV6 value from 0 - 63. DSCPv6 specifies the *Differentiated Services Code Point* version 6 of a classifier assigned to an interface. Use DSCPv6 for IPv6 multicast traffic support.

10 Refer to the **Extended ACL** field and either select an existing extended IP ACL from the drop-down menu, add a new extended IP ACL by selecting the **Create** icon, or modify an existing one by selecting the **Edit** icon. For more information on extended IP ACLs, refer to *EX3500 ACL Extended on page 10-31*.

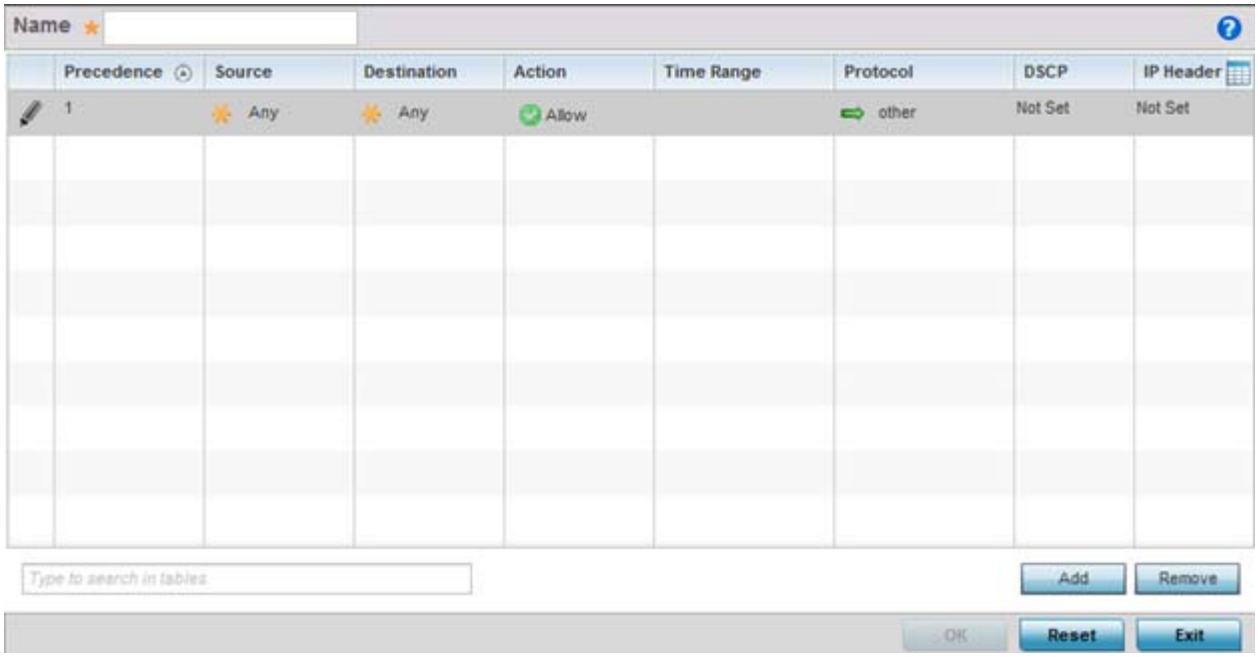


Figure 7-57 *EX3500 QoS Class - Extended ACL*

An extended ACL is comprised of *access control entries* (ACEs). Each ACE specifies a *source* and *destination* for matching and filtering traffic to the EX3500 switch.

Name	If creating a new extended ACL, provide a 32 character maximum name to this extended ACL to differentiate its EX3500 traffic filtering configuration.
Precedence	Specify or modify a precedence for this IP policy between 1-128. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.
Source	Determine whether filtered packet source for this IP firewall rule do not require any classification (*any*), are set as a numeric IP address (*host)* or apply to *any*.
Destination	Determine whether filtered packet destinations for this IP firewall rule do not require any classification (*any*), are set as a numeric IP address (*host)* or apply to *any*.
Action	Every rule is made up of matching criteria rules. The action defines the packet's disposition if it matches the specified criteria. The following actions are supported: *Deny* - Instructs the ACL to restrict a packet from proceeding to its destination when filter conditions are matched. *Allow* - Instructs the ACL to allow a packet to proceed to its destination when filter conditions are matched.

Time Range	Lists time range when each listed ACL is enabled. An EX3500 *Time Range* is a set of configurations consisting of *periodic* and *absolute* time ranges. Periodic ranges can be configured to reoccur based on periodicity such as daily, weekly, weekends, weekdays and on specific week day such as Sunday. Absolute time ranges can be configured to a range of days during a particular period. Absolute time ranges do not reoccur. For more information, see *EX3500 Time Range on page 10-64*.
Protocol	Specify the protocol for which the alias has to be created. Use the drop down to select the protocol from *eigrp, gre, icmp, igmp, ip, vrrp, igp, ospf, tcp, udp* or *other.* Select other if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected.
Source Port	Specify a source port for the TCP or UDP protocols. The source specifies the IP address or FQDN from which the packet is sent.The source port is not displayed by default and must be selected from the upper-right hand side of the screen.
Destination Port	Specify a destination port for the TCP or UDP protocols. The destination specifies the IP address or FQDN to which the packet is being sent. The destination port is not displayed by default and must be selected from the upper-right hand side of the screen.
DSCP	Select this option to specify a DSCP value from 0 - 63. DSCP specifies the *Differentiated Services Code Point* version 6 of a classifier assigned to an interface.
IP Header	Sets the IP precedence level from 0-7.

11 Refer to the **Precedence** field and select **+ Add Row** to assign a precedence (priority) to this EX3500 QoS policy. Rules are applied in order from 0 - 7.

12 Optionally refine the virtual interface (**VLAN**) to which the EX3500 QoS policy is applied by selecting a VLAN from 1 - 4094.

13 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

7.16 EX3500 QoS Policy Map

An EX3500 switch can have its own WiNG defined policy map that can be attached to an interface to specify a QoS service policy. Use a QoS policy map to assign priority to mission critical EX3500 switch data traffic, prevent EX3500 switch bandwidth congestion and prevent packet drops.

To review existing EX3500 QoS policy map configurations and assess whether new ones require creation, modification or deletion:

1 Select **Configuration** > **Network** > **EX3500 QoS Policy Map**.

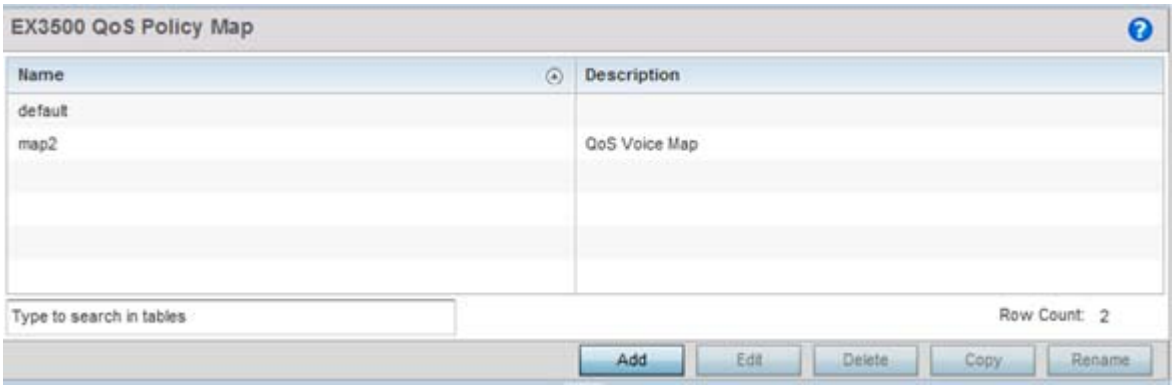


Figure 7-58 *EX3500 QoS Policy Map screen*

2 Select **Add** to create a new EX3500 QoS policy map, or select an existing policy and **Edit** to modify its attributes. Obsolete policy maps can be selected and **Deleted** as needed. **Copy** to duplicate an existing policy map or **Rename** them as needed.

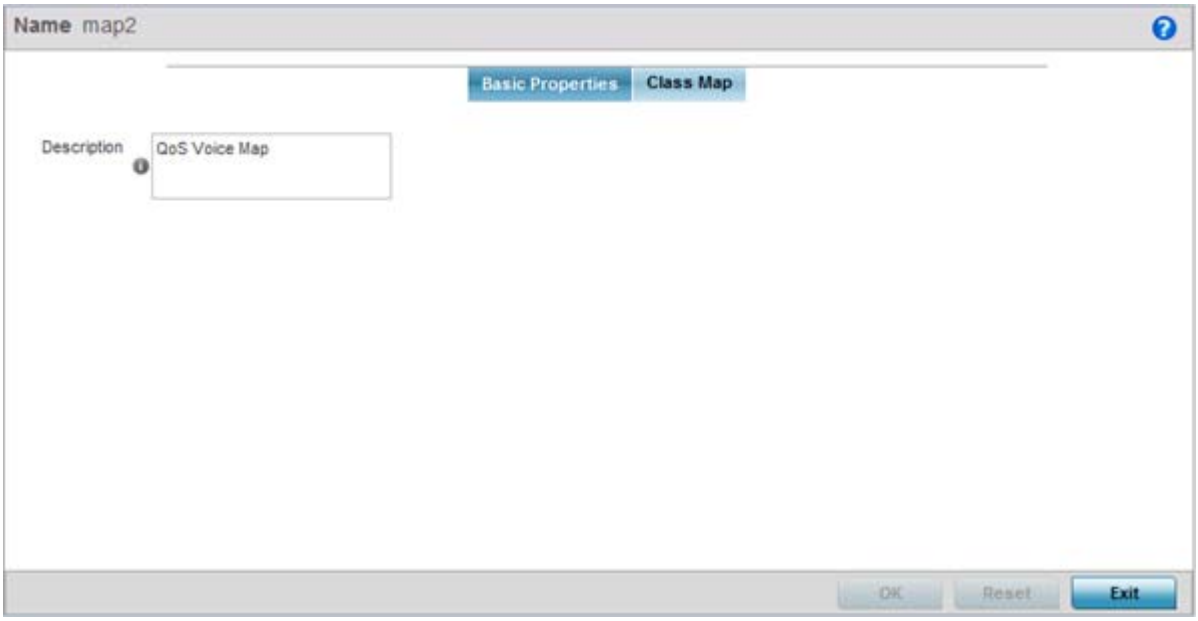


Figure 7-59 *EX3500 QoS Policy Map - Basic Properties screen*

3 If adding a new EX3500 QoS policy map, enter a 32 character maximum **Name** to help differentiate this policy from others with similar attributes.

4 Enter a 64 character maximum **Description** to help differentiate this policy's EX3500 traffic prioritization scheme.

5 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

6 Select the **Class Map** tab.

Existing class map configurations display along with their drop designations defining whether packets will be dropped if exceeding the actions set for this class map configuration.

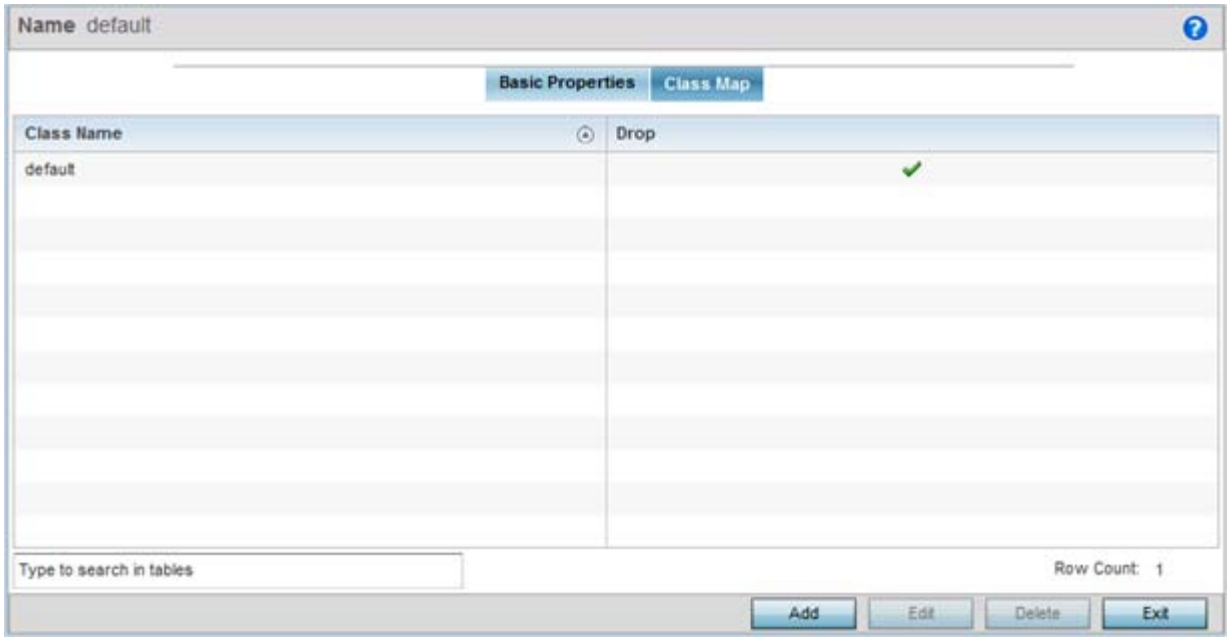


Figure 7-60 *EX3500 QoS Policy Map - Class Map screen*

7 Select **Add** to create a new EX3500 QoS class map, or select an existing class name and **Edit** to modify its attributes. Obsolete class maps can be selected and **Deleted** as needed.

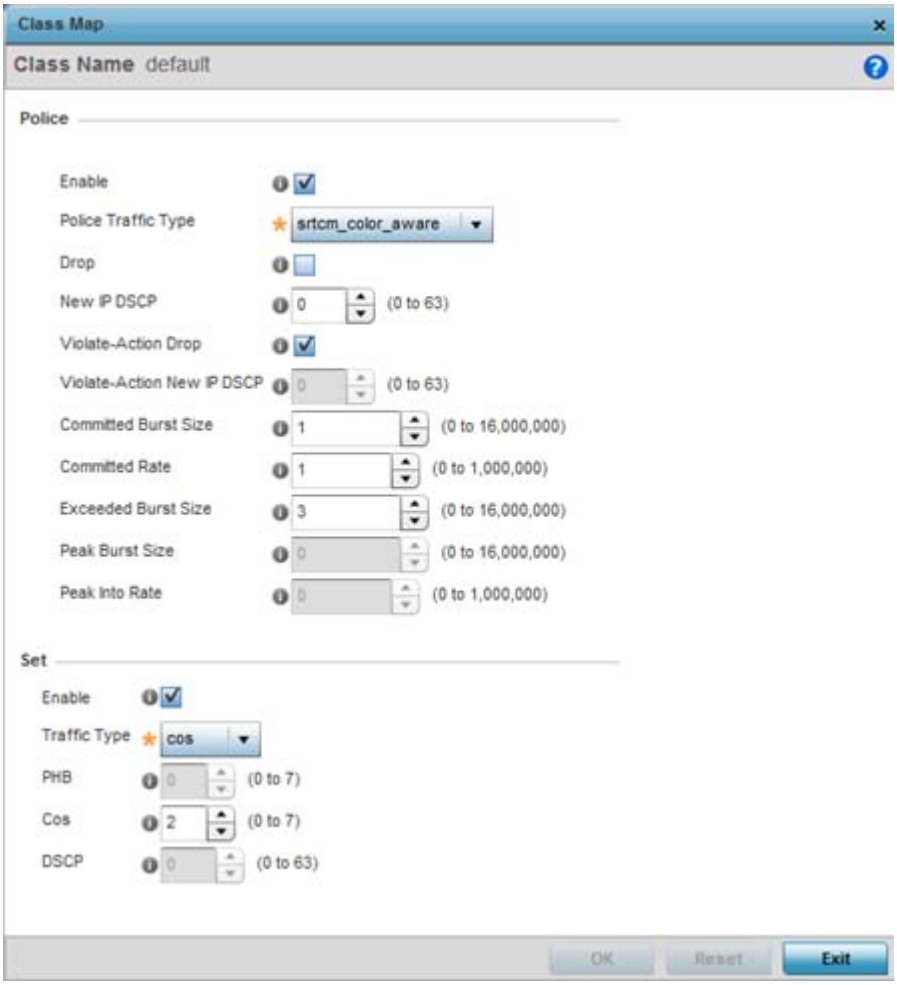


Figure 7-61 *EX3500 QoS Policy Map - Class Map Add/Edit screen*

8 Set the following class map **Police** actions to apply traffic restrictions and packet drop criteria to EX3500 switch data traffic:

Enable	Enable this option to apply traffic type classification restrictions and packet drop criteria to EX3500 switch data traffic. This option is dialed by default.
Police Traffic Type	Use the drop-down menu to specify the EX3500 switch traffic type to drop when the specified violation criteria is exceeded. A policing scheme can be applied before writing packets to the TX port by dropping or changing the *color* (green, yellow or red) of the packet in a static manner, depending on both the input and output colors of the packets. Options include *flow, srtcm_color_aware, srtcm_color_blind, trtcm_color_aware* and *trtcm_color_blind.*
Drop	Select this option to drop EX3500 switch packets when the violation action criteria has been exceeded. This option is not available when *flow* is selected as Police Action Type.
New IP DSCP	Use the spinner control to set a DSCP value (from 0 - 63) as required by an exceeded action criteria. DSCP is the *Differentiated Services Code Point* field in an IP header for packet classification. Packets are filtered based on the traffic class defined in the IP DSCP field. This option is not available when flow is selected as the Police Action Type or when Drop is enabled.

Violate-Action Drop	Select this option to drop packets when the specified traffic type classification restrictions and packet drop criteria are exceeded. When enabled (default setting), the *Violate Action New IP DSCP* setting is disabled.
Violate Action New IP DSCP	If the *Violate-Action Drop* option is disabled, set a DSCP value (from 0 - 63) as required by an exceeded action criteria.
Committed Burst Size	Set a committed (maximum) burst size between 0 - 16,000,000. The smaller the burst, the less likely received EX3500 switch packets result in data traffic congestion.
Committed Rate	Set the *committed information rate* (CIR) from 0 - 1,000,000 for EX3500 switch data traffic. The CIR is a bandwidth (expressed in bits per second) allocated to the connection with the EX3500 switch. This form of rate limiting reduces the maximum rate sent or received, and prevents any single EX3500 switch from overwhelming the WiNG managed network.
Exceeded Burst Size	When *srtcm_color_aware* or *srtcm_color_blind* are selected as the Police Traffic Type, set an excess burst size (from 0 - 16,000,000 bytes). The excess busrt size allows for periods of bursting traffic exceeding both the *committed information rate* (CIR) and committed burst size.
Peak Burst Size	When *trtcm_color_aware* or *trtcm_color_blind* are selected as the Police Traffic Type, set a Peak Burst Size (from 0 - 16,000,000 bytes). The Peak Burst Size defines the maximum number of bytes of unused peak bandwidth capacity that can be accumulated. The accumulated bandwidth allows for periods of bursting traffic exceeding the Peak Info Rate and Committed Burst Size.
Peak Into Rate	When *trtcm_color_aware* or *trtcm_color_blind* are selected as the Police Traffic Type, set a Peak Info Rate (from 0 - 1,000,000 kilobytes per second). The Peak Info Rate is the maximum rate for traffic arriving or departing the interface under peak conditions. Traffic exceeding the *committed information rate (*CIR) and the committed burst size is metered to the Peak Info Rate.

9 Refer to the **Set** field to define the EX3500's traffic type and set its behavior.

Enable	Select enable to refine the EX3500's traffic type to either PHB, COS or DSCP.
Traffic Type	Use the drop-down menu to specify the EX3500 switch traffic type. Options include *phb, cos* and *DSCP*. Once an option is selected, refine that traffic type's behavior.
PHB	When PHB is selected as the Traffic Type, set the per-hop behavior value (from 1 - 7) applied to matching packets. The PHB defines the policy and priority applied to a packet when traversing a hop. PHBs are created (one for each combination of the top 3 bits) as *bbb000* to match precedence behaviors and leaves other DSCP values open, where each *b* may take the value zero or 1.
Cos	When Cos is selected as the Traffic Type, assign a 802.1p priority (0 - 7) as a 3-bit IP precedence value of the IP header used to set the EX3500 switch user priority. The valid values for this field are 0 – *Best Effort*, 1 – *Background*, 2 – *Spare*, 3 – *Excellent Effort*, 4 – *Controlled Load*, 5 – *Video*, 6 – *Voice*, 7 – *Network Control*.

DSCP	When DSCP is selected as the Traffic Type, set a DSCP value (from 0 - 63). DSCP is the *Differentiated Services Code Point* field in an IP header for EX3500 switch packet classification. Packets are filtered based on the traffic class defined in the IP DSCP field.

10 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

7.17 Network Deployment Considerations

Before defining a L2TPV3 configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- In respect to L2TP V3, data transfers on the pseudowire can start as soon as session establishment corresponding to the pseudowire is complete.
- In respect to L2TP V3, the control connection keep-alive mechanism of L2TP V3 can serve as a monitoring mechanism for the pseudowires associated with a control connection.

8 Profile Configuration

Profiles enable administrators to assign a common set of configuration parameters and policies to controllers, service platforms and Access Points. Profiles can be used to assign common or *unique* network, wireless and security parameters to devices across a large, multi segment, site. The configuration parameters within a profile are based on the hardware model the profile was created to support. The controllers, service platforms and Access Points support both default and user defined profiles implementing new features or updating existing parameters. The central benefit of a profile is its ability to update devices collectively without having to modify individual device configurations.

Profiles assign configuration parameters, applicable policies and WLANs to one or more controllers, services platforms and Access Points, thus allowing smart administration across large wireless network segments. However, individual devices can still be assigned unique configuration parameters that follow the flat configuration model supported in previous software releases. As individual device updates are made, these device no longer share the profile based configuration they originally supported. Changes made to the profile are automatically inherited by all assigned devices, but not those devices who have had their configuration customized. These devices require careful administration, as they no longer can be tracked and as profile members. Their customized configurations overwrite their profile configurations until the profile can be re-applied to the device.

Each controller, service platform and Access Point is automatically assigned a default profile unless an AP auto provisioning policy is defined that specifically assigns the Access Point to a user defined profile. A default profile for each supported model is automatically added to a device's configuration file when the device is discovered. Default profiles can also be manually added prior to discovery when needed. Default profiles are ideal for single site deployments where controllers, service platforms or Access Points share a common configuration.

Device Model	Default Profile
anyap	anyap
AP6521	default-ap6521
AP6522	default-ap6522
AP6532	default-ap6532
AP6562	default-ap6562
AP7161	default-ap71xx
AP7502	default-ap7502
AP7522	default-ap7522
AP7532	default-ap7532
AP7562	default-ap7562
AP8122, AP8132, AP8163	default-ap81xx
AP8232	default-ap82xx
AP8432	default-ap8432
AP8533	default-ap8533
EX3524	default-ex3524
EX3548	default-ex3548
NX5500	default-nx5500
NX6500, NX6524	default-nx65xx
NX7500	default-nx75xx

NX9000, NX9500, NX9510	default-nx9000
RFS4000	default-rfs4000
RFS6000	default-rfs6000
T5	default-t5
VX9000	default-vx

User defined profiles are manually created for each supported controller, service platform and Access Point model. User defined profiles can be manually assigned or automatically assigned to Access Points using an AP Auto provisioning policy. AP Adoption policies provide the means to easily assign profiles to Access Points based on model, serial number, VLAN ID, DHCP option, IP address (subnet) and MAC address.

User defined profiles are recommended for larger deployments using centralized controllers and service platforms when groups of devices on different floors, buildings or sites share a common configuration.

Each default and user defined profile contains policies and configuration parameters. Changes made to these parameters are automatically inherited by the devices assigned to the profile.

Review existing profiles to determine whether a new profile requires creation, or an existing profile requires edit or deletion.

To review the existing profiles:

1 Select the **Configuration** tab from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the **Configuration** > **Profiles** menu.

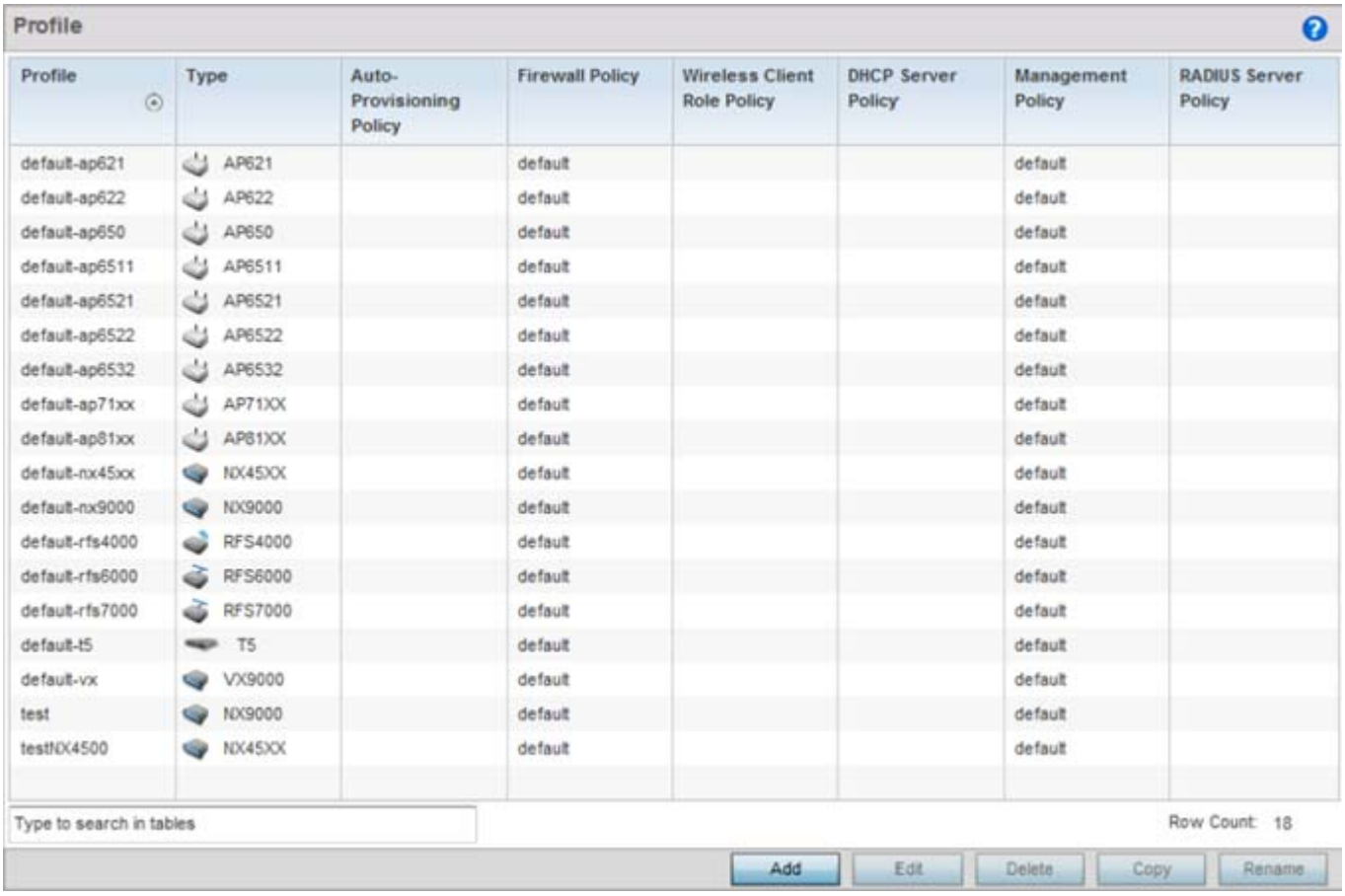


Figure 8-1 *Profile screen*

4 Review the following information on existing profiles:

Profile	Lists the user-assigned name defined for each profile when created. Profile names cannot be edited with a profiles configuration.

Type	Displays the device type (and subsequent device specific configuration) supported by each listed profile. Available device types include: • *AP6521* • *AP6522* • *AP6532* • *AP6562* • *AP71xx* • *AP7502* • *AP7522* • *AP7532* • *AP7562* • *AP81xx* • *AP82xx* • *AP8432* • *AP8533* • *EX3524* • *EX3548* • *RFS4000* • *RFS6000* • *NX5500* • *NX75xx* • *NX9000* • *T5* • *VX9000*
Auto Provisioning Policy	Displays the auto provisioning policy applied to this profile. At adoption, an AP solicits and receives multiple adoption responses. These adoption responses contain preference and loading policy information the AP uses to select the optimum controller, service platform or peer Access Point model for adoption. By default, an auto provisioning policy generally distributes AP adoption evenly amongst available adopters. Modify existing adoption policies or create a new one as needed to meet the adoption requirements of this particular profile.
Firewall Policy	Displays an existing firewall policy, if any, assigned to each listed profile. Firewall policies can be assigned when creating or editing a profile.
Wireless Client Role Policy	Lists the name of the wireless client role policy currently applied to the listed device. The wireless client role policy contains the matching rules and IP and MAC Inbound and Outbound policies used to filter traffic to and from clients.
DHCP Server Policy	Lists the name of the DHCP Server Policy used with each listed profile. An internal DHCP server groups wireless clients based on defined user-class option values. Clients with a defined set of user class values are segregated by class. A DHCP server can associate multiple classes to each pool. Each class in a pool is assigned an exclusive range of IP addresses.
Management Policy	Lists the name of Management policies applied to each listed profile. A management policy is a mechanism to allow/deny management access for separate interfaces and protocols (*HTTP*, *HTTPS*, *Telnet*, *SSH* or *SNMP*). Management access can be enabled/disabled as required for each policy.
RADIUS Server Policy	Displays the name of the RADIUS Server policy applied to each listed profile. A RADIUS Server policy provides customized, profile specific, management of authentication data (usernames and passwords).

5 Select the **Add** button to create a new profile, **Edit** to revise a selected profile configuration or **Delete** to permanently remove a selected profile. Optionally **Copy** or **Rename** profiles as needed.

The following tasks comprise required profile configuration activities:

- *General Profile Configuration*
- *Profile Cluster Configuration (Controllers and Service Platforms)*
- *Profile Adoption Configuration (APs Only)*
- *Profile Adoption Configuration (Controllers Only)*
- *Profile Radio Power (AP71XX, AP81XX Only)*
- *Profile 802.1x Configuration*
- *Profile Interface Configuration*
- *Profile Network Configuration*
- *Profile Security Configuration*
- *Profile VRRP Configuration*
- *Profile Critical Resources Configuration*
- *Profile Services Configuration*
- *Profile Management Configuration*
- *Profile Mesh Point Configuration*
- *Profile Environmental Sensor Configuration (AP8132 Only)*
- *Advanced Profile Configuration*

8.1 General Profile Configuration

Each profile requires a provisioning policy and clock synchronization settings as part of its general configuration. Each profile can have a unique provisioning policy and system time.

Controllers, service platforms and Access Points are automatically assigned a default profile unless an AP provisioning policy has been defined that specifically assigns Access Points to a user defined profile. During the general configuration process, a provisioning policy can be assigned to a specific profile or a new provisioning policy can be created and applied to the profile. Adoption is the process an AP uses to discover potential adopters in the network, pick the most desirable one, establish an association and obtain its configuration.

Network Time Protocol (NTP) manages time and/or network clock synchronization within the network. NTP is a client/server implementation. Controllers, service platforms and Access Points (NTP clients) periodically synchronize their clock with a master clock (an NTP server). For example, a controller resets its clock to 07:04:59 upon reading a time of 07:04:59 from its designated NTP server.

Additionally, if the profile is supporting an Access Point, the profile's general configuration provides an option to disable the device's LEDs.

To define a profile's general configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu.

4 Select **General.**

A General configuration screen displays for the new or existing profile.

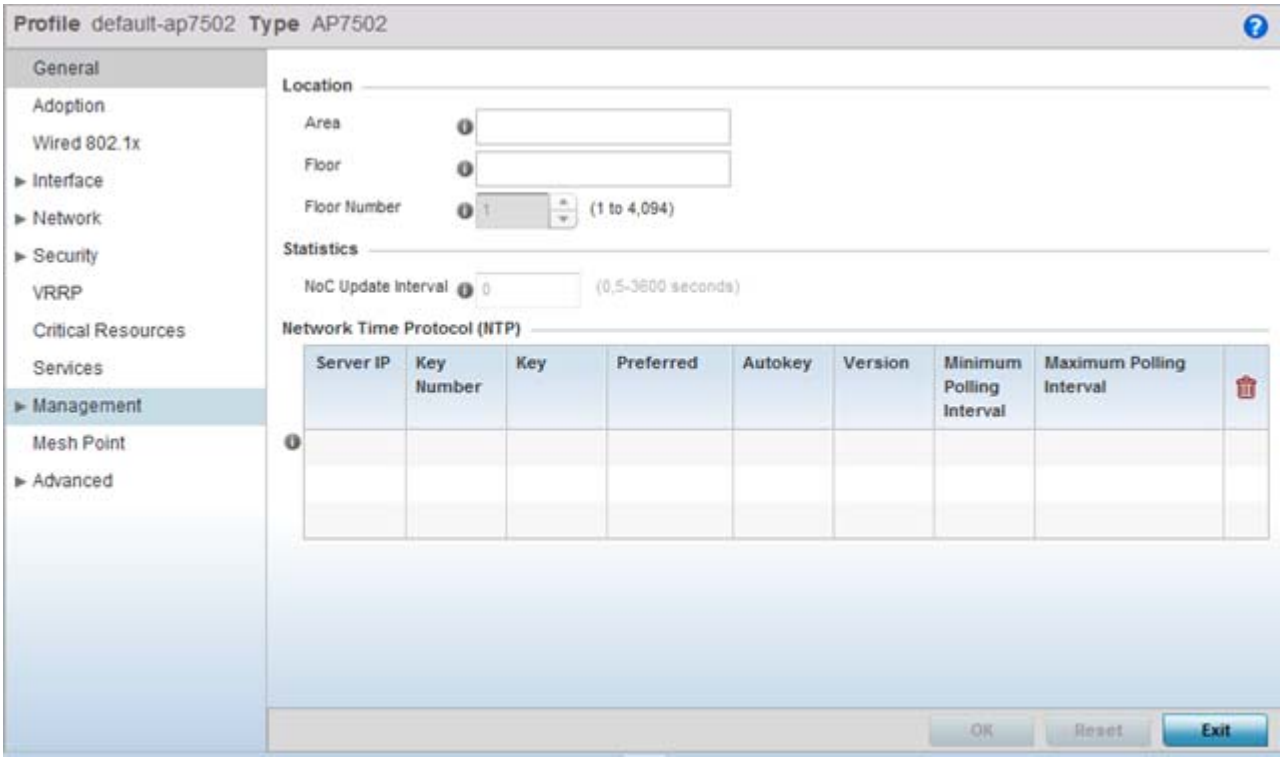


Figure 8-2 *General Profile - screen*

5 If creating a new profile, provide a name (up to 32 characters) within the **Profile** parameter field.

6 Use the **Type** drop-down menu to specify the device model for which the profile applies.

Profiles can only be applied to the same device type selected when the profile is initially created.

7 Refer to the **Location** field to define the device's deployment location area.

Area	Enter a 64 character maximum description for the selected device's physical deployment area. This area can be further refined by floor and floor number descriptions.
Floor	Enter a 32 character maximum description for the selected device's building floor placement. This area can be further refined by floor and floor number descriptions.
Floor Number	Use the spinner control to assign a numeric deployment floor number (from 1 - 4094) for this device. The default floor is 1.

8 Within the **Statistics** field, use the **NoC Update Interval** to set the statistics update interval (from 0, 5 - 3600 seconds) from the RF Domain manager to its adopting controller. The default value is 0.

A value of 0 is allowable for an auto mode where the update interval is auto adjusted by the controller based on load information.

9 Select **+ Add Row** below the **Network Time Protocol (NTP)** table to define the configurations of NTP server resources used to obtain system time. Up to 3 servers can be added. Set the following parameters to define the NTP configuration:

Server IP	Set the IP address of each server added as a potential NTP resource.
Key Number	Select the number of the associated authentication peer key for the NTP resource.

Key	Enter a 64 character maximum key used when the autokey setting is set to false (disabled). Select the Show option to expose the actual character string comprising the key.
Preferred	Select this option to designate this NTP resource as a preferred NTP resource. This setting is disabled by default.
AutoKey	Select the check box to enable an autokey configuration for the NTP resource. The default setting is disabled.
Version	Use the spinner control to specify the version number (from 0 - 4) used by this NTP server resource. The default setting is 0.
Minimum Polling Interval	Use the spinner control to set the minimum polling interval (in seconds) used to contact the NTP server resource. Once set, the NTP resource is polled no sooner then the defined interval. The default setting is 64 seconds.
Maximum Polling Interval	Use the spinner control to set the maximum polling interval (in seconds) used to contact the NTP server resource. Once set, the NTP resource is polled no later then the defined interval. The default setting is 1024 seconds.

10 Refer to the **RAID Alarm** field to either *enable* or *disable* the chassis alarm that sounds when events are detected that degrade RAID support (drive content mirroring) on a series service platform.

NOTE: RAID controller drive arrays are available within NX7500 and NX9000 series service platforms (NX9000, NX9500 and NX9510 models) only. However, they can be administrated on behalf of a profile by a different model service platform or controller.

RAID controller drive arrays are available within NX7530 and NX9000 series service platforms (NX9000, NX9500 and NX9510 models) only. However, they can be administrated on behalf of a profile by a different model service platform or controller.

Service platforms include a single Intel MegaRAID controller (virtual drive) with RAID-1 mirroring support enabled. The online virtual drive supports up to two physical drives that could require hot spare substitution if a drive were to fail. An administrator can manage the RAID controller event alarm and syslogs supporting the array hardware from the service platform user interface and is not required to reboot the service platform BIOS.

For information on setting the service platform drive array configuration and diagnostic behavior of its member drives, refer to *RAID Operations on page 14-19*. To view the service platform's current RAID array status, drive utilization and consistency check information, refer to *RAID Statistics on page 15-114*.

11 Select **OK** to save the changes made to the general profile configuration. Select **Reset** to revert to the last saved configuration.

8.1.1 General Profile Configuration and Deployment Considerations

General Profile Configuration

Before defining a general profile configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- A default profile is applied automatically, and default AP profiles are applied to discovered Access Points.
- Each user defined profile requires a unique name.
- User defined profiles can be automatically assigned to Access Points using AP adoption policies.

- Each controller, service platform and Access Point model is automatically assigned a default profile based on the hardware type selected when the profile is initially created.

8.2 Profile Cluster Configuration (Controllers and Service Platforms)

Configuration and network monitoring are two tasks a network administrator faces as a network grows in terms of the number of managed devices. Such scalability requirements lead network administrators to look for managing and monitoring each node from a single centralized management entity. A controller or service platform not only provides a centralized management solution, it provides a centralized management profile that can be shared by any single cluster member. This eliminates dedicating a management entity to manage all cluster members and eliminates a single point of failure.

A redundancy group (cluster) is a set of controller or services platforms (nodes) uniquely defined by a profile's configuration. Within the redundancy group, members discover and establish connections to other members and provide wireless network self-healing support in the event of cluster member failure.

A cluster's load balance is typically distributed evenly amongst the cluster members. Define how often this profile is load balanced for radio distribution, as radios can come and go and members can join and exit the cluster.

To define a cluster configuration for use with a profile:

1 Select the Configuration tab from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu.

4 Select **Cluster.**
A screen displays where the profile's cluster and AP load balancing configuration can bet set.

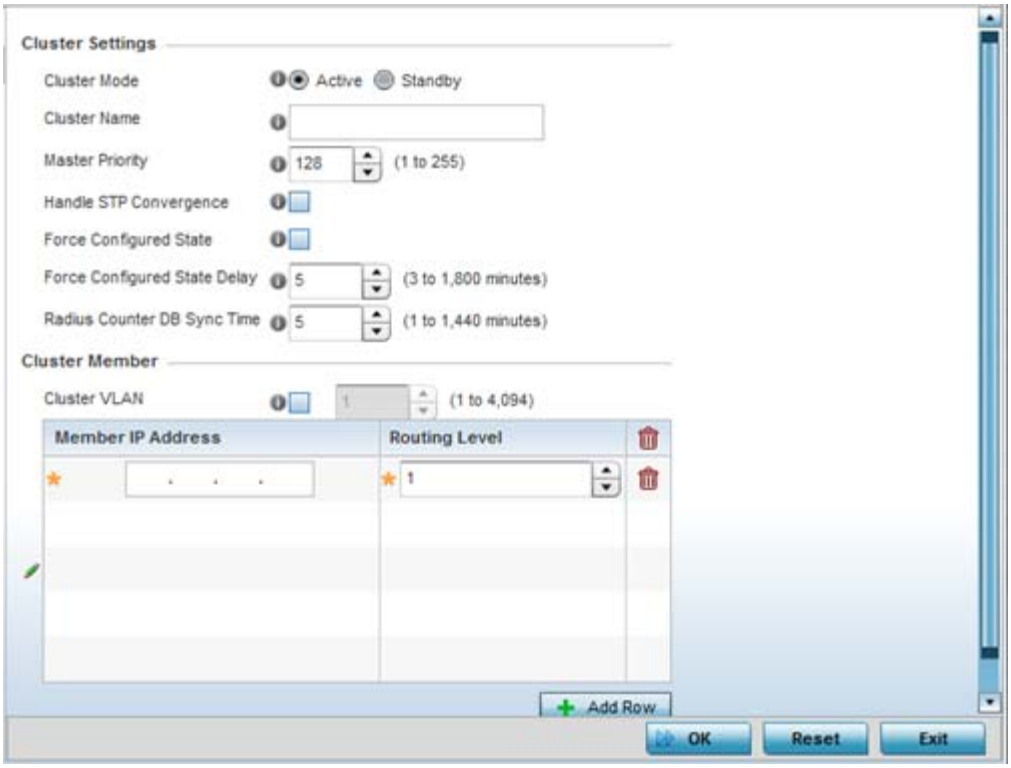


Figure 8-3 *Controller Profile - Cluster screen*

5 Define the following **Cluster Settings** parameters to set this profile's cluster mode and deployment settings:

Cluster Mode	A member can be in either an *Active* or *Standby* mode. All active member can adopt Access Points. Standby members only adopt Access Points when an active member has failed or sees an Access Point not adopted by a controller or service platform. The default cluster mode is *Active* and enabled for use with the profile.
Cluster Name	Define a name for the cluster name unique to its configuration or profile support requirements. The name cannot exceed 64 characters.
Master Priority	Set a priority value from1 - 255, with the higher value given higher priority. This configuration is the device's priority to become the cluster master. In a cluster environment, one device from the cluster is elected as the cluster master. The master priority setting is the device's priority to become cluster master. The active primary controller has the higher master priority. The default value is 128.

Handle STP Convergence	Select the check box to enable *Spanning Tree Protocol* (STP) convergence for the controller or service platform. In general, this protocol is enabled in layer 2 networks to prevent network looping. Spanning Tree is a network layer protocol that ensures a loop-free topology in a mesh network of inter-connected layer 2 controllers or service platforms. The spanning tree protocol disables redundant connections and uses the least costly path to maintain a connection between any two cluster members in the network. If enabled, the network forwards data only after STP convergence. Enabling STP convergence delays the redundancy state machine execution until the STP convergence is completed (the standard protocol value for STP convergence is 50 seconds). Delaying the state machine is important to load balance APs at startup. The default setting is disabled.
Force Configured State	Select the check box to enable this controller or service platform to take over for an active controller or service platform member if it were to fail. A standby node takes over APs adopted by the failed controller or service platform. If the failed controller or service platform were to come available again, the active controller or service platform starts a timer based on the Auto Revert Delay interval. At the expiration of the Auto Revert Delay, the standby node releases all adopted APs and goes back to a monitoring mode. The Auto Revert Delay timer is stopped and restarted if the active controller or service platform goes down and comes up during the Auto Revert Delay interval. The default value is disabled.
Force Configured State Delay	Specify a delay interval (from 3 - 1,800 minutes) a standby node waits before releasing adopted APs and goes back to a monitoring mode when a controller or service platform becomes active again after a failure. The default interval is 5 minutes.
RADIUS Counter DB Sync Time	Specify a sync time (from 1 - 1,440 minutes) a RADIUS counter database uses as its synchronization interval with the dedicated NTP server resource. The default interval is 5 minutes.

6 Within the **Cluster Member** field, select the **Cluster VLAN** checkbox to enable a spinner control to designate the VLAN where cluster members are reachable. Specify a VLAN from 1 - 4094.

Select **+ Add Row** and specify the IP addresses of the VLAN's cluster members. Set a routing level of either 1 or 2, where 1 is local routing and 2 is inter-site routing.

7 Select **OK** to save the changes made to the profile's cluster configuration. Select **Reset** to revert to the last saved configuration.

8.2.1 Cluster Profile Configuration and Deployment Considerations

Profile Cluster Configuration (Controllers and Service Platforms)

Before defining a profile cluster configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- A cluster member cannot adopt more APs than its hardware capacity allows. This is important when the number of pooled AP and AAP licenses exceeds the aggregated AP and AAP capacity available after a cluster member has failed. A cluster supported profile should be designed to ensure adequate AP and AAP capacity exists to address failure scenarios involving both APs and AAPs.
- When clustering is enabled for a profile and a failure occurs, AP and AAP licenses are persistent in the cluster even during reboots or power outages. If a cluster member failure were to occur, clustering should remain enabled on all remaining cluster members or the pooled member licenses will be lost.

8.3 Profile Adoption Configuration (APs Only)

Adoption is the process an Access Point uses to discover available controllers, pick the most desirable controller, establish a controller association and optionally obtain an image upgrade and configuration. Adoption is configurable and supported within a device profile and applied to other Access Points supported by the profile. Individual attributes of an Access Point's auto provisioning policy can be overridden as specific parameters require modification.

At adoption, an Access Point solicits and receives multiple adoption responses from controllers and service platforms available on the network. These adoption responses contain loading policy information the Access Point uses to select the optimum controller or service platform for adoption. By default, an auto provisioning policy generally distributes AP adoption evenly amongst available controllers and service platforms. Modify existing adoption policies or create a new one as needed to meet the adoption requirements of a device and their assigned profile.

To define an Access Point's adoption configuration:

Select the **Configuration** tab from the Web UI.

1 Select **Profiles** from the Configuration tab.

2 Select **Manage Profiles** from the **Configuration > Profiles** menu.

3 Select **Adoption**.

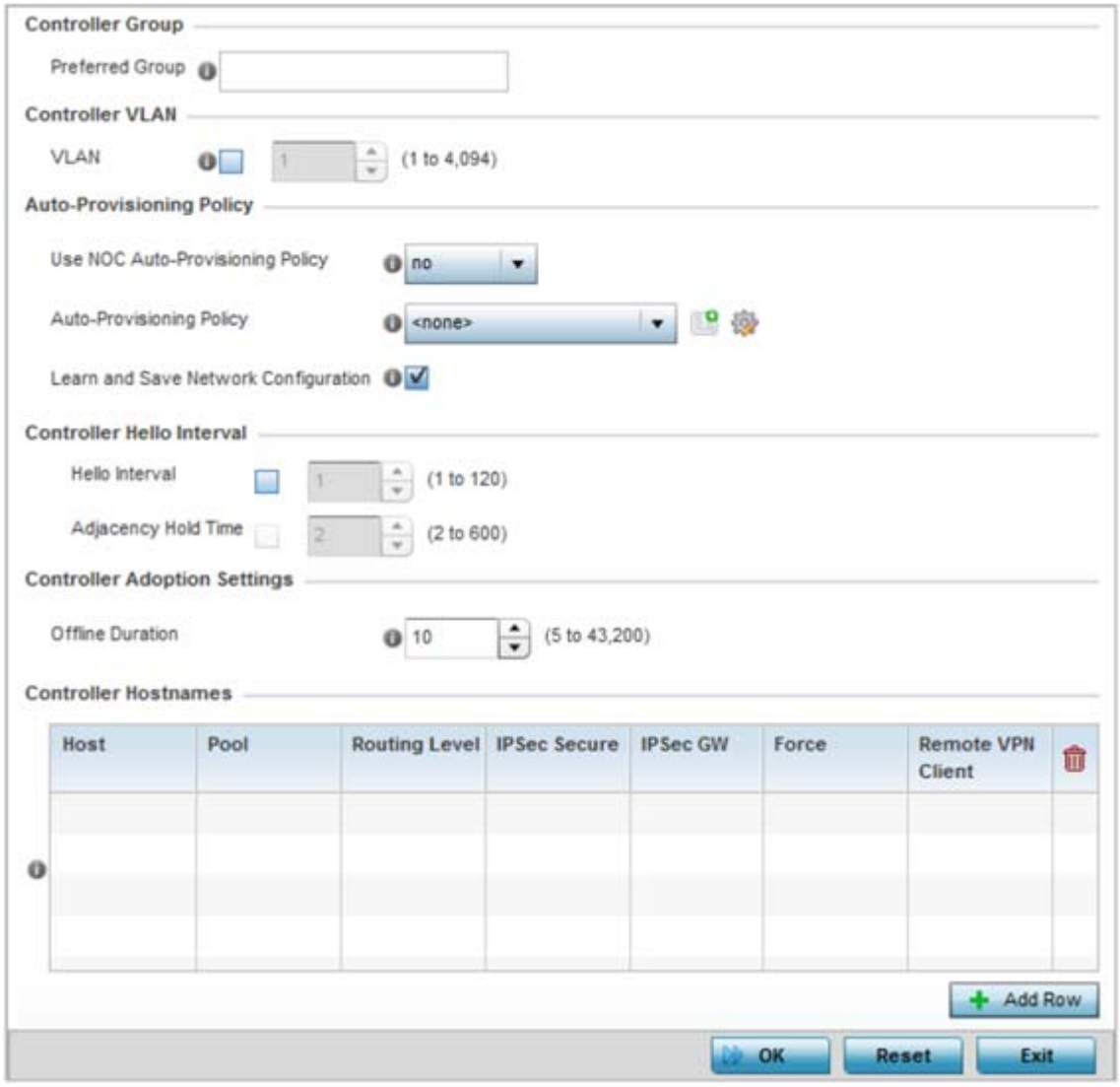


Figure 8-4 *Provisioning Policy - Adoption screen*

4 Within the **Controller Group** field, use the **Preferred Group** item to set an optimal group for the Access Point's adoption. The name of the preferred group cannot exceed 64 characters.

5 Select the check box to define or override a **Controller VLAN** the Access Point's associating controller or service platform is reachable on. VLANs 0 and 4,094 are reserved and cannot be used by a controller or service platform VLAN.

6 Set the following **Auto-Provisioning Policy** settings for Access Point adoptions:

Use NOC Auto-Provisioning Policy	Select this option to use the NOC controller's auto provisioning policy and not the policy maintained locally. The NOC is an elected controller or service platform capable of provisioning all of its peer controllers, service platforms and adopted devices. This setting is disabled by default. NOC controllers are NX9000, NX9500, NX9510, NX7500, NX6500, NX6524 and RFS6000 models.
Auto-Provisioning Policy	Select an auto provisioning policy from the drop-down menu. To create a new auto provisioning policy, select the *Create* icon or modify an existing one by selecting the *Edit* icon.

Learn and Save Network Configuration	Select this option to learn and save the configuration of any device requesting adoption. This setting is enabled by default.

7 Set the following **Controller Hello Interval** parameters:

Hello Interval	Define an interval (from 1 - 120 seconds) between hello keep alive messages exchanged with the adopting device. These messages serve as a connection validation mechanism to ensure the availability of the adopting resource.
Adjacency Hold Time	Set the time (from 2 - 600 seconds) after the last hello packet after which the connection between the controller and Access Point is defined as lost and their connection is re-established.

8 Use the spinner control to define an **Offline Duration** timeout (from 5 - 43,200 minutes) to detect whether an adopted device is offline. The default setting is 10 minutes.

9 Enter **Controller Hostnames** as needed to define resources for Access Point adoption.

Select **+ Add Row** as needed to populate the table with IP Addresses or Hostnames used as Access Point adoption resources into the managed network.

Host	Use the drop-down menu to specify whether the adoption resource is defined as a (non DNS) *IP Address* or a *Hostname*. Once defined, provide the numerical IP or Hostname. A Hostname cannot exceed 64 characters.
Pool	Use the spinner control to set a pool of either 1 or 2. This is the pool the target controller or service platform belongs to.
Routing Level	Define a routing level (either 1 or 2) for the link between adopting devices. The default setting is 1.
IPSec Secure	Enable this option to provide IPSec secure peer authentication on the connection (link) between the adopting devices. This option is disabled by default.
IPSec GW	Select the numerical IP address or administrator defined hostname of the adopting controller resource. A Hostname cannot exceed 64 characters.
Force	Enable this setting to create a forced link between an Access Point and adopting controller, even when not necessarily needed. This setting is disabled by default.
Remote VPN Client	Displays whether a secure controller link has been established using a remote VPN client.

10 Select **OK** to save the changes to the Access Point profile adoption configuration. Select **Reset** to revert to the last saved configuration.

8.4 Profile Adoption Configuration (Controllers Only)

Adoption is the process an Access Point uses to discover available controllers, pick the most desirable controller, establish a controller association and optionally obtain an image upgrade and configuration. Adoption is configurable and supported within a device profile and applied to other Access Points supported by the profile. Individual attributes of an Access Point's auto provisioning policy can be overridden as specific parameters require modification.

At adoption, an Access Point solicits and receives multiple adoption responses from controllers and service platforms available on the network. These adoption responses contain loading policy information the Access Point uses to select the optimum controller or service platform for adoption. By default, an auto provisioning policy generally distributes AP adoption evenly amongst available controllers and service platforms. Modify existing adoption policies or create a new one as needed to meet the adoption requirements of a device and their assigned profile.

To define a controller or service platform's adoption configuration:

Select the **Configuration** tab from the Web UI.

1 Select **Profiles** from the Configuration tab.

2 Select **Manage Profiles** from the **Configuration > Profiles** menu.

3 Select **Adoption**.

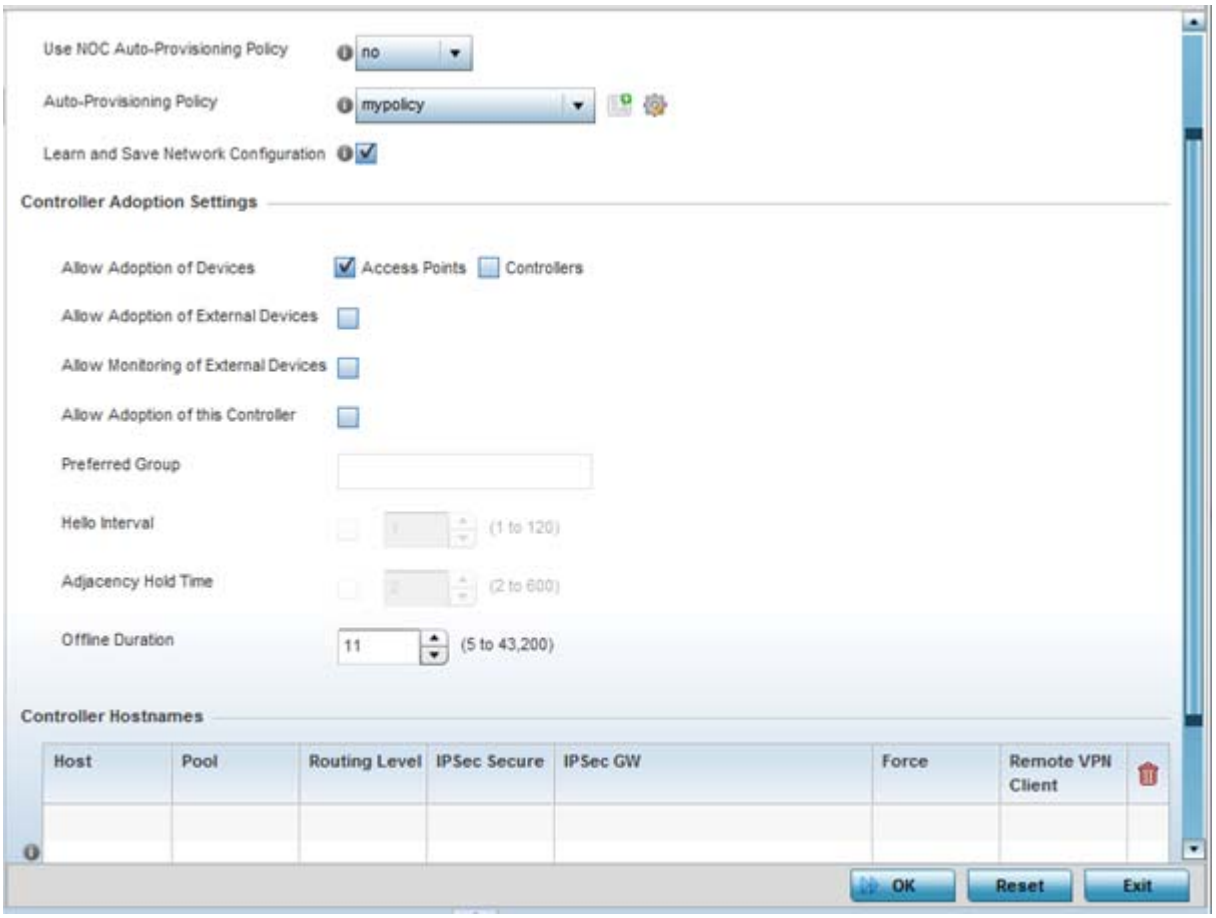


Figure 8-5 *Provisioning Policy - Adoption screen*

4 Within the **Controller Group** field, use the **Group** item to set provide the controller group this controller or service platform belongs to. A preferred group can also be selected for the adoption of this controller or service platform. The name of the preferred group cannot exceed 64 characters.

5 Set the following **Auto Provision Policy** parameters:

Use NOC Auto-Provisioning Policy	Select this option to use the NOC's auto provisioning policy instead of the policy local to the controller or service platform. The NOC is an elected controller or service platform capable of provisioning all of its peer controllers, service platforms and adopted devices. This setting is disabled by default.
Auto-Provisioning Policy	Select an auto provisioning policy from the drop-down menu. To create a new auto provisioning policy, select the *Create* icon or modify an existing one by selecting the *Edit* icon.
Learn and Save Network Configuration	Select this option to enable allow the controller tor service platform to maintain a local configuration records of devices requesting adoption and provisioning. This feature is enabled by default.

6 Set the following **Controller Adoption Settings** settings:

Allow Adoption of Devices	Select either *Access Points* or *Controllers* (or both) to refine whether this controller or service platform can adopt just networked Access Points or peer controller devices as well.
Allow Adoption of External Devices	Select this option to enable this controller or service platform to adopt T5 model devices or EX3500 model switches.
Allow Monitoring of External Devices	Select this option to enable monitoring only of T5 model devices or EX3500 model switches by this controller or service platform. When enabled, WiNG does not configure EX3500 switches or a T5, it only monitors those devices for statistics and events.
Allow Adoption of this Controller	Select the option to enable this controller or service platform to be capable of adoption by other controllers or service platforms. This settings is disabled by default and must be selected to allow peer adoptions.
Preferred Group	If *Allow Adoption of this Controller* is selected, provide the controller group preferred as the adopting entity for this controller or service platform. If utilizing this feature, ensure the appropriate group is provided within the Controller Group field.
Hello Interval	Select this option to define the hello packet exchange interval (from 1 - 120 seconds) between the controller or service platform and an adoption requesting Access Point.
Adjacency Hold Time	Select this option to set a hold time interval (from 2 - 600 seconds) for the transmission of hello packets.
Offline Duration	Use the spinner control to define a timeout (from 5 - 43,200 minutes) to detect whether an adopted device is offline. The default setting is 10 minutes.

7 Enter **Controller Hostnames** as needed to define resources for Access Point adoption.

NOTE: This field is only available when *Allow Adoption of this Controller* is selected.

8 Select **+ Add Row** as needed to populate the table with IP Addresses or Hostnames used as Access Point adoption resources into the managed network. A Hostname cannot exceed 64 characters.

Host	Use the drop-down menu to specify whether the adoption resource is defined as a (non DNS) *IP Address* or a *Hostname*. Once defined, provide the numerical IP or Hostname. A Hostname cannot exceed 64 characters.
Pool	Use the spinner control to set a pool of either 1 or 2. This is the pool the target controller or service platform belongs to.
Routing Level	Define a routing level (either 1 or 2) for the link between adopting devices. The default setting is 1.
IPSec Secure	Enable this option to provide IPSec secure peer authentication on the connection (link) between the adopting devices. This option is disabled by default.
IPSec GW	Select the numerical IP address or administrator defined hostname of the adopting controller resource. A Hostname cannot exceed 64 characters.
Force	Enable this setting to create a forced link between an Access Point and adopting controller, even when not necessarily needed. This setting is disabled by default.
Remote VPN Client	Displays whether a secure controller link has been established using a remote VPN client.

9 Select **OK** to save the changes to the controller or service platform profile adoption configuration. Select **Reset** to revert to the last saved configuration.

8.5 Profile Radio Power (AP71XX, AP81XX Only)

This option is only available for AP7131, AP7161, AP7181, AP8122 and AP8132 Access Points.

Use the *Power* screen to set one of two power modes (*3af* or *Auto*) for the Access Point profile. When *Automatic* is selected, the Access Point safely operates within available power. Once the power configuration is determined, the Access Point configures its operating power characteristics based on its model and power configuration.

An Access Point uses a *complex programmable logic device* (CPLD) to manage power. The CPLD determines proper supply sequencing, the maximum power available and other status information. One of the primary functions of the CPLD is to determine the maximum power budget. When an Access Point is powered on (or performing a cold reset), the CPLD determines the maximum power provided by the POE device and the budget available to the Access Point. The CPLD also determines the Access Point hardware SKU (model) and the number of radios.

If the Access Point's POE resource cannot provide sufficient power to run the Access Point (with all intended interfaces enabled), some of the following interfaces could be disabled or modified:

- The Access Point's transmit and receive algorithms could be negatively impacted
- The Access Point's transmit power could be reduced due to insufficient power
- The Access Point's WAN port configuration could be changed (either enabled or disabled)

To define an Access Point's power configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the **Configuration > Profiles** menu.

4 Select **Power.**
A screen displays where the Access Point profile's power mode can be defined.

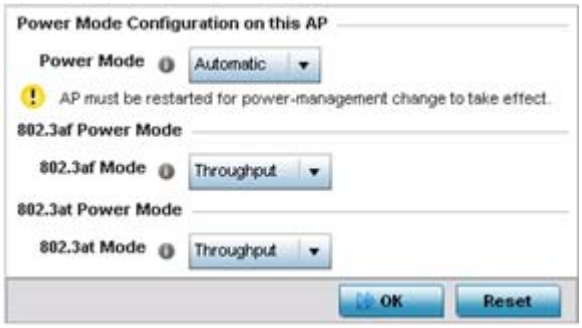


Figure 8-6 *Profile - Power screen*

5 Use the **Power Mode** drop-down menu to set the **Power Mode Configuration on this AP**.

NOTE: Single radio model Access Points always operate using a full power configuration. The power management configurations described in this section do not apply to single radio Access Point models.

When an Access Point is powered on for the first time, it determines the power budget available. Using the *Automatic* setting, the Access Point automatically determines the best power configuration based on the available power budget. *Automatic* is the default setting.

If 802.3af is selected, the Access Point assumes 12.95 watts are available. If the mode is changed, the Access Point requires a reset to implement the change. If 802.3at is selected, the Access Point assumes 23 - 26 watts are available.

6 Set the Access Point radio's **802.3af Power Mode** and the radio's **802.3at Power Mode**.

7 Use the drop-down menu for each power mode to define a mode of either *Range* or *Throughput*.

8 Select *Throughput* to transmit packets at the radio's highest defined basic rate (based on the radio's current basic rate settings). This option is optimal in environments where the transmission range is secondary to broadcast/multicast transmission performance.

9 Select *Range* when range is preferred over performance for broadcast/multicast (group) traffic. The data rates used for range are the lowest defined basic rates. Throughput is the default setting for both 802.3af and 802.3at.

10 Select **OK** to save the changes made to the Access Point power configuration. Select **Reset** to revert to the last saved configuration.

8.6 Profile 802.1x Configuration

802.1X provides administrators secure, identity based access control as another data protection option to utilize with a device profile.

802.1X is an IEEE standard for media-level (Layer 2) access control, offering the capability to *permit* or *deny* network connectivity based on the identity of the user or device.

1 Select the **Configuration** tab from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the **Configuration > Profiles** menu.

4 Select **Wired 802.1x**.

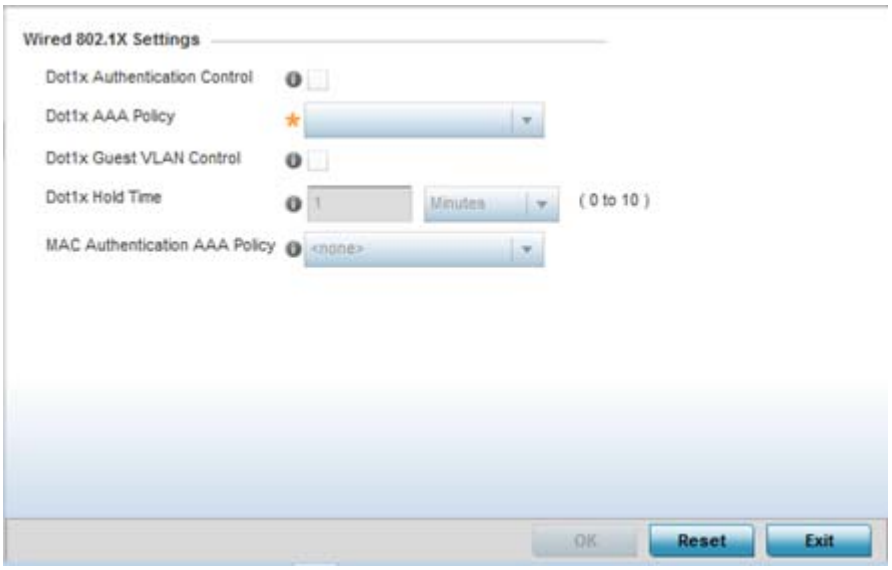


Figure 8-7 *Profile - Wired 802.1x screen*

5 Set the following **Wired 802.1x Settings**:

Dot1x Authentication Control	Select this option to globally enable 802.1x authentication for the selected device. This setting is disabled by default.
Dot1x AAA Policy	Use the drop-down menu to select an AAA policy to associate with the wired 802.1x traffic. If a suitable AAA policy does not exist, click the *Create* icon to create a new policy or the *Edit* icon to modify an existing policy.
Dot1x Guest VLAN Control	Select this option to globally enable 802.1x guest VLANs for the selected device. This setting is disabled by default.
Dot1x Hold Time	Select this option to globally enable 802.1x hold time for the selected device. When Dot1X authentication fails 3 times continuously, this is the time period for which no RADIUS requests are sent. The default value is 1 minute.
MAC Authentication AAA Policy	Use the drop-down menu to select an AAA authentication policy for MAC address authentication. If a suitable MAC AAA policy does not exist, click the *Create* icon to create a new policy or the *Edit* icon to modify an existing policy.

6 Select **OK** to save the changes to the 802.1x configuration. Select **Reset** to revert to the last saved configuration.

8.7 Profile Interface Configuration

A profile's interface configuration can be defined to support separate physical Ethernet configurations both unique and specific to controllers and series service platforms. Ports vary depending on platform, but controller or service platform models do have some of the same physical interfaces

A controller or service platform requires its Virtual Interface be configured for layer 3 (IP) access or layer 3 service on a VLAN. A Virtual Interface defines which IP address is associated with each VLAN ID the controller is connected to.

If the profile is configured to support an Access Point radio, an additional Radios option is available, unique to the Access Point's radio configuration.

A profile's interface configuration process consists of the following:

- *Ethernet Port Configuration*
- *Virtual Interface Configuration*
- *Port Channel Configuration*
- *VM Interface Configuration*
- *Access Point Radio Configuration*
- *WAN Backhaul Configuration*
- *PPPoE Configuration*
- *Bluetooth Configuration*

Additionally, deployment considerations and guidelines for profile interface configurations are available for review prior to defining a configuration that could significantly impact the performance of the network. For more information, see *Profile Interface Deployment Considerations*.

8.7.1 Ethernet Port Configuration

Profile Interface Configuration

The ports available on controllers vary depending RFS controller model. The following ports are available to controllers:

- RFS4000 - ge1, ge2, ge3, ge4, ge5, up1
- RFS6000 - ge1, ge2, ge3, ge4, ge5, ge6, ge7, ge8, me1, up1

GE ports on RFS4000 and RFS6000 models are RJ-45 ports supporting 10/100/1000Mbps. The GE ports on a RFS7000 can be RJ-45 or fiber ports supporting 10/100/1000Mbps.

ME ports are available on RFS6000 and RFS7000 platforms. ME ports are out-of-band management ports used to manage the controller via CLI or Web UI, even when the other ports on the controller are unreachable.

The following ports are available to NX series service platform models:

- *NX4500* - up1, up2
- *NX4524* - ge1-ge24, up1, up2
- *NX6500* - up1, up2
- *NX6524* - ge1-ge24, up1, up2

- *NX5500* - ge1-ge24
- *NX7500* - ge1-ge24, xge1-xge2
- *NX9000 series* - ge1, ge2, xge1-xge4
- EX3524 - ge1-1-ge1-24
- EX3548 - ge1-1-ge1-48

NOTE: For a NX7500 model service platform, there are options for either a 2 port or 4 port network management card. Either card can be managed using WiNG. If the 4 port card is used, ports ge7-ge10 are available. If the 2 port card is used, ports xge1-xge2 are available.

UP ports are available on RFS4000 and RFS6000 controllers and NX4500 and NX6500 series service platforms. An UP port is used to connect to the backbone network. An UP port supports either RJ-45 or fiber. The UP port is the preferred means to connect to the backbone as it has a non-blocking 1gbps connection unlike the GE ports.

To define a profile's Ethernet port configuration:

1 Select **Configuration** > **Profiles** > **Interface**.

2 Expand the Interface menu to display its submenu options.

3 Select **Ethernet Ports.**

The Ethernet Ports screen displays configuration, runtime status and statistics regarding the physical ports on the controller or service platform.

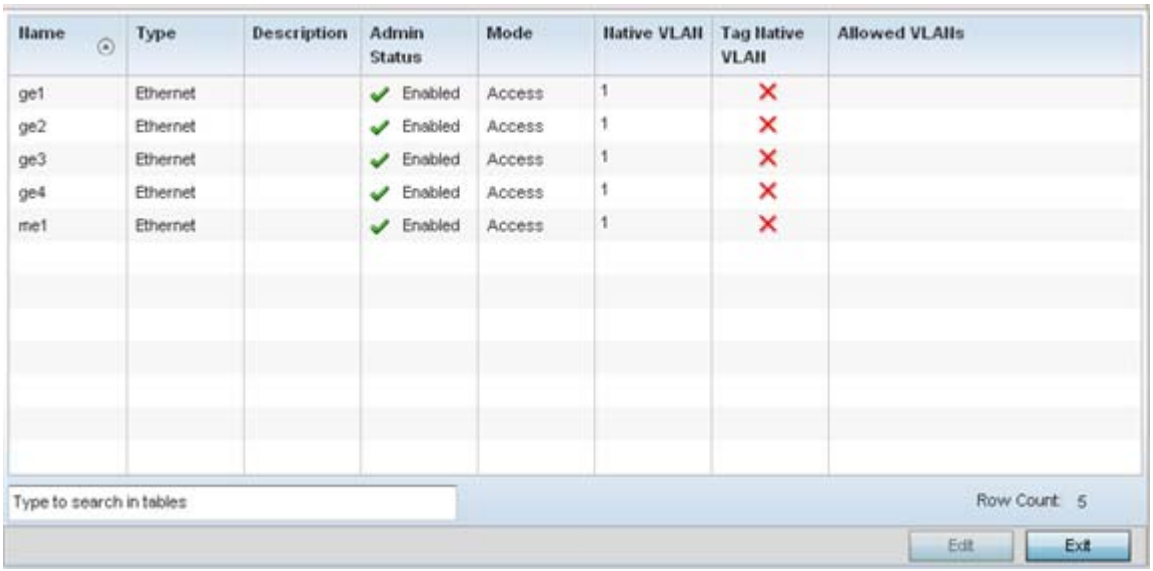


Figure 8-8 *Ethernet Ports screen*

4 Refer to the following to assess port status and performance:

Name	Displays the physical port name reporting runtime data and statistics. Supported ports vary depending on Access Point, controller or service platform model. RFS4000 - ge1, ge2, ge3, ge4, ge5, up1 RFS6000 - ge1, ge2, ge3, ge4, ge5, ge6, ge7, ge8, me1, up1 *NX4500* - up1, up2 *NX4524* - ge1-ge24, up1, up2 *NX5500* - ge1-ge24 *NX6500* - up1, up2 *NX6524* - ge1-ge24, up1, up2 *NX7500* - ge1-ge24, xge1-xge2 *NX9000* series- ge1, ge2, xge1-xge4
Type	Displays the physical port type. Copper is used on RJ45 Ethernet ports and Optical materials are used on fiber optic gigabit Ethernet ports.
Description	Displays an administrator defined description for each listed controller or service platform port.
Admin Status	A green checkmark defines the port as active and currently enabled with the profile. A red "X" defines the port as currently disabled and not available for use. The interface status can be modified with the port configuration as needed.
Mode	Displays the profile's switching mode as currently either *Access* or *Trunk* (as defined within the Ethernet Port Basic Configuration screen). If Access is selected, the listed port accepts packets only from the native VLAN. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and mapped to the native VLAN. If set to Trunk, the port allows packets from a list of VLANs added to the trunk. A port configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged.
Native VLAN	Lists the numerical VLAN ID (1 - 4094) set for the native VLAN. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.
Tag Native VLAN	A green checkmark defines the native VLAN as tagged. A red "X" defines the native VLAN as untagged. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.
Allowed VLANs	Displays those VLANs allowed to send packets over the listed port. Allowed VLANs are only listed when the mode has been set to Trunk.

5 To edit the configuration of an existing port, select it from amongst those displayed and select the **Edit** button. The Ethernet port **Basic Configuration** screen displays by default.

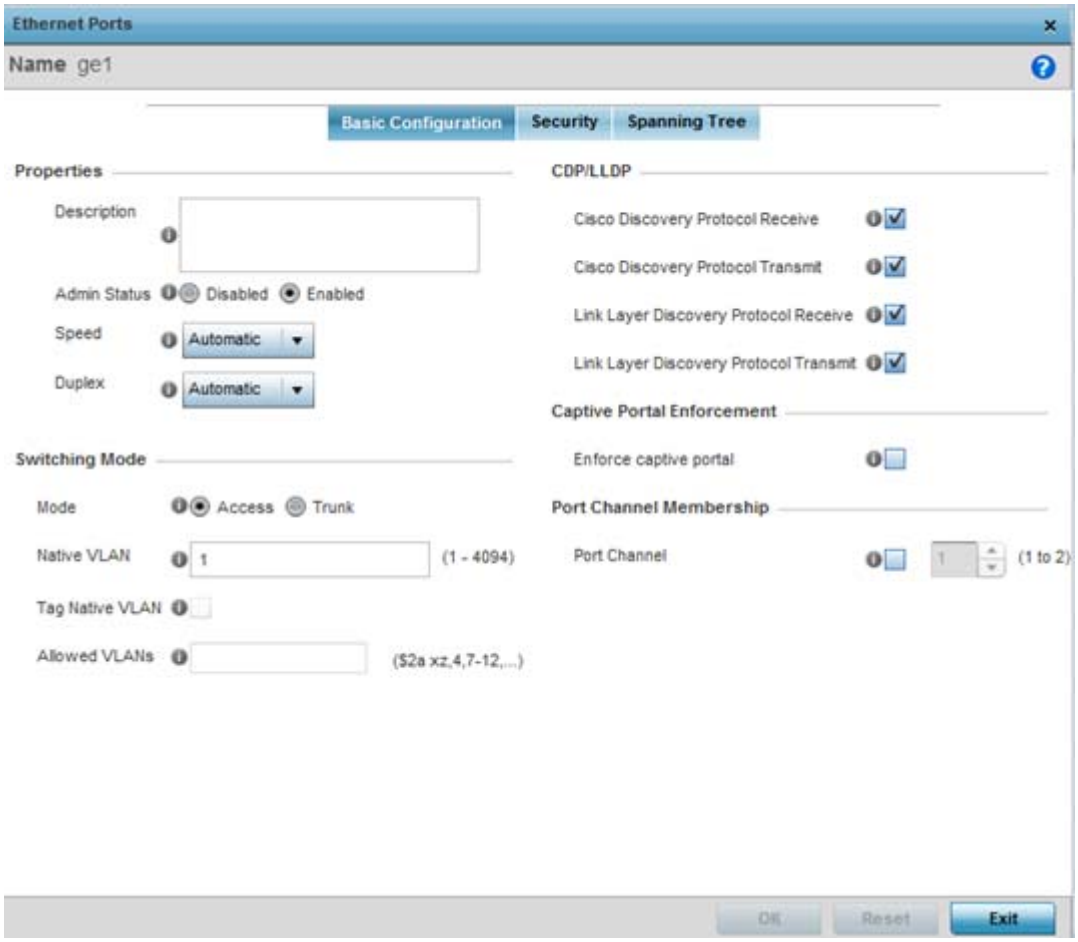


Figure 8-9 *Ethernet Ports - Basic Configuration screen*

6 Set the following Ethernet port **Properties**:

Description	Enter a brief description for the port (64 characters maximum). The description should reflect the port's intended function to differentiate it from others with similar configurations or perhaps just the name of the physical port.
Admin Status	Select the *Enabled* radio button to define this port as active to the profile it supports. Select the *Disabled* radio button to disable this physical port in the profile. It can be activated at any future time when needed.
Speed	Select the speed at which the port can receive and transmit the data. Select either *10 Mbps*, *100 Mbps* or *1000 Mbps*. Select either of these options to establish a 10, 100 or 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission over the port. These options are not available if Auto is selected. Select *Automatic* to enable the port to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis. Automatic is the default setting.

Duplex	Select either half, full or automatic as the duplex option. Select *Half* duplex to send data over the port, then immediately receive data from the same direction in which the data was transmitted. Like a full-duplex transmission, a half-duplex transmission can carry data in both directions, just not at the same time. Select *Full* duplex to transmit data to and from the controller or service platform port at the same time. Using Full duplex, the port can send data while receiving data as well. Select *Automatic* to dynamically duplex as port performance needs dictate. Automatic is the default setting.

7 Enable or disable the following **CDP/LLDP** parameters used to configure Cisco Discovery Protocol and Link Layer Discovery Protocol for this profile's Ethernet port configuration:

Cisco Discovery Protocol Receive	Select this box to allow the Cisco discovery protocol to be received on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default.
Cisco Discovery Protocol Transmit	Select this box to allow the Cisco discovery protocol to be transmitted on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors.
Link Layer Discovery Protocol Receive	Select this box to allow the Link Layer discovery protocol to be received on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors. This option is enabled by default.
Link Layer Discovery Protocol Transmit	Select this box to allow the Link Layer discovery protocol to be transmitted on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors.

8 Set the following **Power Over Ethernet (PoE)** parameters for this profile's Ethernet port configuration:

Enable POE	Select this option to configure the selected controller or service platform port to use Power over Ethernet. To disable PoE on a port, uncheck this option. PoE is supported on RFS4000 and RFS6000 model controllers and NX4524 and NX6524 model service platforms. Each of a NX4524 or NX6524's 24 GE ports supports 3af (15.4W) on each of its 24 ports simultaneously. NX4524 and NX6524 models support up to 30W per port, with a maximum of 360W. NX4500 and NX6500 models do not support PoE over their UP1 and UP2 ports. When enabled, the controller or service platform supports 802.3af PoE on each of its ge ports. The PoE allows users to monitor port power consumption and configure power usage limits and priorities for each ge port.
Power Limit	Use the spinner control to set the total watts available for Power over Ethernet on the defined ge port. Set a value between 0 - 40 watts.
Power Priority	Set the power priority for the listed port to either to either *Low*, *Medium* or *High*. This is the priory assigned to this port versus the power requirements of the other ports on the controller or service platform.

9 Define the following **Switching Mode** parameters to apply to the Ethernet port configuration:

Mode	Select either the *Access* or *Trunk* radio button to set the VLAN switching mode over the port. If Access is selected, the port accepts packets only form the native VLANs. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. If the mode is set to Trunk, the port allows packets from a list of VLANs you add to the trunk. A port configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. Access is the default mode.
Native VLAN	Use the spinner control to define a numerical *Native VLAN ID* between 1 - 4094. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN which untagged traffic will be directed over when using a port in trunk mode. The default VLAN is 1.
Tag Native VLAN	Select the check box to tag the native VLAN. Devices support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is disabled by default.
Allowed VLANs	Selecting Trunk as the mode enables the *Allowed VLANs* parameter. Add VLANs that exclusively send packets over the listed port.

10 Select a **Captive Portal Enforcement** option for the selected Ethernet port interface.

Captive portal enforcement allows wired network users to pass traffic through the captive portal without being redirected to an authentication page. Authentication instead takes place when the RADIUS server is queried against the wired user's MAC address. If the MAC address is in the RADIUS server's user database, the user can pass traffic on the captive portal. If **None** is selected, captive portal policies are not enforced on the wired interface. If **Authentication Failure** is selected, captive portal policies are enforced only when RADIUS authentication of the client's MAC address is not successful. If **Always** is selected, captive portal policies are enforced regardless of whether the client's MAC address is in the RADIUS server's user database.

11 Optionally select the **Port Channel** checkbox and define a setting between 1 - 3 using the spinner control. This sets the channel group for the port. The upper limit depends on the device on which this value is configured.

12 Select **OK** to save the changes made to the Ethernet Port Basic Configuration. Select **Reset** to revert to the last saved configuration.

13 Select the **Security** tab.

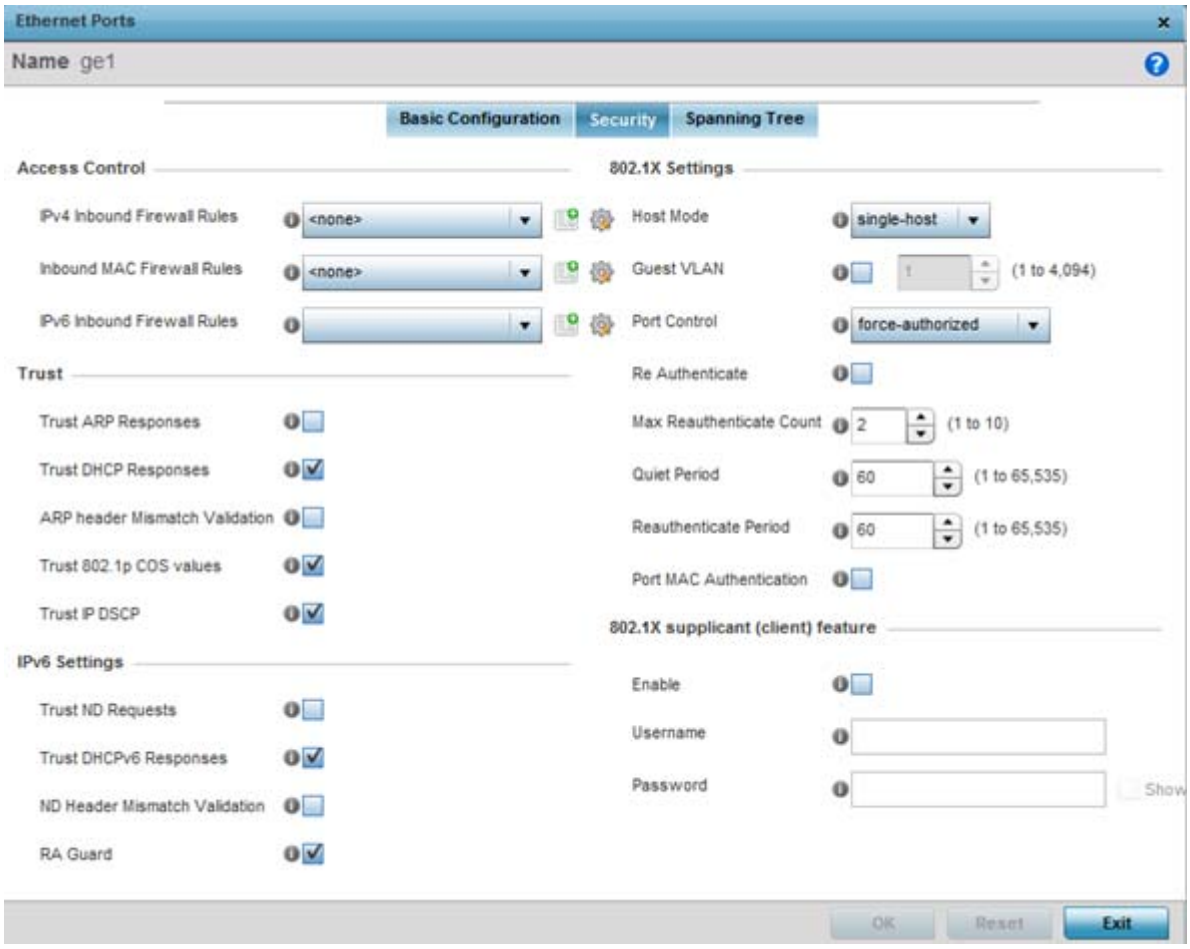


Figure 8-10 *Ethernet Ports - Security screen*

14 Refer to the **Access Control** field. As part of the port's security configuration, inbound IPv4/IPv6 and MAC address firewall rules are required.

Use the drop-down menus to select the firewall rules to apply to this profile's Ethernet port configuration. The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

Use the **IPv4 Inbound Firewall Rules** drop down menu to select the IPv4 specific firewall rules to apply to this profile's Ethernet port configuration. IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity.

Use the **IPv6 Inbound Firewall Rules** drop down menu to select the IPv6 specific firewall rules to apply to this profile's Ethernet port configuration. IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

If a firewall rule does not exist suiting the data protection needs of the target port configuration, select the **Create** icon to define a new rule configuration or select the **Edit** icon to modify an existing configuration.

15 Refer to the **Trust** field to define the following:

Trust ARP Responses	Select the check box to enable ARP trust on this port. ARP packets received on this port are considered trusted and information from these packets is used to identify rogue devices within the network. The default value is disabled.
Trust DHCP Responses	Select the check box to enable DHCP trust on this port. If enabled, only DHCP responses are trusted and forwarded on this port, and a DHCP server can be connected only to a DHCP trusted port. The default value is enabled.
ARP header Mismatch Validation	Select this option to enable a mismatch check for the source MAC in both the ARP and Ethernet header. The default value is disabled.
Trust 802.1p COS values	Select the check box to enable 802.1p COS values on this port. The default value is enabled.
Trust IP DSCP	Select the check box to enable IP DSCP values on this port. The default value is enabled.

NOTE: Some vendor solutions with VRRP enabled send ARP packets with Ethernet SMAC as a physical MAC and inner ARP SMAC as VRRP MAC. If this configuration is enabled, a packet is allowed, despite a conflict existing.

16 Set the following **IPv6 Settings**:

Trust ND Requests	Select this option to enable IPv6 neighbor discovery request trust on this Ethernet port. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery Protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters. This setting is disabled by default.
Trust DHCPv6 Responses	Select this option to enable the trust all DHCPv6 responses on this Ethernet port.DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. DHCPv6 relay agents receive messages from clients and forward them a DHCPv6 server. The server sends responses back to the relay agent, and the relay agent sends the responses to the client on the local link. This setting is enabled by default.
ND Header Mismatch Validation	Select this option to enable a mismatch check for the source MAC within the neighbor discovery header and link layer option. This setting is disabled by default.
RA Guard	Select this option to enable router advertisements or ICMPv6 redirects from this Ethernet port. Router advertisements are periodically sent to hosts or sent in response to neighbor solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.This setting is disabled by default.

17 Set the following **802.1X Settings:**

Host Mode	Use the drop-down menu to select the host mode configuration to apply to this port. Options include *single-host* or *multi-host*. The default setting is single-host.
Guest VLAN	Specify a guest VLAN for this port from 1 - 4094. This is the VLAN traffic is bridged on if this port is unauthorized and the guest VLAN is globally enabled.
Port Control	Use the drop-down menu to set the port control state to apply to this port. Options include *force-authorized*, *force-unauthorized* and *automatic*. The default setting is force-authorized.
Re Authenticate	Select this setting to force clients to reauthenticate on this port. The default setting is disabled, thus clients do not need to reauthenticate for connection over this port until this setting is enabled.
Max Reauthenticate Count	Set the maximum reauthentication attempts (1 - 10) before this port is moved to unauthorized. The default setting is 2.
Quiet Period	Set the quiet period for this port from 1 - 65,535 seconds.This is the maximum wait time 802.1x waits upon a failed authentication attempt. The default setting is 60 seconds.
Reauthenticate Period	Use the spinner control to set the reauthentication period for this port from 1 - 65,535 seconds. The default setting is 60 seconds.
Port MAC Authentication	When enabled, a port's MAC address is authenticated, as only one MAC address is supported per wired port. When successfully authenticated, packets from the source are processed. Packets from all other sources are dropped. Port MAC authentication is supported on RFS4000, RFS6000 model controllers and NX4500, NX6500 and NX9000 series service platforms. Port MAC authentication may be enabled on ports in conjunction with Wired 802.1x settings for a MAC Authentication AAA policy.

18 Select **Enable** within the **802.1x supplicant (client)** field to enable a *username* and *password* pair used when authenticating users on this port. This setting is disabled by default. The password cannot exceed 32 characters.

19 Select **OK** to save the changes made to the Ethernet port's security configuration. Select **Reset** to revert to the last saved configuration.

20 Select the **Spanning Tree** tab.

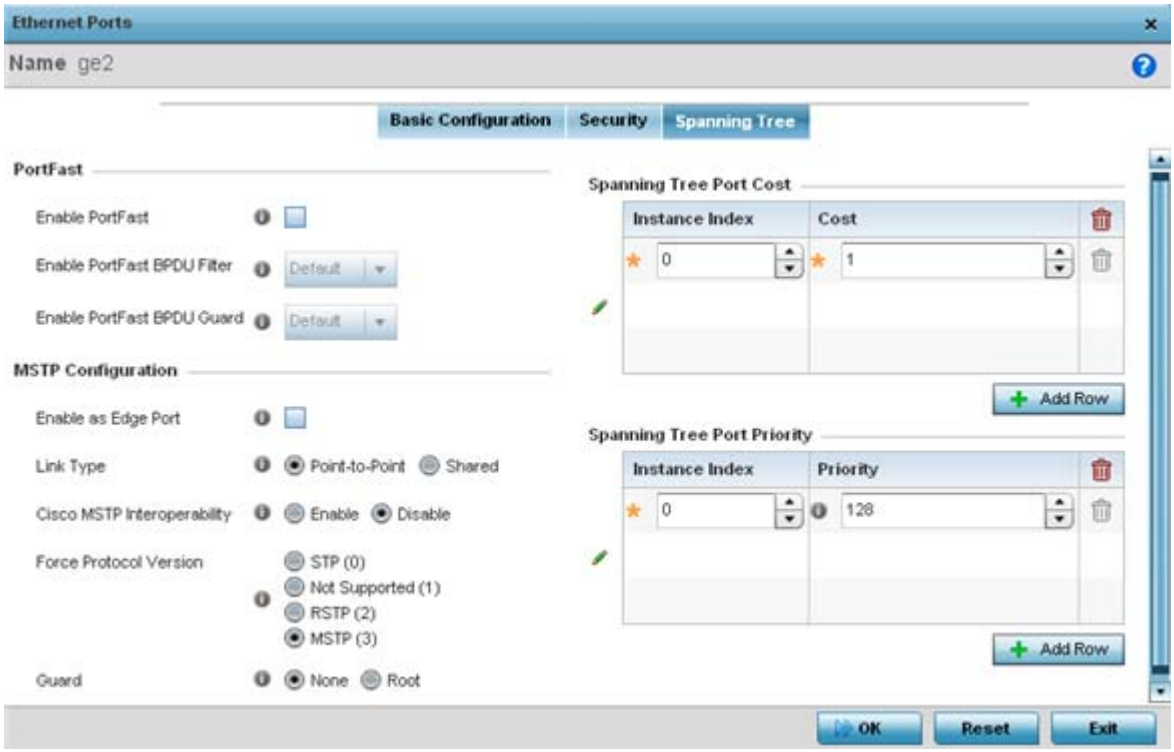


Figure 8-11 *Ethernet Ports - Spanning Tree screen*

21 Define the following **PortFast** parameters for the port's MSTP configuration:

Enable PortFast	Select the check box to enable fast transitions and drop-down menus for both the Enable Portfast BPDU Filter and Enable Portfast BPDU guard options for the port. This setting is disabled by default.
Enable PortFast BPDU Filter	Select enable to invoke a BPDU filter for this portfast enabled port. Enabling the BPDU filter feature ensures this PortFast enabled port does not transmit or receive BPDUs.
Enable PortFast BPDU Guard	Select enable to invoke a BPDU guard for this portfast enabled port. Enabling the BPDU Guard feature means this portfast-enabled port will shutdown on receiving a BPDU. Thus, no BPDUs are processed.

22 Set the following **MSTP Configuration** parameters:

Link Type	Select either the *Point-to-Point* or *Shared* radio button. Selecting Point-to-Point indicates the port should be treated as connected to a point-to-point link. Selecting Shared indicates this port should be treated as having a shared connection. A port connected to a hub is on a shared link, while one the connected to a controller or service platform is a point-to-point link.
Cisco MSTP Interoperability	Select either the *Enable* or *Disable* radio buttons. This enables interoperability with Cisco's version of MSTP over the port, which is incompatible with standard MSTP.
Force Protocol Version	Sets the protocol version to either *STP(0)*, *Not Supported(1)*, *RSTP(2)* or *MSTP(3)*. MSTP is the default setting.

Guard	Determines whether the port enforces root bridge placement. Setting the guard to *Root* ensures the port is a designated port. Typically, each guard root port is a designated port, unless two or more ports (within the root bridge) are connected together. If the bridge receives superior (BPDUs) on a guard root-enabled port, the guard root moves the port to a root-inconsistent STP state. This state is equivalent to a listening state. No data is forwarded across the port. Thus, the guard root enforces the root bridge position.

23 Refer to the **Spanning Tree Port Cost** table.

Define an **Instance Index** using the spinner control, then set the **Cost**. The default path cost depends on the speed of the port. The cost helps determine the role of the port in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, the higher the cost.

Speed	Default Path Cost
<=100000 bits/sec	200000000
<=1000000 bits/sec	20000000
<=10000000 bits/sec	2000000
<=100000000 bits/sec	200000
<=1000000000 bits/sec	20000
<=10000000000 bits/sec	2000
<=100000000000 bits/sec	200
<=1000000000000 bits/sec	20
>1000000000000 bits/sec	2

24 Select **+ Add Row** as needed to include additional indexes.

25 Refer to the **Spanning Tree Port Priority** table.

Define an **Instance Index** using the spinner control and then set the **Priority**. The lower the priority, a greater likelihood of the port becoming a designated port. Thus applying an higher override value impacts the port's likelihood of becoming a designated port.

Select **+ Add Row** needed to include additional indexes.

26 Select **OK** to save the changes made to the Ethernet Port's spanning tree configuration. Select **Reset** to revert to the last saved configuration.

8.7.2 Virtual Interface Configuration

Profile Interface Configuration

A Virtual Interface is required for layer 3 (IP) access or to provide layer 3 service on a VLAN. The Virtual Interface defines which IP address is associated with each connected VLAN ID. A Virtual Interface is created for the default VLAN (VLAN 1) to enable remote administration. A Virtual Interface is also used to map VLANs to IP address ranges. This mapping determines the destination networks for routing.

To review existing Virtual Interface configurations and either create a new Virtual Interface configuration, modify an existing configuration or delete an existing configuration:

1 Select **Configuration** > **Profiles** > **Interface**.

2 Expand the Interface menu to display its submenu options.

3 Select **Virtual Interfaces**.

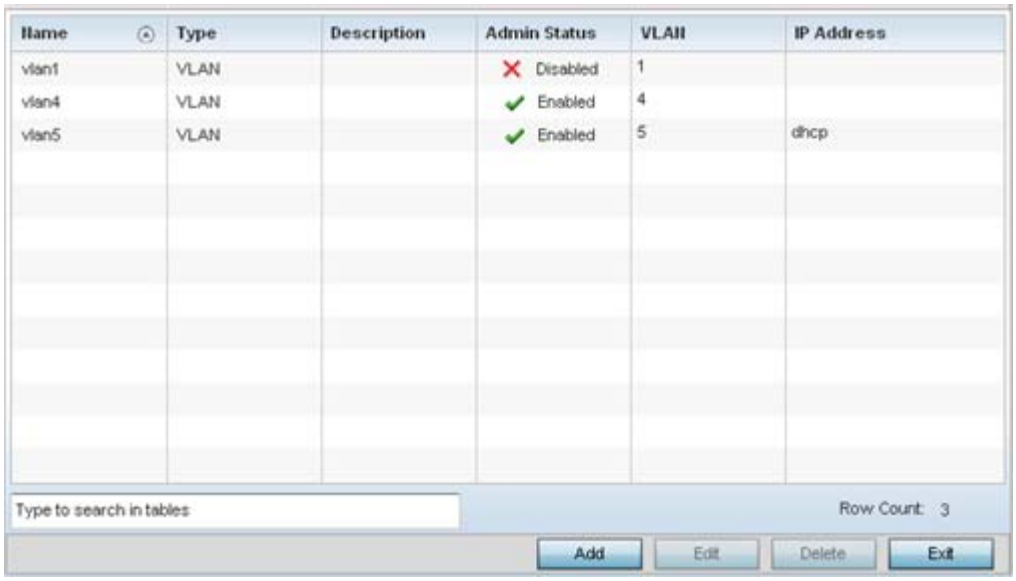


Figure 8-12 *Virtual Interfaces screen*

4 Review the following parameters unique to each virtual interface configuration:

Name	Displays the name of each listed Virtual Interface assigned when it was created. The name is between 1 - 4094, and cannot be modified as part of a Virtual Interface edit.
Type	Displays the type of Virtual Interface for each listed interface.
Description	Displays the description defined for the Virtual Interface when it was either initially created or edited.
Admin Status	A green checkmark defines the listed Virtual Interface configuration as active and enabled with its supported profile. A red “X” defines the Virtual Interface as currently disabled. The interface status can be modified when a new Virtual Interface is created or an existing one modified.
VLAN	Displays the numerical VLAN ID associated with each listed interface.
IP Address	Defines whether DHCP was used to obtain the primary IP address used by the Virtual Interface configuration.

5 Select **Add** to define a new Virtual Interface configuration, **Edit** to modify the configuration of an existing Virtual Interface or **Delete** to permanently remove a selected Virtual Interface.

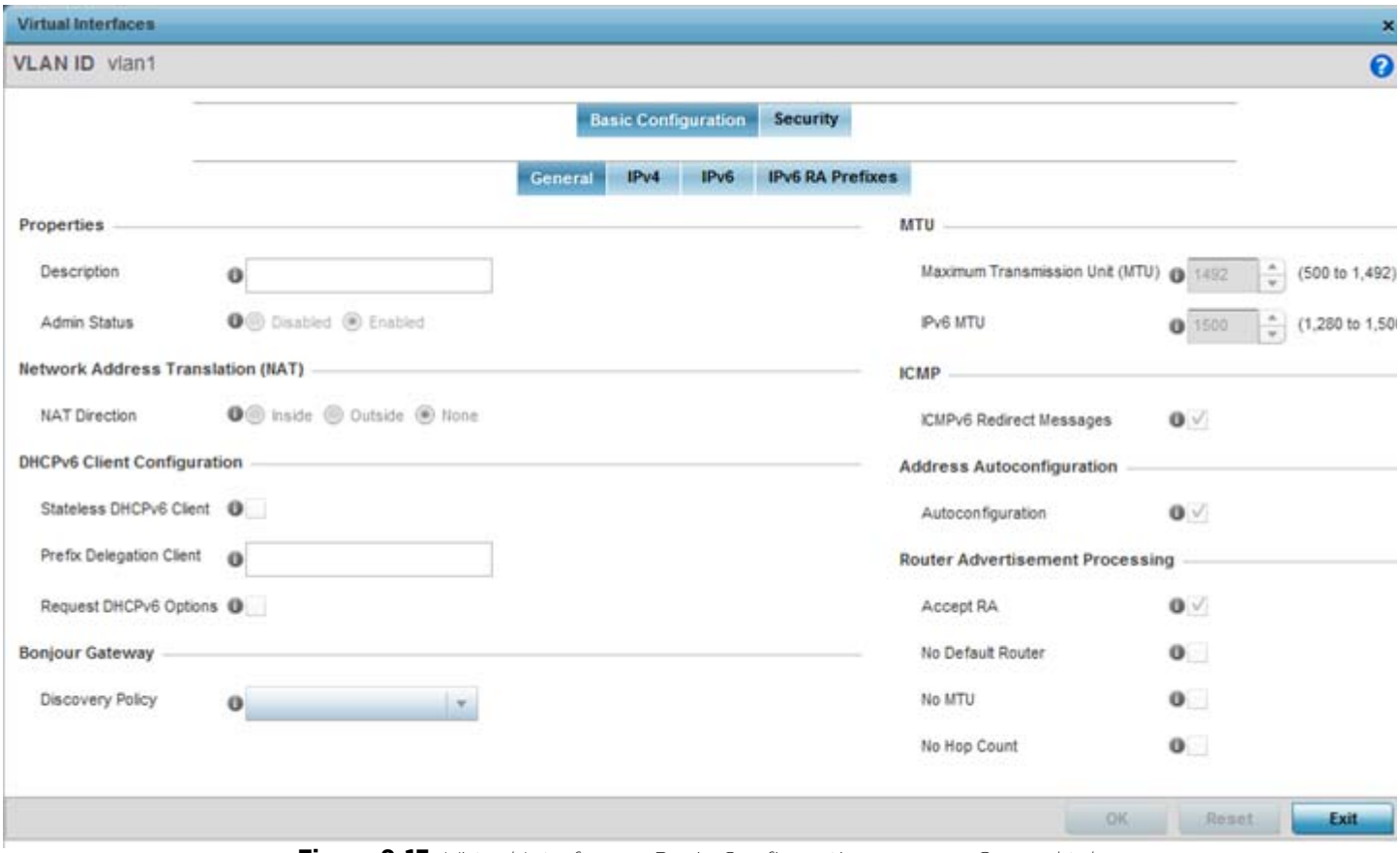


Figure 8-13 *Virtual Interfaces - Basic Configuration screen - General tab*

The **Basic Configuration** screen's **General** tab displays by default, regardless of a whether a new Virtual Interface is created or an existing one is being modified.

6 If creating a new Virtual Interface, use the **VLAN ID** spinner control to define a numeric ID from 1 - 4094. Select the **Continue** button to initialize the rest of the parameters on the screen.

7 Define the following parameters from within the **Properties** field:

Description	Provide or edit a description (up to 64 characters) for the Virtual Interface that helps differentiate it from others with similar configurations.
Admin Status	Either select either the *Disabled* or *Enabled* radio button to define this interface's current status. When set to Enabled, the Virtual Interface is operational and available. The default value is enabled.

8 Define the following NAT parameters from within the **Network Address Translation (NAT)** field:

NAT Direction	Define the *Network Address Translation* (NAT) direction. Options include: *Inside* - The inside network is transmitting data over the network its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address. *Outside* - Packets passing through the NAT on the way back to the controller or service platform managed LAN are searched against to the records kept by the NAT engine. There, the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the network. *None* - No NAT activity takes place. This is the default setting.

9 Set the following **DHCPv6 Client Configuration**. The *Dynamic Host Configuration Protocol* for IPv6 (DHCPv6) provides a framework for passing configuration information.

Stateless DHCPv6 Client	Select this option to request information from the DHCPv6 server using stateless DHCPv6. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is disabled by default.
Prefix Delegation Client	Specify a 32 character maximum request prefix for prefix delegation from a DHCPv6 server over this virtual interface. Devices use prefixes to distinguish destinations that reside on-link from those reachable using a router.
Request DHCPv6 Options	Select this option to request DHCPv6 options on this virtual interface. DHCPv6 options provide configuration information for a node that must be booted using the network rather than locally. This setting is disabled by default.

10 Set the **Bonjour Gateway** settings for the virtual interface.

Bonjour is Apple's implementation of zero-configuration networking (Zeroconf). Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates devices such as printers, other computers and services that these computers offer over a local network.

Bonjour provides a general method to discover services on a *local area network* (LAN). It allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with special DNS configuration, it can be extended to find services across broadcast domains.

From the drop-down, select the Bonjour Gateway discover policy. Select the **Create** icon to define a new Bonjour Gateway policy configuration or select the **Edit** icon to modify an existing Bonjour Gateway policy configuration.

11 Set the following **MTU** settings for the virtual interface:

Maximum Transmission Unit (MTU)	Set the PPPoE client *maximum transmission unit* (MTU) from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492.

IPv6 MTU	Set an IPv6 MTU for this virtual interface from 1,280 - 1,500. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. The default is 1,500.

12 Within the **ICMP** field, define whether ICMPv6 redirect messages are sent. A redirect requests data packets be sent on an alternative route. This setting is enabled by default.

13 Within the **Address Autoconfiguration** field, define whether to configure IPv6 addresses on this virtual interface based on the prefixes received in router advertisement messages. Router advertisements contain prefixes used for link determination, address configuration and maximum hop limits. This setting is enabled by default.

14 Set the following **Router Advertisement Processing** settings for the virtual interface. Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

Accept RA	Enable this option to allow router advertisements over this virtual interface. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet layer configuration parameters.This setting is enabled by default.
No Default Router	Select this option to consider routers unavailable on this interface for default router selection. This setting is disabled by default.
No MTU	Select this option to not use the existing MTU setting for router advertisements on this virtual interface. If the value is set to zero no MTU options are sent. This setting is disabled by default.
No Hop Count	Select this option to not use the hop count advertisement setting for router advertisements on this virtual interface. This setting is disabled by default.

15 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

16 Select the **IPv4** tab to set IPv4 settings for this virtual interface.

IPv4 is a connectionless protocol operating on a best effort delivery model. IPv4 does not guarantee delivery or assures proper sequencing or avoidance of duplicate delivery (unlike TCP).

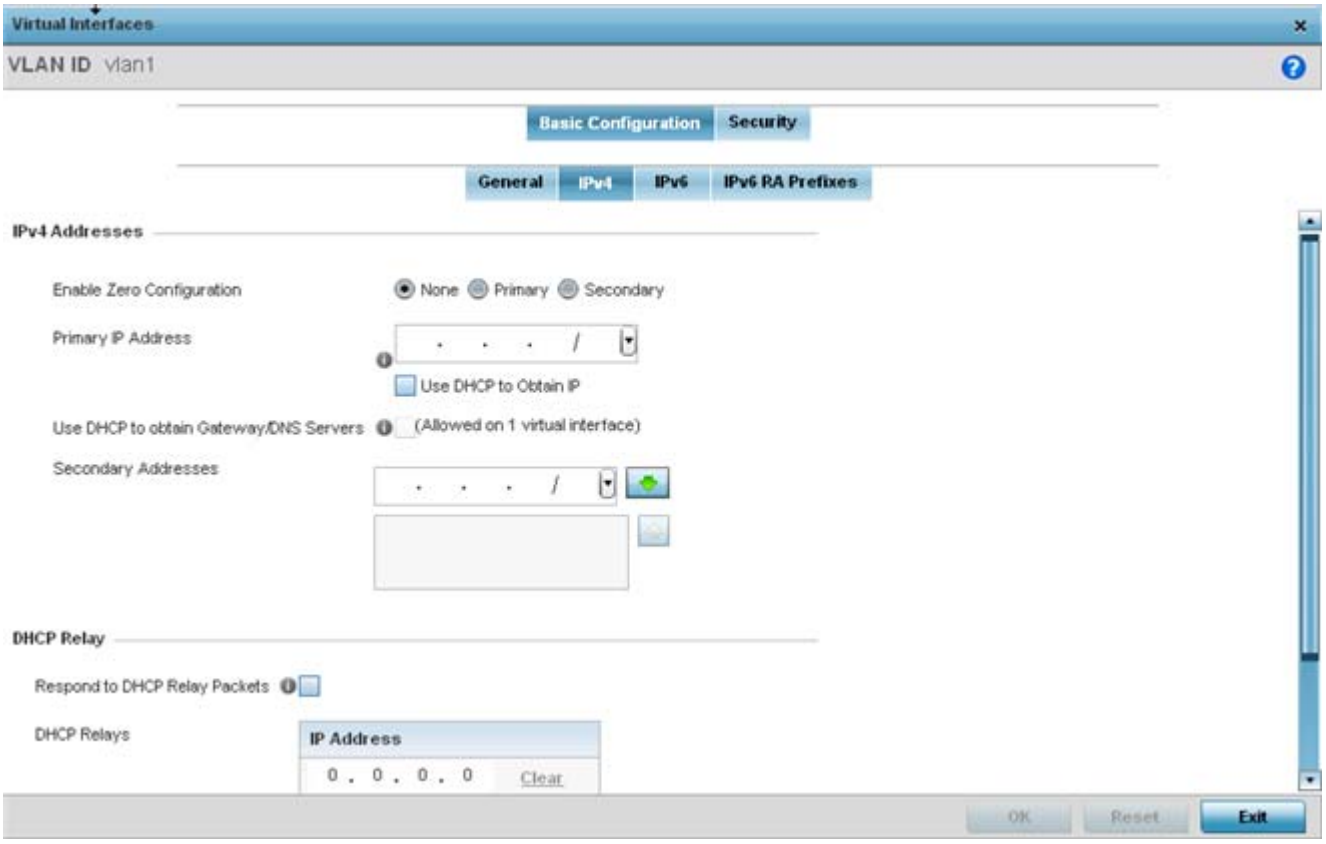


Figure 8-14 *Virtual Interfaces - Basic Configuration screen - IPv4 tab*

17 Set the following network information from within the **IPv4 Addresses** field:

Enable Zero Configuration	Zero configuration can be a means of providing a primary or secondary IP addresses for the virtual interface. Zero configuration (or zero config) is a wireless connection utility included with Microsoft Windows XP and later as a service dynamically selecting a network to connect based on a user's preferences and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device. This value is set to None by default.
Primary IP Address	Define the IP address for the VLAN associated Virtual Interface.
Use DHCP to Obtain IP	Select this option to allow DHCP to provide the IP address for the Virtual Interface. Selecting this option disables the Primary IP address field.
Use DHCP to obtain Gateway/DNS Servers	Select this option to allow DHCP to obtain a default gateway address and DNS resource for *one* virtual interface. This setting is disabled by default and only available when the *Use DHCP to Obtain IP* option is selected.
Secondary Addresses	Use the *Secondary Addresses* parameter to define additional IP addresses to associate with VLAN IDs. The address provided in this field is used if the primary IP address is unreachable.

18 Refer to the **DHCP Relay** field to set the DHCP relay server configuration used with the Virtual Interface.

Respond to DHCP Relay Packets	Select this option to allow the onboard DHCP server to respond to relayed DHCP packets on this interface. This setting is disabled by default.

DHCP Relays	Provide IP addresses for DHCP server relay resources. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When A DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.

19 Select **OK** to save the changes to the IPv4 configuration. Select **Reset** to revert to the last saved configuration.

20 Select the **IPv6** tab to set IPv6 settings for this virtual interface.

IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet layer configuration parameters.

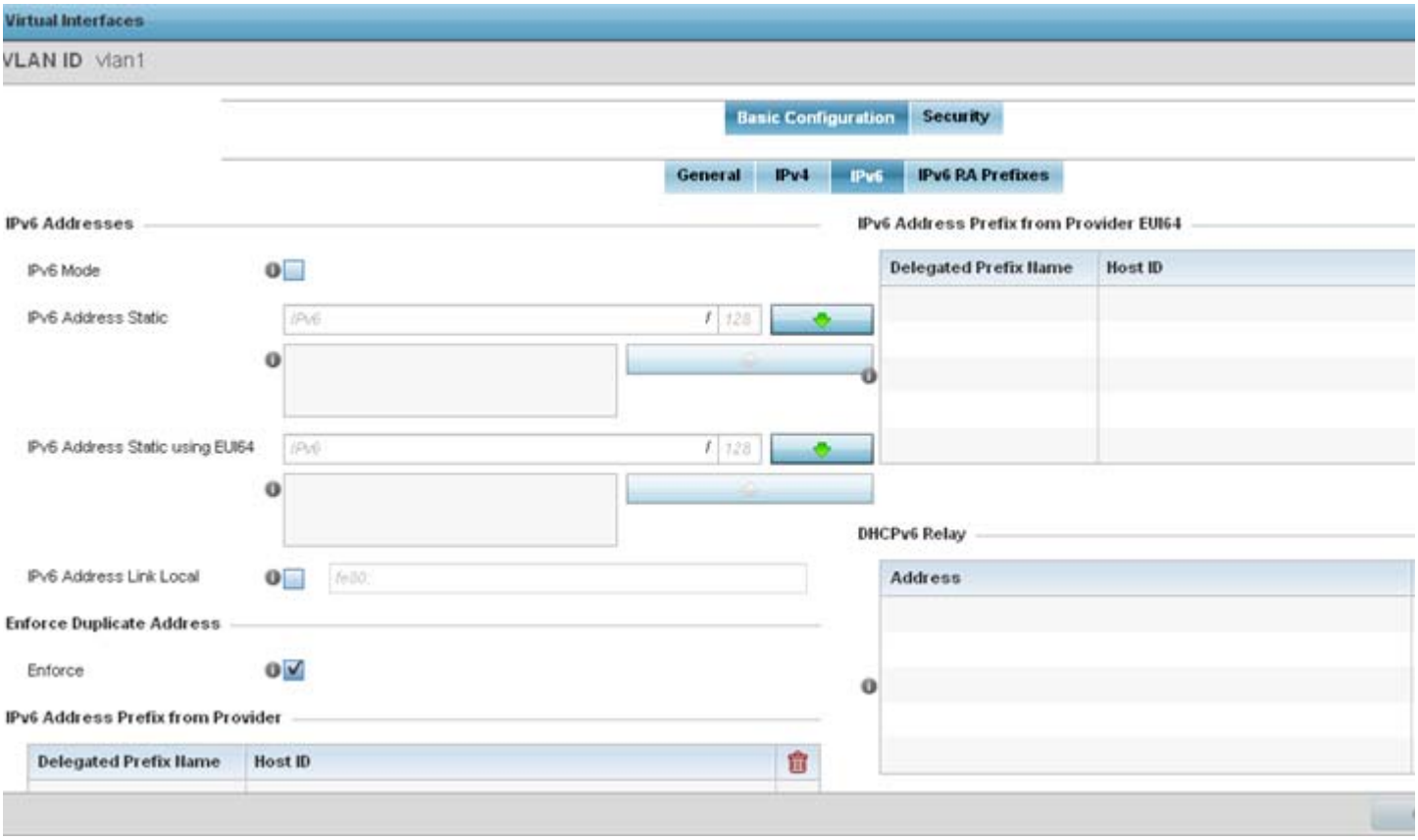


Figure 8-15 *Virtual Interfaces - Basic Configuration screen - IPv6 tab*

21 Enable the **Enforce Duplicate Address** option to enforce duplicate address protection when any wired port is connected and in a forwarding state. This option is enabled by default.

22 Refer to the **IPv6 Address Prefix from Provider** table to create IPv6 format prefix shortcuts as supplied by an ISP.

Select **+ Add Row** to launch a sub screen wherein a new delegated prefix name and host ID can be defined.

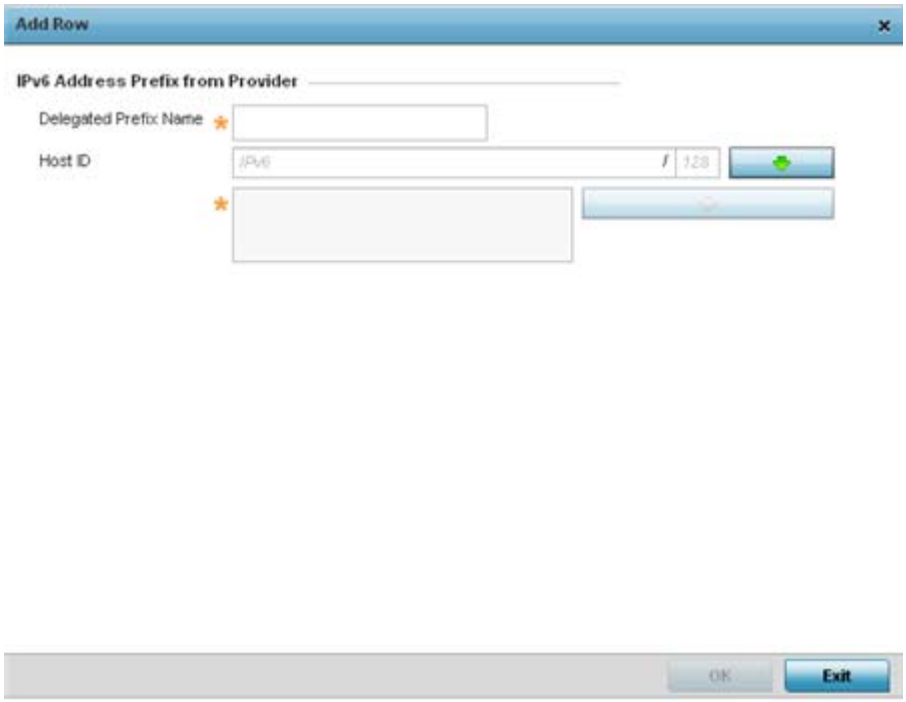


Figure 8-16 *Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider*

Delegated Prefix Name	Enter a 32 character maximum name for the IPv6 address prefix from provider.
Host ID	Define the subnet ID, host ID and prefix length.

Select **OK** to save the changes to the new IPv6 prefix from provider. Select **Exit** to close the screen without saving the updates.

23 Refer to the **IPv6 Address Prefix from Provider EUI64** table to set an (abbreviated) IP address prefix in EUI64 format.

Select **+ Add Row** to launch a sub screen wherein a new delegated prefix name and host ID can be defined in EUI64 format.

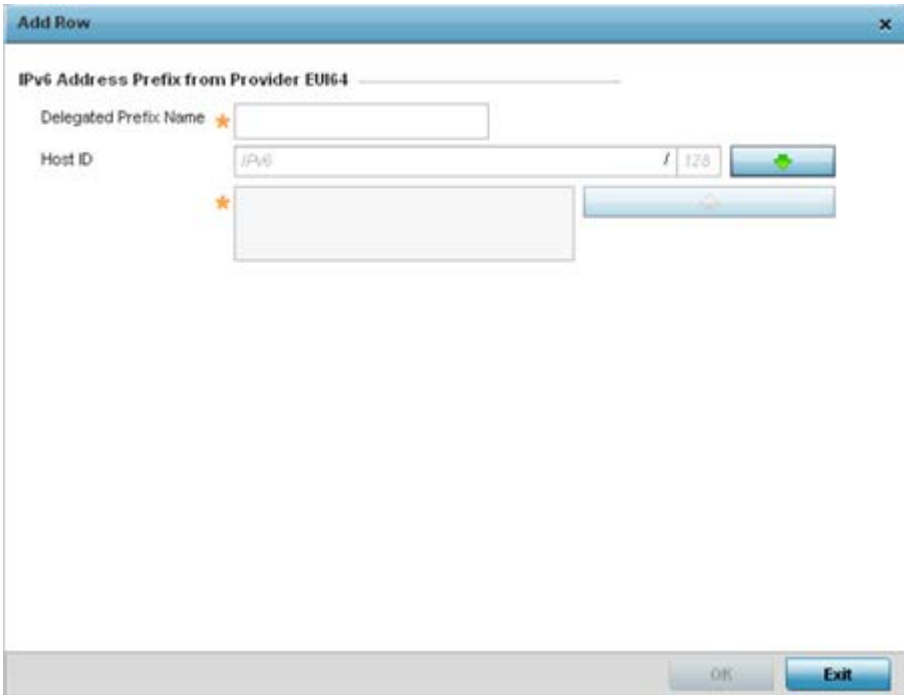


Figure 8-17 *Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider EUI64*

Delegated Prefix Name	Enter a 32 character maximum name for the IPv6 prefix from provider in EUI format. Using EUI64, a host can automatically assign itself a unique 64-bit IPv6 interface identifier without manual configuration or DHCP.
Host ID	Define the subnet ID and prefix length.

24 Select **OK** to save the changes to the new IPv6 prefix from provider in EUI64 format. Select **Exit** to close the screen without saving the updates.

25 Refer to the **DHCPv6 Relay** table to set the address and interface of the DHCPv6 relay.

The DHCPv6 relay enhances an extended DHCP relay agent by providing support in IPv6. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When A DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.

26 Select **+ Add Row** to launch a sub screen wherein a new DHCPv6 relay address and interface VLAN ID can be set.

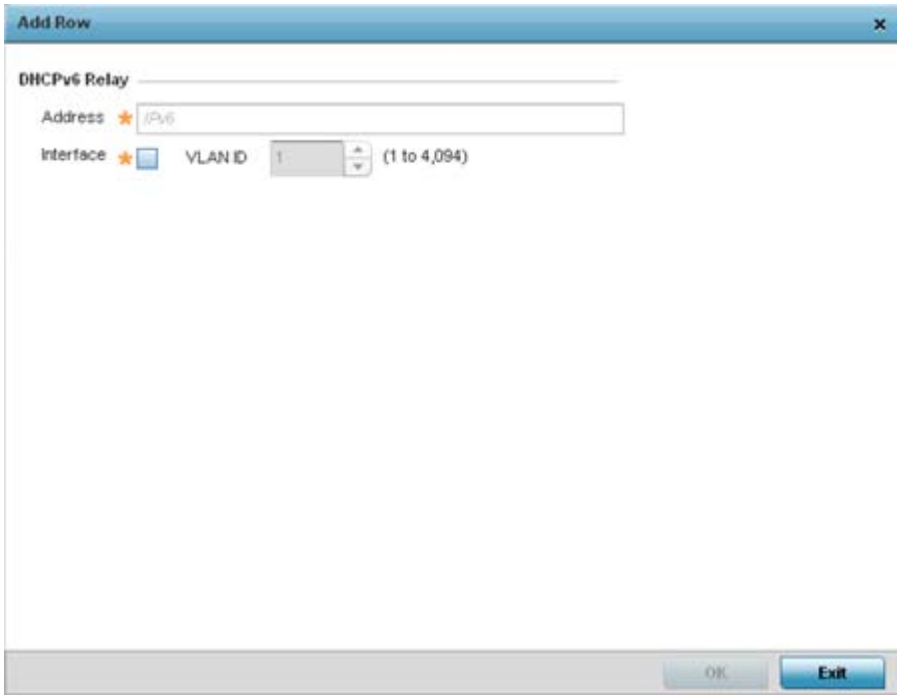


Figure 8-18 *Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add DHCPv6 Relay*

Address	Enter an address for the DHCPv6 relay. These DHCPv6 relay receive messages from DHCPv6 clients and forward them to DHCPv6 servers. The DHCPv6 server sends responses back to the relay, and the relay then sends these responses to the client on the local network link.
Interface	Select this option to enable a spinner control to define a VLAN ID from 1 - 4,094 used as the virtual interface for the DHCPv6 relay. The interface designation is only required for link local and multicast addresses. A local link address is a locally derived address designed for addressing on a single link for automatic address configuration, neighbor discovery or when no routing resources are available.

27 Select **OK** to save the changes to the DHCPv6 relay configuration. Select **Exit** to close the screen without saving the updates.

28 Select the **IPv6 RA Prefixes** tab.

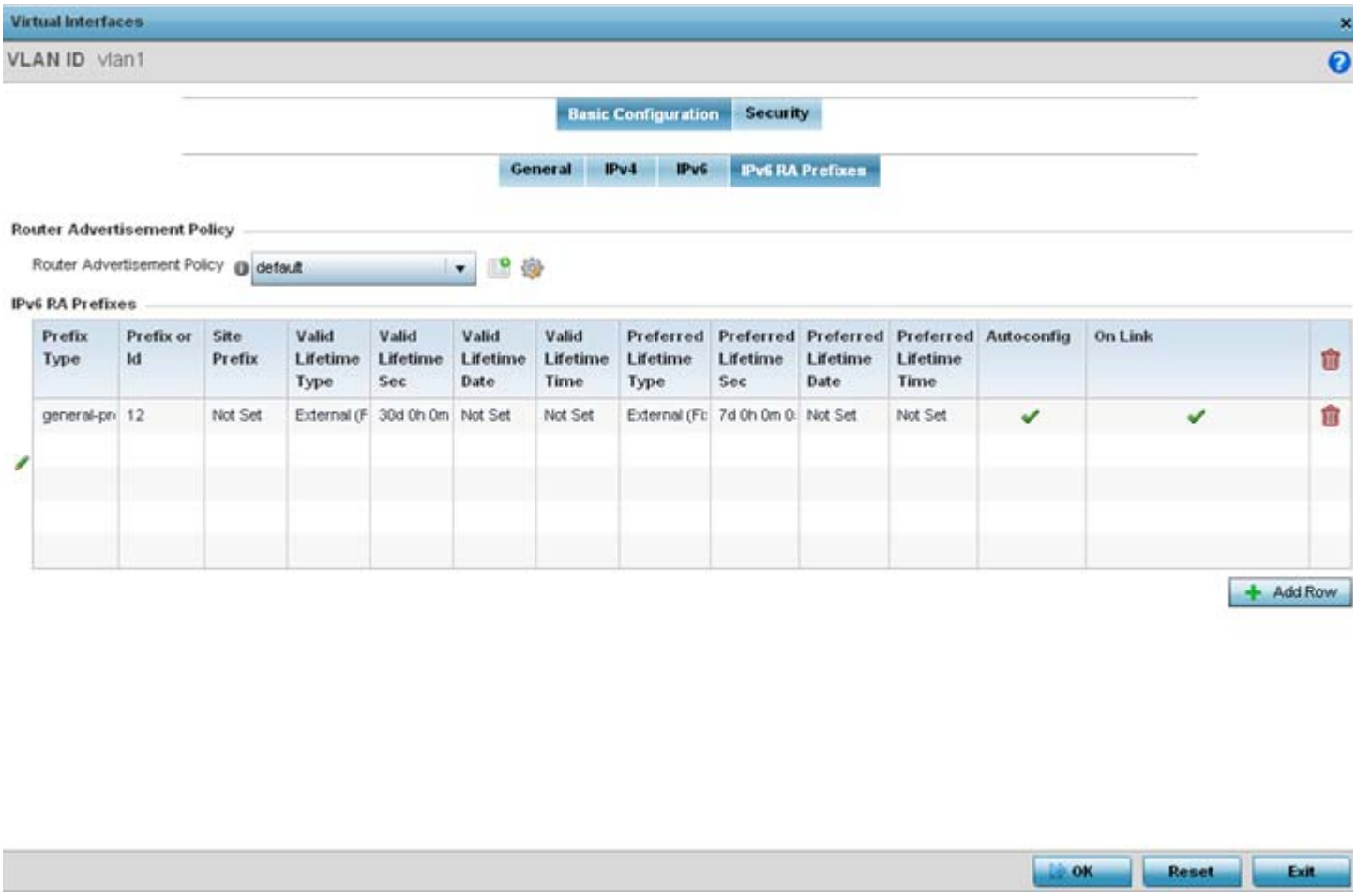


Figure 8-19 *Virtual Interfaces - Basic Configuration screen - IPv6 RA Prefixes tab*

29 Use the **Router Advertisement Policy** drop-down menu to select and apply a policy to the virtual interface.

Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

30 Review the configurations of existing IPv6 advertisement policies. If needed select **+ Add Row** to define the configurations of up to 16 additional IPv6 RA prefix configurations.

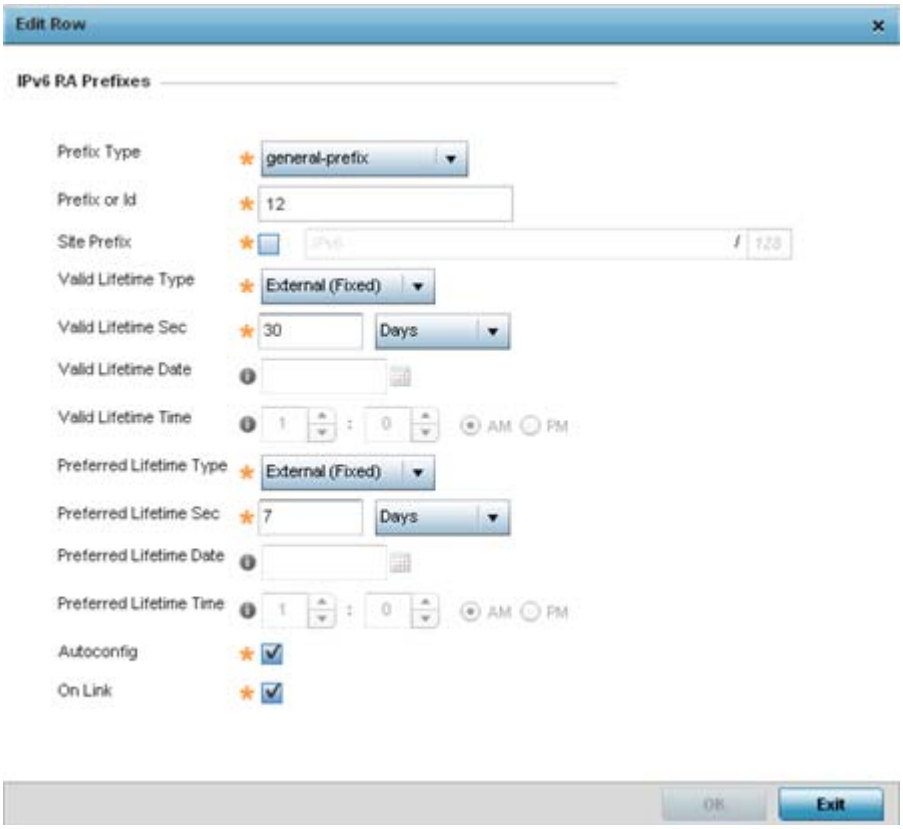


Figure 8-20 *Virtual Interfaces - Basic Configuration screen - Add IPv6 RA Prefix*

31 Set the following **IPv6 RA Prefix** settings:

Prefix Type	Set the prefix delegation type used with this configuration. Options include *general-prefix* (default), *Prefix,* and *prefix-from-provider.* The default setting is Prefix. A provider assigned prefix is made available from an *Internet Service Provider* (ISP) to automate the process of providing and informing the prefixes used.
Prefix or ID	Set the actual prefix or ID used with the IPv6 router advertisement.
Site Prefix	The site prefix is added into a router advertisement prefix. The site address prefix signifies the address is only on the local link.
Valid Lifetime Type	Set the lifetime for the prefix's validity. Options include *External (fixed), decrementing* and *infinite*. If set to External (fixed), just the *Valid Lifetime Sec* setting is enabled to define the exact time interval for prefix validity. If set to decrementing, use the lifetime date and time settings to refine the prefix expiry period. If the value is set for infinite, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is External (fixed).
Valid Lifetime Sec	If the lifetime type is set to *External (fixed),* set the *Seconds, Minutes, Hours* or *Days* value used to measurement criteria for the prefix's expiration. 30 days, 0 hours, 0 minutes and 0 seconds is the default lifetime.
Valid Lifetime Date	If the lifetime type is set to *External (fixed)*, set the date in MM/DD/YYYY format for the expiration of the prefix.

Valid Lifetime Time	If the lifetime type is set to *decrementing*, set the time for the prefix's validity.
Preferred Lifetime Type	Set the administrator preferred lifetime for the prefix's validity. Options include *External (fixed), decrementing* and *infinite*. If set to External (fixed), just the *Valid Lifetime Sec* setting is enabled to define the exact time interval for prefix validity. If set to decrementing, use the lifetime date and time settings to refine the prefix expiry period. If the value is set for infinite, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is External (fixed).
Preferred Lifetime Sec	If the administrator preferred lifetime type is set to *External (fixed)*, set the *Seconds, Minutes, Hours* or *Days* value used to measurement criteria for the prefix's expiration. 30 days, 0 hours, 0 minutes and 0 seconds is the default lifetime.
Preferred Lifetime Date	If the administrator preferred lifetime type is set to *External (fixed),* set the date in MM/DD/YYYY format for the expiration of the prefix.
Preferred Lifetime Time	If the preferred lifetime type is set to *decrementing,* set the time for the prefix's validity.
Autoconfig	Autoconfiguration includes generating a link-local address, global addresses via stateless address autoconfiguration and duplicate address detection to verify the uniqueness of the addresses on a link. This setting is enabled by default.
On Link	Select this option to keep the IPv6 RA prefix on the local link. The default setting is enabled.

32 Select **OK** to save the changes to the IPv6 RA prefix configuration. Select **Exit** to close the screen without saving the updates.

33 Select the **Security** tab.

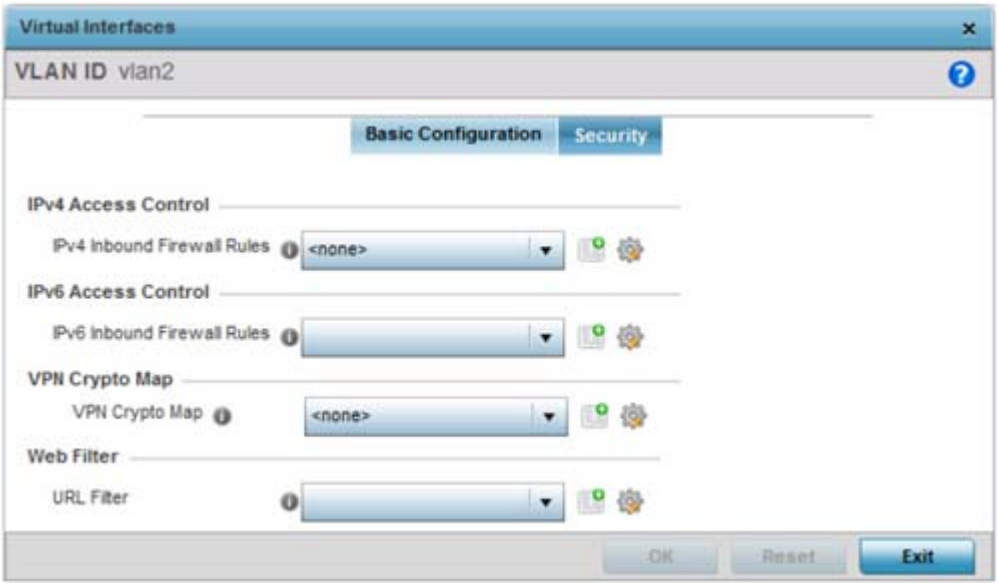


Figure 8-21 *Virtual Interfaces - Security screen*

34 Use the **IPv4 Inbound Firewall Rules** drop down menu to select the IPv4 specific inbound firewall rules to apply to this profile's virtual interface configuration. Select the **Create** icon to define a new IPv4 firewall rule configuration or select the **Edit** icon to modify an existing configuration.

IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, since it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP).

IPv4 and IPv6 are different enough to warrant separate protocols. IPv6 devices can alternatively use stateless address autoconfiguration. IPv4 hosts can use link local addressing to provide local connectivity.

35 Use the **IPv6 Inbound Firewall Rules** drop down menu to select the IPv6 specific inbound firewall rules to apply to this profile's virtual interface configuration. Select the **Create** icon to define a new IPv6 firewall rule configuration or select the **Edit** icon to modify an existing configuration.

IPv6 is the latest revision of the *Internet Protocol* (IP) replacing IPv4. IPV6 provides enhanced identification and location information for systems routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

36 Use the **VPN Crypto Map** drop down menu to select a crypto map to apply to this profile's virtual interface configuration. Crypto maps are sets of configuration parameters for encrypting packets passing through a VPN Tunnel. If a crypto map does not exist suiting the needs of this virtual interface, select the **Create** icon to define a new crypto map configuration or the **Edit** icon to modify an existing crypto map. For more information, see *Overriding a Profile's VPN Configuration on page 5-207*.

37 Use the **Web Filter** drop-down menu to select or override the **URL Filter** configuration applied to this virtual interface.

Web filtering is used to restrict access to specific (administrator defined) resources on the Internet.

38 Select the **Dynamic Routing** tab (if available on your controller or service platform).

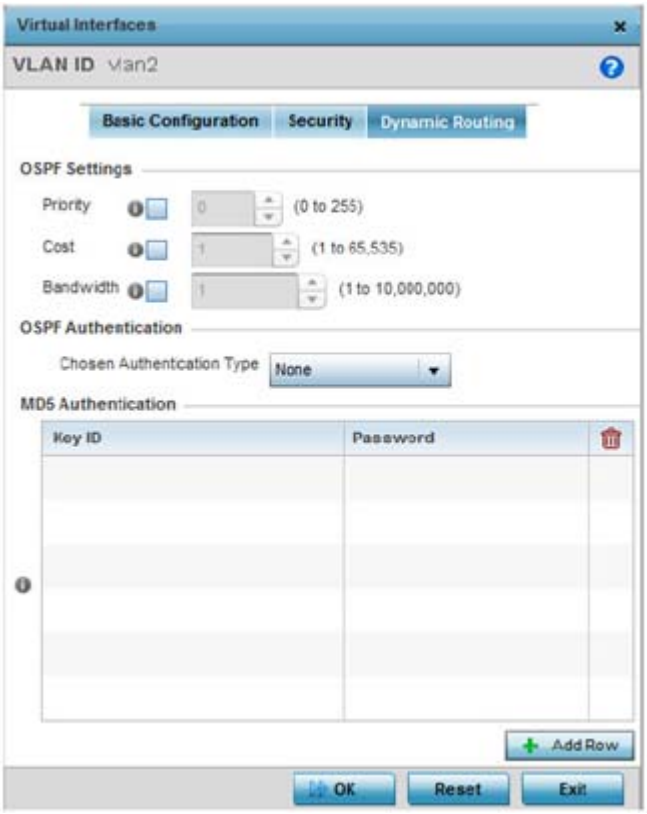


Figure 8-22 *Virtual Interfaces - Dynamic Routing screen*

Open Shortest Path First (OSPF) is a link-state *interior gateway protocol* (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from

neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

39 Define the following **OSPF Settings**:

Priority	Select this option to set the OSPF priority used to select the network designated route. Use the spinner control to set the value from 0 - 255.
Cost	Select this option to set the cost of the OSPF interface. Use the spinner control to set the value from 1 - 65,535.
Bandwidth	Set the OSPF interface bandwidth (in Kbps) from 1 - 10,000,000.

40 Select the authentication type from the **Chosen Authentication Type** drop-down used to validate credentials within the OSPF dynamic route. Options include *simple-password, message-digest, null* and *None*. The default value is None.

41 Select **+ Add Row** at the bottom of the MD5 Authentication table to add the Key ID and Password used for an MD5 validation of authenticator credentials. Use the spinner control to set the OSPF message digest authentication key ID. The available range is from 1 - 255. The password is the OSPF key either displayed as series or asterisks or in plain text (by selecting **Show**).

42 Select **OK** to save the changes to the virtual interface security configuration. Select **Exit** to close the screen without saving the updates.

8.7.3 Port Channel Configuration

Profile Interface Configuration

Profiles can be applied customized port channel configurations as part of their Interface configuration.

To define a port channel configuration for a profile:

1 Select **Configuration** > **Profiles** > **Interface**.

2 Expand the Interface menu to display its submenu options.

3 Select **Port Channels.**

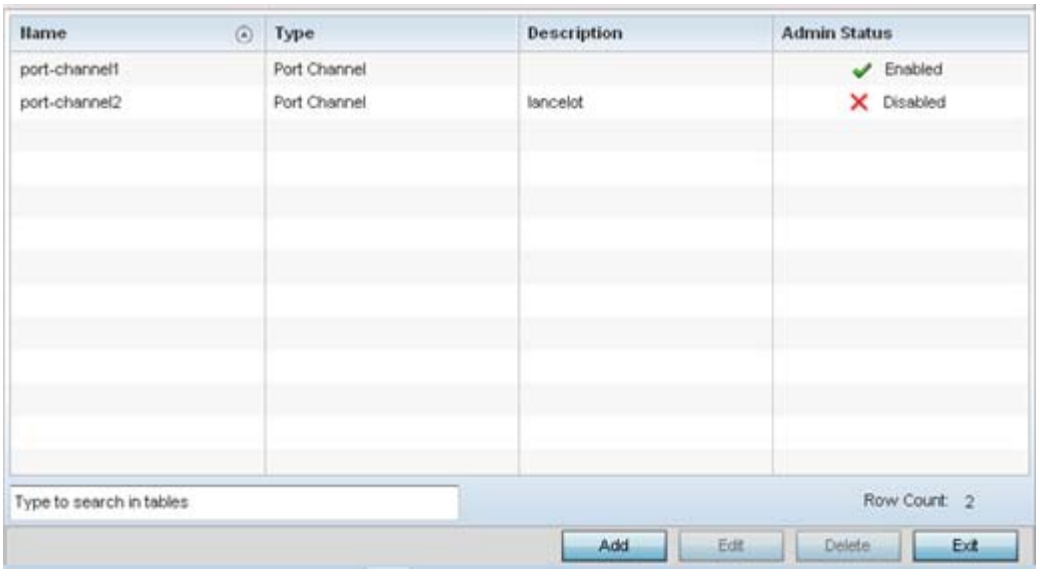


Figure 8-23 *Port Channels screen*

4 Refer to the following to review existing port channel configurations and their current status:

Name	Displays the port channel's numerical identifier assigned to it when it was created. The numerical name cannot be modified as part of the edit process.
Type	Displays whether the type is a port channel.
Description	Lists a a short description (64 characters maximum) describing the port channel or differentiating it from others with similar configurations.
Admin Status	A green checkmark defines the listed port channel as active and currently enabled with the profile. A red "X" defines the port channel as currently disabled and not available for use. The interface status can be modified with the port channel configuration as required.

5 Select **Add** to add a new configuration. To edit the configuration of an existing port channel, select it from amongst those displayed and select the **Edit** button. The port channel **Basic Configuration** screen displays by default. Configurations can be optionally removed by selecting **Delete**.

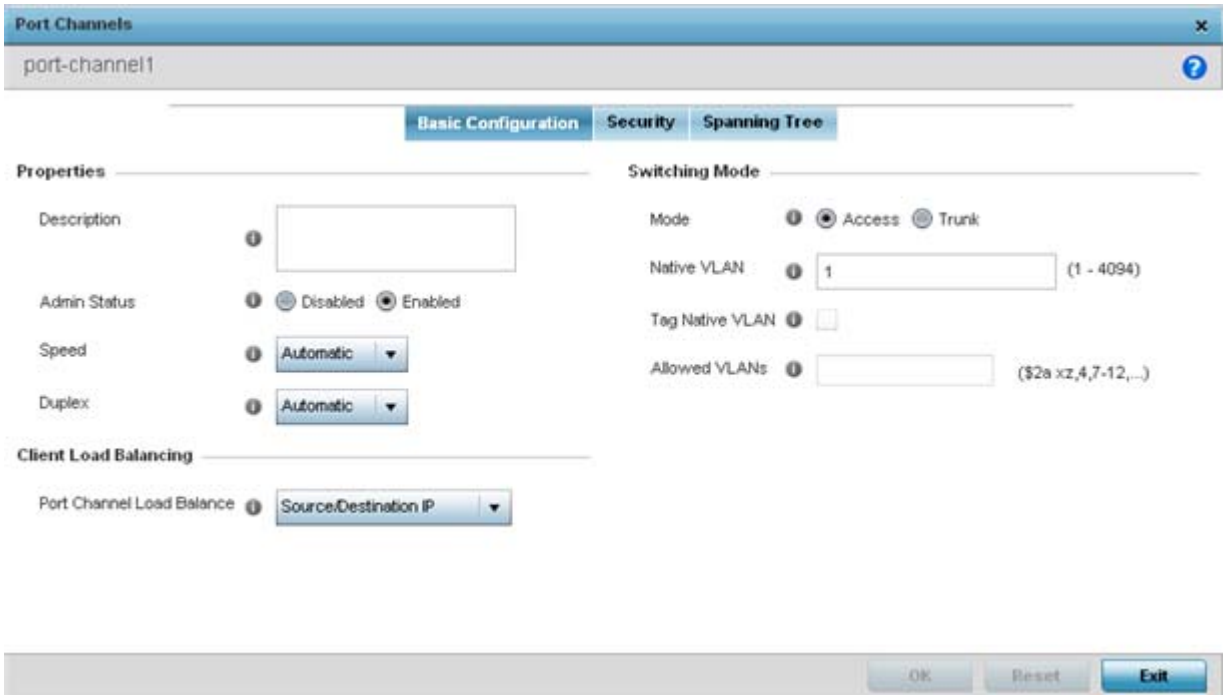


Figure 8-24 *Port Channels - Basic Configuration screen*

6 Set the following port channel **Properties**:

Description	Enter a brief description for the controller or service platform port channel (64 characters maximum). The description should reflect the port channel's intended function.
Admin Status	Select the *Enabled* radio button to define this port channel as active to the profile it supports. Select the *Disabled* radio button to disable this port channel configuration within the profile. It can be activated at any future time when needed. The default setting is enabled.
Speed	Select the speed at which the port channel can receive and transmit the data. Select either *10 Mbps*, *100 Mbps*, *1000 Mbps*. Select either of these options to establish a 10, 100 or 1000 Mbps data transfer rate for the selected half duplex or full duplex transmission over the port. These options are not available if Automatic is selected. Select *Automatic* to enable the port channel to automatically exchange information about data transmission speed and duplex capabilities. Auto negotiation is helpful when in an environment where different devices are connected and disconnected on a regular basis. Automatic is the default setting.
Duplex	Select either *Half*, *Full* or *Automatic* as the duplex option. Select Half duplex to send data over the port channel, then immediately receive data from the same direction in which the data was transmitted. Like a Full duplex transmission, a Half duplex transmission can carry data in both directions, just not at the same time. Select Full duplex to transmit data to and from the port channel at the same time. Using Full duplex, the port channel can send data while receiving data as well. Select Automatic to dynamically duplex as port channel performance needs dictate. Automatic is the default setting.

7 Use the **Port Channel Load Balance** drop-down menu to define whether port channel load balancing is conducted using a *Source/Destination IP* or a *Source/Destination MAC*. Source/Destination IP is the default setting.

8 Define the following **Switching Mode** parameters to apply to the port channel configuration:

Mode	Select either the *Access* or *Trunk* radio button to set the VLAN switching mode over the port channel. If Access is selected, the port channel accepts packets only form the native VLANs. Frames are forwarded out the port untagged with no 802.1Q header. All frames received on the port are expected as untagged and are mapped to the native VLAN. If the mode is set to Trunk, the port channel allows packets from a list of VLANs you add to the trunk. A port channel configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. Access is the default setting.
Native VLAN	Use the spinner control to define a numerical ID between 1 - 4094. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN which untagged traffic will be directed over when using trunk mode. The default value is 1.
Tag the Native VLAN	Select the checkbox to tag the native VLAN. Devices support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This setting is disabled by default.
Allowed VLANs	Selecting *Trunk* as the mode enables the Allowed VLANs parameter. Add VLANs that exclusively send packets over the port channel.

9 Select **OK** to save the changes made to the port channel Basic Configuration. Select **Reset** to revert to the last saved configuration.

10 Select the **Security** tab.

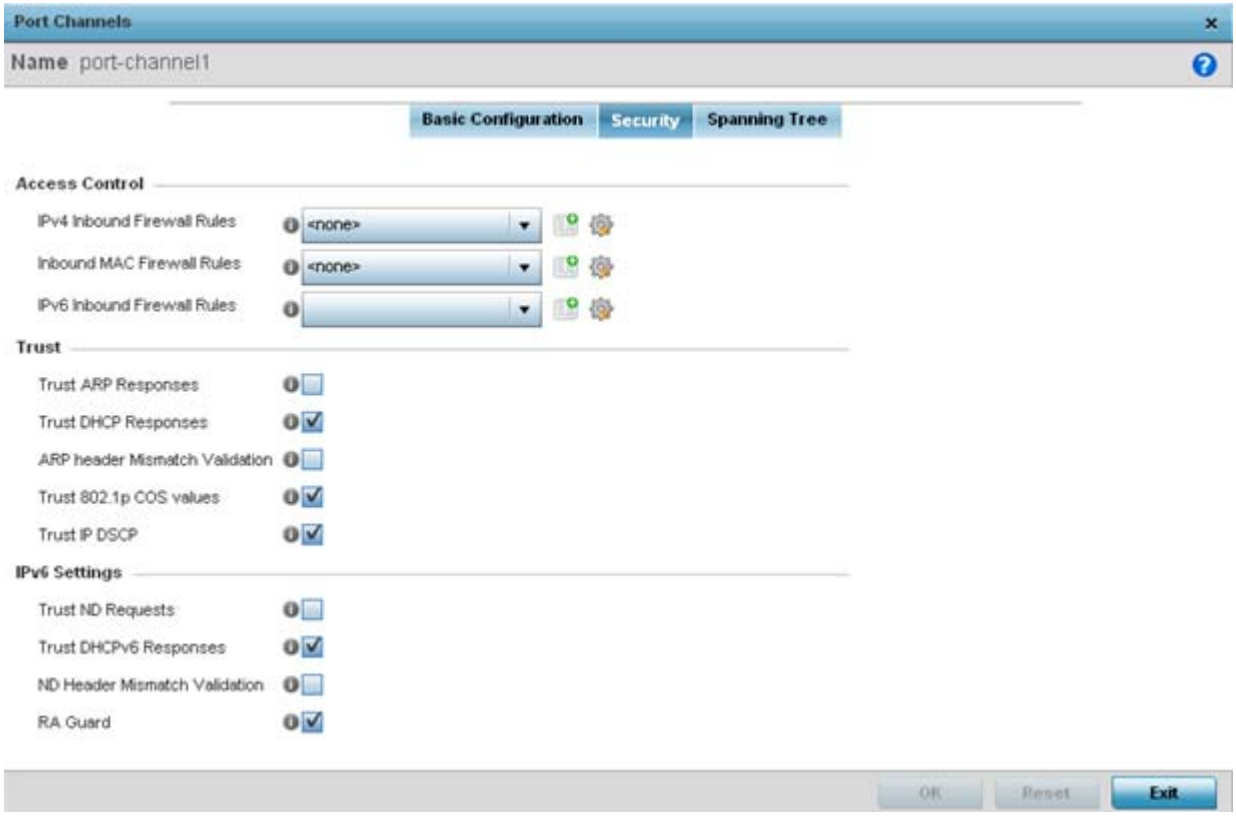


Figure 8-25 *Port Channels - Security screen*

11 Refer to the **Access Control** section. As part of the port channel's security configuration, Inbound IPv4 IP, IPv6 IP and MAC address firewall rules are required.

Use the drop-down menus to select the firewall rules to apply to this profile's port configuration. The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances

Use the **IPv4 Inbound Firewall Rules** drop down menu to select the IPv4 specific firewall rules to apply to this profile's port channel configuration. IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity.

Use the **IPv6 Inbound Firewall Rules** drop down menu to select the IPv6 specific firewall rules to apply to this profile's port channel configuration. IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

12 If a firewall rule does not exist suiting the data protection needs of the target port channel configuration, select the **Create** icon to define a new rule configuration or the **Edit** icon to modify an existing firewall rule configuration.

13 Refer to the **Trust** field to define the following:

Trust ARP Responses	Select the check box to enable ARP trust on this port channel. ARP packets received on this port are considered trusted and information from these packets is used to identify rogue devices within the network. The default value is disabled.
Trust DHCP Responses	Select the check box to enable DHCP trust. If enabled, only DHCP responses are trusted and forwarded on this port channel, and a DHCP server can be connected only to a DHCP trusted port. The default value is enabled.
ARP header Mismatch Validation	Select the check box to enable a mismatch check for the source MAC in both the ARP and Ethernet header. The default value is enabled.
Trust 802.1p COS values	Select the check box to enable 802.1p COS values on this port channel. The default value is enabled.
Trust IP DSCP	Select the check box to enable IP DSCP values on this port channel. The default value is enabled.

14 Refer to the **IPv6 Settings** field to define the following:

Trust ND Requests	Select the check box to enable *neighbor discovery* (ND) request trust on this port channel (neighbor discovery requests received on this port are considered trusted). Use ND to determine the link-layer addresses for neighbors known to reside on attached links, similar to *Address Resolution Protocol* (ARP) on Ethernet in IPv4. The default value is disabled.
Trust DHCPv6 Responses	Select the check box to enable DHCPv6 trust. If enabled, only DHCPv6 responses are trusted and forwarded on this port channel, and a DHCPv6 server can be connected only to a trusted port. DHCPv6 relay agents receive messages from clients and forward them to a DHCPv6 server. The server sends responses back to the relay agent, and the relay agent sends the responses to the client on the local link. The default value is enabled.
ND header Mismatch Validation	Select the check box to enable a mismatch check for the source MAC in both the ND header and link layer option. The default value is disabled.
RA Guard	Select this option to allow router advertisements or IPv6 redirects from this port. Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.This setting is enabled by default.

15 Select **OK** to save the changes to the security configuration. Select **Reset** to revert to the last saved configuration.

16 Select the **Spanning Tree** tab.

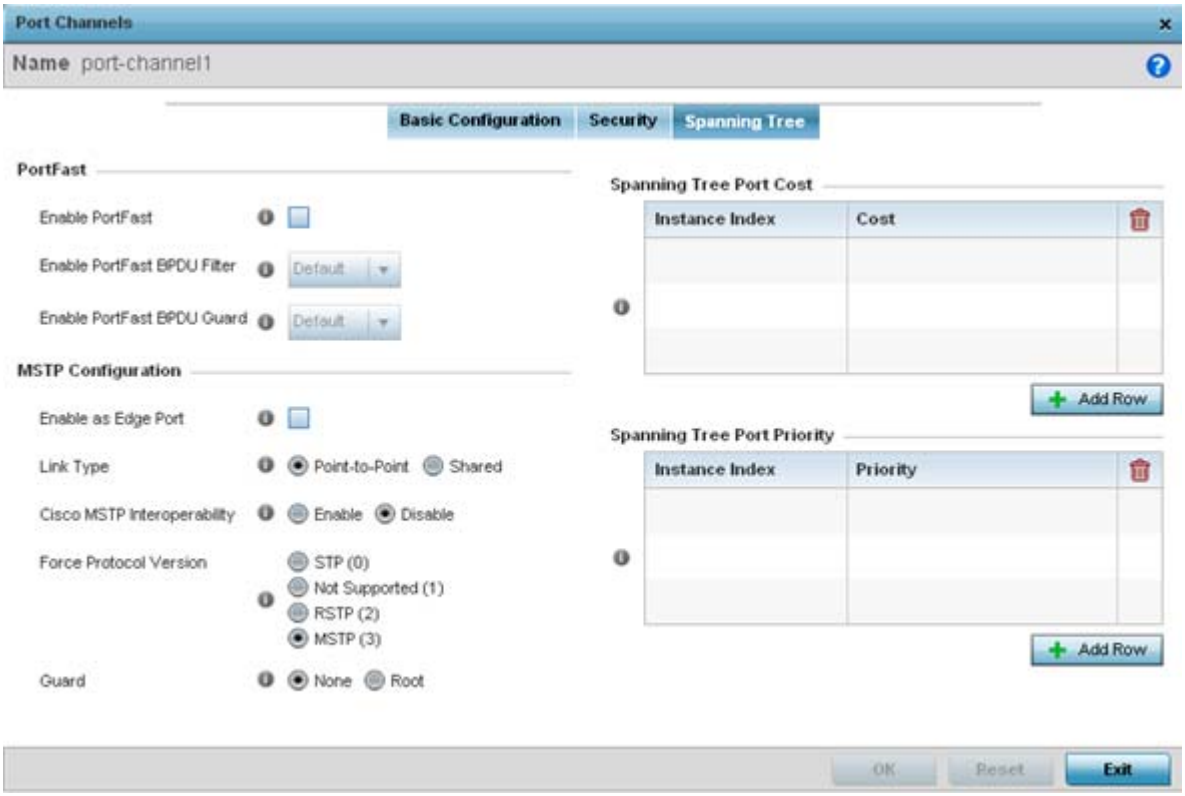


Figure 8-26 *Port Channels - Spanning Tree screen*

17 Define the following **PortFast** parameters for the port channel's MSTP configuration:

Enable PortFast	Select the check box to enable drop-down menus for both the port Enable Portfast BPDU Filter and Enable Portfast BPDU guard options. This setting is disabled by default.
Enable PortFast BPDU Filter	Select *Enable* to invoke a BPDU filter for this portfast enabled port channel. Enabling the BPDU filter feature ensures this port channel does not transmit or receive any BPDUs. The default setting is None.
Enable PortFast BPDU Guard	Select *Enable* to invoke a BPDU guard for this portfast enabled port channel. Enabling the BPDU Guard feature means this port will shutdown on receiving a BPDU. Thus, no BPDUs are processed. The default setting is None.

18 Set the following **MSTP Configuration** parameters for the port channel:

Link Type	Select either the *Point-to-Point* or *Shared* radio button. Selecting Point-to-Point indicates the port should be treated as connected to a point-to-point link. Selecting Shared indicates this port should be treated as having a shared connection. A port connected to a hub is on a shared link, while the one connected to a controller or service platform is a point-to-point link. Point-to-Point is the default setting.
Cisco MSTP Interoperability	Select either the *Enable* or *Disable* radio buttons. This enables interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default.
Force Protocol Version	Sets the protocol version to either *STP(0)*, *Not Supported(1)*, *RSTP(2)* or *MSTP(3)*. MSTP is the default setting.

Guard	Determines whether the port channel enforces root bridge placement. Setting the guard to *Root* ensures the port is a designated port. Typically, each guard root port is a designated port, unless two or more ports (within the root bridge) are connected together. If the bridge receives superior (BPDUs) on a guard root-enabled port, the guard root moves the port to a root-inconsistent STP state. This state is equivalent to a listening state. No data is forwarded across the port. Thus, the guard root enforces the root bridge position.

19 Refer to the **Spanning Tree Port Cost** table.

Define an **Instance Index** using the spinner control and then set the cost. The default path cost depends on the user defined port speed.The cost helps determine the role of the port channel in the MSTP network. The designated cost is the cost for a packet to travel from this port to the root in the MSTP configuration. The slower the media, the higher the cost.

Speed	Default Path Cost
<=100000 bits/sec	200000000
<=1000000 bits/sec	20000000
<=10000000 bits/sec	2000000
<=100000000 bits/sec	200000
<=1000000000 bits/sec	20000
<=10000000000 bits/sec	2000
<=100000000000 bits/sec	200
<=1000000000000 bits/sec	20
>1000000000000 bits/sec	2

20 Select **+ Add Row** as needed to include additional indexes.

21 Refer to the **Spanning Tree Port Priority** table.

Define an **Instance Index** using the spinner control and then set the **Priority**. The lower the priority, a greater likelihood of the port becoming a designated port.

22 Select **+ Add Row** needed to include additional indexes.

23 Select **OK** to save the changes made to the Ethernet Port Spanning Tree configuration. Select **Reset** to revert to the last saved configuration.

8.7.4 VM Interface Configuration

Profile Interface Configuration

WiNG provides a dataplane bridge for external network connectivity for *Virtual Machines* (VMs). VM Interfaces define which IP address is associated with each VLAN ID the service platform is connected to and enables remote service platform administration. Each custom VM can have up to a maximum of two VM interfaces. Each VM interface can be mapped to one of sixteen VMIF ports on the dataplane bridge. This mapping determines the destination for service platform routing.

By default, VM interfaces are internally connected to the dataplane bridge via VMIF1. VMIF1 is an untagged port providing access to VLAN 1 to support the capability to connect the VM interfaces to any of the VMIF ports. This provides the flexibility to move a VM interface onto different VLANs as well as configure specific firewall and QOS rules.

NOTE: VM interfaces are only supported for NX4500, NX6500, NX7500 and NX9000 series service platforms.

To define a VM interface profile configuration:

1 Select **Configuration** > **Profiles** > **Interface**.

2 Expand the Interface menu to display its submenu options.

3 Select **VM.**

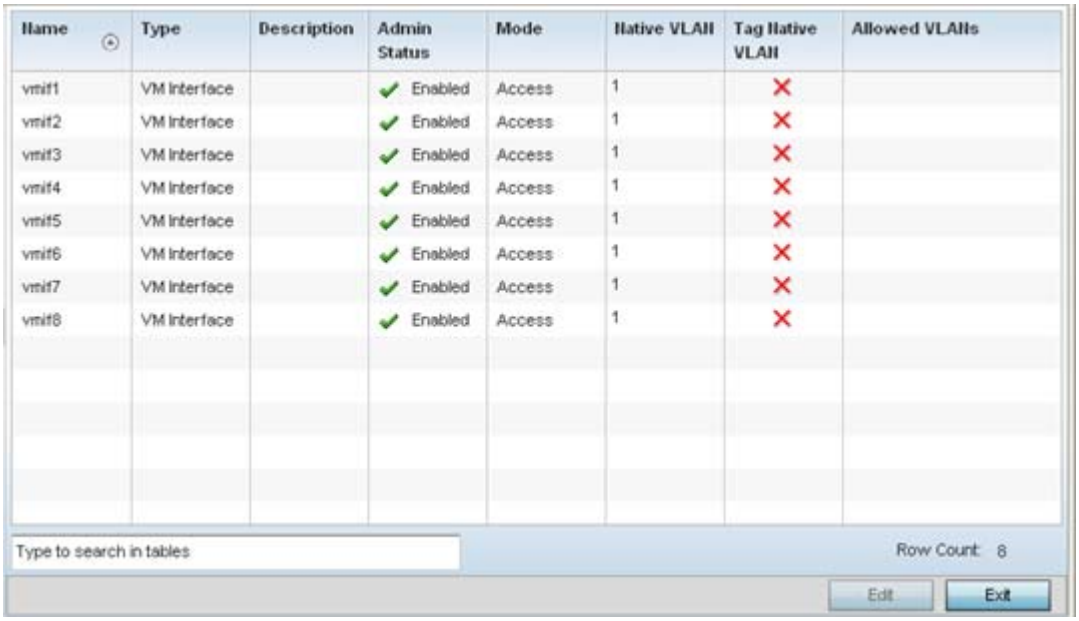


Figure 8-27 *Profile - VM Interfaces screen*

4 Refer to the following to review VM interface configurations and status:

Name	Displays the VM interface numerical identifier assigned when it was created. The numerical name cannot be modified as part of the edit process.
Type	Displays whether the type is VM interface.
Description	Lists a short description (64 characters maximum) describing the VM interface or differentiating it from others with similar configurations.
Admin Status	A green check mark defines the listed VM interface as active and currently enabled with the profile. A red “X” defines the VM interface as currently disabled and not available for use. The interface status can be modified with the VM interface Basic Configuration screen as required.

Mode	Displays the layer 3 mode of the VM interface as either *Access* or *Trunk* (as defined within the VM Interfaces Basic Configuration screen). If Access is selected, the listed VM interface accepts packets only from the native VLAN. Frames are forwarded untagged with no 802.1Q header. All frames received on the port are expected as untagged and mapped to the native VLAN. If set to Trunk, the port allows packets from a list of VLANs added to the trunk. A VM interface configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged.
Native VLAN	Lists the numerical VLAN ID (1 - 4094) set for the native VLAN. The native VLAN allows a VM interface to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a VM interface in trunk mode.
Tag Native VLAN	A green check mark defines the native VLAN as tagged. A red "X" defines the native VLAN as untagged. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream VM interface ports know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream VM interface classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows a VM interface to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.
Allowed VLANs	Displays those VLANs allowed to send packets over the listed VM interface. Allowed VLANs are only listed when the mode has been set to Trunk.

5 To edit the configuration of an existing VM interface, select it from amongst those displayed and select the **Edit** button. The VM Interfaces **Basic Configuration** screen displays by default.

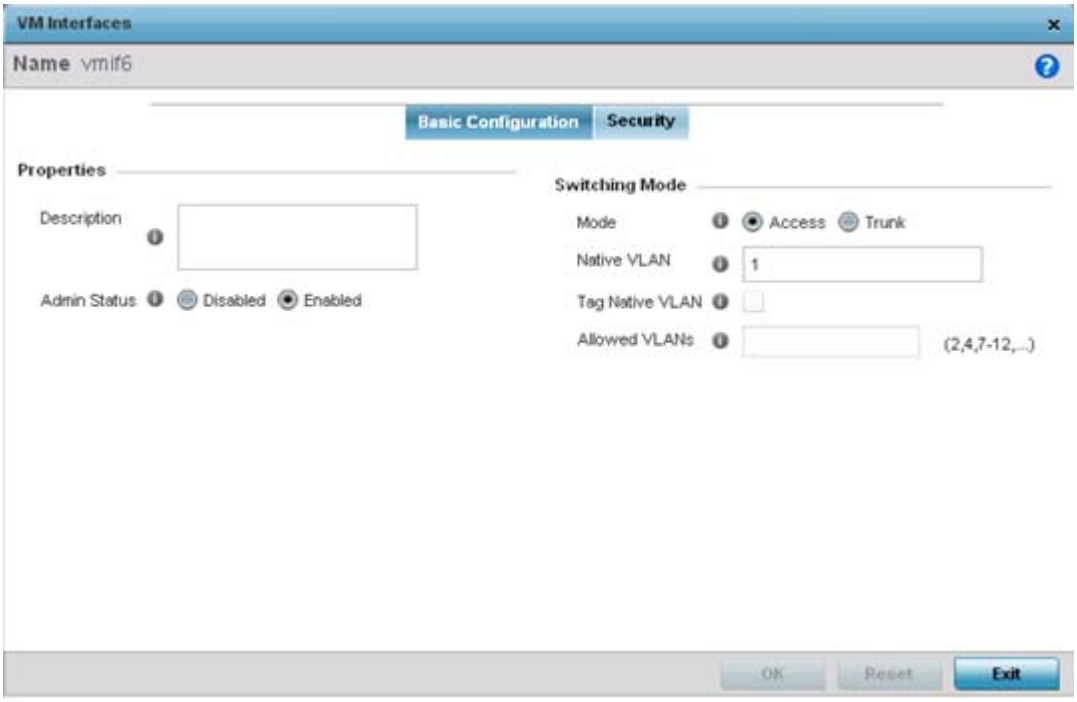


Figure 8-28 *Profile - VM Interfaces Basic Configuration screen*

6 Set the following VM interface **Properties**:

Description	Enter a brief description for the controller or service platform VM interface (64 characters maximum).
Admin Status	Select the *Enabled* radio button to define this VM interface as active to the profile it supports. Select the *Disabled* radio button to disable this VM interface configuration in the profile. It can be activated at any future time when needed.

7 Set the following **Switching Mode** parameters to apply to the VM Interface configuration:

Mode	Select either the *Access* or *Trunk* radio button to set the VLAN switching mode over the VM interface. If Access is selected, the VM interface accepts packets only from the native VLAN. Frames are forwarded untagged with no 802.1Q header. All frames received on the VMIF port are expected as untagged and are mapped to the native VLAN. If the mode is set to Trunk, the VM interface allows packets from a list of VLANs you add to the trunk. A VM interface configured as Trunk supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. Access is the default setting.
Native VLAN	Use the spinner control to define a numerical *Native VLAN ID* from 1 - 4094. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic will be directed over when using trunk mode. The default value is 1.
Tag the Native VLAN	Select this option to tag the native VLAN. Service platforms support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream VMIF that the frame belongs. If the upstream VMIF does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between VM interface ports, both VM interfaces must support tagging and be configured to accept tagged VLANs. When a frame is tagged, a 12 bit frame VLAN ID is added to the 802.1Q header, so upstream VM interfaces know which VLAN ID the frame belongs to. The 12 bit VLAN ID is read and the frame is forwarded to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream VMIF classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows a VM interface to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This setting is disabled by default.
Allowed VLANs	Selecting *Trunk* as the mode enables the *Allowed VLANs* parameter. Add VLANs that exclusively send packets over the VM interface. The available range is from 1 - 4094. The maximum number of entries is 256.

8 Select **OK** to save the changes to the VM interface basic configuration. Select **Reset** to revert to the last saved configuration.

9 Select the **Security** tab.

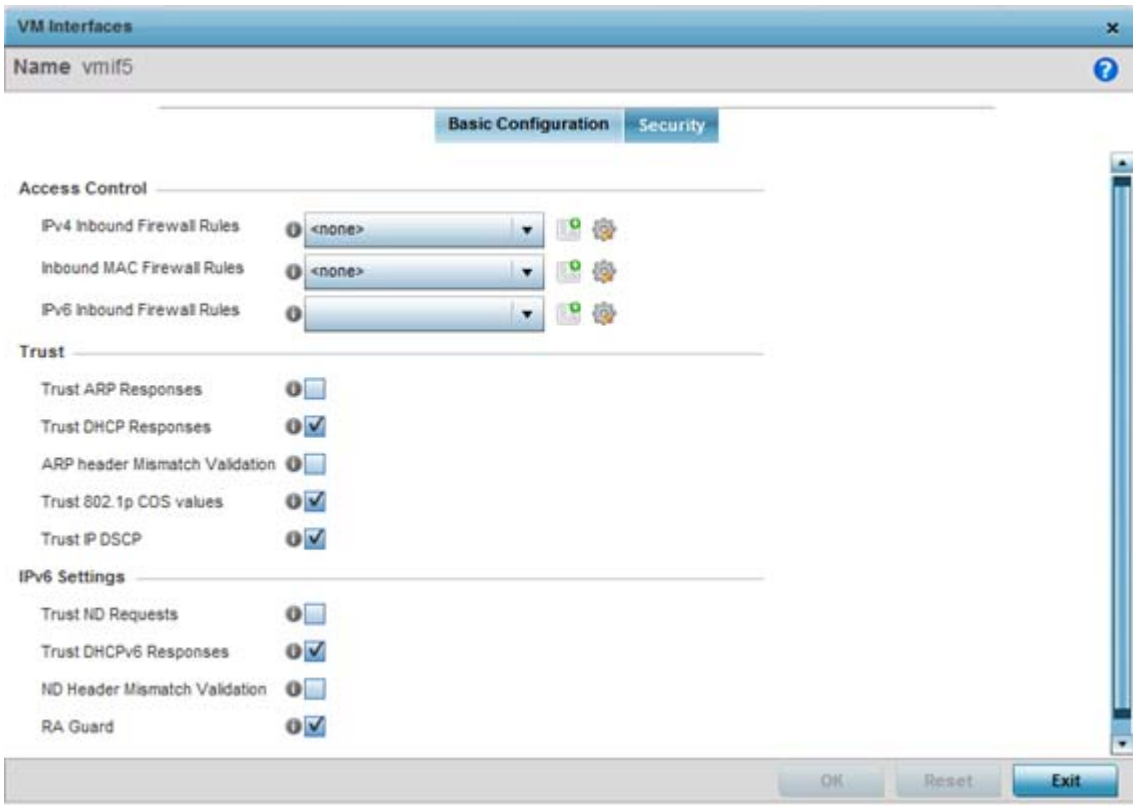


Figure 8-29 *Profile - VM Interfaces Security screen*

10 Refer to the **Access Control** field. As part of the VM interface's security configuration, IPv4 and IPv6 Inbound and MAC Inbound address firewall rules are required.

Use the drop-down menus to select the firewall rules to apply to this profile's VM interface configuration. The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

Use the **IPv4 Inbound Firewall Rules** drop down menu to select the IPv4 specific firewall rules to apply to this profile's VM interface configuration. IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity.

Use the **IPv6 Inbound Firewall Rules** drop down menu to select the IPv6 specific firewall rules to apply to this profile's VM interface configuration. IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

If a firewall rule does not exist suiting the data protection needs of the target VM interface configuration, select the **Create** icon to define a new rule configuration, or the **Edit** icon to modify an existing firewall rule configuration.

11 Refer to the **Trust** field to set the following:

Trust ARP Responses	Select this option to enable ARP trust on this VM interface. ARP packets received on this port are considered trusted, and information from these packets is used to identify rogue devices. The default value is disabled.

Trust DHCP Responses	Select this option to enable DHCP trust on this VM interface. If enabled, only DHCP responses are trusted and forwarded on this VM interface, and a DHCP server can be connected only to a DHCP trusted port. The default value is enabled.
ARP header Mismatch Validation	Select this option to enable a source MAC mismatch check in both the ARP and Ethernet header. The default value is enabled.
Trust 802.1p COS values	Select this option to enable 802.1p COS values on this VM interface. The default value is enabled.
Trust IP DSCP	Select this option to enable IP DSCP values on this VM interface. The default value is enabled.

12 Set the following **IPv6 Settings** required for unique IPv6 support:

Trust ND Requests	Select this option to enable the trust of neighbor discovery requests required on an IPv6 network on this VM interface. This setting is disabled by default.
Trust DHCPv6 Responses	Select this option to enable the trust all DHCPv6 responses on this VM interface. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. DHCPv6 relay agents receive messages from clients and forward them to a DHCPv6 server. The server sends responses back to the relay agent, and the relay agent sends the responses to the client on the local link. This setting is enabled by default.
ND Header Mismatch Validation	Select this option to enable a mismatch check for the source MAC within the ND header and link layer option. This setting is disabled by default.
RA Guard	Select this option to enable router advertisements or ICMPv6 redirects from this VM interface. Router advertisements are periodically sent to hosts or sent in response to neighbor solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information. This setting is disabled by default.

Select **OK** to save the changes to the security configuration. Select **Reset** to revert to the last saved configuration.

8.7.5 Access Point Radio Configuration

Profile Interface Configuration

Access Points can have their radio configurations modified once their radios have successfully associated to an adopting peerAccess Point, wireless controller or a service platform. Take care not to modify an Access Point's configuration using its resident Web UI, CLI or SNMP interfaces when managed by a profile, or risk the Access Point having a configuration independent from the profile until the profile can be uploaded to the Access Point again.

To define a Access Point radio configuration from the Access Point's associated controller or service platform:

1 Select **Configuration** > **Profiles** > **Interface**.

2 Expand the Interface menu to display its submenu options.

3 Select **Radios**.

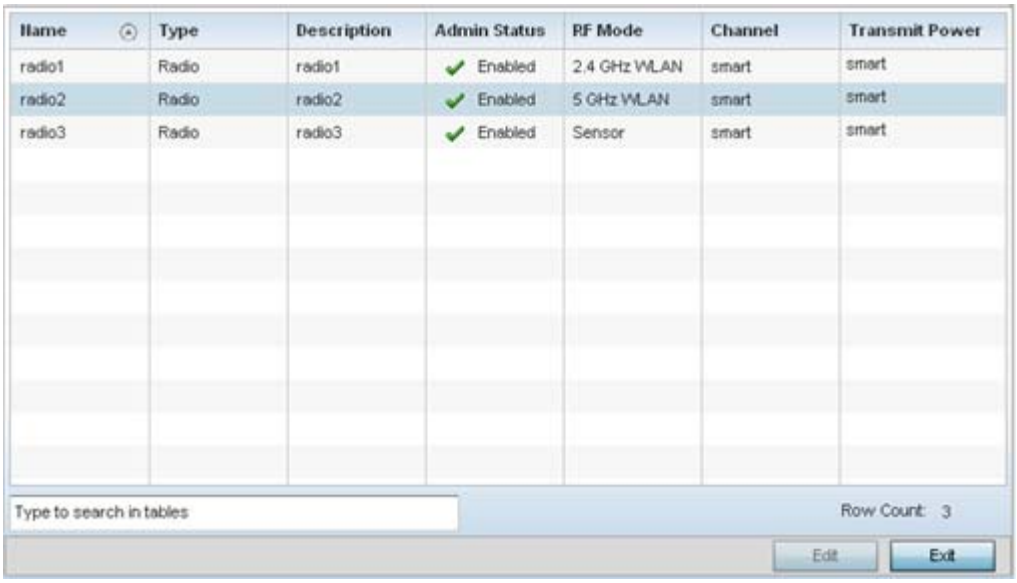


Figure 8-30 *Access Point - Radios screen*

4 Review the following to determine whether a radio configuration requires modification to better support the managed network:

Name	Displays whether the reporting radio is the Access Point's radio1, radio2 or radio3.
Type	Displays the type of radio housed by each listed Access Point.
Description	Displays a brief description of the radio provided by the administrator when the radio's configuration was added or modified.
Admin Status	A green checkmark defines the listed radio as active and enabled with its supported profile. A red "X" defines the radio as currently disabled.
RF Mode	Displays whether each listed radio is operating in the 802.11a/n or 802.11b/g/n radio band. If the radio is a dedicated sensor, it will be listed as a sensor to define the radio as not providing typical WLAN support. If the radio is a client-bridge, it provides a typical bridging function and does not provide WLAN support. The radio band is set from within the Radio Settings tab.
Channel	Lists the channel setting for the radio. Smart is the default setting. If set to smart, the Access Point scans non-overlapping channels listening for beacons from other Access Points. After the channels are scanned, it selects the channel with the fewest Access Points. In the case of multiple Access Points on the same channel, it selects the channel with the lowest average power level.
Transmit Power	Lists the transmit power for each radio displayed as a value in miliwatts. If *smart* is displayed, the radio has been set to make compensations for failed or poorly performing neighbor radios.

5 If required, select a radio configuration and select the **Edit** button to modify its configuration.

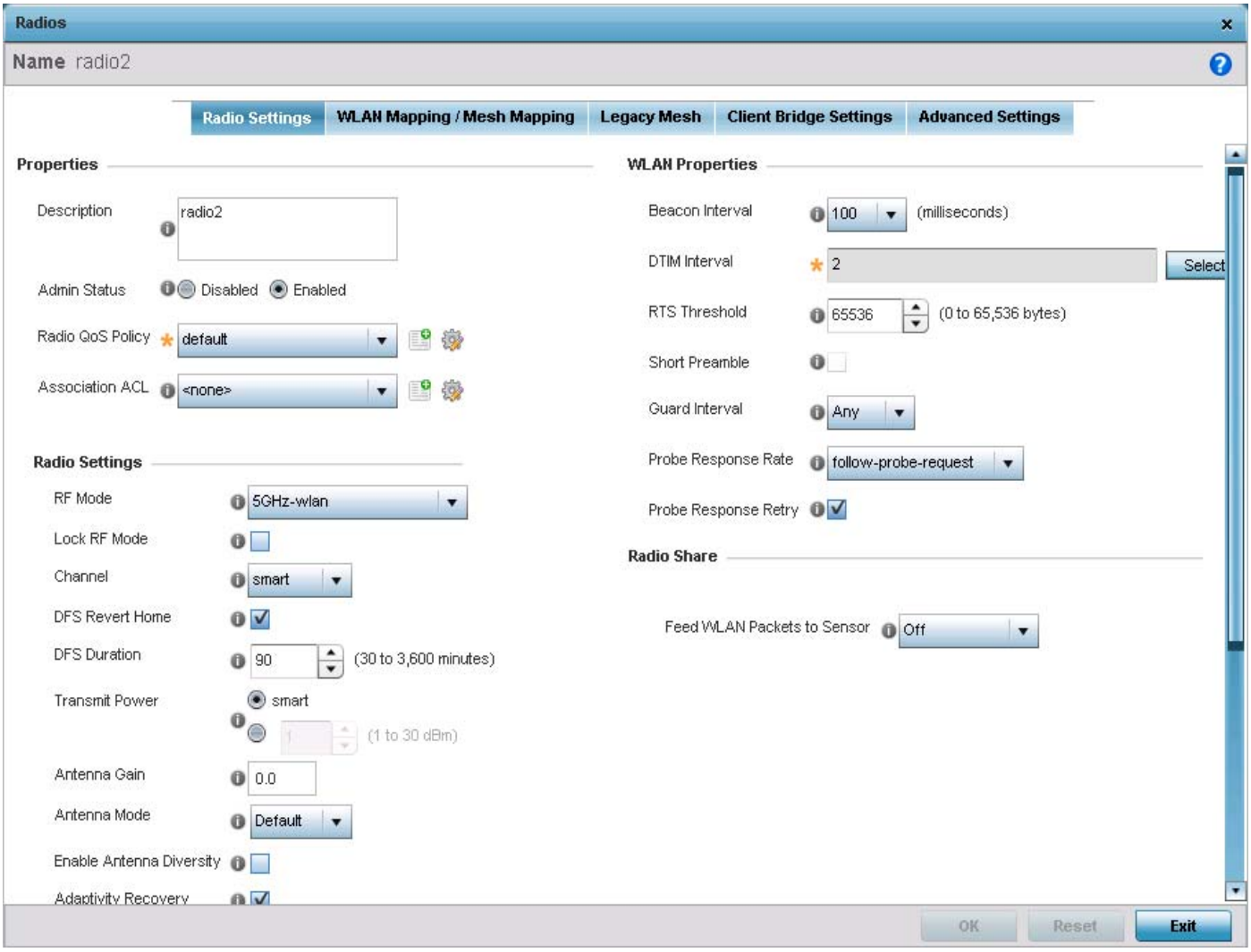


Figure 8-31 *Access Point Radio - Radio Settings tab*

The **Radio Settings** tab displays by default.

6 Define the following radio configuration parameters from within the **Properties** field:

Description	Provide or edit a description (1 - 64 characters in length) for the radio that helps differentiate it from others with similar configurations.
Admin Status	Select the *Enabled* radio button to define this radio as active to the profile it supports. Select the *Disabled* radio button to disable this radio configuration within the profile. It can be activated at any future time when needed. The default setting is enabled.
Radio QoS Policy	Use the drop-down menu to specify an existing QoS policy to apply to the Access Point radio in respect to its intended radio traffic. If there's no existing suiting the radio's intended operation, select the *Create* icon to define a new QoS policy that can be applied to this profile.

Association ACL	Use the drop-down menu to specify an existing Association ACL policy to apply to the Access Point radio. An Association ACL is a policy-based ACL that either prevents or allows wireless clients from connecting to an Access Point radio. An ACL is a sequential collection of permit and deny conditions that apply to packets. When a packet is received on an interface, its compared against applied ACLs to verify the packet has the required permissions to be forwarded. If a packet does not meet any of the criteria specified in the ACL, the packet is dropped. Select the *Create* icon to define a new Association ACL that can be applied to this profile.

7 Set the following profile **Radio Settings** for the selected Access Point radio:

RF Mode	Set the mode to either *2.4 GHz WLAN* or *5 GHz WLAN* depending on the radio's intended client support requirement. Set the mode to *Sensor* if using the radio for rogue device detection. To a radio as a detector, disable Sensor support on the other radio. Set the mode to *scan-ahead* to use the secondary radio to scan for an active channel for backhaul transmission in the event of a radio trigger on the principal radio. The Access Point should then switch radios allowing transmission to continue. This is required in environments where handoff is required and DFS triggers are common.
Lock RF Mode	Select the check box to lock Smart RF for this radio. The default setting is disabled.
Channel	Use the drop-down menu to select the channel of operation for the radio. Only a trained installation professional should define the radio channel. Select *Smart* for the radio to scan non-overlapping channels listening for beacons from other Access Points. After channels are scanned, the radio selects the channel with the fewest Access Points. In the case of multiple Access Points on the same channel, it selects the channel with the lowest average power level. The default value is Smart. Channels with a "w" appended to them are unique to the 40 MHz band. Channels with a "ww" appended to them are 802.11ac specific, only appear when using an AP8232, and are unique to the 80 MHz band.
DFS Revert Home	Select this option to revert to the home channel after a DFS evacuation period.
DFS Duration	Set the DFS holdtime from 30 to 3,600 minutes. The default is 90 minutes.
Transmit Power	Set the transmit power of the selected Access Point radio. If using a dual or three radio model Access Point, each radio should be configured with a unique transmit power in respect to its intended client support function. A setting of 0 defines the radio as using Smart RF to determine its output power. 20 dBm is the default value. Selecting *smart* deactivates the spinner control and automatically reflects a "0" in the spinner control's grayed out box.

Antenna Gain	Set the antenna between 0.00 - 15.00 dBm. The Access Point's *Power Management Antenna Configuration File* (PMACF) automatically configures the Access Point's radio transmit power based on the antenna type, its antenna gain (provided here) and the deployed country's regulatory domain restrictions. Once provided, the Access Point calculates the power range. Antenna gain relates the intensity of an antenna in a given direction to the intensity that would be produced ideally by an antenna that radiates equally in all directions (isotropically), and has no losses. Although the gain of an antenna is directly related to its directivity, its gain is a measure that takes into account the efficiency of the antenna as well as its directional capabilities. Only a professional installer should set the antenna gain. The default value is 0.00.
Antenna Mode	Use the drop-down menu to select the number of transmit and receive antennas on the Access Point. 1x1 is used for transmissions over just the single "A" antenna, 1x3 is used for transmissions over the "A" antenna and all three antennas for receiving. 2x2 is used for transmissions and receipts over two antennas for dual antenna models. The default setting is dynamic based on the Access Point model deployed and its transmit power settings.
Enable Antenna Diversity	Select this box to enable antenna diversity on supported antennas. Antenna diversity uses two or more antennas to increase signal quality and strength. This option is disabled by default.
Adaptivity Recovery	Select this option to switch channels when an Access Point's radio is in adaptivity mode. In adaptivity mode, an Access Point monitors interference on its set channel and stops functioning when the radio's defined interference tolerance level is exceeded. When the defined adaptivity timeout is exceeded, the radio resumes functionality on a different channel. This option is enabled by default.
Adaptivity Timeout	Set the adaptivity timeout from 30 to 3,600 minutes. The default setting is 90 minutes.
Wireless Client Power	Select this option to specify the transmit power on supported wireless clients. If this is enabled set a client power level between 0 to 20 dBm. This option is disabled by default.
Dynamic Chain Selection	Select this option for the radio to dynamically change the number of transmit chains. This option is enabled by default.
Data Rates	Once the radio band is provided, the Data Rates drop-down menu populates with rate options depending on the 2.4 or 5 GHz band selected. If the radio band is set to Sensor or Detector, the Data Rates drop-down menu is not enabled, as the rates are fixed and not user configurable. If 2.4 GHz is selected as the radio band, select separate 802.11b, 802.11g and 802.11n rates and define how they are used in combination. If 5 GHz is selected as the radio band, select separate 802.11a and 802.11n rates then define how they are used together. When using 802.11n (in either the 2.4 or 5 GHz band), Set a MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. A MCS defines (based on RF channel conditions) an optimal combination of 8 data rates, bonded channels, multiple spatial streams, different guard intervals and modulation types. Clients can associate as long as they support basic MCS (as well as non-11n basic rates).

Radio Placement	Use the drop-down menu to specify whether the radio is located *Indoors* or *Outdoors*. The placement should depend on the country of operation and its regulatory domain requirements for radio emissions.The default setting is Indoors.
Max Clients	Use the spinner control to set a maximum permissible number of clients to connect with this radio. The available range is between 0 - 256 clients. The default value is 256.
Rate Selection Method	Specify a radio selection method for the radio. The selection methods are: *Standard* - standard monotonic radio selection method will be used. *Opportunistic* - sets opportunistic radio link adaptation as the radio selection method. This mode uses opportunistic data rate selection to provide the best throughput.

8 Set the following profile **WLAN Properties** for the selected Access Point radio.

Beacon Interval	Set the interval between radio beacons in milliseconds (either 50, 100 or 200). A beacon is a packet broadcast by adopted radios to keep the network synchronized. The beacon includes the WLAN service area, radio address, broadcast destination addresses, time stamp and indicators about traffic and delivery such as a DTIM. Increase the DTIM/beacon settings (lengthening the time) to let nodes sleep longer and preserve battery life. Decrease these settings (shortening the time) to support streaming-multicast audio and video applications that are jitter-sensitive. The default value is 100 milliseconds.
DTIM Interval BSSID	Set a DTIM Interval to specify a period for *Delivery Traffic Indication Messages* (DTIM). A DTIM is periodically included in a beacon frame transmitted from adopted radios. The DTIM period determines how often the beacon contains a DTIM, for example, 1 DTIM for every 10 beacons. The DTIM indicates broadcast and multicast frames (buffered at the Access Point) are soon to arrive. These are simple data frames that require no acknowledgement, so nodes sometimes miss them. Increase the DTIM/ beacon settings (lengthening the time) to let nodes sleep longer and preserve their battery life. Decrease these settings (shortening the time) to support streaming multicast audio and video applications that are jitter-sensitive.

RTS Threshold	Specify a *Request To Send* (RTS) threshold (between 1 - 65,536 bytes) for use by the WLAN's adopted Access Point radios. RTS is a transmitting station's signal that requests a *Clear To Send* (CTS) response from a receiving client. This RTS/CTS procedure clears the air where clients are contending for transmission time. Benefits include fewer data collisions and better communication with nodes that are hard to find (or hidden) because of other active nodes in the transmission path. Control RTS/CTS by setting an RTS threshold. This setting initiates an RTS/CTS exchange for data frames larger than the threshold, and sends (without RTS/CTS) any data frames smaller than the threshold. Consider the trade-offs when setting an appropriate RTS threshold for the WLAN's Access Point radios. A lower RTS threshold causes more frequent RTS/CTS exchanges. This consumes more bandwidth because of additional latency (RTS/CTS exchanges) before transmissions can commence. A disadvantage is the reduction in data-frame throughput. An advantage is quicker system recovery from electromagnetic interference and data collisions. Environments with more wireless traffic and contention for transmission make the best use of a lower RTS threshold. A higher RTS threshold minimizes RTS/CTS exchanges, consuming less bandwidth for data transmissions. A disadvantage is less help to nodes that encounter interference and collisions. An advantage is faster data-frame throughput. Environments with less wireless traffic and contention for transmission make the best use of a higher RTS threshold.
Short Preamble	If using an 802.11bg radio, select this checkbox for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectraLink/Polycomm phones) require long preambles. The default value is disabled.
Guard Interval	Use the drop-down menu to specify a *Long* or *Any* guard interval. The guard interval is the space between the packets being transmitted. The guard interval is there to eliminate *inter-symbol interference* (ISI). ISI occurs when echoes or reflections from one transmission interfere with another. Adding time between transmissions allows echo's and reflections to settle before the next packet is transmitted. A shorter guard interval results in a shorter times which reduces overhead and increases data rates by up to 10%.The default value is Long.
Probe Response Rate	Use the drop-down menu to specify the data transmission rate used for the transmission of probe responses. Options include, *highest-basic*, *lowest-basic* and *follow-probe-request* (default setting).
Probe Response Retry	Select the check box to retry probe responses if they are not acknowledged by the target wireless client. The default value is enabled.

9 Select a mode from the **Feed WLAN Packets to Sensor** menu (within the **Radio Share** field) to enable this feature.

Select either *Inline* or *Promiscuous* mode to allow the packets the radio is switching to also be used by the WIPS analysis module. This feature can be enabled in two modes: an inline mode where the wips sensor receives the packets from the radios with radio operating in normal mode. A promiscuous mode where the radio is configured to a mode where it receives all packets on the channel whether the destination address is the radio or not, and the wips module can analyze them.

10 Select the **WLAN Mapping/Mesh Mapping** tab.

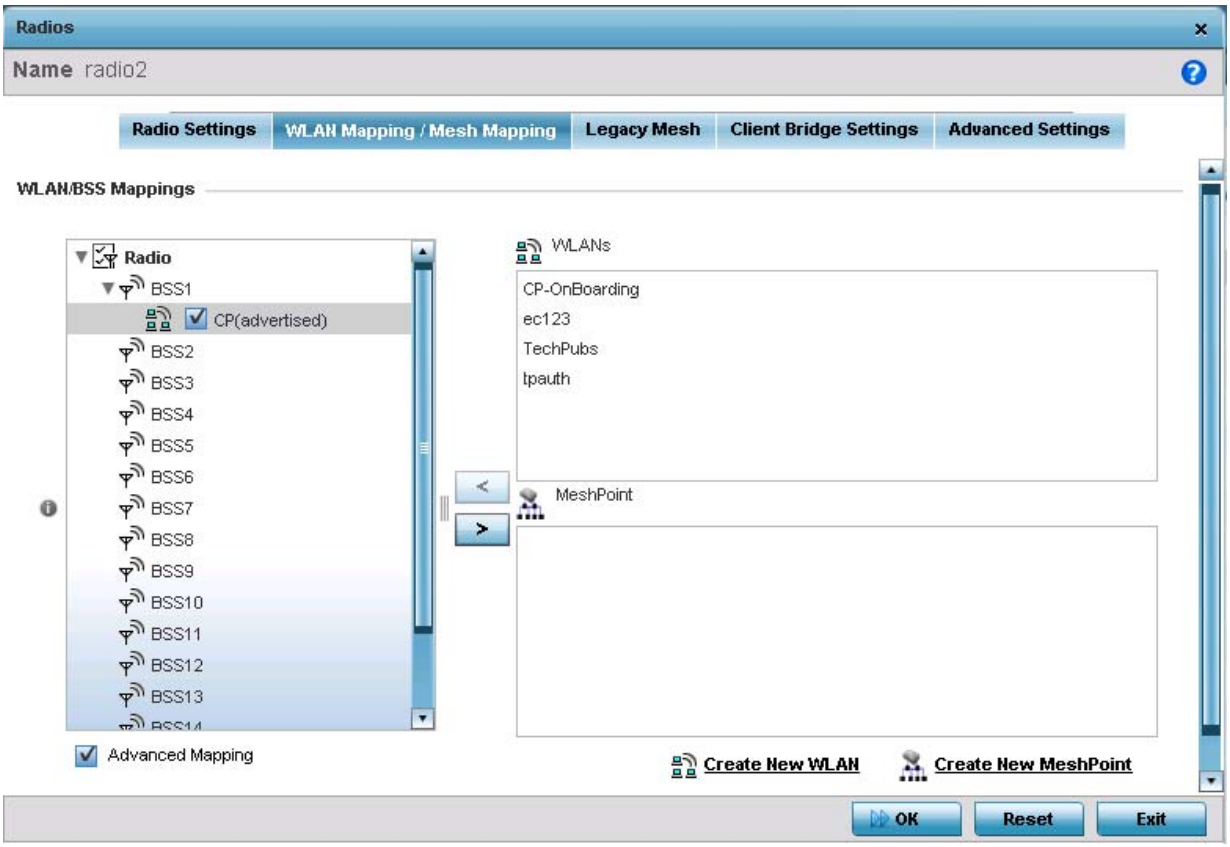


Figure 8-32 *Access Point Radio - WLAN Mapping/Mesh Mapping screen*

11 Refer to the **WLAN/BSS Mappings** field to set WLAN BSSID assignments for an existing Access Point deployment.

Administrators can assign each WLAN its own BSSID. If using a single-radio Access Point, there are 8 BSSIDs available. If using a dual-radio Access Point there are 8 BSSIDs for the 802.11b/g/n radio and 8 BSSIDs for the 802.11a/n radio.

12 Select **Advanced Mapping** to enable WLAN mapping to a specific BSS ID.

13 Select **OK** to save the changes to the WLAN Mapping. Select **Reset** to revert to the last saved configuration.

14 Select the **Legacy Mesh** tab.

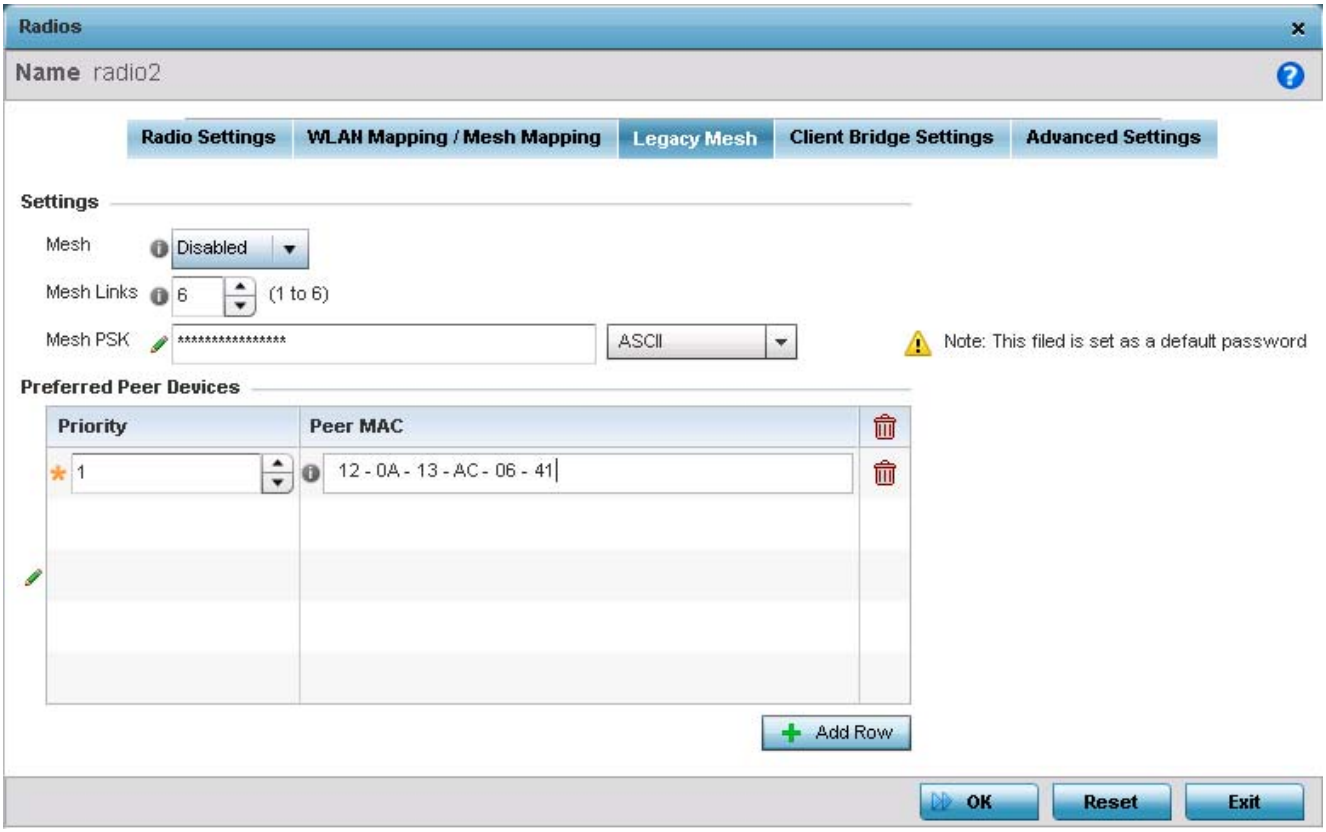


Figure 8-33 *Profile - Access Point Legacy Mesh tab*

15 Refer to the **Settings** field to define mesh settings for the Access Point radio.

Mesh	Use the drop-down menu to set the mesh mode for this radio. Available options are *Disabled*, *Portal* or *Client*. Setting the mesh mode to Disabled deactivates all mesh activity on this radio. Setting the mesh mode to Portal turns the radio into a mesh portal. This will start the radio beaconing immediately and accept connections from other mesh nodes. Setting the mesh mode to client enables the radio to operate as a mesh client and scan and connect to mesh portals or nodes connected to portals.
Mesh Links	Specify the number of mesh links allowed by the radio. The radio can have between 1-6 mesh links when the radio is configured as a Portal or Client.
Mesh PSK	Provide the encryption key in either ASCII or Hex format. Administrators must ensure this key is configured on the Access Point when staged for mesh, added to the mesh client and to the portal Access Point's configuration on the controller or service platform. Select *Show* to expose the characters used in the PSK.

NOTE: Only single hop mesh links are supported at this time.

NOTE: The mesh encryption key is configurable from the *Command Line Interface* (CLI) using the command '**`mesh psk`**'. Administrators must ensure that this key is configured on the AP when it is being staged for mesh, and also added to the mesh client as well as to the portal APs configuration on the controller or service platform.

16 Refer to the **Preferred Peer Device** table to add mesh peers. For each peer added, enter its MAC Address and a Priority between 1 and 6. The lower the priority number the higher priority it'll be given when connecting to mesh infrastructure.

17 Select the **+ Add Row** button to add preferred peer devices for the radio to connect to in mesh mode.

18 Select the **Client Bridge Settings** tab to configure the selected radio as a client-bridge. Note, before configuring the client-bridge parameters, set the radio's rf-mode to *bridge*.

An Access Point's radio can be configured to form a bridge between its wireless/wired clients and an infrastructure WLAN. The bridge radio authenticates and associates with the infrastructure WLAN Access Point. After successful association, the Access Point switches frames between its bridge radio and wired/wireless client(s) connected either to its GE port(s) or to the other radio, there by providing the clients access to the infrastructure WLAN resources. This feature is supported only on the AP6522, AP6562, AP7522, AP7532 and AP7562 model Access Points.

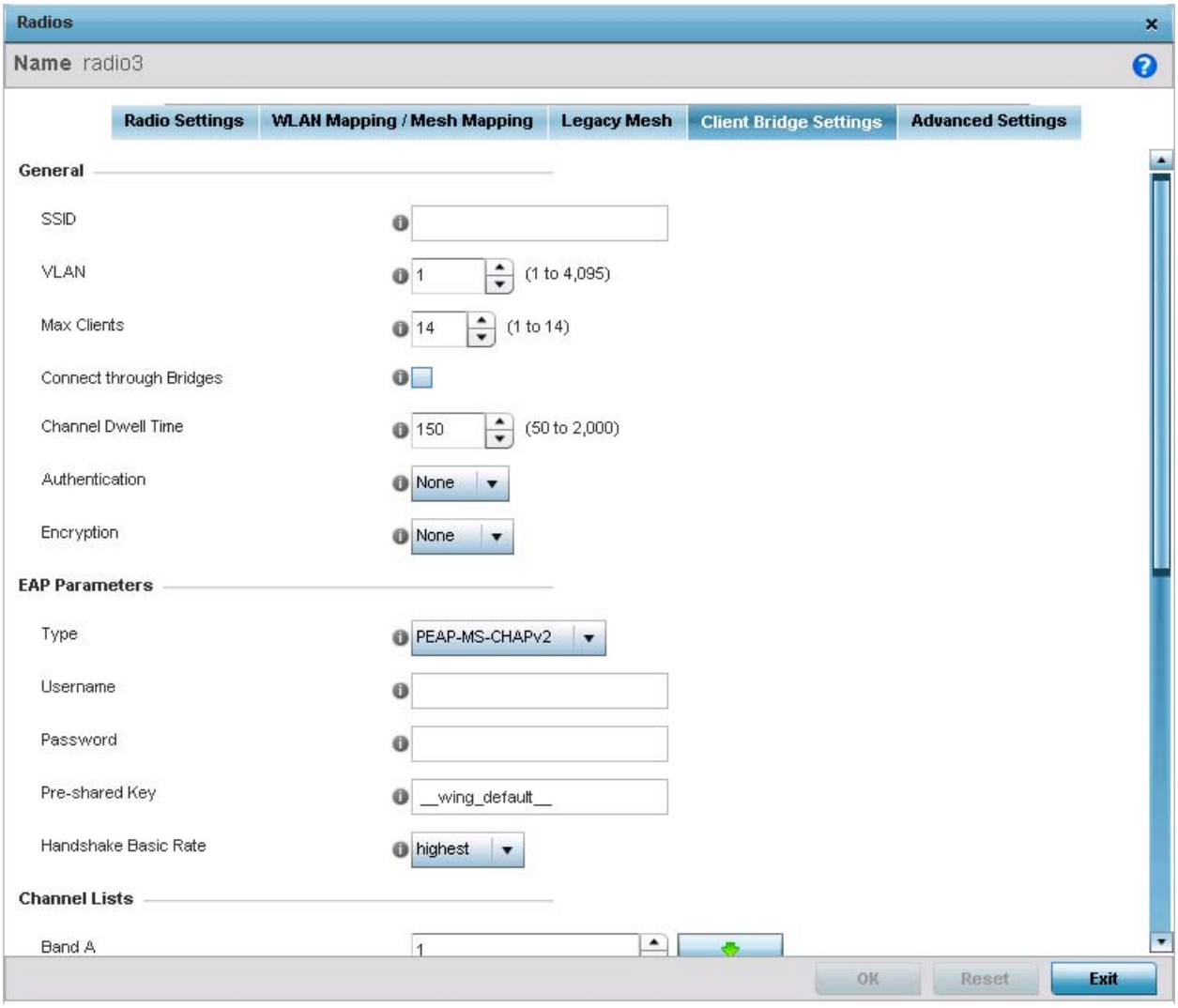


Figure 8-34 *Profile - Access Point Client Bridge Settings tab*

19 Refer to the **General** field and define the following configurations:

SSID	Set the infrastructure WLAN's SSID the client-bridge Access Point associates with.
VLAN	Set the VLAN to which the bridged clients' sessions are mapped after successful association with the infrastructure WLAN. Once mapped, the client bridge communicates with permitted hosts over the infrastructure WLAN. Specify the VLAN from 1 to 4095.
Max Clients	Set the maximum number of bridge MAC addresses form 1 to 14. This is the maximum number of client-bridge Access Points that can associate with an infrastructure WLAN. The default value is 14.
Connect through Bridges	Set the maximum number of client-bridge Access Points that can associate with the infrastructure WLAN. Specify a value from 1 to 14. The default value is 14.

Channel Dwell Time	Set the channel-dwell time from 50 to 2000 milliseconds. This is the time the client-bridge radio dwells on each channel (configured in the list of channels) when scanning for an infrastructure WLAN. The default is 150 milliseconds.
Authentication	Set the mode of authentication with the infrastructure WLAN. The authentication mode specified here should be the same as that configured on the infrastructure WLAN. The options are *None* and *EAP*. If selecting EAP, specify the EAP authentication parameters. The default setting in None. For information on WLAN authentication, see *Configuring WLAN Security*.
Encryption	Set the packet encryption mode. The encryption mode specified here should be the same as that configured on the infrastructure WLAN. The options are *None*, *CCMP* and *TKIP*. The default setting is None. For information on WLAN encryption, see *Configuring WLAN Security*.

20 Refer to the **EAP Parameters** field and define the following EAP authentication parameters:

Type	Use the drop-down menu to select the EAP authentication method used by the supplicant. The options are TLS and PEAP-MS-CHAPv2. The default EAP type is PEAP-MS-CHAPv2.
Username	Set the 32 character maximum user name for an EAP authentication credential exchange.
Password	Set the 32 character maximum password for the EAP user name specified above.
Pre-shared Key	Set the *pre-shared key* (PSK) used with EAP. Note, the authenticating algorithm and PSK configured should be same as that on the infrastructure WLAN.
Handshake Basic Rate	Set the basic rate of exchange of handshake packets between the client-bridge and infrastructure WLAN Access Points. The options are highest and normal. The default value is highest.

21 Refer to the **Channel Lists** field and define the list of channels the client-bridge radio scans when scanning for an infrastructure WLAN.

Band A	Define a list of channels for scanning across all the channels in the 5.0 GHz radio band.
Band BG	Define a list of channels for scanning across all the channels in the 2.4 GHz radio band.

22 Refer to the **Keepalive Parameters** field and define the following configurations:

Keepalive Type	Set the keepalive frame type exchanged between the client-bridge and infrastructure Access Points. This is the type of packets exchanged between the client-bridge and infrastructure Access Points, at specified intervals, to keep the client-bridge link up and active. The options are *null-data* and *WNMP* packets. The default value is null-data.
Keepalive Interval	Set the keepalive interval from 0 to 86,400 seconds. This is the interval between two successive keepalive frames exchanged between the client-bridge and infrastructure Access Points. The default value is 300 seconds.

Inactivity Timeout	Set the inactivity timeout for each bridge MAC address from 0 to 8,64,000 seconds. This is the time for which the client-bridge Access Point waits before deleting a wired/wireless client's MAC address from which a frame has not been received for more than the time specified here. For example, if the inactivity time is set at 120 seconds, and if no frames are received from a client (MAC address) for 120 seconds, it is deleted. The default value is 600 seconds.

23 Refer to the **Radio Link Behaviour** field and define the following configurations:

Shutdown Other Radio when Link Goes Down	Select this option to enable shutting down of the *non-client bridge* radio (this is the radio to which wireless-clients associate) when the link between the *client-bridge* and *infrastructure* Access Points is lost. When enabled, wireless clients associated with the non-client bridge radio are pushed to search for and associate with other Access Points having backhaul connectivity. This option is disabled by default. If enabling this option, specify the time for which the non-client bridge radio is shut down. Use the spinner to specify a time from 1 - 1,800 seconds.
Refresh VLAN Interface when Link Comes Up	Select this option to enable the SVI to refresh on re-establishing client bridge link to the infrastructure Access Point. If using a DHCP assigned IP address, it also causes a DHCP renew. This option is enabled by default.

24 Refer to the **Roam Criteria** field and define the following configuration:Select **OK** to save or override the

Seconds for Missed Beacons	Set the interval from 0 - 60 seconds. This is the time for which the client-bridge Access Point waits, after missing a beacon from the associated infrastructure WLAN Access Point, before roaming to another infrastructure Access Point. For example, if the missed-beacon time is set to 30 seconds, and if more than 30 seconds have passed since the last beacon was received from the associated infrastructure Access Point, the client-bridge Access Point resumes scanning for another infrastructure Access Point. The default value s 20 seconds.
Minimum Signal Strength	Set the minimum signal-strength threshold for signals received from the infrastructure Access Point. Specify a value from -128 to -40 dBm. If the RSSI value of signals received from the infrastructure Access Point falls below the value specified here, the client-bridge Access Point resumes scanning for another infrastructure Access Point. The default is -75 dBm.

25 Select **OK** to save or override the changes to the Client Bridge Settings screen. Select **Reset** to revert to the last saved configuration.

26 Select the **Advanced Settings** tab.

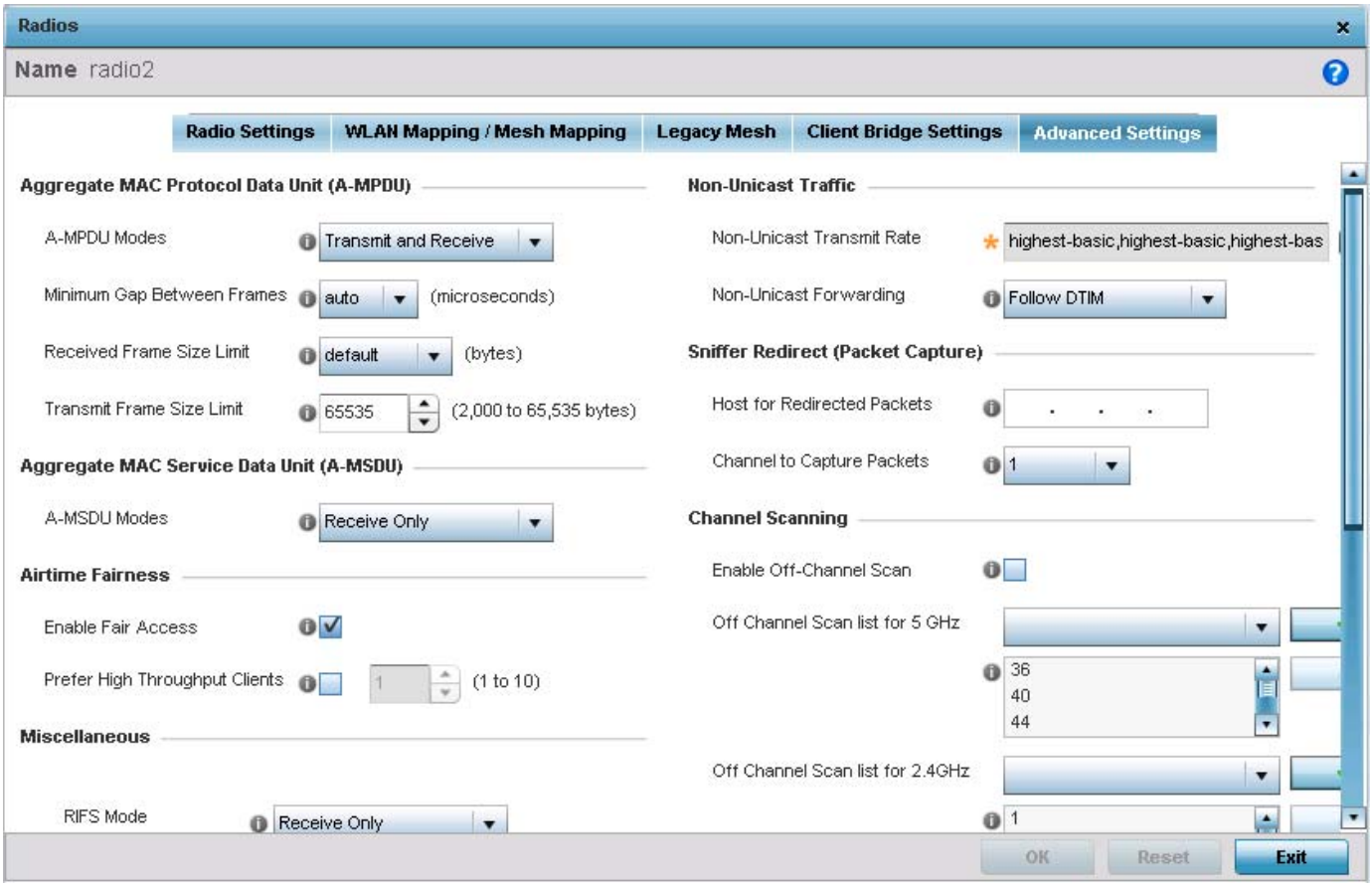


Figure 8-35 *Access Point Radio - Advanced Settings screen*

27 Refer to the **Aggregate MAC Protocol Data Unit (A-MPDU)** field to define how MAC service frames are aggregated by the Access Point radio.

A-MPDU Modes	Use the drop-down menu to define the A-MPDU mode supported. Options include *Transmit Only*, *Receive Only*, *Transmit and Receive* and *None*. The default value is Transmit and Receive. Using the default value, long frames can be both sent and received (up to 64 KB). When enabled, define either a transmit or receive limit (or both).
Minimum Gap Between Frames	Use the drop-down menu to define the minimum gap between A-MPDU frames (in microseconds). A setting of *auto* defines the gap as system defined. The default value is 4 microseconds.
Received Frame Size Limit	If a support mode is enabled allowing A-MPDU frames, define an advertised maximum limit for received A-MPDU aggregated frames. Options include *8191*, *16383*, *32767* or *65535* bytes. The default value is 65535 bytes.
Transmit Frame Size Limit	Use the spinner control to set limit on transmitted A-MPDU aggregated frames. The available range is between 2,000 - 65,535 bytes). The default value is 65535 bytes.

28 Use the **A-MSDU Modes** drop-down menu in the **Aggregate MAC Service Data Unit (A-MSDU)** section to set the supported A-MSDU mode.

Available modes include *Receive Only* and *Transmit and Receive*. Transmit and Receive is the default value. Using Transmit and Receive, frames up to 4 KB can be sent and received. The buffer limit is not configurable.

29 Use the **Airtime Fairness** fields to optionally prioritize wireless access to devices.

Select **Prefer High Throughput Clients** to prioritize clients with higher throughput (802.11n clients) over clients with slower throughput (802.11 a/b/g) clients. Use the spinner control to set a weight for the higher throughput clients.

Enable Fair Access	Select *Enable Fair Access* to enable this feature and provide equal access client access to radio resources.
Prefer High Throughput Clients	Select *Prefer High Throughput Clients* to prioritize clients with higher throughput (802.11n clients) over clients with slower throughput (802.11 a/b/g) clients. Use the spinner control to set a weight for the higher throughput clients.

30 Set or override the following **Miscellaneous** advanced radio settings:

RIFS Mode	Define a RIFS mode to determine whether interframe spacing is applied to Access Point transmissions or received packets, both, or neither The default mode is *Transmit and Receive*. Interframe spacing is an interval between two consecutive Ethernet frames to enable a brief recovery between packets and allow target devices to prepare for the reception of the next packet. Consider setting this value to *None* for high priority traffic to reduce packet delay.
STBC Mode	Select a *space–time block coding* (STBC) option to transmit multiple data stream copies across Access Point antennas to improve signal reliability. An Access Point's transmitted signal traverses a problematic environment, with scattering, reflection and refraction all prevalent. The signal can be further corrupted by noise at the receiver. Consequently, some of the received data copies are less corrupt and better than others. This redundancy means there's a greater chance of using one, or more, of the received copies to successfully decode the signal. STBC effectively combines all the signal copies to extract as much information from each as possible.
Transmit Beamforming	Enable beamforming to steer signals to peers in a specific direction to enhance signal strength and improve throughput amongst meshed devices (not clients). Each Access Point radio support up to 16 beamforming capable mesh peers. When enabled, a *beamformer* steers its wireless signals to its peers. A *beamformee* device assists the beamformer with channel estimation by providing a *feedback* matrix. The feedback matrix is a set of values sent by the beamformee to assist the beamformer in computing a *steering* matrix. A steering matrix is an additional set of values used to steer wireless signals at the beamformer so constructive signals arrive at the beamformee for better SNR and throughput. Any beamforming capable mesh peer connecting to a radio whose capacity is exhausted cannot enable beamforming itself. Transmit beamforming is available on AP81XX (AP8122, AP8132 and AP8163) model Access Points only, and is disabled by default.

31 Set the following **Aeroscout Properties**:

Forward	Select enable to forward Aeroscout packets to a specified MAC address. Aeroscout tags associate with an Access Point, then communicate with a location engine. This setting is disabled by default.
MAC to be forwarded	Specify the MAC address to be forwarded.

32 Set the following **Ekahau Properties**:

Forward Host	Specify the Ekahau engine IP address. Using Ekahau small, battery powered Wi-Fi tags are attached to tracked assets or carried by people. Ekahau processes locations, rules, messages and environmental data and turns the information into locationing maps, alerts and reports.
Forwarding Port	Use the spinner control to set the Ekahau TZSP port used for processing information from locationing tags.
MAC to be forwarded	Specify the MAC address to be forwarded.

33 Set the following **Non-Unicast Traffic** values for the profile's supported Access Point radio and its connected wireless clients:

Broadcast/Multicast Transmit Rate	Use the drop-down menu to define the data rate broadcast and multicast frames are transmitted. Seven different rates are available, if the not using the same rate for each BSSID, each with a separate menu.
Broadcast/Multicast Forwarding	Define whether client broadcast and multicast packets should always follow DTIM, or only follow DTIM when using Power Save Aware mode. The default setting is Follow DTIM.

34 Refer to the **Sniffer Redirect (Packet Capture)** field to define the radio's captured packet configuration.

Host for Redirected Packets	If packets are re-directed from a connected Access Point radio, define an IP address for a resource (additional host system) used to capture the re-directed packets. This address is the numerical (non DNS) address of the host used to capture the re-directed packets.
Channel to Capture Packets	Use the drop-down menu to specify the channel used to capture re-directed packets. The default value is channel 1.

35 Refer to the **Channel Scanning** field to define the radio's captured packet configuration.

Enable Off-Channel Scan	Enable this option to scan across all channels using this radio. Channel scans use Access Point resources and can be time consuming, so only enable when your sure the radio can afford the bandwidth be directed towards to the channel scan and does not negatively impact client support.
Off Channel Scan list for 5GHz	Define a list of channels for off channel scans using the 5GHz Access Point radio. Restricting off channel scans to specific channels frees bandwidth otherwise utilized for scanning across all the channels in the 5GHz radio band.
Off Channel Scan list for 2.4GHz	Define a list of channels for off channel scans using the 2.4GHz Access Point radio. Restricting off channel scans to specific channels frees bandwidth otherwise utilized for scanning across all the channels in the 2.4GHz radio band.
Max Multicast	Set the maximum number (from 0 - 100) of multicast/broadcast messages used to perform off channel scanning. The default setting is 4.
Scan Interval	Set the interval (from 2 - 100 dtims) off channel scans occur. The default setting is 20dtims.
Sniffer Redirect	Specify the IP address of the host to which captured off channel scan packets are redirected.

36 If deploying an AP7161 or AP7181 model Access Point, the following **AP7161** settings are available:

Enable Antenna Downtilt	Enable this settings to allow the Access Point to physically transmit in a downward orientation (ADEPT mode).
Extended Range	Set an extended range (from 1 - 25 kilometers) to allow AP7161 and AP7181 model Access Points to transmit and receive with their clients at greater distances without being timed out.

37 Select **OK** to save the changes to the Advanced Settings screen. Select **Reset** to revert to the last saved configuration.

8.7.6 WAN Backhaul Configuration

Profile Interface Configuration

A *Wireless Wide Area Network* (WWAN) card is a specialized network interface card that allows a network device to connect, transmit and receive data over a Cellular Wide Area Network. The AP7161, RFS4000 and RFS6000 all have a PCI Express card slot that supports 3G WWAN cards. The WWAN card uses *point-to-point protocol* (PPP) to connect to the *Internet Service Provider* (ISP) and gain access to the Internet. PPP is the protocol used for establishing internet links over dial-up modems, DSL connections, and many other types of point-to-point communications. PPP packages your system's TCP/IP packets and forwards them to the serial device where they can be put on the network. PPP is a full-duplex protocol used on various physical media, including twisted pair or fiber optic lines or satellite transmission. It uses a variation of *High Speed Data Link Control* (HDLC) for packet encapsulation.

Nx4500 and NX6500 series services platforms support an optional NX Expansion module for modular WAN and Telephony Gateway support. The NX Series Expansion Module kit (KT-NXMODC-01) allows for the installation and implementation of up to four *Peripheral Component Interconnect Express* (PCIe) cards. The Expansion Module kit can be installed in NX4500, NX4524, NX6500 or NX6524 model services platforms.

To define a WAN Backhaul configuration:

1 Select **Configuration** > **Profiles** > **Interface**.

2 Expand the Interface menu to display its submenu options.

3 Select **WAN Backhaul**.

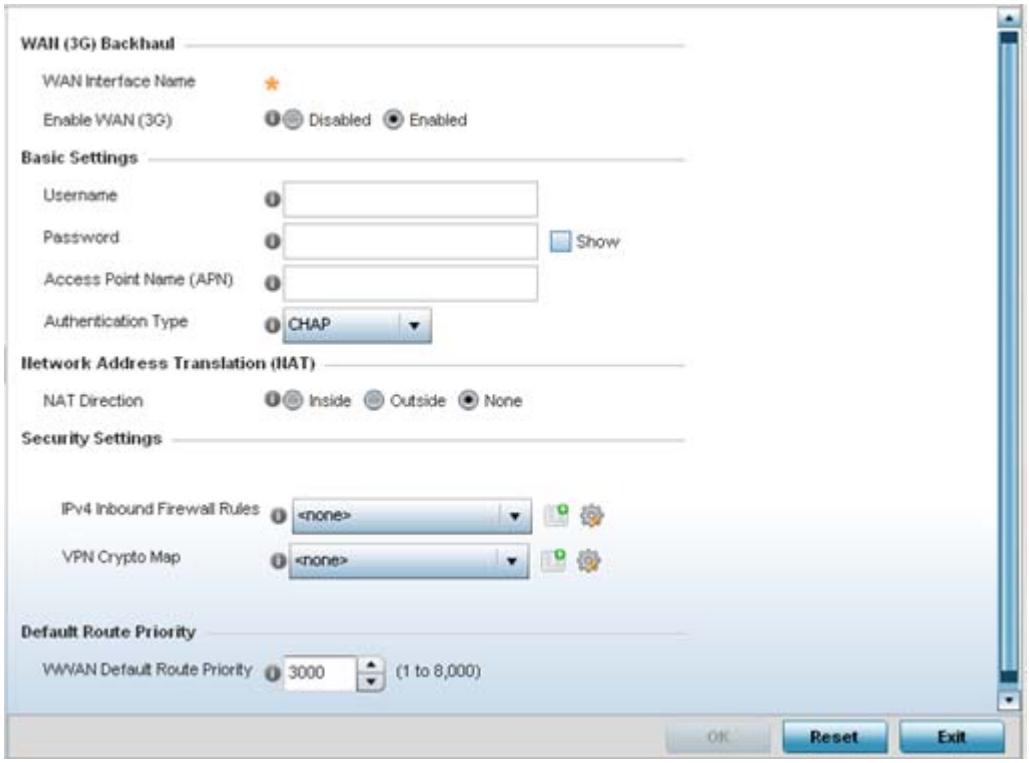


Figure 8-36 *Profile -WAN Backhaul screen*

4 Refer to the **WAN (3G) Backhaul** configuration to specify WAN card settings:

WAN Interface Name	Displays the WAN Interface name for the WAN 3G Backhaul card.
Enable WAN (3G)	Select this option to enable 3G WAN card support on the device. A supported 3G card must be connected to the device for this feature to work.

5 Set the following authentication parameters from within the **Basic Settings** field:

Username	Provide a 32 character maximum username for authentication support by the cellular data carrier.
Password	Provide a password for authentication support by the cellular data carrier.
Authentication Type	Use the drop-down menu to specify authentication type used by your cellular data provider. Supported authentication types are *None*, *PAP*, *CHAP*, *MSCHAP*, and *MSCHAP-v2*.

6 Define the following NAT parameters from within the **Network Address Translation (NAT)** field:

NAT Direction	Define the *Network Address Translation* (NAT) direction. Options include: *Inside* - The inside network is transmitting data over the network its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address. *Outside* - Packets passing through the NAT on the way back to the controller or service platform managed LAN are searched against to the records kept by the NAT engine. There, the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the network. *None* - No NAT activity takes place. This is the default setting.

7 Define the following security parameters from within the **Security Settings** field:

IPv4 Inbound Firewall Rules	Use the drop-down menu to select an inbound IPv4 ACL to associate with traffic on the WAN backhaul. This setting pertains to IPv4 inbound traffic only and not IPv6. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity. If an appropriate IP ACL does not exist, select the *Add* button to create a new one.
VPN Crypto Map	If necessary, specify a crypto map for the wireless WAN. A crypto map can be up to 256 characters long. If a suitable crypto map is not available, click the *Create* button to configure a new one.

8 Define the following route parameters from within the **Default Route Priority** field:

WWAN Default Route Priority	Use the spinner control to define a priority from 1 - 8,000 for the default route learned by the wireless WAN. The default value is 3000.

9 Select **OK** to save the changes to the screen. Select **Reset** to revert to the last saved configuration.

8.7.7 PPPoE Configuration

Profile Interface Configuration

PPP over Ethernet (PPPoE) is a data-link protocol for dialup connections. PPPoE allows an Access Point to use a broadband modem (DSL, cable modem, etc.) for access to high-speed data and broadband networks. Most DSL providers are currently supporting (or deploying) the PPPoE protocol. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables a point-to-point connection to an ISP over existing Ethernet interface.

To provide a point-to-point connection, each PPPoE session determines the Ethernet address of a remote PPPoE client, and establishes a session. PPPoE uses both a discover and session phase to identify a client and establish a point-to-point connection. By using such a connection, a Wireless WAN failover is available to maintain seamless network access if the Wired WAN were to fail.

NOTE: Devices with PPPoE enabled continue to support VPN, NAT, PBR and 3G failover over the PPPoE interface. Multiple PPPoE sessions are supported using a single user account user account if RADIUS is configured to allow simultaneous access.

When PPPoE client operation is enabled, it discovers an available server and establishes a PPPoE link for traffic slow. When a wired WAN connection failure is detected, traffic flows through the WWAN interface in fail-over mode (if the WWAN network is configured and available). When the PPPoE link becomes accessible again, traffic is redirected back through the Access Point's wired WAN link.

When the Access Point initiates a PPPoE session, it first performs a discovery to identify the Ethernet MAC address of the PPPoE client and establish a PPPoE session ID. In discovery, the PPPoE client discovers a server to host the PPPoE connection.

To create a PPPoE point-to-point configuration

1 Select **Configuration** > **Profiles** > **Interface**.

2 Expand the Interface menu to display its submenu options.

3 Select **PPPoE**.

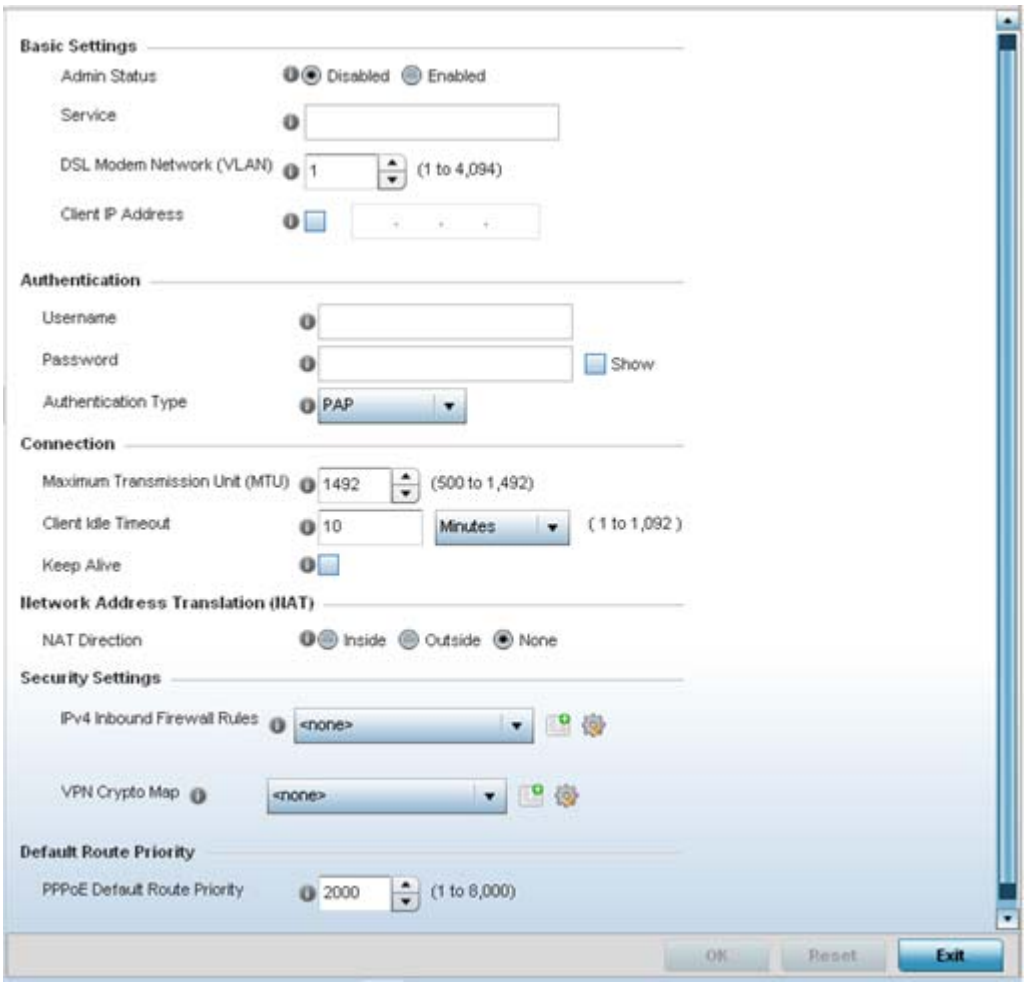


Figure 8-37 *Profile -PPPoE screen*

4 Use the **Basic Settings** field to enable PPPoE and define a PPPoE client

Admin Status	Select *Enable* to support a high speed client mode point-to-point connection using the PPPoE protocol. The default setting is disabled.
Service	Enter the 128 character maximum PPPoE client service name provided by the service provider.

DSL Modem Network (VLAN)	Use the spinner control to set the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to DSL modem. The available range is 1 - 4,094. The default VLAN is VLAN1.
Client IP Address	Provide the numerical (non hostname) IP address of the PPPoE client.

5 Define the following **Authentication** parameters for PPPoE client interoperation:

Username	Provide the 64 character maximum username used for authentication support by the PPPoE client.
Password	Provide the 64 character maximum password used for authentication by the PPPoE client.
Authentication Type	Use the drop-down menu to specify authentication type used by the PPPoE client, and whose credentials must be shared by its peer Access Point. Supported authentication options include *None, PAP, CHAP, MSCHAP*, and *MSCHAP-v2*.

6 Define the following **Connection** settings for the PPPoE point-to-point connection with the PPPoE client:

Maximum Transmission Unit (MTU)	Set the PPPoE client *maximum transmission unit* (MTU) from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492.
Client Idle Timeout	Set a timeout in either *Seconds* (1 - 65,535), *Minutes* (1 - 1,092) or *Hours* (1 - 18). The Access Point uses the defined timeout so it does not sit idle waiting for input from the PPPoE client and server that may never come. The default setting is 10 minutes.
Keep Alive	Select this option to ensure the point-to-point connection to the PPPoE client is continuously maintained and not timed out. This setting is disabled by default.

7 Set the **Network Address Translation (NAT)** direction for the PPPoE configuration.

Network Address Translation (NAT) converts an IP address in one network to a different IP address or set of IP addresses in another network. The Access Point maps its local (Inside) network addresses to WAN (Outside) IP addresses, and translates the WAN IP addresses on incoming packets to local IP addresses. NAT is useful because it allows the authentication of incoming and outgoing requests, and minimizes the number of WAN IP addresses needed when a range of local IP addresses is mapped to each WAN IP address. The default setting is None (neither inside or outside).

8 Define the following **Security Settings** for the PPPoE configuration:

IPv4 Inbound Firewall Rules	Use the drop-down menu to select a firewall (set of IP access connection rules) to apply to the PPPoE client connection. If a firewall rule does not exist suiting the data protection needs of the PPPoE client connection, select the *Create* icon to define a new rule configuration or the *Edit* icon to modify an existing rule. For more information, see *Setting an IPv4 or IPv6 Firewall Policy on page 10-21*.
VPN Crypto Map	Use the drop-down menu to apply an existing crypt map configuration to this PPPoE interface. Crypto Maps are sets of configuration parameters for encrypting packets that pass through the VPN Tunnel.

9 Use the spinner control to set the **Default Route Priority** for the default route learnt using PPPoE. Select from 1 - 8,000. The default setting is 2,000.

10 Select **OK** to save the changes to the PPPoE screen. Select **Reset** to revert to the last saved configuration. Saved configurations are persistent across reloads.

8.7.8 Bluetooth Configuration

Profile Interface Configuration

AP-8432 and AP-8533 model Access Points utilize a built in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network. AP-8432 and AP-8533 models support both Bluetooth *classic* and Bluetooth *low energy* technology. These platforms can use their Bluetooth classic enabled radio to sense other Bluetooth enabled devices and report device data (MAC address, RSSI and device calls) to an ADSP server for intrusion detection. If the device presence varies in an unexpected manner, ADSP can raise an alarm.

NOTE: AP-8132 model Access Points support an external USB Bluetooth radio providing ADSP Bluetooth classic sensing functionality only, not the Bluetooth low energy beaconing functionality available for AP-8432 and AP-8533 model Access Points described in this section.

AP-8432 and AP-8533 model Access Points support Bluetooth beaconing to emit either iBeacon or Eddystone-URL beacons. The Access Point's Bluetooth radio sends non-connectable, undirected *low-energy* (LE) advertisement packets on a periodic basis. These advertisement packets are short, and sent on Bluetooth advertising channels that conform to already-established iBeacon and Eddystone-URL standards. Portions of the advertising packet are still customizable however.

To define a profile's Bluetooth radio interface configuration:

1 Select **Configuration** > **Profiles** > **Interface**.

2 Expand the Interface menu to display its submenu options.

3 Select **Bluetooth**.

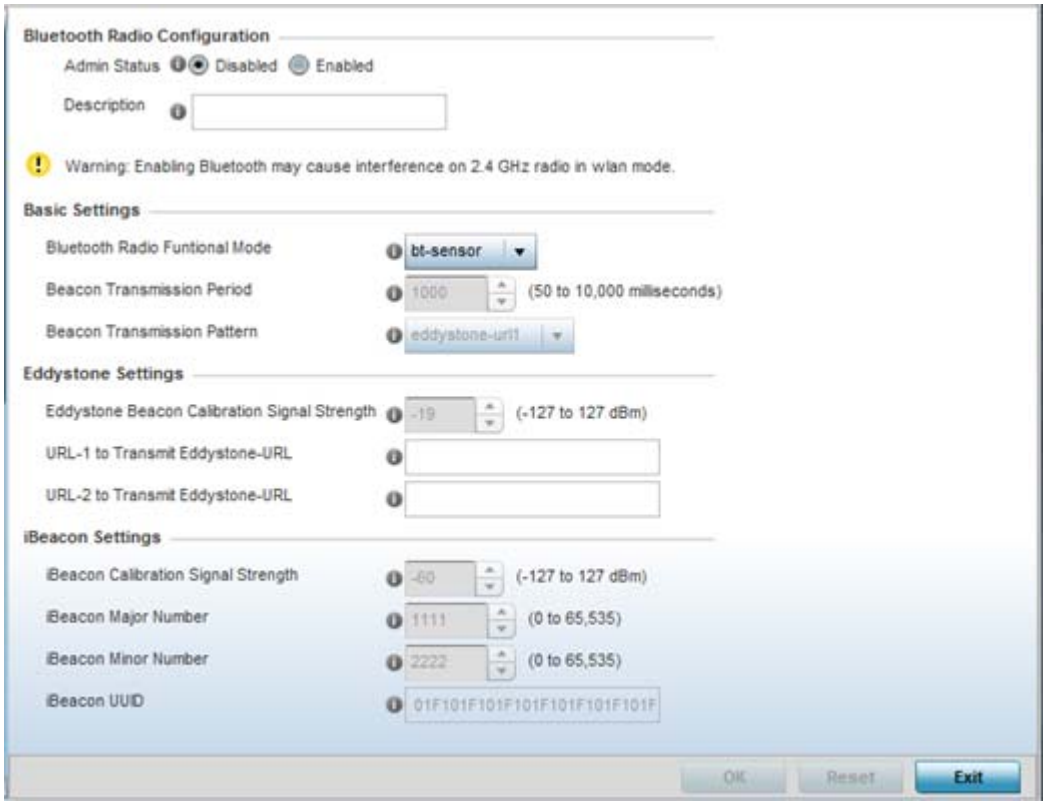


Figure 8-38 *Profile Overrides - Bluetooth screen*

4 Set the following **Bluetooth Radio Configuration**:

Admin Status	*Enable* or *Disable* Bluetooth support capabilities for AP-8432 or AP-8533 model Access Point Bluetooth radio transmissions. The default value is disabled.
Description	Define a 64 character maximum description for the Access Point's Bluetooth radio to differentiate this radio interface from other Bluetooth supported radio's that may be members of the same RF Domain.

5 Set the following **Basic Settings**:

Bluetooth Radio Functional Mode	Set the Access Point's Bluetooth radio functional mode to either *bt-sensor* or *le-beacon*. Use bt-sensor mode for ADSP Bluetooth classic sensing. Use le-beacon mode to have the Access Point transmit both ibeacon and Eddystone-URL low energy beacons. le-beacon is the default setting.
Beacon Transmission Period	Set the Bluetooth radio's beacon transmission period from 100 - 10,000 milliseconds. The default setting is 1,000 milliseconds.

Beacon Transmission Pattern	When the Bluetooth radio's mode is set to le-beacon, use the enabled drop-down menu to set the beacon's emitted transmission pattern to either *eddystone_url1*, *eddystone_url2* or *ibeacon*. An eddystone-URL frame broadcasts a URL using a compressed encoding scheme to better fit within a limited advertisement packet. Once decoded, the URL can be used by a client for Internet access. iBeacon was created by Apple for use in iOS devices (beginning with iOS version 7.0). There are three data fields Apple has made available to iOS applications, a *UUID* for device identification, a *Major* value for device class and a *Minor* value for more refined information like product category.

6 Define the following **Eddystone Settings** if the Beacon Transmission Pattern has been set to either eddystone_url1 or eddystone_url2:

Eddystone Beacon Calibration Signal Strength	Set the eddystone beacon measured calibration signal strength, from -127 to 127 dBm, at 0 meters. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 0 meters. The default setting is -19 dBm.
URL-1 to Transmit Eddystone-URL	Enter a 64 character maximum eddystone-URL1. The URL must be 18 characters or less once auto-encoding is applied. The encoding process is for getting the URL to fit within the beacon's payload.
URL-2 to Transmit Eddystone-URL	Enter a 64 character maximum eddystone-URL2. The URL must be 18 characters or less once auto-encoding is applied. The encoding process is for getting the URL to fit within the beacon's payload.

7 Define the following **iBeacon Settings** if the Beacon Transmission Pattern has been set to iBeacon:

iBeacon Calibration Signal Strength	Set the ibeacon measured calibration signal strength, from -127 to 127 dBm, at 1 meter. Mobile devices can approximate their distance to beacons based on received signal strength. However, distance readings can fluctuate since they depend on several external factors. The closer you are to a beacon, the more accurate the reported distance. This setting is the projected calibration signal strength at 1 meter. The default setting is -60 dBm.
iBeacon Major Number	Set the iBeacon Major value from 0 - 65,535. Major values identify and distinguish groups. For example, each beacon on a specific floor in a building could be assigned a unique major value. The default is 1,111.
iBeacon Minor Number	Set the iBeacon Minor value from 0 - 65,535. Minor values identify and distinguish individual beacons. Minor values help identify individual beacons within a group of beacons assigned a major value. The default setting is 2,222.
iBeacon UUID	Define a 32 hex character maximum UUID. The *Universally Unique IDentifier* (UUID) classification contains 32 hexadecimal digits. The UUID distinguishes iBeacons in the network from all other beacons in networks outside of your direct administration.

8 Select **OK** to save the changes to the Bluetooth configuration. Select **Reset** to revert to the last saved configuration. Saved configurations are persistent across reloads.

8.7.9 Profile Interface Deployment Considerations

Profile Interface Configuration

Before defining a profile's interface configuration (supporting Ethernet port, Virtual Interface, port channel and Access Point radio configurations) refer to the following deployment guidelines to ensure these configuration are optimally effective:

- Power over Ethernet is supported on RFS4000 and RFS6000 model controllers and NX4524 and NX6524 model service platforms only. When enabled, the controller supports 802.3af PoE on each of its ge ports.
- When changing from a default DHCP address to a fixed IP address, set a static route first. This is critical when the controller or service platform is being accessed from a subnet not directly connected to the controller or service platform and the default route was set from DHCP.
- Take care not to modify an Access Point's configuration using its resident Web UI, CLI or SNMP interfaces when managed by a profile, or risk the Access Point having a configuration independent from the profile until the profile can be uploaded to the Access Point once again.

8.8 Profile Network Configuration

Setting a profile's network configuration is a large task comprised of numerous administration activities.

A profile's network configuration process consists of the following:

- *Setting a Profile's DNS Configuration*
- *Setting a Profile's ARP Configuration*
- *Setting a Profile's L2TPV3 Configuration*
- *Setting a Profile's GRE Configuration*
- *Setting a Profile's IGMP Snooping Configuration*
- *Setting a Profile's MLD Snooping Configuration*
- *Setting a Profile's Quality of Service (QoS) Configuration*
- *Setting a Profile's Spanning Tree Configuration*
- *Setting a Profile's Routing Configuration*
- *Setting a Profile's Dynamic Routing (OSPF) Configuration*
- *Setting a Profile's Border Gateway Protocol (BGP) Configuration*
- *Setting a Profile's Forwarding Database Configuration*
- *Setting a Profile's Bridge VLAN Configuration*
- *Setting a Profile's Cisco Discovery Protocol Configuration*
- *Setting a Profile's Link Layer Discovery Protocol Configuration*
- *Setting a Profile's Miscellaneous Network Configuration*
- *Setting a Profile's Alias Configuration*
- *Setting a Profile's IPv6 Neighbor Configuration*

Before beginning any of the profile network configuration activities described in the sections above, review the configuration and deployment considerations available in *Profile Network Configuration and Deployment Considerations*.

8.8.1 Setting a Profile's DNS Configuration

Profile Network Configuration

Domain Naming System (DNS) DNS is a hierarchical naming system for resources connected to the Internet or a private network. Primarily, DNS resources translate domain names into IP addresses. If one DNS server doesn't know how to translate a particular domain name, it asks another one until the correct IP address is returned. DNS enables access to resources using human friendly notations. DNS converts human friendly domain names into notations used by different networking equipment for locating resources.

As a resource is accessed (using human-friendly hostnames), it's possible to access the resource even if the underlying machine friendly notation name changes. Without DNS, in the simplest terms, you would need to remember a series of numbers (123.123.123.123) instead of an easy to remember domain name (for example, *www.domainname.com*).

To define the DNS configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **DNS.**

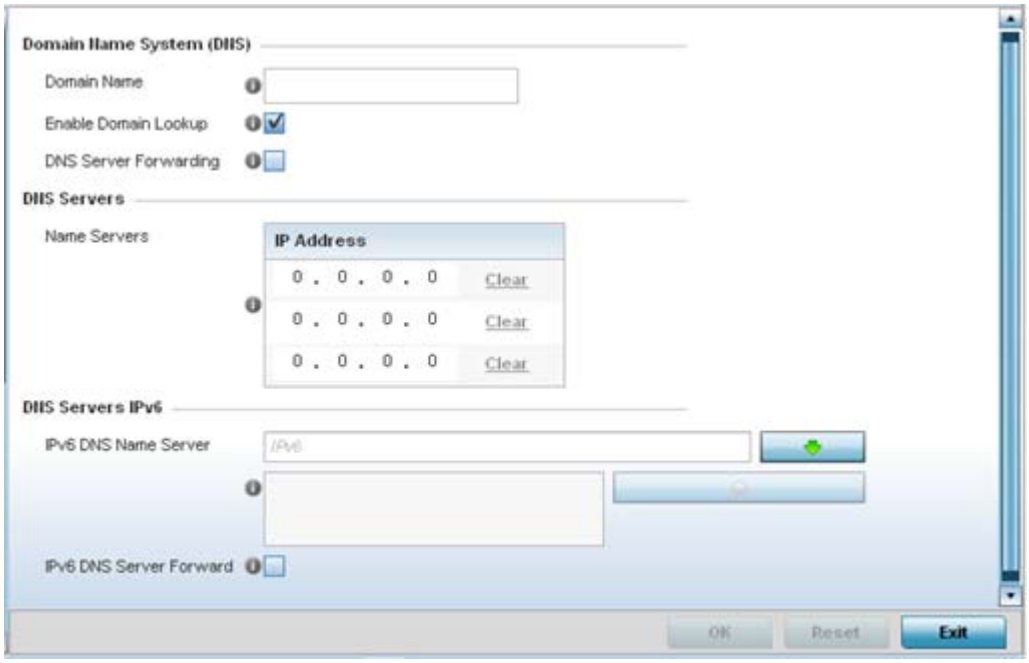


Figure 8-39 *DNS screen*

4 Set the following **Domain Name System (DNS)** configuration data:

Domain Name	Provide the default domain name used to resolve DNS names. The name cannot exceed 64 characters.
Enable Domain Lookup	Select the check box to enable DNS. When enabled, human friendly domain names are converted into numerical IP destination addresses. The radio button is selected by default.
DNS Server Forwarding	Select this option to enable the forwarding DNS queries to external DNS servers if a DNS query cannot be processed by local DNS resources. This feature is disabled by default.

5 Set the following **DNS Server** configuration data:

Name Servers	Provide a list of up to three DNS servers to forward DNS queries if local DNS resources are unavailable. The DNS name servers are used to resolve IP addresses. Use the *Clear* link (next to each DNS server) to clear the DNS name server's IP address from the list.

6 Set the following **DNS Servers IPv6** configuration data when using IPv6:

IPv6 DNS Name Server	Provide the default domain name used to resolve IPv6 DNS names. When an IPv6 host is configured with the address of a DNS server, the host sends DNS name queries to the server for resolution. A maximum of three entries are permitted.
IPv6 DNS Server Forward	Select the check box to enable IPv6 DNS domain names to be converted into numerical IP destination addresses. The setting is disabled by default.

Select **OK** to save the changes made to the DNS configuration. Select **Reset** to revert to the last saved configuration.

8.8.2 Setting a Profile's ARP Configuration

Profile Network Configuration

Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a hardware MAC address recognized on the network. ARP provides protocol rules for making this correlation and providing address conversion in both directions.

When an incoming packet destined for a host arrives, ARP is used to find a physical host or MAC address that matches the IP address. ARP looks in its ARP cache and, if it finds the address, provides it so the packet can be converted to the right packet length and format and sent to its destination. If no entry is found for the IP address, ARP broadcasts a request packet in a special format on the LAN to see if a device knows it has that IP address associated with it. A device that recognizes the IP address as its own returns a reply indicating it. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

To define an ARP supported configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **ARP**.

4 Select **+ Add Row** from the lower right-hand side of the screen to populate the ARP table with rows used to define ARP network address information.

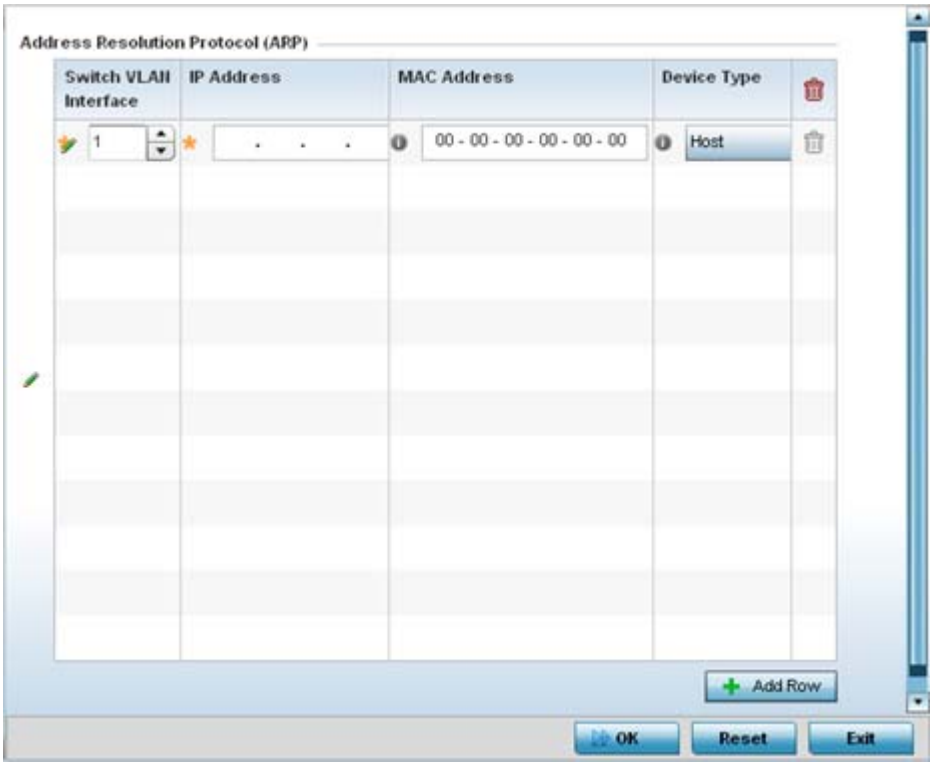


Figure 8-40 *ARP screen*

5 Set the following parameters to define the ARP configuration:

Switch VLAN Interface	Use the spinner control to select a VLAN interface for an address requiring resolution.
IP Address	Define the IP address used to fetch a MAC Address.
MAC Address	Set the target MAC address subject to resolution. This is the MAC used for mapping an IP address to a MAC address recognized on the network.
Device Type	Specify the device type the ARP entry supports. Host is the default setting.

6 To add additional ARP configurations, select **+ Add Row** button and enter the configuration information.

7 Select the **OK** button located at the bottom right of the screen to save the changes to the ARP configuration. Select **Reset** to revert to the last saved configuration.

8.8.3 Setting a Profile's L2TPV3 Configuration

Profile Network Configuration

L2TP V3 is an IETF standard used for transporting different types of layer 2 frames in an IP network (and Access Point profile). L2TP V3 defines control and encapsulation protocols for tunneling layer 2 frames between two IP nodes.

Use L2TP V3 to create tunnels for transporting layer 2 frames. L2TP V3 enables wireless devices to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TP V3 tunnels can be defined between other vendor devices supporting the L2TP V3 protocol.

Multiple pseudowires can be created within an L2TP V3 tunnel. Access Points support an Ethernet VLAN pseudowire type exclusively.

NOTE: A pseudowire is an emulation of a layer 2 point-to-point connection over a *packet-switching network* (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.

Ethernet VLAN pseudowires transport Ethernet frames to and from a specified VLAN. One or more L2TP V3 tunnels can be defined between tunnel end points. Each tunnel can have one or more L2TP V3 sessions. Each tunnel session corresponds to one pseudowire. An L2TP V3 control connection (a L2TP V3 tunnel) needs to be established between the tunneling entities before creating a session.

For optimal pseudowire operation, both the L2TP V3 session originator and responder need to know the psuedowire type and identifier. These two parameters are communicated during L2TP V3 session establishment. An L2TP V3 session created within an L2TP V3 connection also specifies multiplexing parameters for identifying a pseudowire type and ID.

The working status of a pseudowire is reflected by the state of the L2TP V3 session. If a L2TP V3 session is down, the pseudowire associated with it must be shut down. The L2TP V3 control connection keep-alive mechanism can serve as a monitoring mechanism for the pseudowires associated with a control connection.

NOTE: If connecting an Ethernet port to another Ethernet port, the pseudowire type must be *Ethernet port*, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be *Ethernet VLAN*.

To define an L2TPV3 configuration for an Access Point profile:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Expand the **Network** menu and select **L2TPv3**.
The **General** tab displays by default with additional **L2RPv3 Tunnel** and **Manual Session** tabs available.

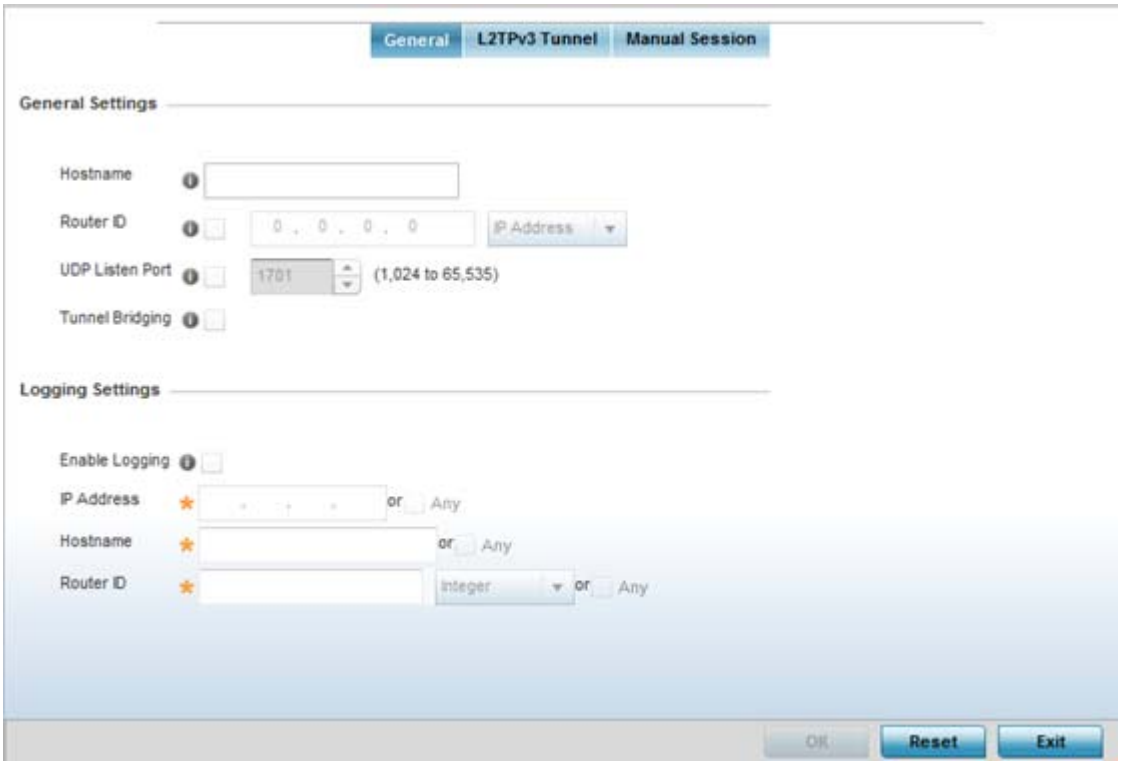


Figure 8-41 *Network - L2TPv3 screen, General tab*

4 Set the following **General Settings** for a L2TPv3 profile configuration:

Hostname	Define a 64 character maximum host name to specify the name of the host that's sent tunnel messages. Tunnel establishment involves exchanging 3 message types (*SCCRQ*, *SCCRP* and *SCCN*) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host.
Router ID	Set either the numeric IP address or the integer used as an identifier for tunnel AVP messages. AVP messages assist in the identification of a tunnelled peer.
UDP Listen Port	Select this option to set the port used for listening to incoming traffic. Select a port from 1,024 - 65,535.
Tunnel Bridging	Select this option to enable bridge packets between two tunnel end points. This setting is disabled by default.

5 Set the following **Logging Settings** for a L2TPv3 profile configuration:

Enable Logging	Select the is option to enable the logging of Ethernet frame events to and from bridge VLANs and physical ports on a defined IP address, host or router ID. This setting is disabled by default.
IP Address	Optionally use a peer tunnel ID address to capture and log L2TPv3 events. Use *Any* to log any IP address.
Hostname	If not using an IP address for event logging, optionally use a peer tunnel hostname to capture and log L2TPv3 events. Use *Any* to log all hostnames. A Hostname cannot exceed 64 characters.
Router ID	If not using an IP address or a hostname for event logging, use a router ID to capture and log L2TPv3 events. Use *Any* to log all routers.

6 Select the **L2TPv3 Tunnel** tab.

Figure 8-42 *Network - L2TPv3 screen, T2TP tunnel tab*

7 Review the following L2TPv3 tunnel configuration data:

Name	Displays the name of each listed L2TPv3 tunnel assigned upon creation.
Local IP Address	Lists the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address.
MTU	Displays the *maximum transmission unit* (MTU) size for each listed tunnel. The MTU is the size (in bytes) of the largest protocol data unit that the layer can pass between tunnel peers.
Use Tunnel Policy	Lists the L2TPv3 tunnel policy assigned to each listed tunnel.
Local Hostname	Lists the tunnel specific hostname used by each listed tunnel. This is the host name advertised in tunnel establishment messages.
Local Router ID	Specifies the router ID sent in the tunnel establishment messages.
Establishment Criteria	Specifies the criteria required for a tunnel between two peers.
Critical Resource	Specifies the critical resource that should exist for a tunnel between two peers. Critical resources are device IP addresses or interface destinations interpreted as critical to the health of the network. Critical resources allow for the continuous monitoring of these defined addresses. A critical resource, if not available, can result in the network suffering performance degradation. A critical resource can be a gateway, AAA server, WAN interface or any hardware or service on which the stability of the network depends. Critical resources are pinged regularly. If there's a connectivity issue, an event is generated stating a critical resource is unavailable.

Peer IP Address	Specifies the IP address of the tunnel peer device.
Host Name	Specifies the host name of the tunnel device.

8 Either select **Add** to create a new L2TPv3 tunnel configuration, **Edit** to modify an existing tunnel configuration or **Delete** to remove a tunnel from those available to this profile.

9 If creating a new tunnel configuration, assign it a 31 character maximum **Name**. Select **OK** to create a L2TPv3 tunnel.

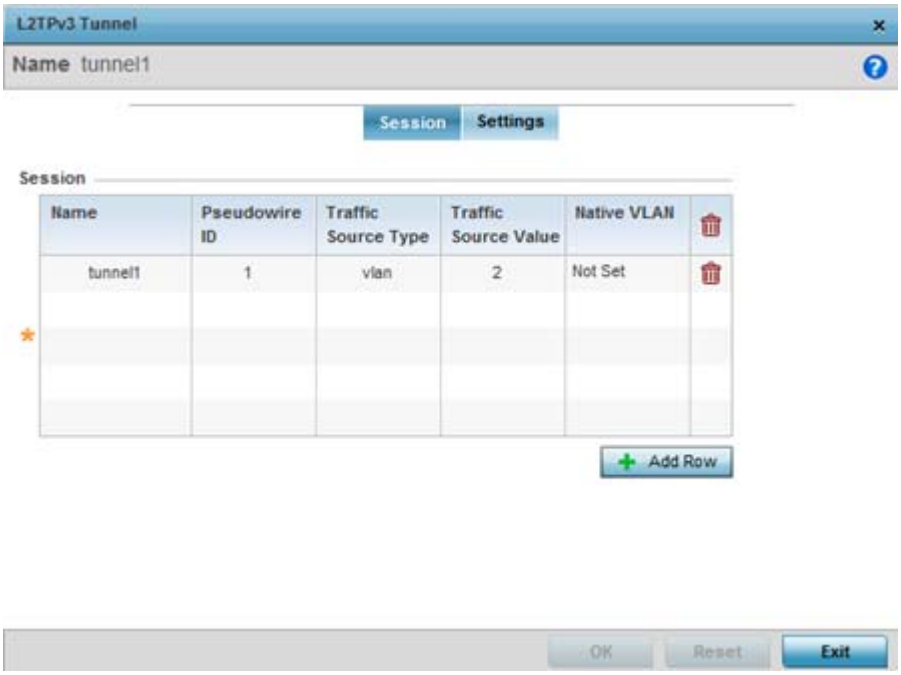


Figure 8-43 *Network - L2TPv3 screen, L2TPv3 Tunnel Session Information*

Refer to the **Session** table to review the configurations of the peers available for tunnel connection. Select **+ Add Row** to populate the table with configurable session parameters for this tunnel configuration.

10 Define the following **Session** values required for the L2TPv3 tunnel configuration:

Name	Enter a 31 character maximum session name. There is no idle timeout for a tunnel. A tunnel is not usable without a session and a subsequent session name. The tunnel is closed when the last session tunnel session is closed.
Pseudowire ID	Define a psuedowire ID for this session. A pseudowire is an emulation of a layer 2 point-to-point connection over a *packet-switching network* (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.
Traffic Source Type	Lists the type of traffic tunnelled in this session (VLAN etc.).
Traffic Source Value	Define a VLAN range to include in the tunnel session. Available VLAN ranges are from 1 - 4,094.
Native	Select this option to provide a VLAN ID that will not be tagged in tunnel establishment and packet transfer.

11 Select **Settings**.

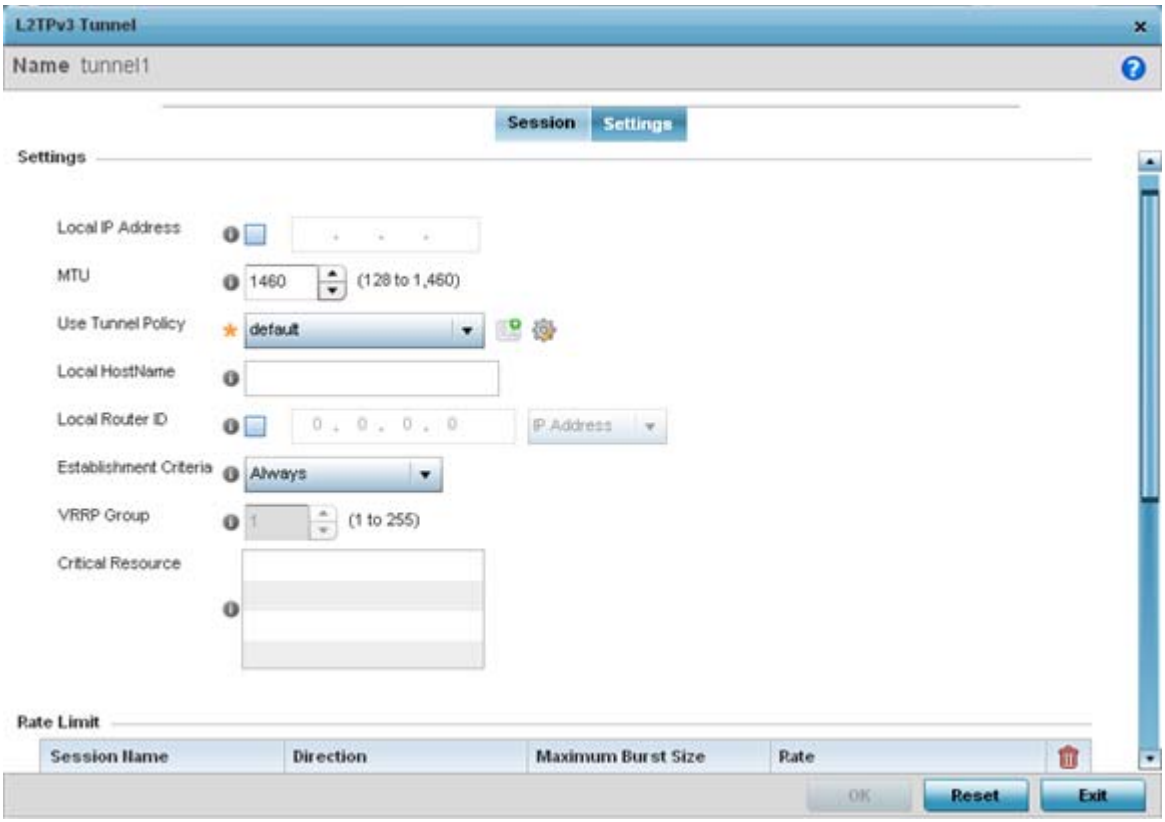


Figure 8-44 *Network - L2TPv3 screen - Add L2TPv3 Tunnel Settings*

12 Define the following **Settings** required for the L2TPv3 tunnel configuration:

Local IP Address	Enter the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address. This parameter is applicable when establishing the tunnel and responding to incoming tunnel create requests.
MTU	Set the *maximum transmission unit* (MTU). The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers. Define a MTU from 128 - 1,460 bytes. The default setting is 1,460. A larger MTU means processing fewer packets for the same amount of data.
Use Tunnel Policy	Select the L2TPv3 tunnel policy. The policy consists of user defined values for protocol specific parameters which can be used with different tunnels. If none is available, a new policy can be created or an existing one can be modified.
Local Hostname	Provide the tunnel specific hostname used by this tunnel. This is the host name advertised in tunnel establishment messages. A Hostname cannot exceed 64 characters.
Local Router ID	Specify the router ID sent in tunnel establishment messages with a target peer device.

Establishment Criteria	Specify the establishment criteria for creating a tunnel. The tunnel is only created if this device is one of the following: vrrp-master cluster-master rf-domain-manager The tunnel is always created if *Always* is selected. This indicates the device need not be any one of the above three (3) to establish a tunnel.
VRRP Group	Set the VRRP group ID. VRRP groups is only enabled when the Establishment Criteria is set to vrrp-master.
Critical Resource	The *Critical Resources* table lists important resources defined for this system. The tunnel is created and maintained only if these critical resources are available. The tunnel is removed if any one of the defined resources goes down or is unreachable.

13 Select **+ Add Row** and define the following **Rate Limit** settings for the L2TPv3 tunnel configuration. Rate limiting limits the maximum rate sent to or received from L2TPv3 tunnel members.

Session Name	Use the drop-down menu to select the tunnel session that will have the direction, burst size and traffic rate settings applied.
Direction	Select the direction for L2TPv3 tunnel traffic rate limiting. *Egress* traffic is outbound L2TPv3 tunnel data coming to the controller, service platform or Access Point. *Ingress* traffic is inbound L2TPv3 tunnel data coming to the controller, service platform or Access Point.
Maximum Burst Size	Set the maximum burst size for egress or ingress traffic rate limiting (depending on which direction is selected) on a L2TPv3 tunnel. Set a maximum burst size between 2 - 1024 kbytes. The smaller the burst, the less likely the upstream packet transmission will result in congestion for L2TPv3 tunnel traffic. The default setting is 320 bytes.
Rate	Set the data rate (from 50 - 1,000,000 kbps) for egress or ingress traffic rate limiting (depending on which direction is selected) for an L2TPv3 tunnel. The default setting is 5000 kbps.
Background	Set the *Random Early Detection* threshold in percentage (%) of the *Maximum Burst Size* value for low priority traffic. The default value is 50%.
Best-Effort	Set the *Random Early Detection* threshold in percentage (%) of the *Maximum Burst Size* value for normal priority traffic. The default value is 50%.
Video	Set the *Random Early Detection* threshold in percentage (%) of the *Maximum Burst Size* value for video traffic. The default value is 25%.
Voice	Set the *Random Early Detection* threshold in percentage (%) of the *Maximum Burst Size* value for voice traffic. The default value is 0%.

Refer to the **Peer** table to review the configurations of the peers available for tunnel connection.

14 Select **+ Add Row** to populate the table with a maximum of two peer configurations.

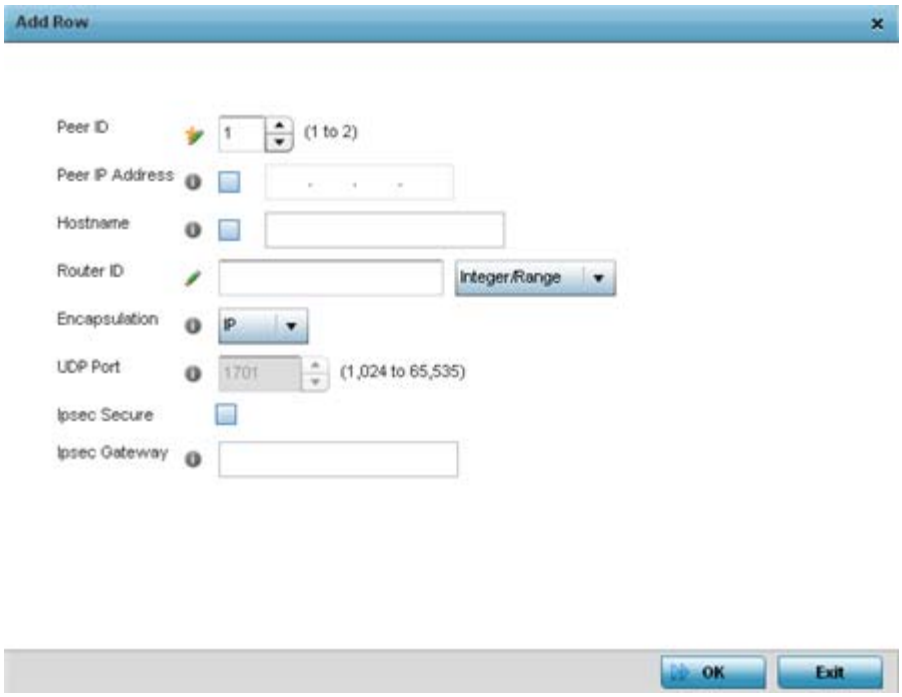


Figure 8-45 *Network - L2TPv3 screen, Add L2TPv3 Peer Configuration*

15 Define the following **Peer** settings:

Peer ID	Define the primary peer ID used to set the *primary* and *secondary* peer for tunnel failover. If the peer is not specified, tunnel establishment does not occur. However, if a peer tries to establish a tunnel with this Access Point, it creates the tunnel if the hostname and/or Router ID matches.
Peer IP Address	Select this option to enter the numeric IP address used as the tunnel destination peer address for tunnel establishment.
Hostname	Assign the peer a hostname used as matching criteria in the tunnel establishment process. A Hostname cannot exceed 64 characters.
Router ID	Specify the router ID sent in tunnel establishment messages with this specific peer.
Encapsulation	Select either *IP* or *UDP* as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes.
UDP Port	If UDP encapsulation is selected, use the spinner control to define the UDP encapsulation port.
IPsec Secure	Enable this option to enable security on the connection between the Access Point and the Virtual Controller resource.
IPsec Gateway	Specify the IP Address of the IPSec's secure gateway resource used to protect tunnel traffic.

16 From back at the **Settings** tab, set the following **Fast Failover** parameters.

Enable	When enabled, the device starts sending tunnel requests on both peers, and in turn, establishes the tunnel on both peers. If disabled, tunnel establishment only occurs on one peer, with failover and other functionality the same as legacy behavior. If fast failover is enabled after establishing a single tunnel the establishment is restarted with two peers. One tunnels defined as active and the other standby. Both tunnels perform connection health checkups with individual hello intervals. This setting is disabled by default.
Enable Aggressive Mode	When enabled, tunnel initiation hello requests are set to zero. For failure detections, hello attempts are not retried, regardless of defined retry attempts. This setting is disabled by default.

17 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

18 Select the **Manual Session** tab.

After a successful tunnel connection and establishment, individual sessions can be created. Each session is a single data stream. After successful session establishment, data corresponding to that session (pseudowire) can be transferred. If a session is down, the pseudowire associated with it is shut down as well.

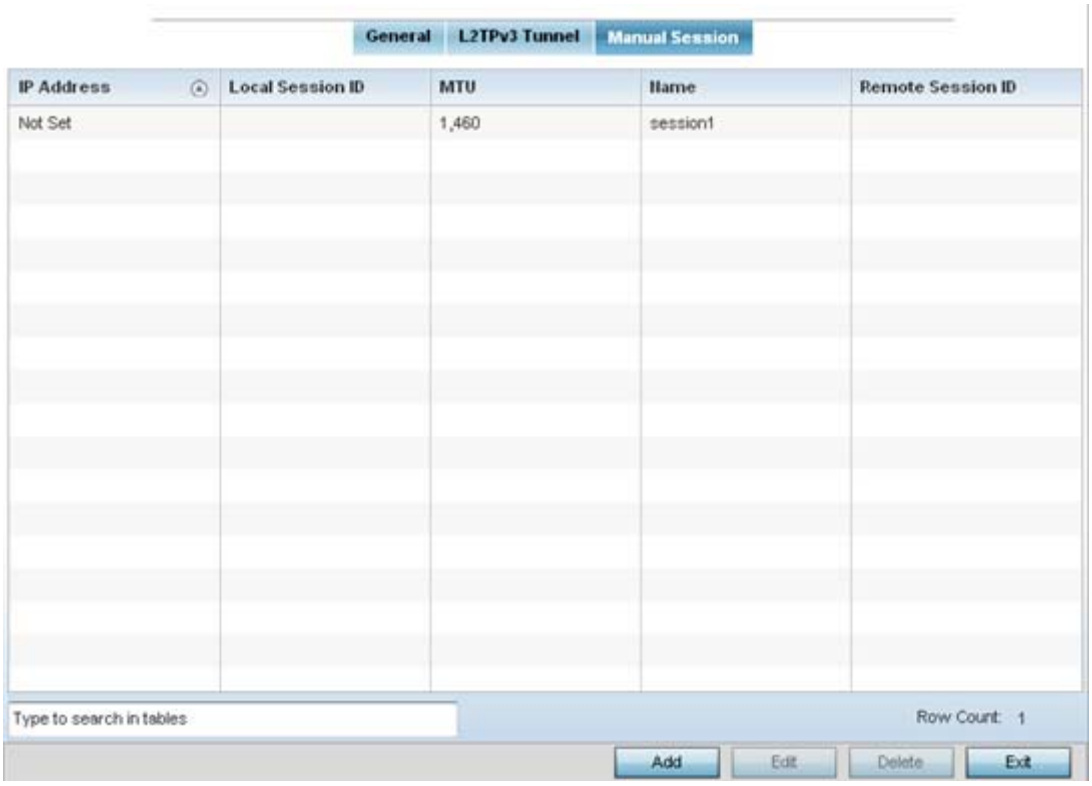


Figure 8-46 *Network - L2TPv3 screen, Manual Session tab*

19 Refer to the following manual session configurations to determine whether one should be created or modified:

IP Address	Lists the IP address assigned as the local tunnel end point address, not the interface IP address. This IP is used as the tunnel source IP address. If this parameter is not specified, the source IP address is chosen automatically based on the tunnel peer IP address. This parameter is applicable when establishing the session and responding to incoming requests.
Local Session ID	Displays the numeric identifier assigned to each listed tunnel session. This is the pseudowire ID for the session. This pseudowire ID is sent in a session establishment message to the L2TP peer.
MTU	Displays each sessions's *maximum transmission unit* (MTU). The MTU is the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data.
Name	Lists the name assigned to each listed manual session.
Remote Session ID	Lists the remote session ID passed in the establishment of the tunnel session.

20 Select **Add** to create a new manual session, **Edit** to modify an existing session configuration or **Delete** to remove a selected manual session.

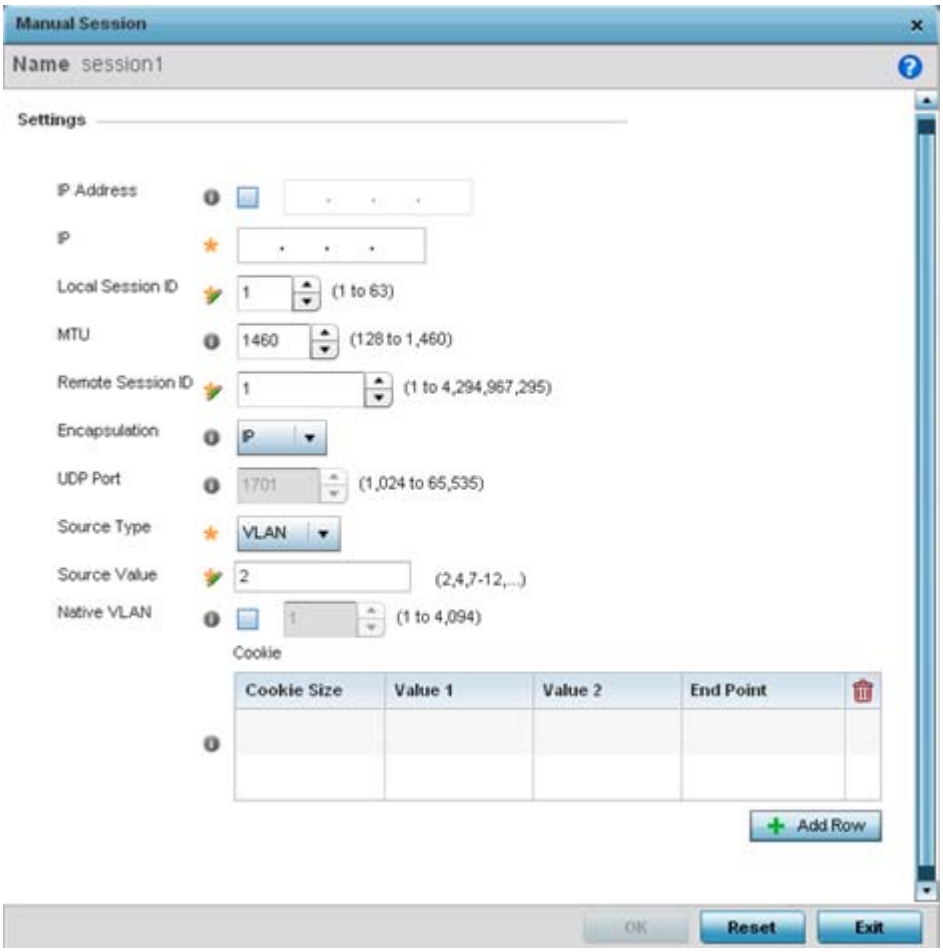


Figure 8-47 *Network - L2TPv3 screen, Add Manual Session Configuration*

21 Set the following **Manual Session** parameters:

Name	Define a 31 character maximum name for this tunnel session. The session is created after a successful tunnel connection and establishment. Each session name represents a single data stream.
IP Address	Specify the IP address used as the tunnel source IP address. If not specified, the tunnel source IP address is selected automatically based on the tunnel peer IP address. This address is applicable only for initiating the tunnel. When responding to incoming tunnel create requests, it would use the IP address received in the tunnel creation request.
IP	Set the IP address of an L2TP tunnel peer. This is the peer allowed to establish the tunnel.
Local Session ID	Set the numeric identifier for the tunnel session. This is the pseudowire ID for the session. This pseudowire ID is sent in session establishment message to the L2TP peer.
MTU	Define the session *maximum transmission unit* (MTU) as the size (in bytes) of the largest protocol data unit the layer can pass between tunnel peers in this session. A larger MTU means processing fewer packets for the same amount of data.
Remote Session ID	Use the spinner control to set the remote session ID passed in the establishment of the tunnel session. Assign an ID in the range of 1 - 4,294,967,295.
Encapsulation	Select either *IP* or *UDP* as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes.
UDP Port	If UDP encapsulation is selected, use the spinner control to define the UDP encapsulation port. This is the port where the L2TP service is running.
Source Type	Select a VLAN as the virtual interface source type.
Source Value	Define the *Source Value* range (1 - 4,094) to include in the tunnel. Tunnel session data includes VLAN tagged frames.
Native VLAN	Select this option to define the native VLAN that will not be tagged.

22 Select the **+ Add Row** button to set the following:

Cookie Size	Set the size of the cookie field within each L2TP data packet. Options include 0, 4 and 8. The default setting is 0.
Value 1	Set the cookie value first word.
Value 2	Set the cookie value second word.
End Point	Define whether the tunnel end point is *local* or *remote.*

23 Select **OK** to save the changes to the configuration. Select **Reset** to revert to the last saved configuration.

8.8.4 Setting a Profile's GRE Configuration

Profile Network Configuration

Generic routing encapsulation (GRE) tunneling can be configured to bridge Ethernet packets between WLANs and a remote WLAN gateway over a GRE tunnel. The tunneling of 802.3 packets using GRE is an alternative to MiNT or L2TPv3. Related features like ACLs for extended VLANs are still available using layer 2 tunneling over GRE.

Using GRE, Access Points map one or more VLANs to a tunnel. The remote endpoint is a user-configured WLAN gateway IP address, with an optional secondary IP address should connectivity to the primary GRE peer be lost. VLAN traffic is expected in both directions in the GRE tunnel. A WLAN mapped to these VLANs can be either open or secure. Secure WLANs require authentication to a remote RADIUS server available within your deployment using standard RADIUS protocols. Access Points can reach both the GRE peer as well as the RADIUS.

Previous releases supported only IPv4 tunnel end points, now support for both IPv4 or IPv6 tunnel endpoints is available. However, a tunnel needs to contain either IPv4 or IPv6 formatted device addresses and cannot be mixed. With the new IPv6 tunnel implementation, all outbound packets are encapsulated with the GRE header, then the IPv6 header. The header source IP address is the local address of the IPv6 address of tunnel interface, and the destination address peer address of the tunnel. All inbound packets are de-capsulated by removing the IPv6 and GRE header before sending it over to the IP stack.

To define a GRE configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **GRE**.

The screen displays existing GRE configurations.

4 Select the **Add** button to create a new GRE tunnel configuration or select an existing tunnel and select **Edit** to modify its current configuration. To remove an existing GRE tunnel, select it from amongst those displayed and select the **Delete** button.

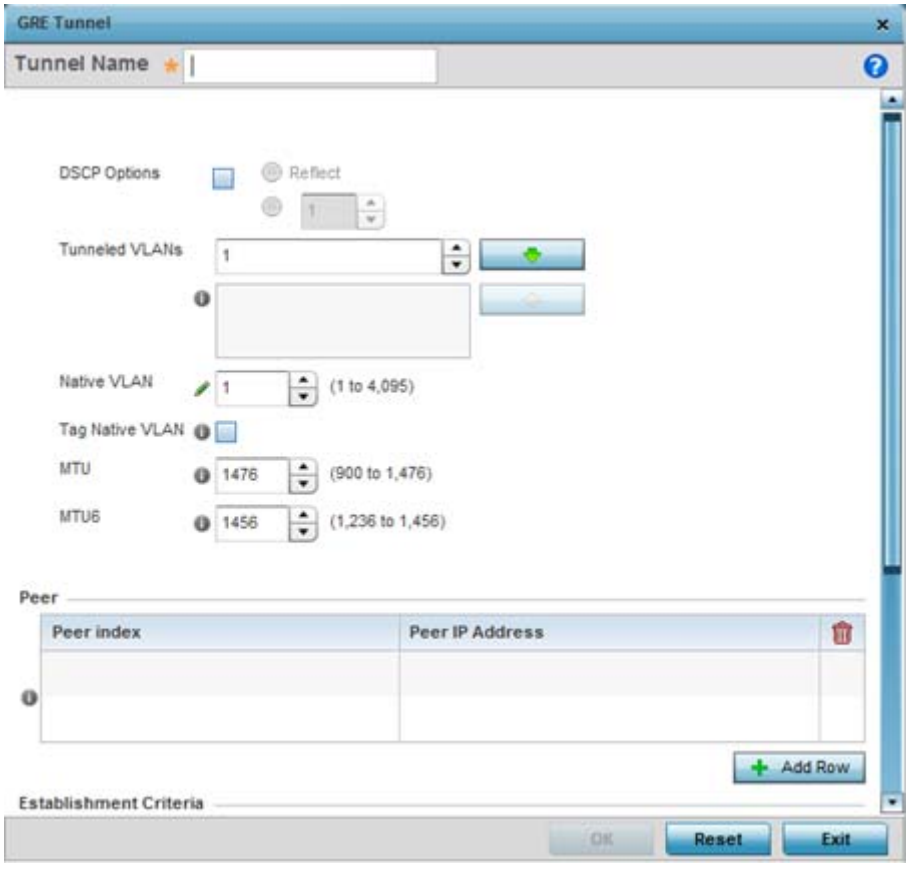


Figure 8-48 *Profile - Network GRE screen*

5 If creating a new GRE configuration, assign it a name to distinguish its configuration.

6 Define the following settings for the GRE configuration:

DSCP Options	Use the spinner control to set the tunnel DSCP / 802.1q priority value from encapsulated packets to the outer packet IPv4 header.
Tunneled VLANs	Define the VLAN connected clients use to route GRE tunneled traffic within their respective WLANs.
Native VLAN	Set a numerical VLAN ID (1 - 4095) for the native VLAN. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.
Tag Native VLAN	Select this option to tag the native VLAN. The IEEE 802.1Q specification is supported for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If the upstream Ethernet device does not support IEEE 802.1Q tagging, it does not interpret the tagged frames. When VLAN tagging is required between devices, both devices must support tagging and be configured to accept tagged VLANs. When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. This feature is disabled by default.
MTU	Set an IPv4 tunnel's *maximum transmission unit* (MTU) from 128 - 1,476. The MTU is the largest physical packet size (in bytes) transmittable within the tunnel. Any messages larger than the MTU are divided into smaller packets before being sent. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. For IPv4, the overhead is 24 bytes (20 bytes IPv4 header + 4 bytes GRE Header), thus the default setting for an IPv4 MTU is 1,476.
MTU6	Set an IPv6 tunnel's MTU from 128 - 1,456. The MTU is the largest physical packet size (in bytes) transmit able within the tunnel. Any messages larger than the MTU are divided into smaller packets before being sent. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. For IPv6, the overhead is 44 bytes (40 bytes IPv6 header + 4 bytes GRE header), thus the default setting for an IPv6 MTU is 1,456.

7 The **Peer** table lists the credentials of the GRE tunnel end points. Add new table rows as needed to add additional GRE tunnel peers.

Select **+ Add Row** to populate the table with a maximum of two peer configurations.

8 Define the following **Peer** parameters:

Peer Index	Assign a numeric index to each peer to help differentiate tunnel end points.
Peer IP Address	Define the IP address of the added GRE peer to serve as a network address identifier. Designate whether the IP is formatted as an IPv4 or IPv6 address. *IPv4* is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike TCP). IPv4 hosts can use link local addressing to provide local connectivity. *IPv6* is the latest revision of the Internet Protocol (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

9 Set the following **Establishment Criteria** for the GRE tunnel configuration:

Criteria	Specify the establishment criteria for creating a GRE tunnel. In a multi-controller within a RF domain, it's always the master node with which the tunnel is established. The tunnel is only created if the tunnel device is designated one of the following: vrrp-master cluster-master rf-domain-manager The tunnel is automatically created if *Always* (default setting) is selected. This indicates the device need not be any one of the above three (3) to establish a tunnel.
VRRP Group	Set the VRRP group ID only enabled when the *Establishment Criteria* is set to *vrrp-master*. A *virtual router redundancy group* (VRRP) enables the creation of a group of routers as a default gateway for redundancy. Clients can point to the IP address of the VRRP virtual router as their default gateway and utilize a different group member if a master becomes unavailable.

10 Define the following **Failover** parameters to apply to the GRE tunnel configuration:

Enable Failover	Select this option to periodically ping the primary gateway to assess its availability for failover support.
Ping Interval	Set the duration between two successive pings to the gateway. Define this value in seconds from 0 - 86,400.
Number of Retries	Set the number of retry ping opportunities before the session is terminated.

11 Select the **OK** button located to save the changes. Select **Reset** to revert to the last saved configuration.

8.8.5 Setting a Profile's IGMP Snooping Configuration

Profile Network Configuration

The *Internet Group Management Protocol* (IGMP) is used for managing IP multicast group members. The controller or service platform listens to IGMP network traffic and forwards the IGMP multicast packets to radios on which the

interested hosts are connected. On the wired side of the network, the controller or service platform floods all the wired interfaces. This feature reduces unnecessary flooding of multicast traffic in the network.

To define a Profile's IGMP settings:

1 Select **Configuration** > **Profiles** > **Network**.

Expand the Network menu to display its submenu options.

Select **IGMP Snooping**.

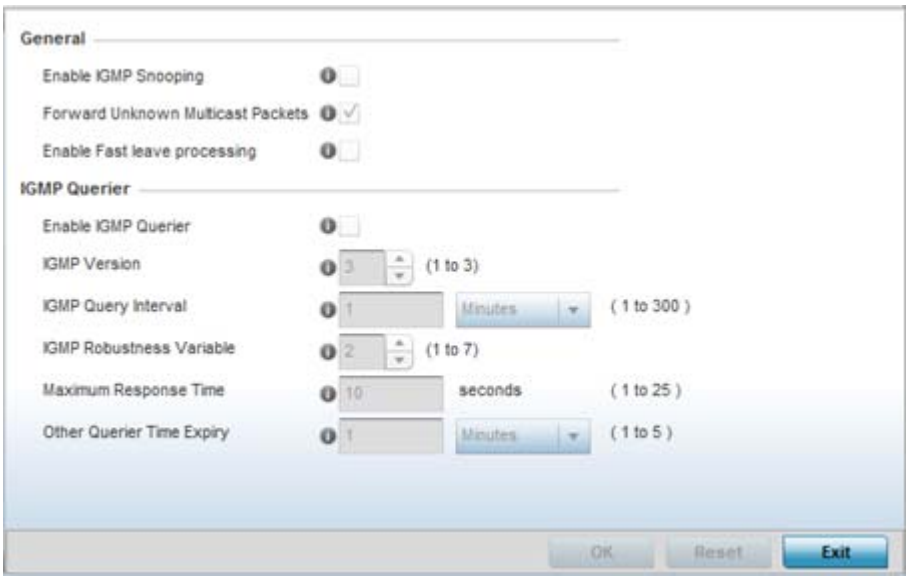


Figure 8-49 *Profile - Network IGMP Snooping screen*

2 Define or override the following **General** IGMP parameters configuration:

Enable IGMP Snooping	Select this option to enable IGMP snooping. If disabled, snooping on a per VLAN basis is also disabled. This feature is enabled by default. If disabled, the settings under the bridge configuration are overridden. For example, if IGMP snooping is disabled, but the bridge VLAN is enabled, the effective setting is disabled.
Forward Unknown Multicast Packets	Select this option to enable the forwarding of multicast packets from unregistered multicast groups. If disabled, the unknown multicast forward feature is also disabled for individual VLANs. This setting is enabled by default.
Enable Fast leave processing	Select this option to remove a Layer 2 LAN interface from the IGMP snooping forwarding table entry without initially sending IGMP group-specific queries to the interface. When receiving a group-specific IGMPv2 leave message, IGMP snooping removes the interface from the Layer 2 forwarding table entry for that multicast group, unless a multicast router was learned on the port. Fast-leave processing enhances bandwidth management for each host on the network.

3 Set or override the following **IGMP Querier** parameters for the profile's bridge VLAN configuration:

Enable IGMP Querier	Select this option to enable IGMP querier. IGMP snoop querier is used to keep host memberships alive. It's primarily used in a network where there's a multicast streaming server and hosts subscribed to the server and no IGMP querier present. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then it is forwarded on that port.
IGMP Version	Use the spinner control to set the IGMP version compatibility to either version 1, 2 or 3. IGMPv1 is defined by RFC 1112, IGMPv2 is defined by RFC 2236 and IGMPv3 defined by RFC 4604 which defines both IGMPv3 and MLDv2. IGMPv2 improves over IGMPv1 by adding the ability for a host to signal desire to leave a multicast group. IGMPv3 improves over IGMPv2 by adding the ability to listen to multicast traffic originating from a set of source IP addresses exclusively. The default setting is 3.
IGMP Query Interval	Set the interval IGMP queries are made. Options include *Seconds* (1 - 18,000), *Minutes* (1 - 300) and *Hours* (1 - 5). The default setting is one minute.
IGMP Robustness Variable	IGMP utilizes a robustness value used by the sender of a query. The robustness variable enables refinements to account for expected packet loss on a subnet. Increasing the robust count allows for more packet loss, but increases the leave latency of the subnetwork unless the value is zero. The default variable is 2.
Maximum Response Time	Specify the maximum interval (from 1 - 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the snooping table. The controller or service platform only forwards multicast packets to radios present in the snooping table. For IGMP reports from wired ports, the controller or service platform forwards these reports to the multicast router ports. The default setting is 10 seconds.
Other Querier Timer Expiry	Specify an interval in either *Seconds* (60 - 300) or *Minutes* (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute.

4 Select the **OK** button located to save the changes. Select **Reset** to revert to the last saved configuration.

8.8.6 Setting a Profile's MLD Snooping Configuration

Profile Network Configuration

Multicast Listener Discovery (MLD) snooping enables a controller, service platform or Access Point to examine MLD packets and make forwarding decisions based on content. MLD is used by IPv6 devices to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups.

MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or Access Point VLANs. When enabled, MLD messages are examined between hosts and multicast routers and to discern which hosts are

receiving multicast group traffic. The controller, service platform or Access Point then forwards multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces.

To set an IPv6 MLD snooping configuration for the profile:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **MLD Snooping**.

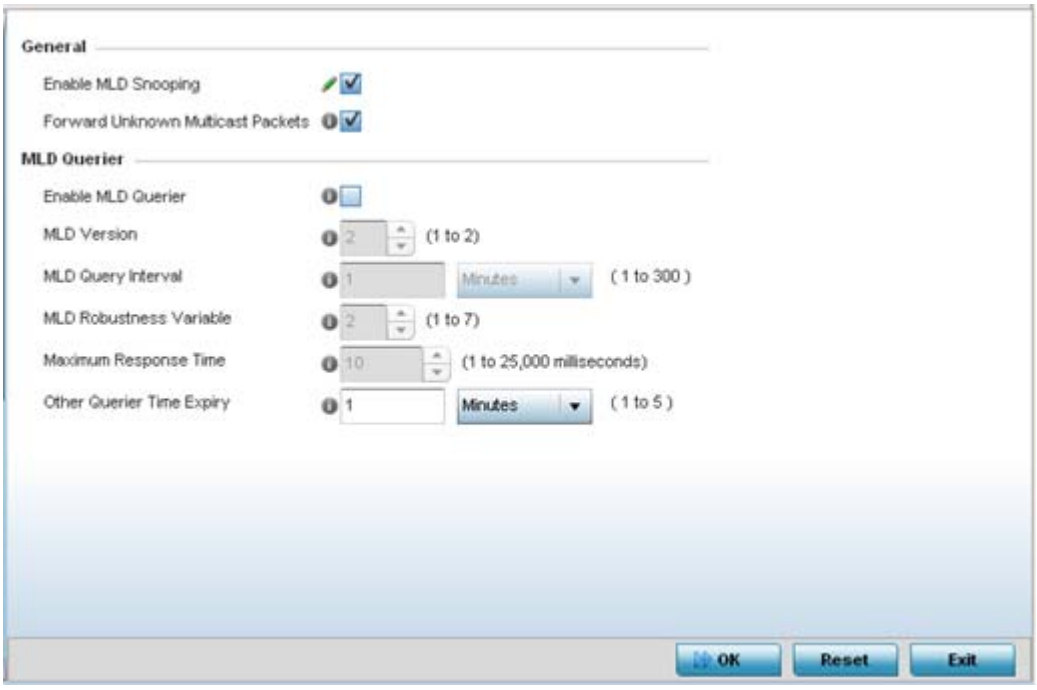


Figure 8-50 *Profile - Network MLD Snooping screen*

4 Define the following **General MLD** snooping settings:

Enable MLD Snooping	Enable MLD snooping to examine MLD packets and provide content forwarding for this profile. Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability, just like IPv6 unicast. MLD snooping is disabled by default.
Forward Unknown Multicast Packets	Use this option to either enable or disable IPv6 unknown multicast forwarding. This setting is enabled by default.

5 Define the following **MLD Querier** settings for the MLD snooping configuration:

Enable MLD Querier	Select the option to enable MLD querier on the controller, service platform or Access Point. When enabled, the device sends query messages to discover which network devices are members of a given multicast group. This setting is disabled by default.
MLD Version	Define whether MLD version *1* or *2* is utilized as the MLD querier. MLD version 1 is based on IGMP version 2 for IPv4. MLD version 2 is based on IGMP version 3 for IPv4 and is fully backward compatible. IPv6 multicast uses MLD version 2. The default MLD version is 2.

MLD Query Interval	Set the interval in which query messages are sent to discover device multicast group memberships. Set an interval in either *Seconds* (1 - 18,000), *Minutes* (1 - 300) or *Hours* (1 - 5). The default interval is 1 minute.
MLD Robustness Variable	Set a MLD IGMP robustness value (1 - 7) used by the sender of a query. The MLD robustness variable enables refinements to account for expected packet loss on a subnet. Increasing the robust count allows for more packet loss, but increases the leave latency of the subnetwork unless the value is zero. The default variable is 2.
Maximum Response Time	Specify the maximum response time (from 1 - 25,000 milliseconds) before sending a responding report. Queriers use MLD reports to join and leave multicast groups and receive group traffic. The default setting is 10 milliseconds.
Other Querier time Expiry	Specify an interval in either *Seconds* (60 - 300) or *Minutes* (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute.

6 Select the **OK** button located to save the changes. Select **Reset** to revert to the last saved configuration.

8.8.7 Setting a Profile's Quality of Service (QoS) Configuration

Profile Network Configuration

QoS values are required to provide priority to some packets over others. For example, voice packets get higher priority than data packets to provide a better quality of service for high priority voice traffic.

The profile QoS screen maps the 6-bit *Differentiated Service Code Point* (DSCP) code points to the older 3-bit IP Precedent field located in the Type of Service byte of an IP header. DSCP is a protocol for specifying and controlling network traffic by class so certain traffic types get precedence. DSCP specifies a specific per-hop behavior applied to a packet.

To define an QoS configuration for DSCP and IPv6 traffic class mappings:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **Quality of Service**.
The **Traffic Shaping** screen displays with the **Basic Configuration** tab displayed by default.

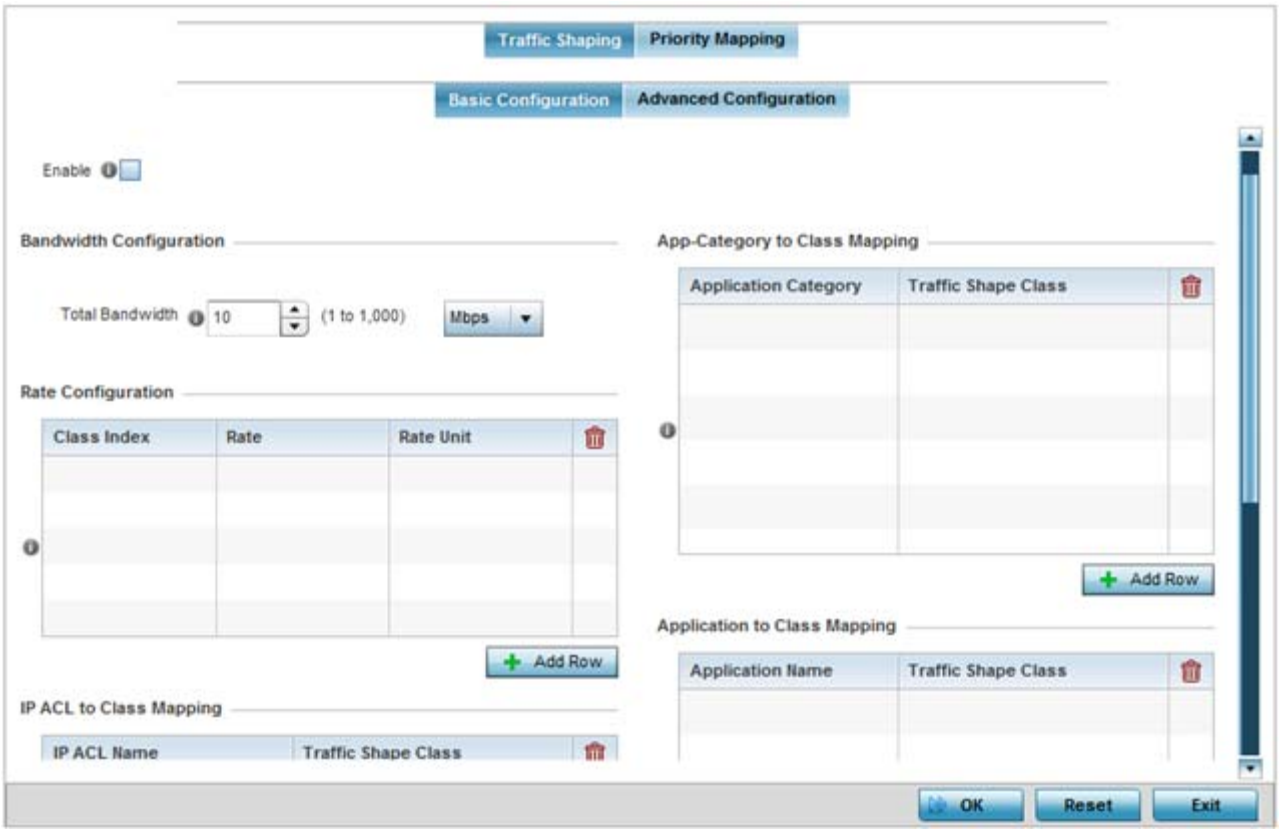


Figure 8-51 *Profile Overrides - Network QoS Traffic Shaping Basic Configuration screen*

Apply traffic shaping to specific applications to apply application categories. When application and ACL rules are conflicting, applications have priority, followed by application categories, then ACLs.

4 Select **Enable** to provide traffic shaping using the defined bandwidth, rate and class mappings.

5 Set the **Total Bandwidth** configurable for the traffic shaper. Set the value from either 1 - 1,000 Mbps, or from 250 - 1,000,000 Kbps.

Select **+ Add Row** within the **Rate Configuration** table to set the **Class Index** (1 - 4) and **Rate** (in either Kbps, Mbps or percentage) for the traffic shaper class. Use the rate configuration to control the maximum traffic rate sent or received on the device. Consider this form of rate limiting on interfaces at the edge of a network to limit traffic into or out of the network. Traffic within the set limit is sent and traffic exceeding the set limit is dropped or sent with a different priority.

Refer to the **IP ACL Class Mapping** table and select **+ Add Row** to apply an IPv4 formatted ACL to the shaper class mapping. Select **+ Add Row** to add mappings. For more information on creating IP based firewall rules, refer to *Configuring IP Firewall Rules on page 10-20* and *Setting an IPv4 or IPv6 Firewall Policy on page 10-21*.

Refer to the **IPv6 ACL Class Mapping** table and select **+ Add Row** to apply an IPv6 formatted ACL to the shaper class mapping. Select **+ Add Row** to add mappings. For more information on creating IP based firewall rules, refer to *Configuring IP Firewall Rules on page 10-20* and *Setting an IPv4 or IPv6 Firewall Policy on page 10-21*.

Refer to the **App-Category to Class Mapping** table and select **+ Add Row** to apply an application category to shaper class mapping. Select **+ Add Row** to add mappings by selecting the application category and its traffic shaper class. For more information on creating an application category, refer to *Application on page 7-58*.

Refer to the **Application to Class Mapping** table and select **+ Add Row** to apply an application to shaper class mapping. Select **+ Add Row** to add mappings by selecting the application and its traffic shaper class. For more information on creating an application, refer to *Application on page 7-58*.

6 Select the **OK** button located to save the changes to the traffic shaping basic configuration. Select **Reset** to revert to the last saved configuration.

7 Select the **Advanced Configuration** tab.

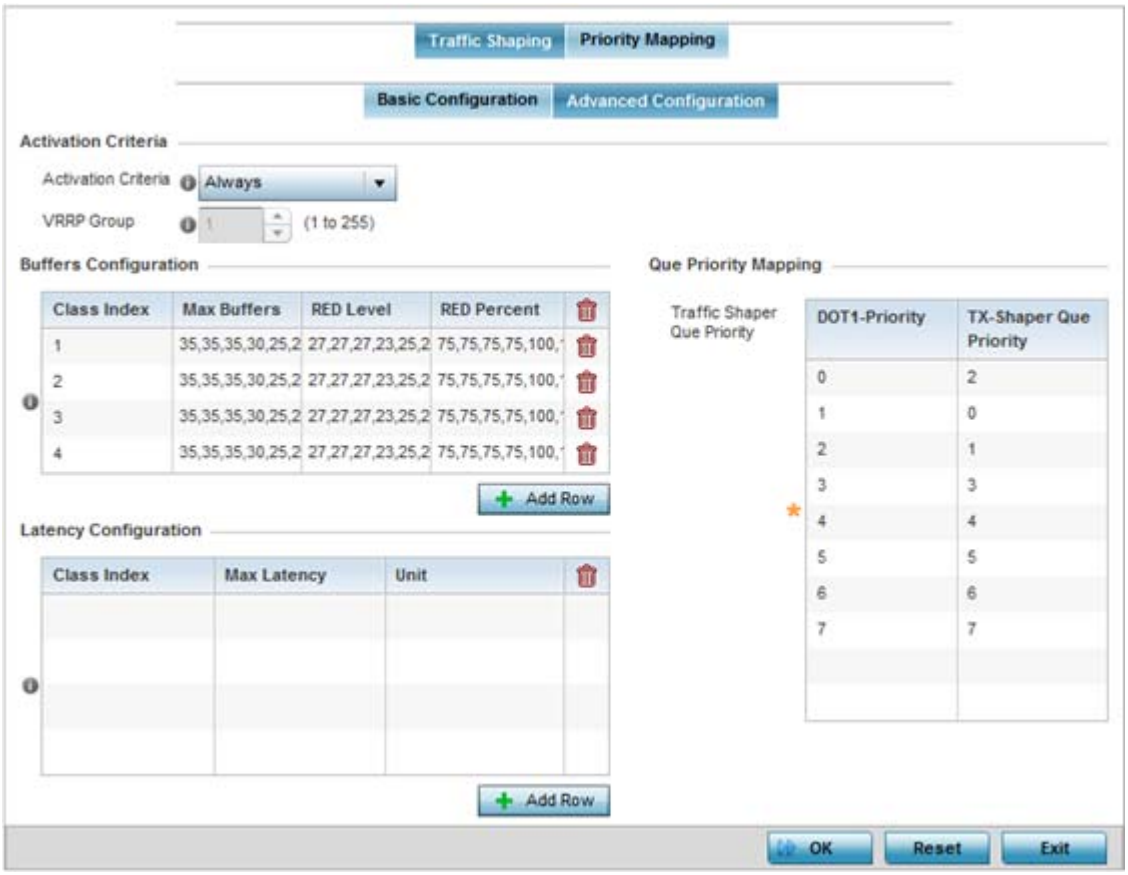


Figure 8-52 *Profile Overrides - Network QoS Traffic Shaping Advanced Configuration screen*

8 Set the following **Activation Criteria** for traffic shaper activation:

Activation Criteria	Use the drop-down menu to determine when the traffic shaper is invoked. Options include *vrrp-master, cluster-master*, *rf-domain-manager* and *Always*. A *VRRP master* responds to ARP requests, forwards packets with a destination link MAC layer address equal to the virtual router MAC layer address, rejects packets addressed to the IP associated with the virtual router and accepts packets addressed to the IP associated with the virtual router. The solitary *cluster master* is the cluster member elected, using a priority assignment scheme, to provide management configuration and Smart RF data to other cluster members. Cluster requests go through the elected master before dissemination to other cluster members. The *RF Domain manager* is the elected member capable of storing and provisioning configuration and firmware images for other members of the RF Domain.
VRRP Group	Set the VRRP group ID from 1 - 255. VRRP groups is only enabled when the Establishment Criteria is set to vrrp-master.

9 Select **+ Add Row** within the **Buffers Configuration** table to set the following:

Class Index	Set a class index from 1 - 4.

Max Buffers	Set the *Max Buffers* to specify the queue length limit after which the queue starts to drop packets. Set the maximum queue lengths for packets. The upper length is 400 for Access Points
RED Level	Set the packet queue length for RED. The upper limit is 400 for Access Points. The rate limiter uses the *random early detection* (RED) algorithm for rate limiting traffic. RED is a queueing technique for congestion avoidance. RED monitors the average queue size and drops or marks packets. If the buffer is near empty, all incoming packets are accepted. When the queue grows, the probability for dropping an incoming packet also grows. When the buffer is full, the probability has reached 1 and all incoming packets are dropped.
RED Percent	Set a percentage (1 - 100) for RED rate limiting at a percentage of maximum buffers.

Select **+ Add Row** within the **Latency Configuration** table to set the **Class Index** (1 - 4), **Max Latency** and latency measurement **Unit**. Max latency specifies the time limit after which packets start dropping (maximum packet delay in the queue). The maximum number of entries is 8. Select whether *msec* (default) or *usec* is unit for latency measurement.

When a new packet arrives it knows how much time to wait in the queue. If a packet takes longer than the latency value it's dropped. By default latency is not set, so packets remain in queue for long time.

Refer to the **Queue Priority Mapping** table to set the traffic shaper queue priority and specify a particular queue inside a class. There are 8 queues (0 - 7), and traffic is queued in each based on incoming packets mark 802.1p markings.

10 Select the **OK** button located to save the changes to the traffic shaping advanced configuration. Select **Reset** to revert to the last saved configuration.

11 Select the **Priority Mapping** tab.

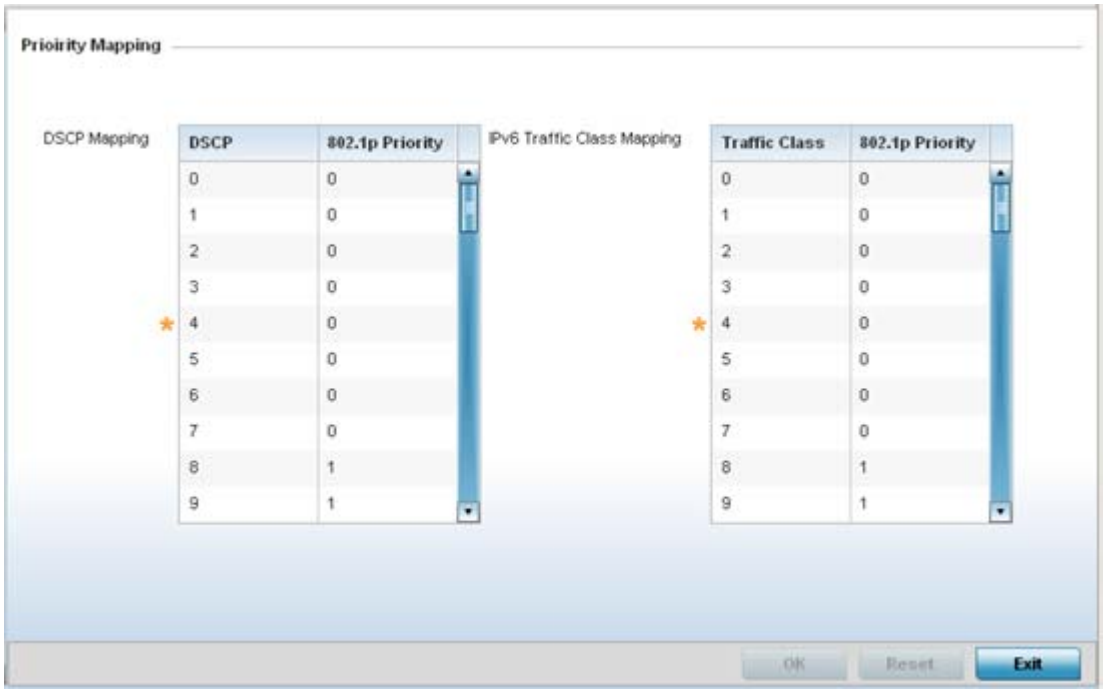


Figure 8-53 *Profile - Network QoS screen*

12 Set the following **DSCP Mapping** for untagged frames:

DSCP	Lists the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification.
802.1p Priority	Assign a 802.1p priority as a 3-bit IP precedence value in the Type of Service field of the IP header used to set the priority. The valid values for this field are 0-7. Up to 64 entries are permitted. The priority values are: 0 – *Best Effort* 1 – *Background* 2 – *Spare* 3 – *Excellent Effort* 4 – *Controlled Load* 5 – *Video* 6 – *Voice* 7 – *Network Control*

13 Use the spinner controls within the **802.1p Priority** field for each **DSCP** row to change the priority value.

14 Set a **IPv6 Traffic Class Mapping** to map IPv6 traffic classes to 802.1p priority mappings for untagged frames.

Traffic Class	Devices that originate a packet must identify different classes or priorities for IPv6 packets. Devices use the traffic class field in the IPv6 header to set this priority.
802.1p Priority	Assign a 802.1p priority as a 3-bit IP precedence value in the Type of Service field of the IP header used to set the priority. The valid values for this field are 0-7. Up to 64 entries are permitted. The priority values are: 0 – *Best Effort* 1 – *Background* 2 – *Spare* 3 – *Excellent Effort* 4 – *Controlled Load* 5 – *Video* 6 – *Voice* 7 – *Network Control*

15 Use the spinner controls within the **802.1p Priority** field for each **Traffic Class** row to change the priority value.

16 Select the **OK** button located to save the changes. Select **Reset** to revert to the last saved configuration.

8.8.8 Setting a Profile's Spanning Tree Configuration

Profile Network Configuration

The *Multiple Spanning Tree Protocol* (MSTP) provides an extension to STP to optimize the usefulness of VLANs. MSTP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.

If there's just one VLAN in the Access Point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it's possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

A MSTP supported deployment uses multiple MST regions with *multiple MST instances* (MSTI). Multiple regions and other STP bridges are interconnected using one single *common spanning tree* (CST).

MSTP includes all of its spanning tree information in a single *Bridge Protocol Data Unit* (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. MSTP encodes additional region information after the standard RSTP BPDU as well as a number of MSTI messages. Each MSTI messages conveys spanning tree information for each instance. Each instance can be assigned a number of configured VLANs. The frames assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, the Access Point encodes an MD5 digest of their VLAN to an instance table in the MSTP BPDU. This digest is used by other MSTP supported devices to determine if the neighboring device is in the same MST region as itself. MD5 is a message digest algorithm using a cryptographic hash producing a 128-bit (16-byte) hash value, usually expressed in text as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

To define a spanning tree configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **Spanning Tree**.

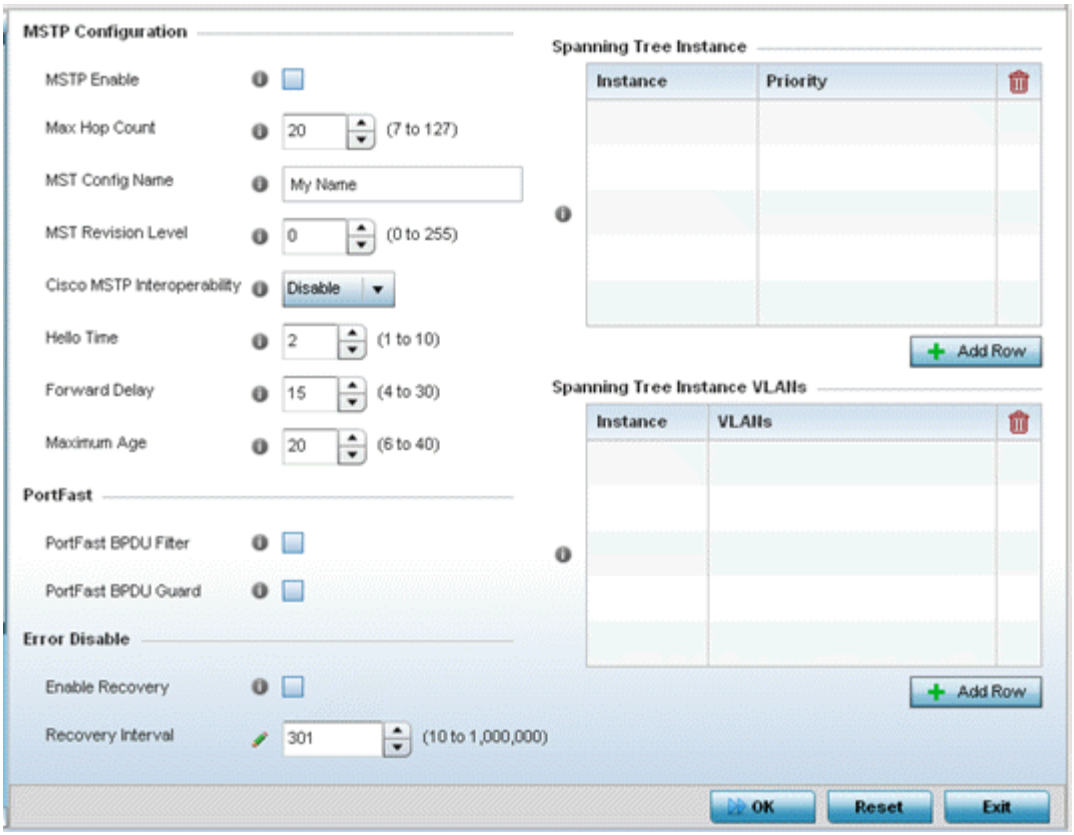


Figure 8-54 *Profile - Network Spanning Tree screen*

4 Set the following **MSTP Configuration** parameters

MSTP Enable	Select this option to enable MSTP for this profile. MSTP is disabled by default, so if requiring different (groups) of VLANs with the profile supported network segment.
Max Hop Count	Define the maximum number of hops the BPDU will consider valid in the spanning tree topology. The available range is from 7 -127. The default setting is 20.
MST Config Name	Define a 64 character maximum name for the MST region as an identifier.
MST Revision Level	Set a numeric revision value ID for MST configuration information. Set a value from 0 - 255. The default setting is 0.
Cisco MSTP Interoperability	Select either the *Enable* or *Disable* radio buttons to enable/disable interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default.
Hello Time	Set a BPDU hello interval from 1 - 10 seconds. BPDUs are exchanged regularly (every 2 seconds by default) and enable supported devices to keep track of network changes and star/stop port forwarding as required.

Forward Delay	Set the forward delay time from 4 - 30 seconds. When a device is first attached to a port, it does not immediately start to forward data. It first processes BPDUs and determines the network topology. When a host is attached the port always goes into the forwarding state, after a delay of while it goes through the listening and learning states. The time spent in the listening and learning states is defined by the forward delay (15 seconds by default).
Maximum Age	Use the spinner control to set the maximum time (in seconds) to listen for the root bridge. The root bridge is the spanning tree bridge with the smallest (lowest) bridge ID. Each bridge has a unique ID and a configurable priority number, the bridge ID contains both. The available range is from 6 - 40. The default setting is 20.

5 Set the following **PortFast** parameters for the profile configuration:

PortFast BPDU Filter	Select *Enable* to invoke a BPDU filter for this portfast enabled port. Enabling the BPDU filter feature ensures this port channel does not transmit or receive any BPDUs. BPDUs are exchanged regularly and enable the Access Point to keep track of network changes and to start and stop port forwarding as required. The default setting is disabled.
PortFast BPDU Guard	Select *Enable* to invoke a BPDU guard for the portfast enabled port. Enabling the BPDU Guard feature means this port shuts down on receiving a BPDU. Thus, no BPDUs are processed. BPDUs are exchanged regularly and enable the Access Point to track network changes and start and stop port forwarding as required. The default is disabled.

6 Set the following **Error Disable** parameters for the profile configuration:

Enable Recovery	Select this option to enable a error disable timeout resulting from a BPDU guard. This setting is disabled by default.
Recovery Interval	Define the recovery interval used to enable disabled ports. The available range is from 10 - 1,000,000 seconds with a default setting of 300.

7 Use the **Spanning Tree Instance** table to add indexes to the spanning tree topology. Add up to 16 indexes and use the Priority setting to define the bridge priority used to determine the root bridge. The lower the setting defined, the greater the likelihood of becoming the root bridge in the spanning tree topology.

8 Use the **Spanning Tree Instance VLANs** table to add VLAN instance indexes (by numeric ID) and VLANs to the spanning tree topology.

9 Select the **OK** button located to save the changes. Select **Reset** to revert to the last saved configuration

8.8.9 Setting a Profile's Routing Configuration

Profile Network Configuration

Routing is the process of selecting IP paths to strategically route network traffic. Set Destination IP and Gateway addresses enabling the assignment of static IP addresses for requesting clients without creating numerous host pools with manual bindings. This eliminates the need for a long configuration file, and reduces the resource space required to maintain address pools.

Both IPv4 and IPv6 routes are separately configurable using their appropriate tabs. For IPv6 networks, routing is the part of IPv6 that provides forwarding between hosts located on separate segments within a larger IPv6 network where IPv6 routers provide packet forwarding for other IPv6 hosts.

To create a profile's static routes:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **Routing**. The **IPv4 Routing** tab displays by default.

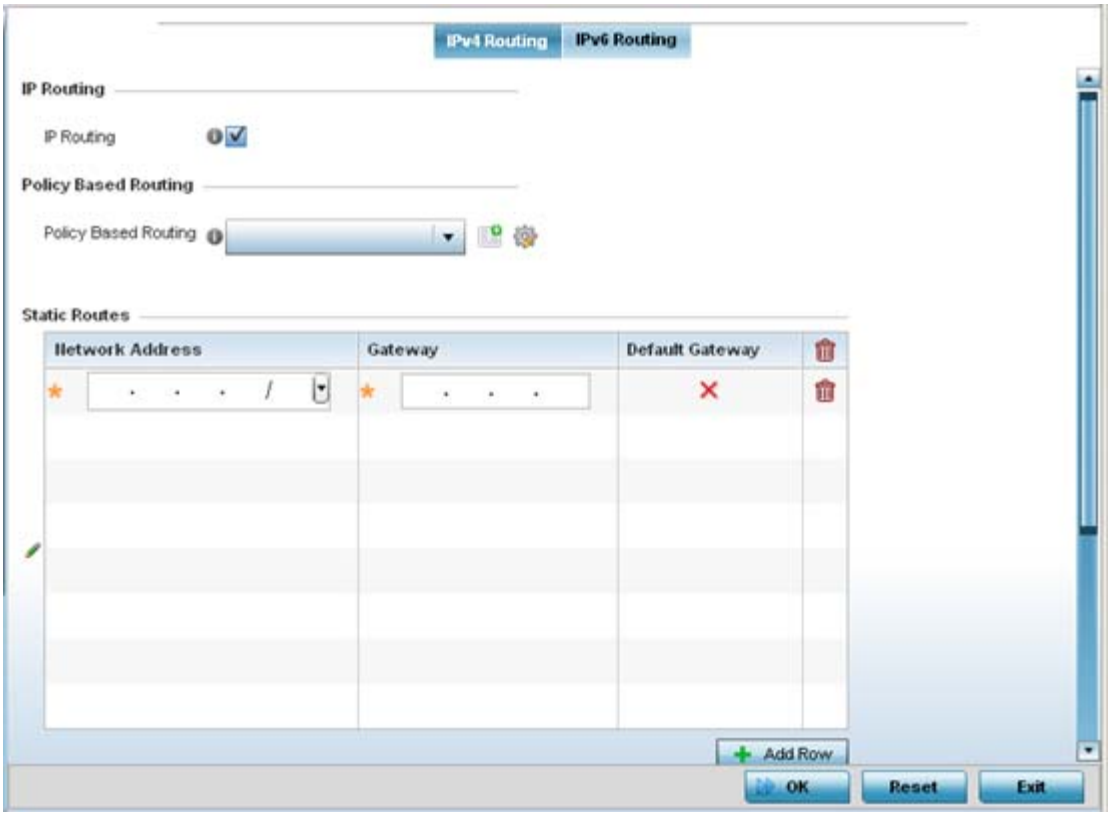


Figure 8-55 *Static Routes screen, IPv4 Routing tab*

4 Select **IP Routing** to enable static routes using IP addresses. This sets *Destination IP* and *Gateway* addresses enabling the assignment of static IP addresses for requesting clients. This option is enabled by default.

Use the drop-down menu to select a Policy Based Routing policy. If a suitable policy is unavailable, select the **Create** icon or modify an existing policy-based routing policy by selecting the **Edit** icon.

Policy-based routing (PBR) is a means of expressing and forwarding (routing) data packets based on policies defined by administrators. PBR provides a flexible mechanism for routing packets through routers, complementing existing routing protocols. PBR is applied to incoming packets. Packets received on an interface with PBR enabled are considered are passed through enhanced packet filters (route maps). Based on the route maps, packets are forwarded/routed to their next hop.

5 Refer to the **Static Routes** table to set Destination IP and Gateway addresses enabling the assignment of static IP addresses to requesting clients (without creating numerous host pools with manual bindings).

- Add IP addresses and network masks in the **Network Address** column.

- Provide the **Gateway** address used to route traffic.
- Provide an IP address for the **Default Gateway** used to route traffic.

Note, when routing packets, the system, by default, obtains IP addresses of the Default Gateway and Name Servers from the DHCP server policy. But, if manually configuring the Default Gateway for static routing, also configure the Name Server's IP address in the device/profile config contexts. For more information on using the GUI to configure Name Servers, see *Setting a Profile's DNS Configuration*. If using the CLI, in the device/profile config context, execute the following command: *ip > name-server > <NAME-SERVER-IP-ADDRESS>*.

6 Refer to the **Default Route Priority** field to set the following:

Static Default Route Priority	Use the spinner control to set the priority value (1 - 8,000) for the default static route. This is the weight assigned to this route versus others that have been defined. The default setting is 100.
DHCP Client Default Route Priority	Use the spinner control to set the priority value (1 - 8,000) for the default route learnt from the DHCP client. The default setting is 1000.
Enable Routing Failure	When selected, all default gateways are monitored for activity. The system will failover to a live gateway if the current gateway becomes unusable. This feature is enabled by default.

7 Select the **OK** button located at the bottom right of the screen to save the changes to the IPv4 routing configuration. Select **Reset** to revert to the last saved configuration.

8 Select the **IPv6 Routing** tab. IPv6 networks are connected by IPv6 routers. IPv6 routers pass IPv6 packets from one network segment to another.

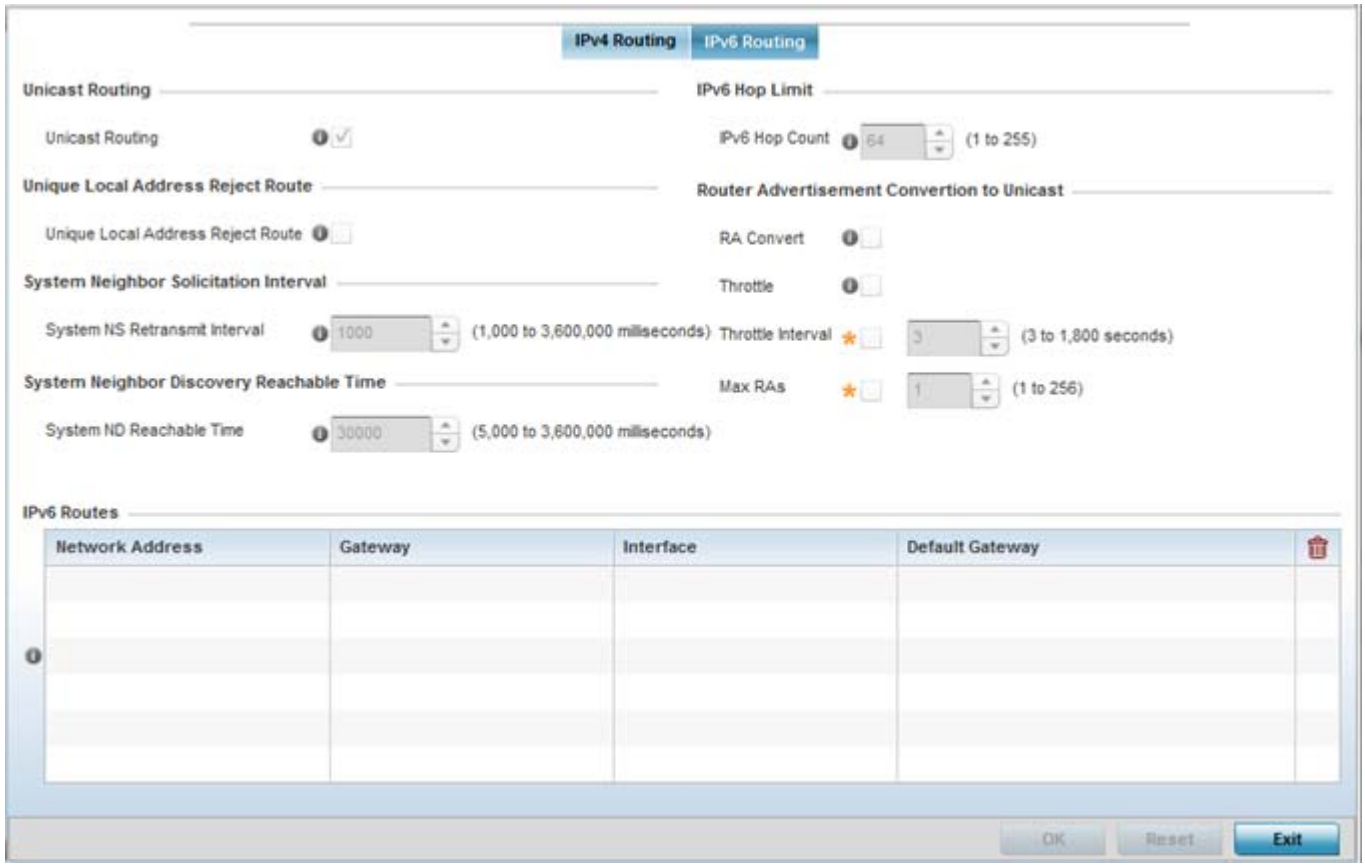


Figure 8-56 *Static Routes screen, IPv6 Routing tab*

9 Select **Unicast Routing** to enable IPv6 unicast routing for this profile. Keeping unicast enabled allows the profile's neighbor advertisements and solicitations in unicast (as well as multicast) to provide better neighbor discovery. This setting is enabled by default.

10 Select **Unique Local Address Reject Route** to reject *Unique Local Address* (ULA). ULA is an IPv6 address block (fc00::/7) that is an approximate IPv6 counterpart to IPv4 private addresses. When selected, a reject entry is added to the IPv6 routing table to reject packets with Unique Local Address.

11 Set a **System Neighbor Solicitation Retransmit Interval** (from 1,000 to 3,600,000 milliseconds) as the interval between *neighbor solicitation* (NS) messages. NS messages are sent by a node to determine the link layer address of a neighbor, or verify a neighbor is still reachable via a cached link-layer address. The default is 1,000 milliseconds.

12 Set a **System Neighbor Discovery Reachable Time** (from 5,000 to 3,600,000 milliseconds) as the time a neighbor is assumed to be reachable after receiving a receiving a *neighbor discovery* (ND) confirmation for their reachability. The default is 30,000 milliseconds.

13 Set an **IPv6 Hop Count** (from 1 - 255) as the maximum number of hops considered valid when sending IP packets. The default setting is 64.

14 Set the **Router Advertisement Conversion to Unicast** settings:

RA Convert	Select this option to convert multicast *router advertisements* (RA) to unicast router advertisements at the dot11 layer. Unicast addresses identify a single network interface, whereas a multicast address is used by multiple hosts. This setting is disabled by default.
Throttle	Select this option to throttle RAs before converting to unicast. Once enabled, set the throttle interval and maximum number of RAs. This setting is disabled by default.
Throttle Interval (milliseconds)	Enable this setting to define the throttle interval (3 - 1,800 seconds). The default setting is 3 seconds.
Max RAs	Enable this setting to define the maximum number of router advertisements per router (1 - 256) during the throttle interval. The default setting is 1.

15 Select **+ Add Row** as needed within the **IPv6 Routes** table to add an additional 256 IPv6 route resources.

Figure 8-57 *Static Routes screen, Add IPv6 Route*

Network Address	Set the IPv6 network address. Other than the length and slightly different look versus an IPv4 address, the IPv6 address concept is same as IPv4.
Gateway	Set the IPv6 route gateway. A network gateway in IPv6 is the same as in IPv4. A gateway address designates how traffic is routed out of the current subnet.
Interface	If using a link local address, set the VLAN (1 - 4,094) used a virtual routing interface for the local address.

16 Select the **OK** button located at the bottom right of the screen to save the changes to the IPv6 routing configuration. Select **Reset** to revert to the last saved configuration.

8.8.10 Setting a Profile's Dynamic Routing (OSPF) Configuration

Profile Network Configuration

Open Shortest Path First (OSPF) is a link-state *interior gateway protocol* (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

OSPF detects changes in the topology, like a link failure, and plots a new loop-free routing structure. It computes the shortest path for each route using a shortest path first algorithm. Link state data is maintained on each router and is periodically updated on all OSPF member routers.

OSPF uses a route table managed by the link *cost* (external metrics) defined for each routing interface. The cost could be the distance of a router (round-trip time), link throughput or link availability. Setting a cost value provides a dynamic way to load balancing traffic between routes of equal cost.

An OSPF network can be subdivided into routing areas to simplify administration and optimize traffic utilization. Areas are logical groupings of hosts and networks, including routers having interfaces connected to an included network. Each area maintains a separate link state database whose information may be summarized towards the rest of the network by the connecting router. Areas are identified by 32-bit IDs, expressed either in decimal, or octet-based dot-decimal notation. Areas can defined as:

stub area - A stub area is an area which does not receive route advertisements external to the autonomous system (AS) and routing from within the area is based entirely on a default route.

totally-stub - A totally stubby area does not allow summary routes and external routes. A default route is the only way to route traffic outside of the area. When there's only one route out of the area, fewer routing decisions are needed, lowering system resource utilization.

non-stub - A non-stub area imports autonomous system external routes and send them to other areas. However. it still cannot receive external routes from other areas.

nssa - NSSA is an extension of a stub that allows the injection of limited external routes into a stub area. If selecting NSSA, no external routes, except a default route, enter the area.

totally nssa - Totally nssa is an NSSA using 3 and 4 summary routes are not flooded into this type of area. It is also possible to declare an area both totally stubby and not-so-stubby, which means that the area will receive only the default route from area 0.0.0.0, but can also contain an autonomous system boundary router (ASBR) that accepts external routing information and injects it into the local area, and from the local area into area 0.0.0.0.

A router running OSPF sends hello packets to discover neighbors and elect a designated router. The hello packet includes link state information and list of neighbors. OSPF is savvy with layer 2 topologies. If on a *point-to-point* link, OSPF knows it is sufficient, and the link stays *up*. If on a *broadcast* link, the router waits for election before determining if the link is functional.

To define a dynamic routing configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Expand the **Network** menu and select **OSPF.**
The **OSPF Settings** tab displays by default, with additional **Area Settings** and **Interface Settings** tabs available.

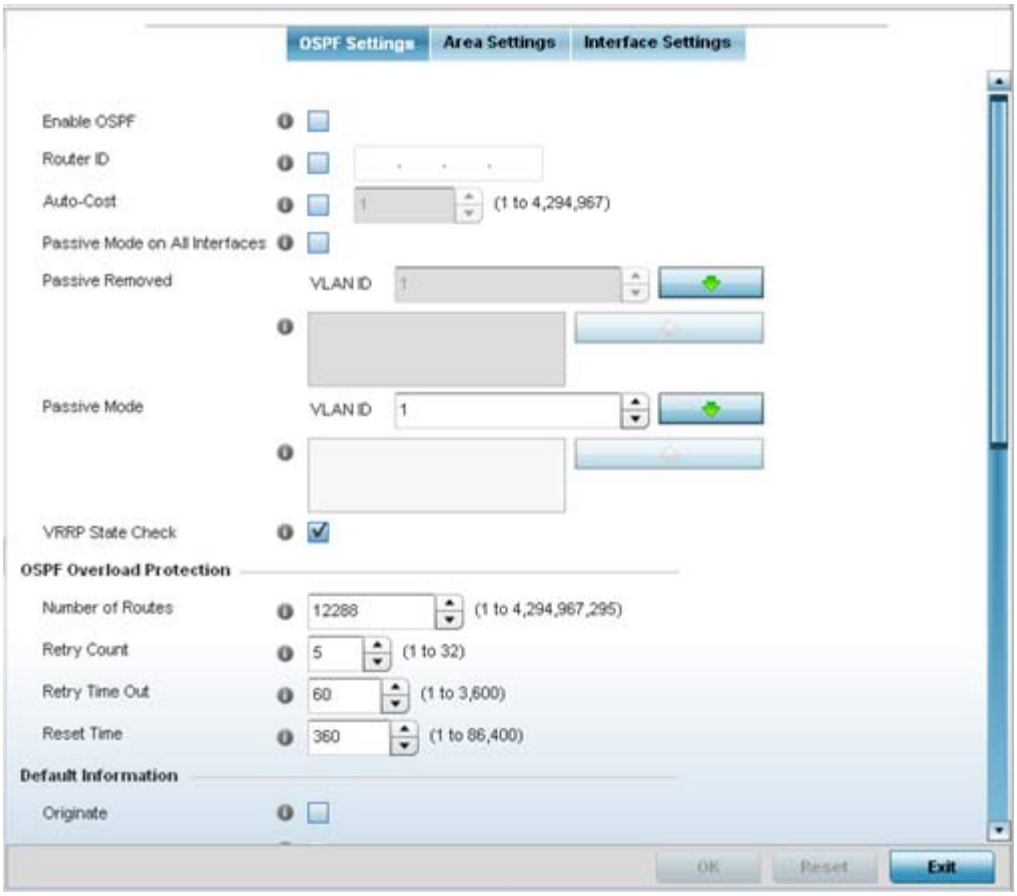


Figure 8-58 *OSPF Settings screen*

4 Enable/disable OSPF and provide the following dynamic routing settings:

Enable OSPF	Select this option to enable OSPF for this Access Point. OSPF is disabled by default.
Router ID	Select this option to define a router ID (numeric IP address) for this Access Point. This ID must be established in every OSPF instance. If not explicitly configured, the highest logical IP address is duplicated as the router identifier. However, since the router identifier is not an IP address, it does not have to be a part of any routable subnet in the network.
Auto-Cost	Select this option to specify the reference bandwidth (in Mbps) used to calculate the OSPF interface cost if OSPF is either STUB or NSSA. The default setting is 1.
Passive Mode on All Interfaces	When selected, all layer 3 interfaces are set as an OSPF passive interface. This setting is disabled by default.
Passive Removed	If *enabling* Passive Mode on All Interfaces, use the spinner control to select VLANs (by numeric ID) as OSPF *non* passive interfaces. Multiple VLANs can be added to the list.
Passive Mode	If *disabling* Passive Mode on All Interfaces, use the spinner control to select VLANs (by numeric ID) as OSPF passive interfaces. Multiple VLANs can be added to the list.

VRRP State Check	Select this option to use OSPF only if the VRRP interface is not in a backup state. The *Virtual Router Redundancy Protocol* (VRRP) provides automatic assignments of available Internet Protocol (IP) routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork. This setting is enabled by default.

5 Set the following **OSPF Overload Protection** settings:

Number of Routes	Use the spinner control to set the maximum number of OSPN routes permitted. The available range is from 1 - 4,294,967,295.
Retry Count	Set the maximum number of retries (OSPF resets) permitted before the OSPF process is shut down. The available range is from 1 - 32. The default setting is 5.
Retry Time Out	Set the duration (in seconds) the OSPF process remains off before initiating its next retry. The available range is from 1 - 3,600 seconds. The default is 60 seconds.
Reset Time	Set the reset time (in seconds) that, when exceeded, changes the retry count is zero. The available range is from 1 - 86,400. The default is 360 seconds.

6 Set the following **Default Information**:

Originate	Select this option to make the default route a distributed route. This setting is disabled by default.
Always	Enabling this setting continuously maintains a default route, even when no routes appear in the routing table. This setting is disabled by default.
Metric Type	Select this option to define the exterior metric type (*1* or *2*) used with the default route.
Route Metric	Select this option to define route metric used with the default route. OSPF uses path cost as its routing metric. It's defined by the speed (bandwidth) of the interface supporting a given route.

7 Refer to the **Route Redistribution** table to set the types of routes that can be used by OSPF.

Select the **+ Add Row** button to populate the table. Set the **Route Type** used to define the redistributed route. Options include *connected*, *kernal* and *static*.

Select the **Metric Type** option to define the exterior metric type (1 or 2) used with the route redistribution. Select the **Metric** option to define route metric used with the redistributed route.

8 Use the **OSPF Network** table to define networks (IP addresses) to connect using dynamic routes.

Select the **+ Add Row** button to populate the table. Add the IP address and mask of the **Network(s)** participating in OSPF. Additionally, define the OSPF area (IP address) to which the network belongs.

9 Set an **OSPF Default Route Priority** (1 - 8,000) as the priority of the default route learnt from OSPF. The default value is 7000.

10 Select the **Area Settings** tab.

An OSPF *Area* contains a set of routers exchanging *Link State Advertisements* (LSAs) with others in the same area. Areas limit LSAs and encourage aggregate routes.

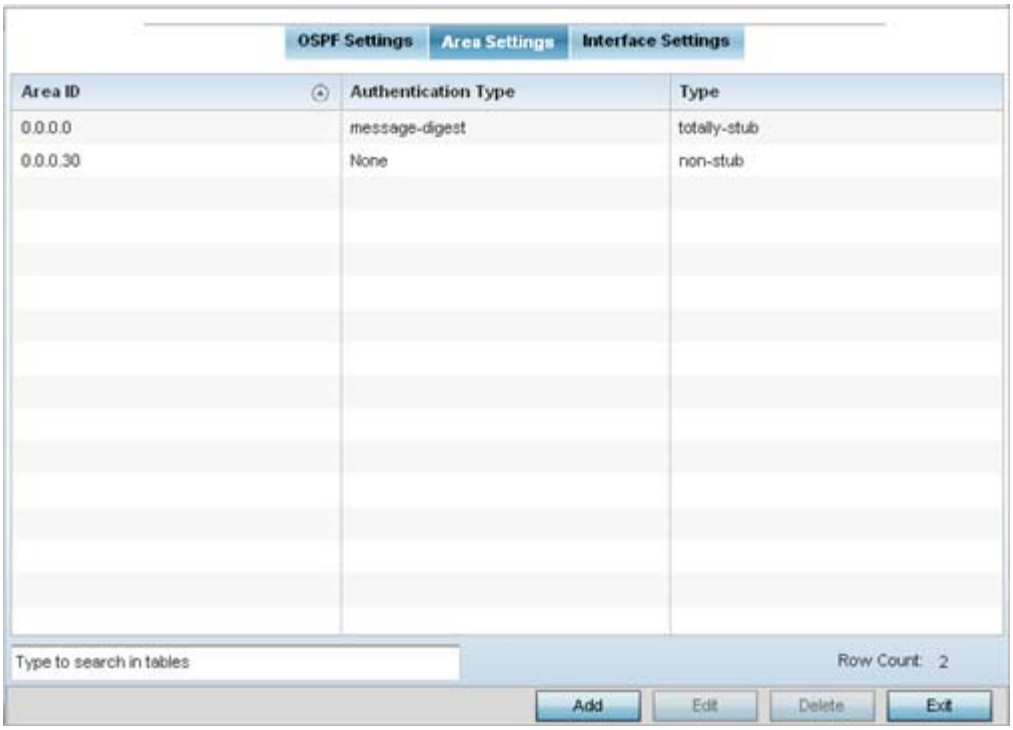


Figure 8-59 *OSPF Area Settings screen*

11 Review existing **Area Setting** configurations:

Area ID	Displays either the *IP address* or *integer* representing the OSPF area.
Authentication Type	Lists the authentication schemes used to validate the credentials of dynamic route connections.
Type	Lists the OSPF area type in each listed configuration.

12 Select **Add** to create a new OSPF configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.

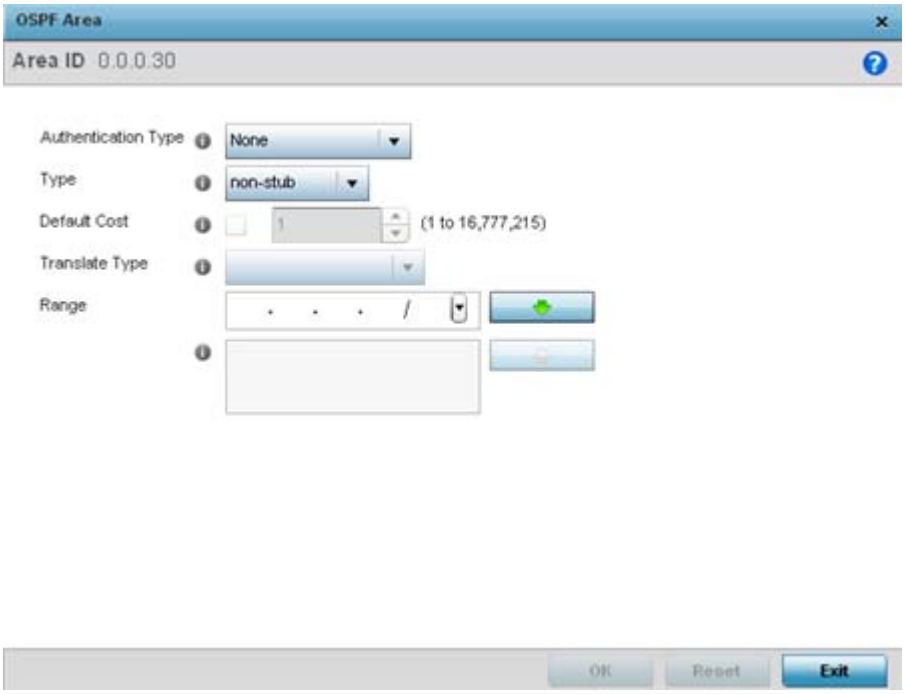


Figure 8-60 *OSPF Area Configuration screen*

13 Set the **OSPF Area** configuration.

Area ID	Use the drop down menu and specify either an *IP address* or *Integer* for the OSPF area.
Authentication Type	Select either *None*, *simple-password* or *message-digest* as the credential validation scheme used with the OSPF dynamic route. The default setting is None.
Type	Set the OSPF area type as either *stub*, *totally-stub*, *nssa*, *totally-nssa* or *non-stub*.
Default Cost	Select this option to set the default summary cost advertised if creating a stub. Set a value from 1 - 16, 777,215.
Translate Type	Define how messages are translated. Options include *translate-candidate*, *translate always* and *translate-never.* The default setting is translate-candidate.
Range	Specify a range of addresses for routes matching the address/mask for OSPF summarization.

14 Select the **OK** button to save the changes to the area configuration. Select **Reset** to revert to the last saved configuration.

15 Select the **Interface Settings** tab.

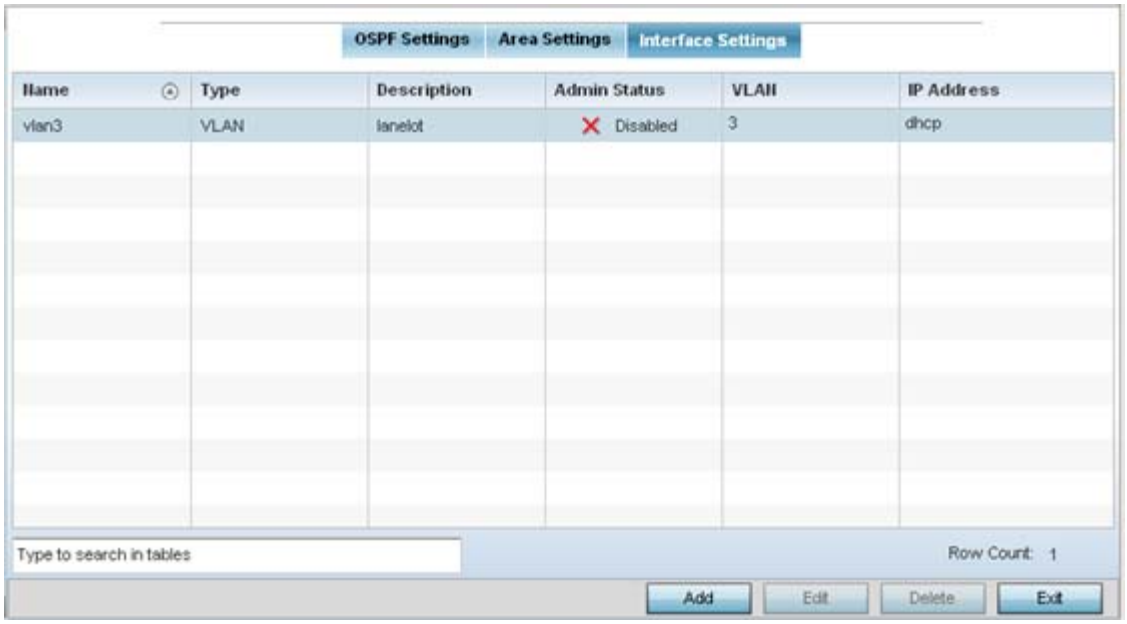


Figure 8-61 *OSPF Interface Settings screen*

16 Review existing **Interface Settings** using the following:

Name	Displays the name defined for the interface configuration.
Type	Displays the type of interface.
Description	Lists each interface's 32 character maximum description.
Admin Status	Displays whether administrative privileges have been *enabled* (with a green checkmark) or *disabled* (defined by a red X) for the OSPF route's virtual interface connection.
VLAN	Lists the VLAN IDs set for each listed OSPF route virtual interface.
IP Address	Displays the IP addresses defined as virtual interfaces for dynamic OSPF routes. Zero config and DHCP can be used to generate route addresses, or a primary and secondary address can be manually provided.

17 Select the **Add** button to define a new set of virtual interface basic settings, or **Edit** to update the settings of an existing virtual interface configuration.

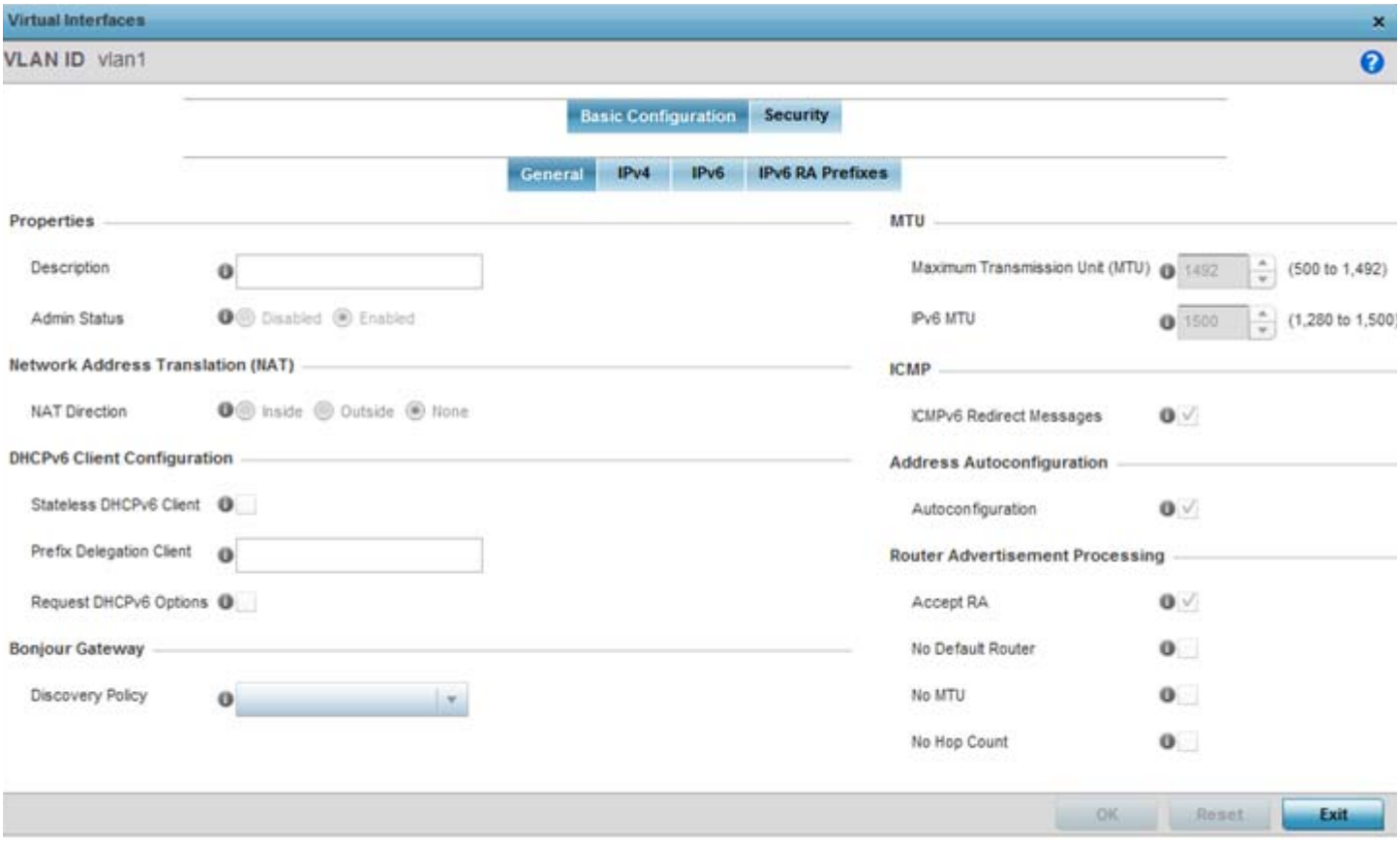


Figure 8-62 *Virtual Interfaces - Basic Configuration screen - General tab*

The **Basic Configuration** screen's **General** tab displays by default, regardless of a whether a new Virtual Interface is created or an existing one is being modified for the OSPF configuration.

18 If creating a new Virtual Interface, use the **VLAN ID** spinner control to define a numeric ID from 1 - 4094. Select the **Continue** button to initialize the rest of the parameters on the screen.

19 Define the following parameters from within the **Properties** field:

Description	Provide or edit a description (up to 64 characters) for the Virtual Interface that helps differentiate it from others with similar configurations.
Admin Status	Either select either the *Disabled* or *Enabled* radio button to define this interface's current status. When set to Enabled, the Virtual Interface is operational and available. The default value is enabled

20 Define the following NAT parameters from within the **Network Address Translation (NAT)** field:

NAT Direction	Define the *Network Address Translation* (NAT) direction. Options include: *Inside* - The inside network is transmitting data over the network its intended destination. On the way out, the source IP address is changed in the header and replaced by the (public) IP address. *Outside* - Packets passing through the NAT on the way back to the controller or service platform managed LAN are searched against to the records kept by the NAT engine. There, the destination IP address is changed back to the specific internal private class IP address in order to reach the LAN over the network. *None* - No NAT activity takes place. This is the default setting.

21 Set the following **DHCPv6 Client Configuration**. The *Dynamic Host Configuration Protocol* for IPv6 (DHCPv6) provides a framework for passing configuration information.

Stateless DHCPv6 Client	Select this option to request information from the DHCPv6 server using stateless DHCPv6. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is disabled by default.
Prefix Delegation Client	Specify a 32 character maximum request prefix for prefix delegation from a DHCPv6 server over this virtual interface.
Request DHCPv6 Options	Select this option to request DHCPv6 options on this virtual interface. DHCPv6 options provide configuration information for a node that must be booted using the network rather than from locally. This setting is disabled by default.

22 Set the following **Bonjour Gateway** settings.Bonjour is Apple's implementation of zero-configuration networking (Zeroconf). Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates devices such as printers, other computers and services that these computers offer over a local network.

Bonjour provides a general method to discover services on a local area network (LAN). It allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with special DNS configuration, it can be extended to find services across broadcast domains.

From the drop-down, select the Bonjour Gateway **Discovery Policy**. Select the **Create** icon to define a new Bonjour Gateway policy configuration or select the **Edit** icon to modify an existing Bonjour Gateway policy configuration.

23 Set the following **MTU** settings for the virtual interface:

Maximum Transmission Unit (MTU)	Set the PPPoE client *maximum transmission unit* (MTU) from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size. The default MTU is 1,492.

IPv6 MTU	Set an IPv6 MTU for this virtual interface from 1,280 - 1,500. A larger MTU provides greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays, remain fixed; the resulting higher efficiency means a slight improvement in bulk protocol throughput. A larger MTU results in the processing of fewer packets for the same amount of data. The default is 1,500.

24 Within the **ICMP** field, define whether ICMPv6 redirect messages are sent. Redirect requests data packets be sent on an alternative route. This setting is enabled by default.

25 Within the **Address Autoconfiguration** field, define whether to configure IPv6 addresses on this virtual interface based on the prefixes received in router advertisement messages. This setting is enabled by default.

26 Set the following **Router Advertisement Processing** settings for the virtual interface. Router advertisements are periodically sent to hosts or sends in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

Accept RA	Enable this option to allow router advertisements over this virtual interface. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters.This setting is enabled by default.
No Default Router	Select this option to not consider routers present on this interface for default router selection. This setting is disabled by default.
No MTU	Select this option to not use the set MTU value for router advertisements on this virtual interface. This setting is disabled by default.
No Hop Count	Select this option to not use the hop count advertisement setting for router advertisements on this virtual interface. This setting is disabled by default.

27 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

28 Select the **IPv4** tab to set IPv4 settings for this virtual interface.

IPv4 is a connectionless protocol It operates on a best effort delivery model that does not guarantee delivery or assures proper sequencing or avoidance of duplicate delivery (unlike TCP).

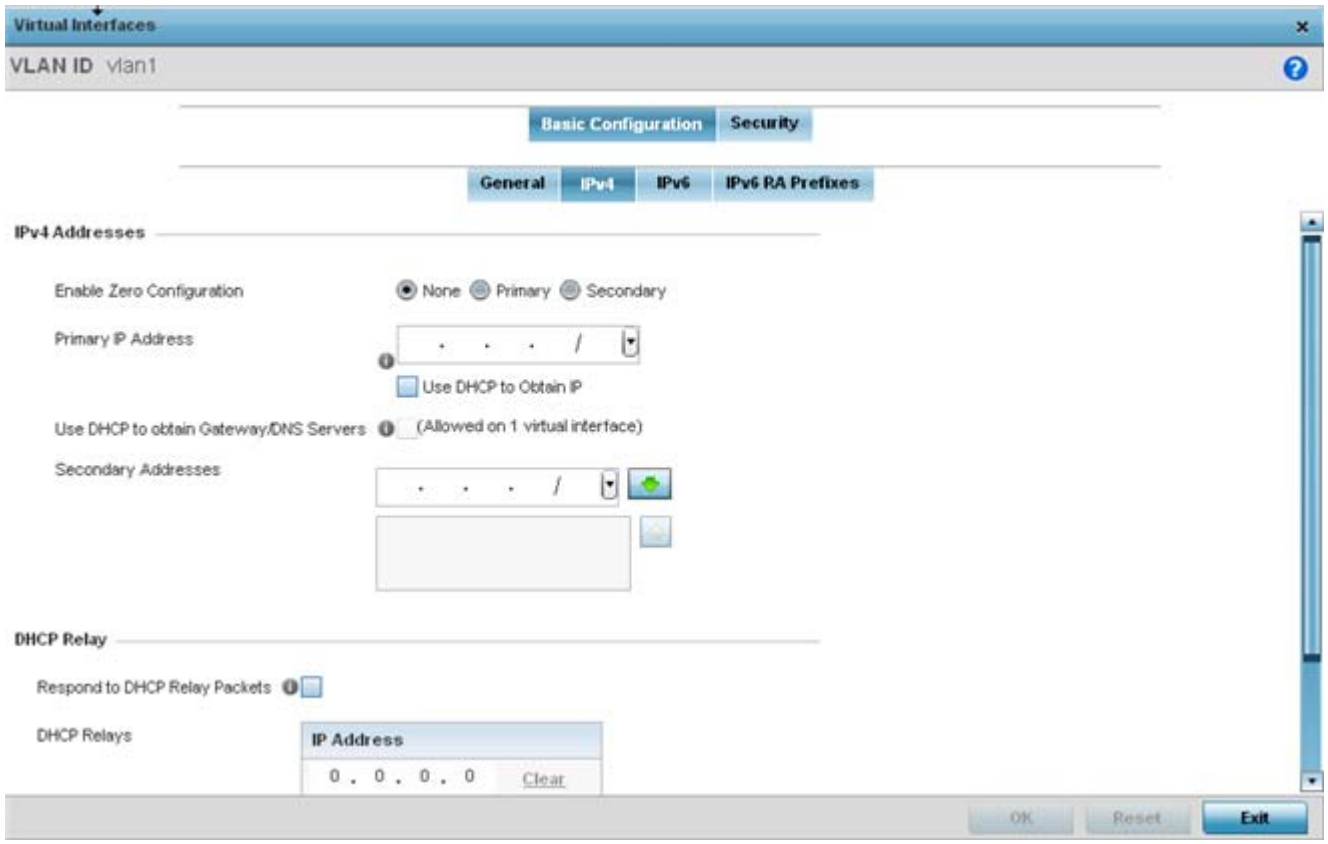


Figure 8-63 *Virtual Interfaces - Basic Configuration screen - IPv4 tab*

29 Set the following network information from within the **IPv4 Addresses** field:

Enable Zero Configuration	Zero Configuration can be a means of providing a primary or secondary IP addresses for the virtual interface. Zero configuration (or zero config) is a wireless connection utility included with Microsoft Windows XP and later as a service dynamically selecting a network to connect based on a user's preferences and various default settings. Zero config can be used instead of a wireless network utility from the manufacturer of a computer's wireless networking device. This value is set to None by default.
Primary IP Address	Define the IP address for the VLAN associated Virtual Interface.
Use DHCP to Obtain IP	Select this option to allow DHCP to provide the IP address for the Virtual Interface. Selecting this option disables the Primary IP address field.
Use DHCP to obtain Gateway/DNS Servers	Select this option to allow DHCP to obtain a default gateway address, and DNS resource for *one* virtual interface. This setting is disabled by default and only available when the Use DHCP to Obtain IP option is selected.
Secondary Addresses	Use the Secondary Addresses parameter to define additional IP addresses to associate with VLAN IDs. The address provided in this field is used if the primary IP address is unreachable.

30 Refer to the **DHCP Relay** field to set the DHCP relay server configuration used with the Virtual Interface.

Respond to DHCP Relay Packets	Select the *Respond to DHCP Relay Packets* option to allow the onboard DHCP server to respond to relayed DHCP packets on this interface. This setting is disabled by default.

DHCP Relays	Provide IP addresses for DHCP server relay resources. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When A DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.

31 Select **OK** to save the changes to the IPv4 configuration. Select **Reset** to revert to the last saved configuration.

32 Select the **IPv6** tab to set IPv6 settings for this virtual interface.

IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters.

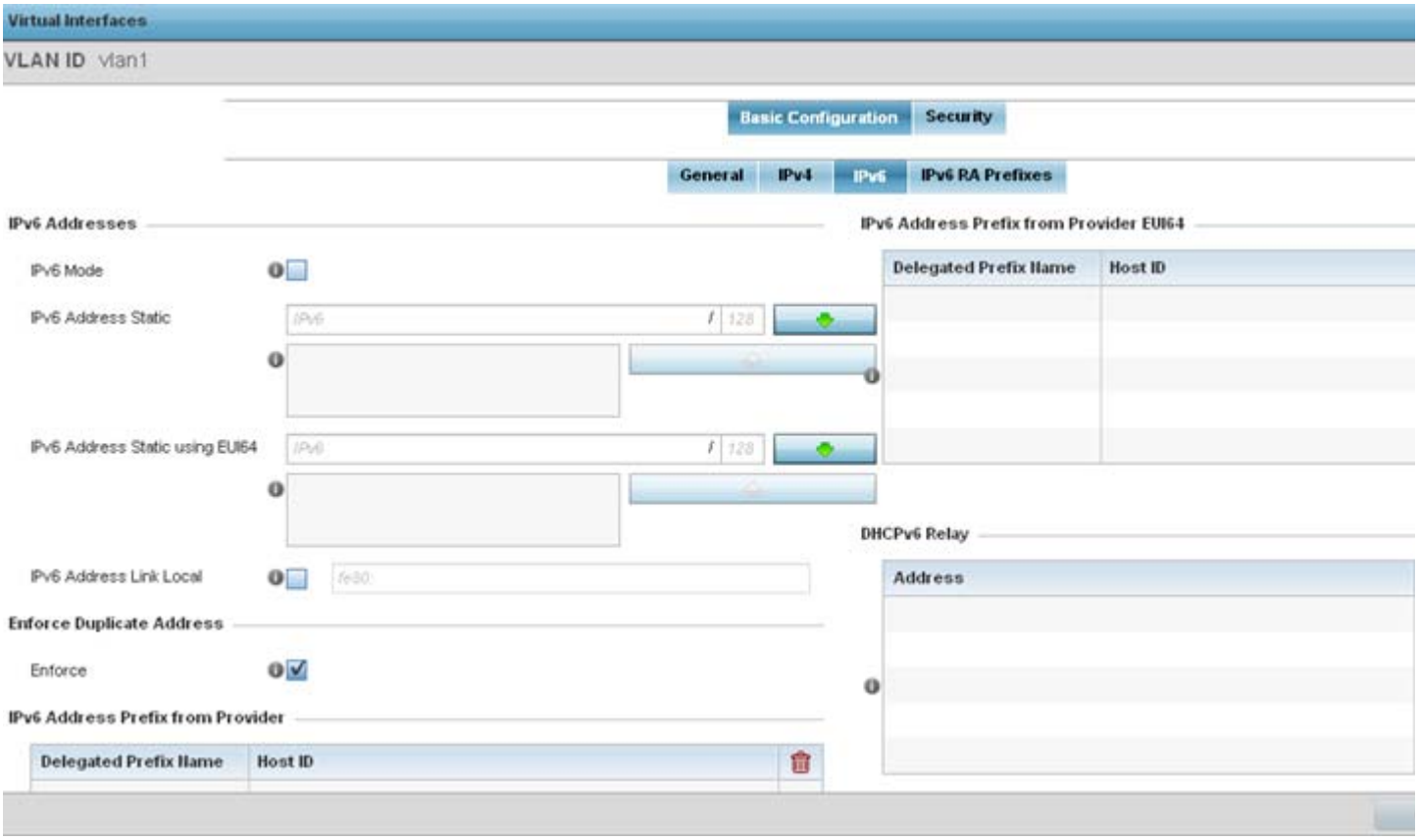


Figure 8-64 *Virtual Interfaces - Basic Configuration screen - IPv6 tab*

33 Refer to the **IPv6 Addresses** field to define how IP6 addresses are created and utilized.

IPv6 Mode	Select this option to enable IPv6 support on this virtual interface.

IPv6 Address Static	Define up to 15 global IPv6 IP addresses that can created statically. IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons.
IPv6 Address Static using EUI64	Optionally set up to 15 global IPv6 IP addresses (in the EUI-64 format) that can created statically. The IPv6 EUI-64 format address is obtained through a 48-bit MAC address. The MAC is initially separated into two 24-bits, with one being an OUI (*Organizationally Unique Identifier*) and the other being client specific. A 16-bit 0xFFFE is then inserted between the two 24-bits for the 64-bit EUI address. IEEE has chosen FFFE as a reserved value which can only appear in EUI-64 generated from the an EUI-48 MAC address.
IPv6 Address Link Local	Provide the IPv6 local link address. IPv6 requires a link local address assigned to every interface the IPv6 protocol is enabled, even when one or more routable addresses are assigned.

34 Enable the **Enforce Duplicate Address** option to enforce duplicate address protection when any wired port is connected and in a forwarding state. This option is enabled by default

35 Refer to the **IPv6 Address Prefix from Provider** table use prefix abbreviations as shortcuts of the entire character set comprising an IPv6 formatted IP address.

Select **+ Add Row** to launch a sub screen wherein a new delegated prefix name and host ID can be defined.

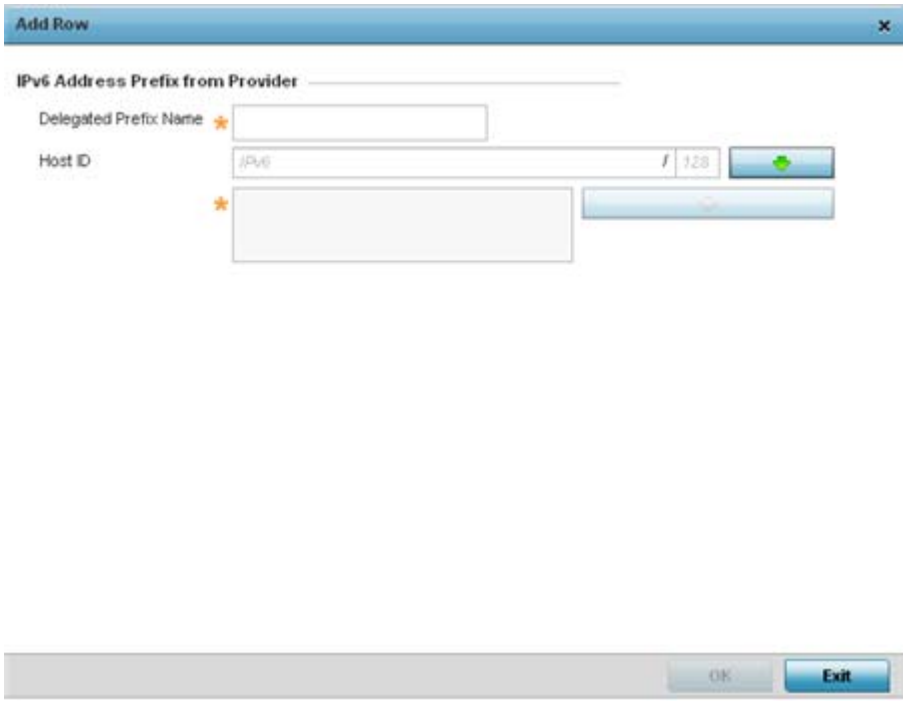


Figure 8-65 *Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider*

Delegated Prefix Name	Enter a 32 character maximum name for the IPv6 address prefix from provider.
Host ID	Define the subnet ID, host ID and prefix length.

36 Select **OK** to save the changes to the new IPv6 prefix from provider. Select **Exit** to close the screen without saving the updates.

37 Refer to the **IPv6 Address Prefix from Provider EUI64** table to review ISP provided address prefix abbreviations.

38 Select **+ Add Row** to launch a sub screen wherein a new delegated prefix name and host ID can be defined in EUI64 format.

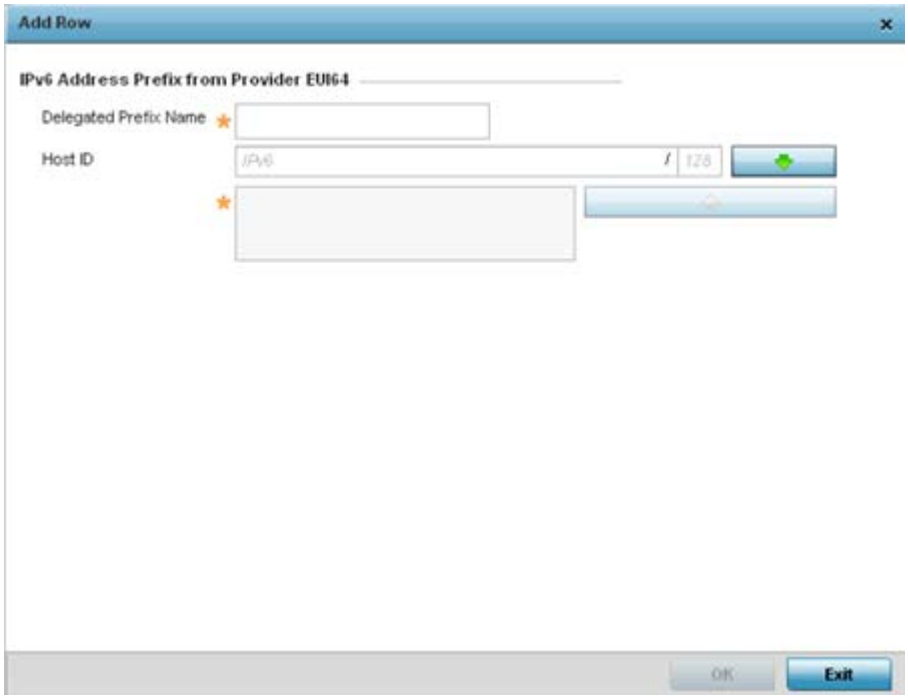


Figure 8-66 *Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider EUI64*

Delegated Prefix Name	Enter a 32 character maximum name for the IPv6 prefix from provider in EUI format.
Host ID	Define the subnet ID and prefix length.

39 Select **OK** to save the changes to the new IPv6 prefix from provider in EUI64 format. Select **Exit** to close the screen without saving the updates.

40 Refer to the **DHCPv6 Relay** table to set the address and interface of the DHCPv6 relay. The DHCPv6 relay enhances an extended DHCP relay agent by providing support in IPv6. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When A DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.

41 Select **+ Add Row** to launch a sub screen wherein a new DHCPv6 relay address and interface VLAN ID can be set.

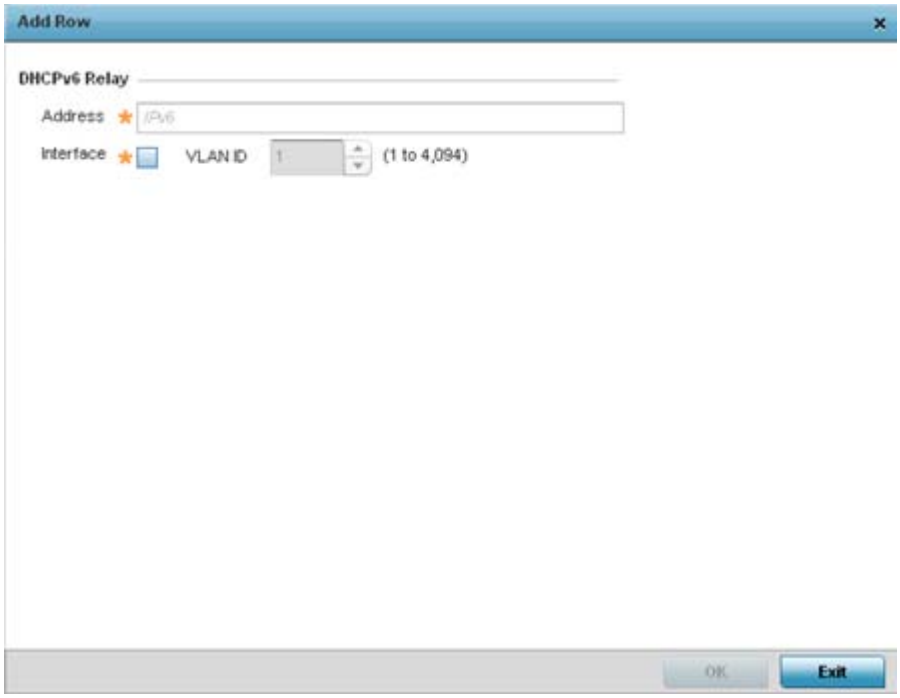


Figure 8-67 *Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add DHCPv6 Relay*

Address	Enter an address for the DHCPv6 relay. These DHCPv6 relay receive messages from DHCPv6 clients and forward them to DHCPv6 servers. The DHCPv6 server sends responses back to the relay, and the relay then sends these responses to the client on the local network link.
Interface	Select this option to enable a spinner control to define a VLAN ID from 1 - 4,094 used as the virtual interface for the DHCPv6 relay. The interface designation is only required for link local and multicast addresses. A local link address is a locally derived address designed for addressing on a single link for automatic address configuration, neighbor discovery or when no routing resources are available.

42 Select **OK** to save the changes to the DHCPv6 relay configuration. Select **Exit** to close the screen without saving the updates.

43 Select the **IPv6 RA Prefixes** tab.

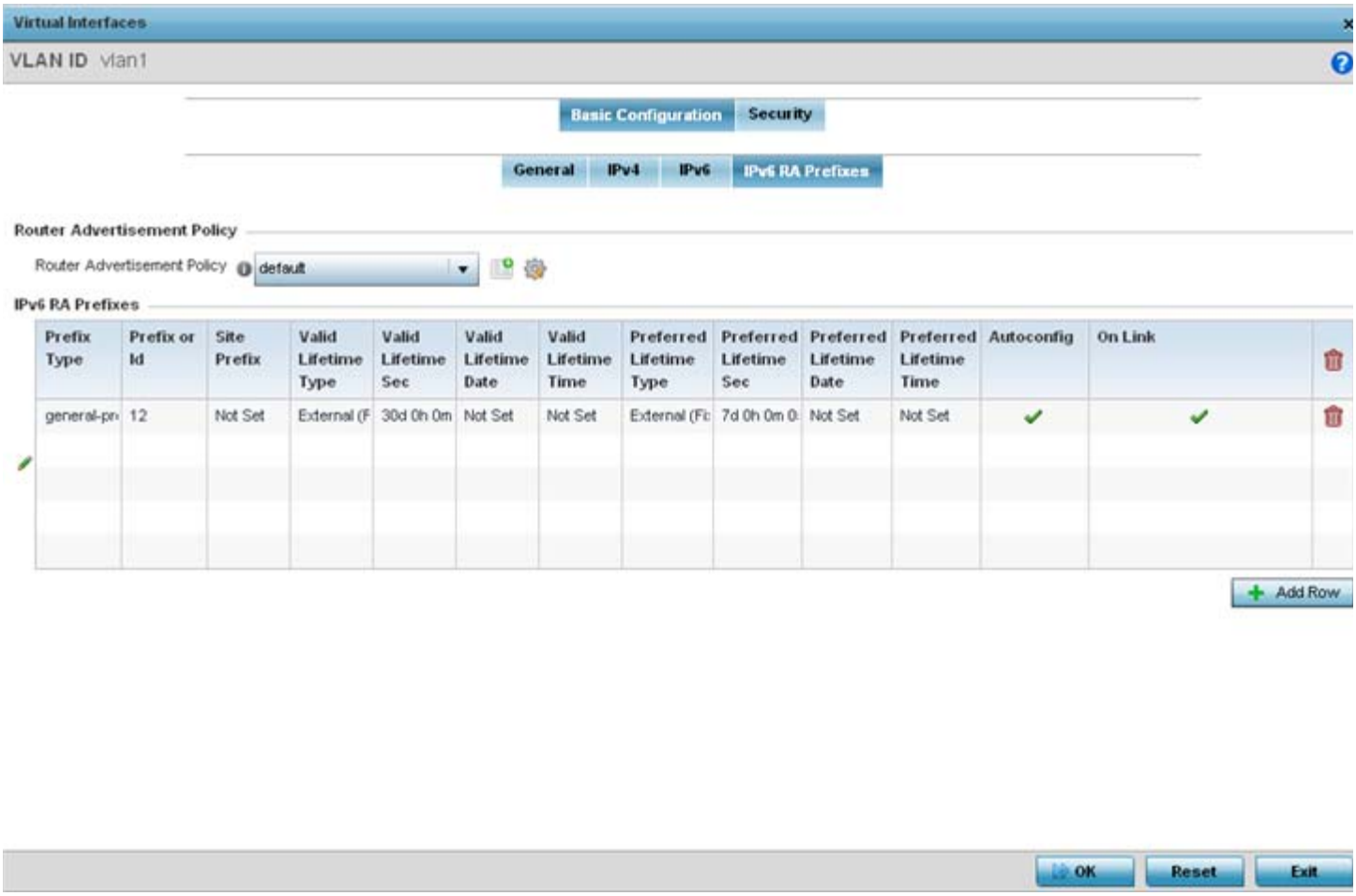


Figure 8-68 *Virtual Interfaces - Basic Configuration screen - IPv6 RA Prefixes tab*

44 Use the **Router Advertisement Policy** drop-down menu to select and apply a policy to the virtual interface.

Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

Review the configurations of existing IPv6 advertisement policies. If needed select **+ Add Row** to define the configuration of an additional IPv6 RA prefix.

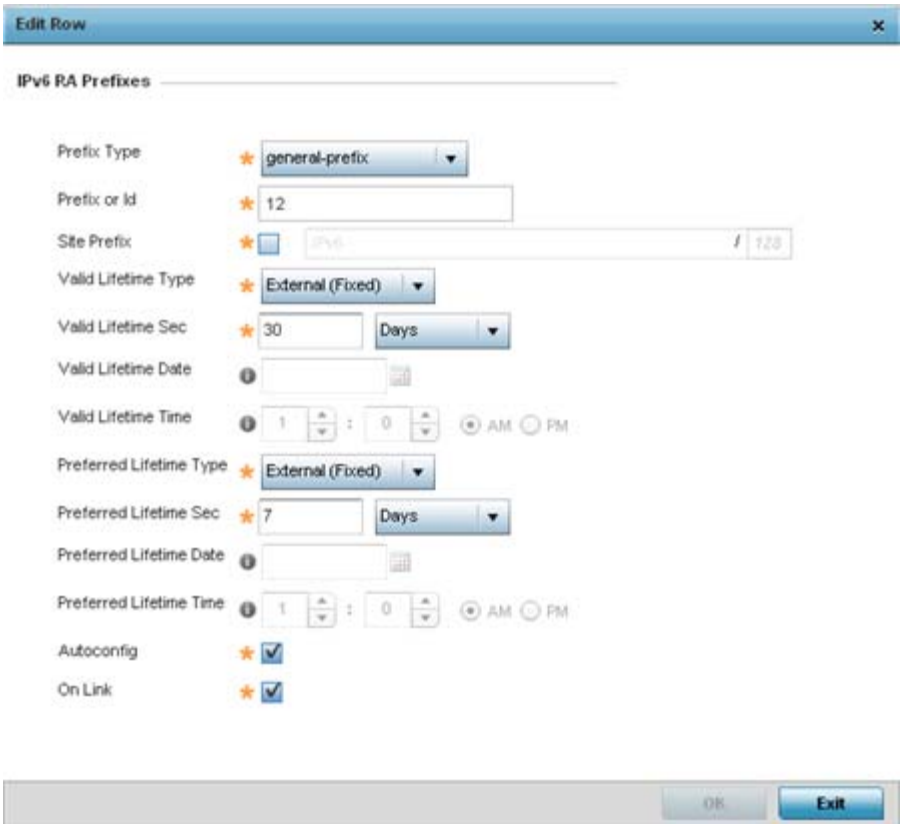


Figure 8-69 *Virtual Interfaces - Basic Configuration screen - Add IPv6 RA Prefix*

45 Set the following **IPv6 RA Prefix** settings:

Prefix Type	Set the prefix delegation type used with this configuration. Options include, *Prefix*, and *prefix-from-provider*. The default setting is Prefix. A provider assigned prefix is made available from an *Internet Service Provider* (ISP) to automate the process of providing and informing the prefixes used.
Prefix or ID	Set the actual prefix or ID used with the IPv6 router advertisement.
Site Prefix	The site prefix is added into a router advertisement prefix. The site address prefix signifies the address is only on the local link.
Valid Lifetime Type	Set the lifetime for the prefix's validity. Options include *External (fixed), decrementing* and *infinite*. If set to External (fixed), just the *Valid Lifetime Sec* setting is enabled to define the exact time interval for prefix validity. If set to decrementing, use the lifetime date and time settings to refine the prefix expiry period. If the value is set for infinite, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is External (fixed).
Valid Lifetime Sec	If the lifetime type is set to *External (fixed),* set the *Seconds, Minutes, Hours* or *Days* value used to measurement criteria for the prefix's expiration. 30 days, 0 hours, 0 minutes and 0 seconds is the default lifetime.
Valid Lifetime Date	If the lifetime type is set to *External (fixed)*, set the date in MM/DD/YYYY format for the expiration of the prefix.

Valid Lifetime Time	If the lifetime type is set to *decrementing*, set the time for the prefix's validity.
Preferred Lifetime Type	Set the administrator preferred lifetime for the prefix's validity. Options include *External (fixed), decrementing* and *infinite*. If set to External (fixed), just the *Valid Lifetime Sec* setting is enabled to define the exact time interval for prefix validity. If set to decrementing, use the lifetime date and time settings to refine the prefix expiry period. If the value is set for infinite, no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is External (fixed).
Preferred Lifetime Sec	If the administrator preferred lifetime type is set to *External (fixed)*, set the *Seconds, Minutes, Hours* or *Days* value used to measurement criteria for the prefix's expiration. 30 days, 0 hours, 0 minutes and 0 seconds is the default lifetime.
Preferred Lifetime Date	If the administrator preferred lifetime type is set to *External (fixed),* set the date in MM/DD/YYYY format for the expiration of the prefix.
Preferred Lifetime Time	If the preferred lifetime type is set to *decrementing,* set the time for the prefix's validity.
Autoconfig	Autoconfiguration includes generating a link-local address, global addresses via stateless address autoconfiguration and duplicate address detection to verify the uniqueness of the addresses on a link. This setting is enabled by default.
On Link	Select this option to keep the IPv6 RA prefix on the local link. The default setting is enabled.

46 Select **OK** to save the changes to the IPv6 RA prefix configuration. Select **Exit** to close the screen without saving the updates.

47 Select the **Security** tab.

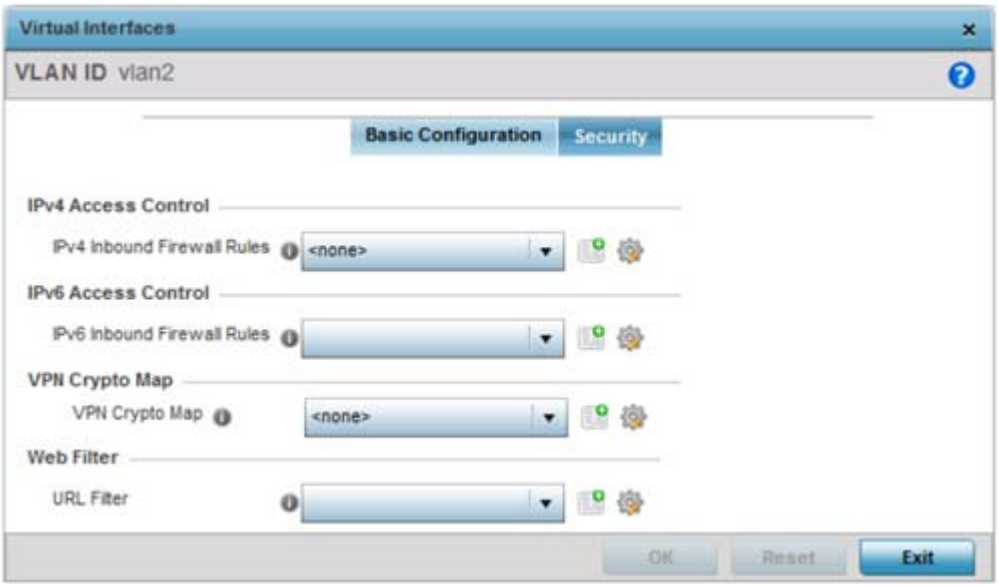


Figure 8-70 *Virtual Interfaces - Security screen*

48 Use the **IPv4 Inbound Firewall Rules** drop down menu to select the IPv4 specific inbound firewall rules to apply to this profile's virtual interface configuration. Select the **Create** icon to define a new IPv4 firewall rule configuration or select the **Edit** icon to modify an existing configuration.

IPv4 is a connectionless protocol for packet switched networking. IPv4 operates as a best effort delivery method, since it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP).

IPv4 and IPv6 are different enough to warrant separate protocols. IPv6 devices can alternatively use stateless address autoconfiguration. IPv4 hosts can use link local addressing to provide local connectivity.

49 Use the **IPv6 Inbound Firewall Rules** drop down menu to select the IPv6 specific inbound firewall rules to apply to this profile's virtual interface configuration. Select the **Create** icon to define a new IPv6 firewall rule configuration or select the **Edit** icon to modify an existing configuration.

IPv6 is the latest revision of the *Internet Protocol* (IP) replacing IPv4. IPV6 provides enhanced identification and location information for systems routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

50 Use the **VPN Crypto Map** drop down menu to select a crypto map to apply to this profile's virtual interface configuration. Crypto maps are sets of configuration parameters for encrypting packets passing through a VPN Tunnel. If a crypto map does not exist suiting the needs of this virtual interface, select the **Create** icon to define a new crypto map configuration or the **Edit** icon to modify an existing crypto map. For more information, see *Overriding a Profile's VPN Configuration on page 5-207*.

51 Select **OK** to save the changes to the OSPF configuration. Select **Reset** to revert to the last saved configuration.

52 Select the **Dynamic Routing** tab (if available in your profile).

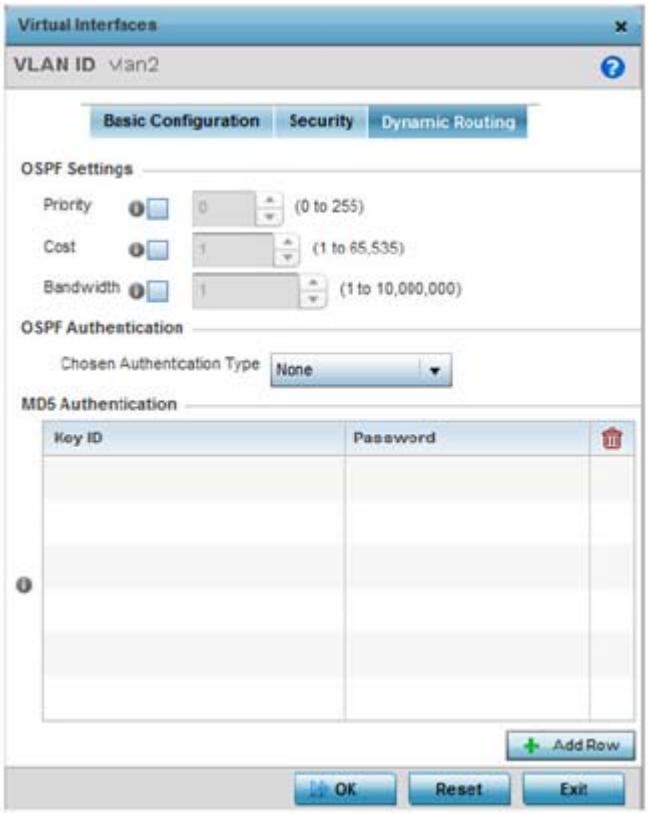


Figure 8-71 *OSPF Virtual Interface - Dynamic Routing screen*

53 Define or override the following parameters from within the **OSPF Settings** field:

Priority	Select this option to set the OSPF priority used to select the network designated route. Use the spinner control to set the value from 0 - 255.

Cost	Select this option to set the cost of the OSPF interface. Use the spinner control to set the value from 1 - 65,535.
Bandwidth	Set the OSPF interface bandwidth (in Kbps) from 1 - 10,000,000.

54 Select the authentication type from the **Chosen Authentication Type** drop-down used to validate credentials within the OSPF dynamic route. Options include *simple-password, message-digest, null* and *None*. The default value is None.

55 Select **+ Add Row** at the bottom of the **MD5 Authentication** table to add the Key ID and Password used for an MD5 validation of authenticator credentials. Use the spinner control to set the OSPF message digest authentication key ID. The available range is from 1 - 255. The password is the OSPF key either displayed as series or asterisks or in plain text (by selecting **Show**).

MD5 is a message digest algorithm using a cryptographic hash producing a 128-bit (16-byte) hash value, usually expressed in text as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

56 Select **OK** to save the changes to the configuration. Select **Reset** to revert to the last saved configuration.

8.8.11 Setting a Profile's Border Gateway Protocol (BGP) Configuration

Profile Network Configuration

Border Gateway Protocol (BGP) is an inter-ISP routing protocol which establishes routing between ISPs. ISPs use BGP to exchange routing and reachability information between *Autonomous Systems* (AS) on the Internet. BGP makes routing decisions based on paths, network policies and/or rules configured by network administrators. The primary role of a BGP system is to exchange network reachability information with other BGP peers. This information includes information on AS that the reachability information traverses. This information is sufficient to create a graph of AS connectivity from which routing decisions can be created and rules enforced.

An *Autonomous System* (AS) is a set of routers under the same administration that use *Interior Gateway Protocol* (IGP) and common metrics to define how to route packets within the AS. AS uses inter-AS routing to route packets to other ASs. For an external AS, an AS appears to have a single coherent interior routing plan and presents a consistent picture of the destinations reachable through it.

Routing information exchanged through BGP supports only destination based forwarding (it assumes a router forwards packets based on the destination address carried in the IP header of the packet).

BGP uses TCP as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgement, and sequencing. BGP listens on TCP port 179. The error notification mechanism used in BGP assumes that TCP supports a *graceful* close (all outstanding data is delivered before the connection is closed).

To define a profile's BGP configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **BGP**.

NOTE: BGP is only supported on RFS4000, RFS6000, NX4500, NX6500, NX9000 and NX9500 model controllers and service platforms.

The **General** tab displays by default.

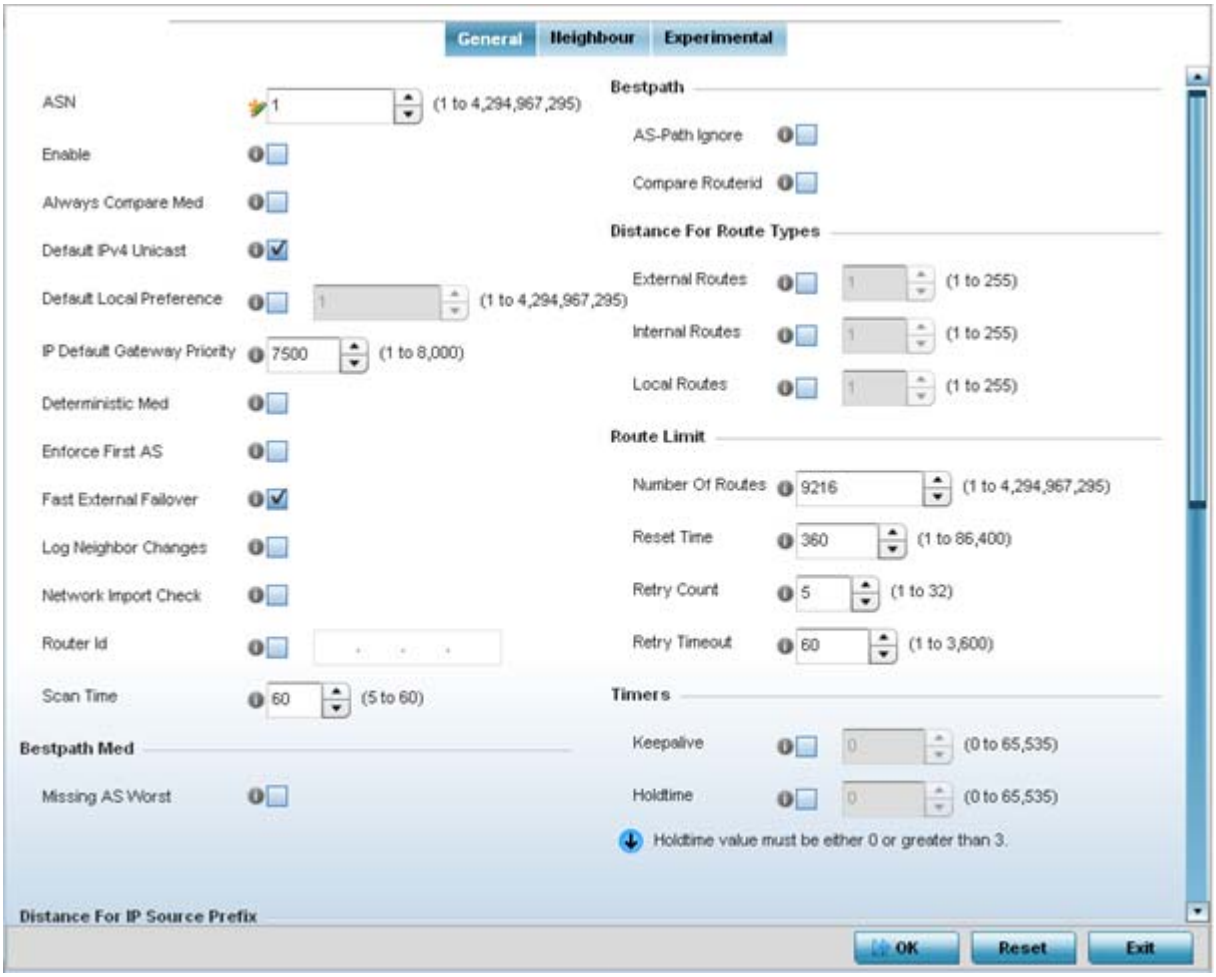


Figure 8-72 *Border Gateway Protocol - General tab*

4 Review the following BGP general configuration parameters to determine whether an update is warranted.

ASN	Define the *Autonomous System Number* (ASN). ASN is a set of routers under the same administration that use *Interior Gateway Protocol* (IGP) and common metrics to define how to route packets. Select a value from 1 - 4,294,967,295.
Enable	Enable to start BGP on this controller or service platform. BGP is only supported on RFS4000, RFS6000, NX4500, NX6500, NX9000 and NX9500 model controllers and service platforms. The default is disabled.
Always Compare MED	*Multi-exit Discriminator* (MED) is a value used by BGP peers to select the best route among multiple routes. When enabled, the MED value encoded in the route is always compared when selecting the best route to the host network. A route with a lower MED value is always selected over a route with a higher MED value. BGP does not discriminate between iBGP and eBGP when using MED for route selection. This option is mutually exclusive to the *Deterministic MED* option.
Default IPv4 Unicast	Select this option to enable IPv4 unicast traffic for neighbors. This option is disabled by default.

Default Local Preference	Select this option to enable a local preference for the neighbor. When enabled, set the local preference value (1 - 4,294,967,295).
IP Default Gateway Priority	Set the default priority value for the IP Default Gateway. Set a value from 1 - 8000. The default is 7500.
Deterministic MED	*Multi-exit Discriminator* (MED) is used by BGP peers to select the best route among multiple routes. When enabled, MED route values (from the same AS) are compared to select the best route. This best route is then compared with other routes in the BGP route table to select the best overall route. This option is mutually exclusive to the *Always Compare MED* option.
Enforce First AS	Select this option to deny any updates received from an external neighbor that does not have the neighbor's configured AS at the beginning of the received AS path parameter. This enhances security by not allowing traffic from an unauthorized AS. This setting is disabled by default.
Fast External Failover	Select this option to immediately reset the BGP session on the interface once the BGP connection goes down. Normally, when a BGP connection goes down, the device waits for the expiry of the duration specified in *Holdtime* parameter before bringing down the interface. This setting is enabled by default.
Log Neighbor Changes	Select this option to enable logging of changes in routes to neighbor BGP peers. This enables the logging of only the changes in neighbor routes. All other events must be explicitly turned on using debug commands. This setting is disabled by default.
Network Import Check	Select this option to enable a network import check to ensure consistency in advertisements. This setting is disabled by default.
Router ID	Select this option to manually configure the router ID for this BGP supported controller or service platform. The router ID identifies the device uniquely. When no router ID is specified, the IP address of the interface is considered the router ID. This setting is disabled by default.
Scan Time	Select this option to set the scanning interval for updating BGP routes. This interval is the period between two consecutive scans the BGP device checks for the validity of routes in its routing table. To disable this setting, set the value to Zero (0). The default setting is 60 seconds.

5 Optionally select the **Missing AS Worst** option to treat any path that does not contain a MED value as the least preferable route. This setting is disabled by default.

6 Set the following **Bestpath** parameters:

AS-Path Ignore	Select this option to prevent an AS path from being considered as a criteria for selecting a preferred route. The route selection algorithm uses the AS path as one of the criteria when selecting the best route. When this option is enabled, the AS path is ignored.
Compare Router ID	Select this option to use the router ID as a selection criteria when deermining a preferred route. The route selection algorithm uses various criteria when selecting the best route. When this option is enabled, the router ID is used to select the best path between two identical BGP routes. The route with the lower route ID is selected over a route with a higher route id.

7 Set or override the following **Distance for Route Types**. The distance parameter is a rating of route trustworthiness. The greater the distance, the lower the trust rating. The distance can be set for each type of route indicating its trust rating:

External Routes	External routes are those routes learned from a neighbor of this BGP device. Set a value from 1 - 255.
Internal Routes	Internal routes are those routes learned from another router within the same AS. Set a value from 1 - 255.
Local Routes	Local routes are those routes being redistributed from other processes within this BGP router. Set a value from 1 - 255.

8 Set or override the following **Route Limit** parameters:

Number of Routes	Configures the number of routes that can be stored on this BGP router. Set this value based on the available memory on this BGP router. Configure a value from 1 - 4,294,967,295. The default value is 9,216 routes.
Reset Time	Configures the reset time. This is the time limit after which the *Retry Count* value is set to Zero (0). Set a value from 1- 86,400 seconds.
Retry Count	Configures the number of time the BGP process is reset before it is shut down. Once shut down, the BGP process has to be started manually. The BGP process is reset if it is flooded with route entries that exceed its number of routes. Set a value from 1 - 32.
Retry Timeout	Configures the time duration in seconds the BGP process is shutdown temporarily before a reset of the process is attempted. Set a value from 1 - 3,600 seconds.

9 Set the following **Timers**:

Keepalive	Set the duration, in seconds, for the keep alive timer used to maintain connections between BGP neighbors. Set a value from 1 - 65,535 seconds.
Holdtime	Set the time duration, in seconds, for the hold (delay) of packet transmissions.

10 Set the following **Aggregate Address** fields:

Aggregate addresses are used to minimize the size of the routing tables. Aggregation combines the attributes of several different routes and advertises a single route. This creates an aggregation entry in the BGP routing table if more specific BGP routes are available in the specified address range.

IP Prefix	Enter an IP address and mask used as the aggregate address.
Summary Only	Select this option to advertise the IP Prefix route to the BGP neighbor while suppressing the detailed and more specific routes.
As Set	Generates AS set path information. Select to enable. When selected, it creates an aggregate entry advertising the path for this route, consisting of all elements contained in all the paths being summarized. Use this parameter to reduce the size of path information by listing the AS number only once, even if it was included in the multiple paths that were aggregated.

11 Set the following **Distance for IP Source Prefix** fields:

IP Source Prefix	Enter an IP address and mask used as the prefix source address.

Admin Distance	Use the spinner control to set the BGP route's admin distance from 1 - 255.
IP Access List	Provide the IP address used to define the prefix list rule.

12 Configure the following **Network** values:

Network	Configure an IP address to broadcast to neighboring BGP peers. This network can be a single IP address or a range of IP addresses in *A.B.C.D/M* format.
Pathlimit	Configure the maximum path limit for this AS. Set a value from 1 - 255 AS hops.
Backdoor	Select this option to indicate to border devices this network is reachable using a backdoor route. A backdoor network is treated the same as a local network, except it is not advertised. This setting is disabled by default.
Route Map	Select an existing route map as a method of controlling and modifying routing information. The control of route information occurs using route redistribution keys.

13 Configure the following **Route Redistribute** values:

Route Type	Use the drop-down menu to define the route type as either *connected*, *kernal*, *ospf* or *static*.
Metric	Select this option to set a numeric route metric used for route matching and permit designations.
Route Map	Select an existing route map as a method of controlling and modifying routing information. The control of route information occurs using route redistribution keys.

14 Select **OK** to save the changes and overrides. Select **Reset** to revert to the last saved configuration.

15 Select the **Neighbor** tab.

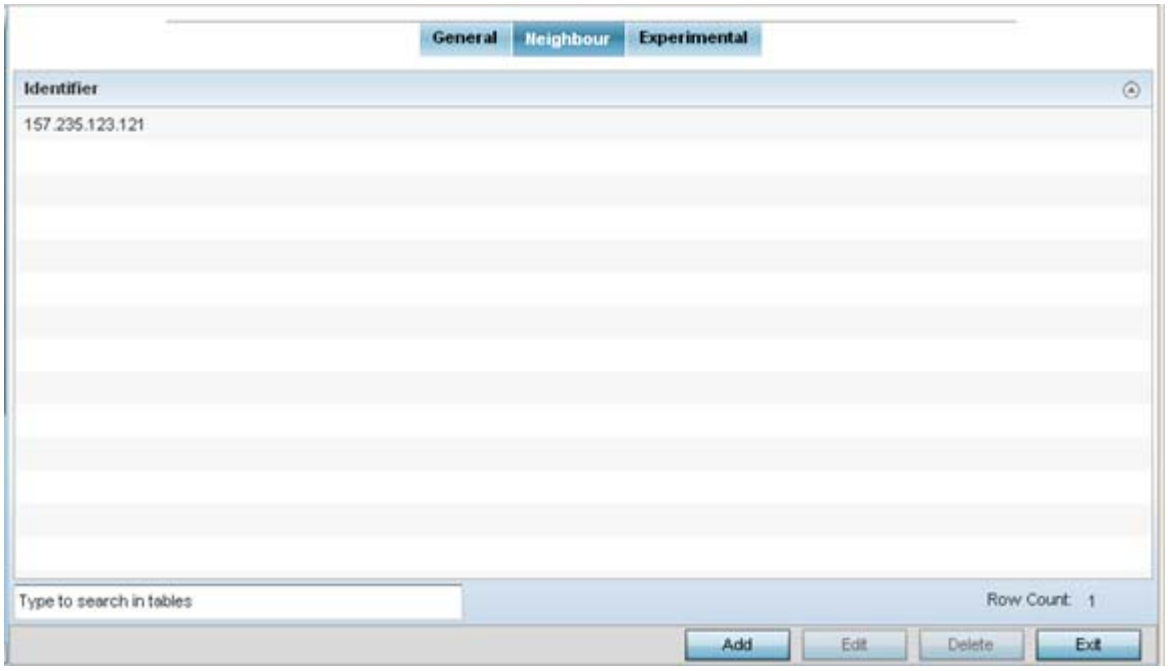


Figure 8-73 *Border Gateway Protocol - Neighbor tab*

The **Neighbor** tab displays a list of configured BGP neighbor devices identified by their IP address. Select **Add** to add a new BGP neighbor configuration or select an existing **Identifier** and select **Edit** to modify it. The following screen displays with the **General** tab displayed by default.

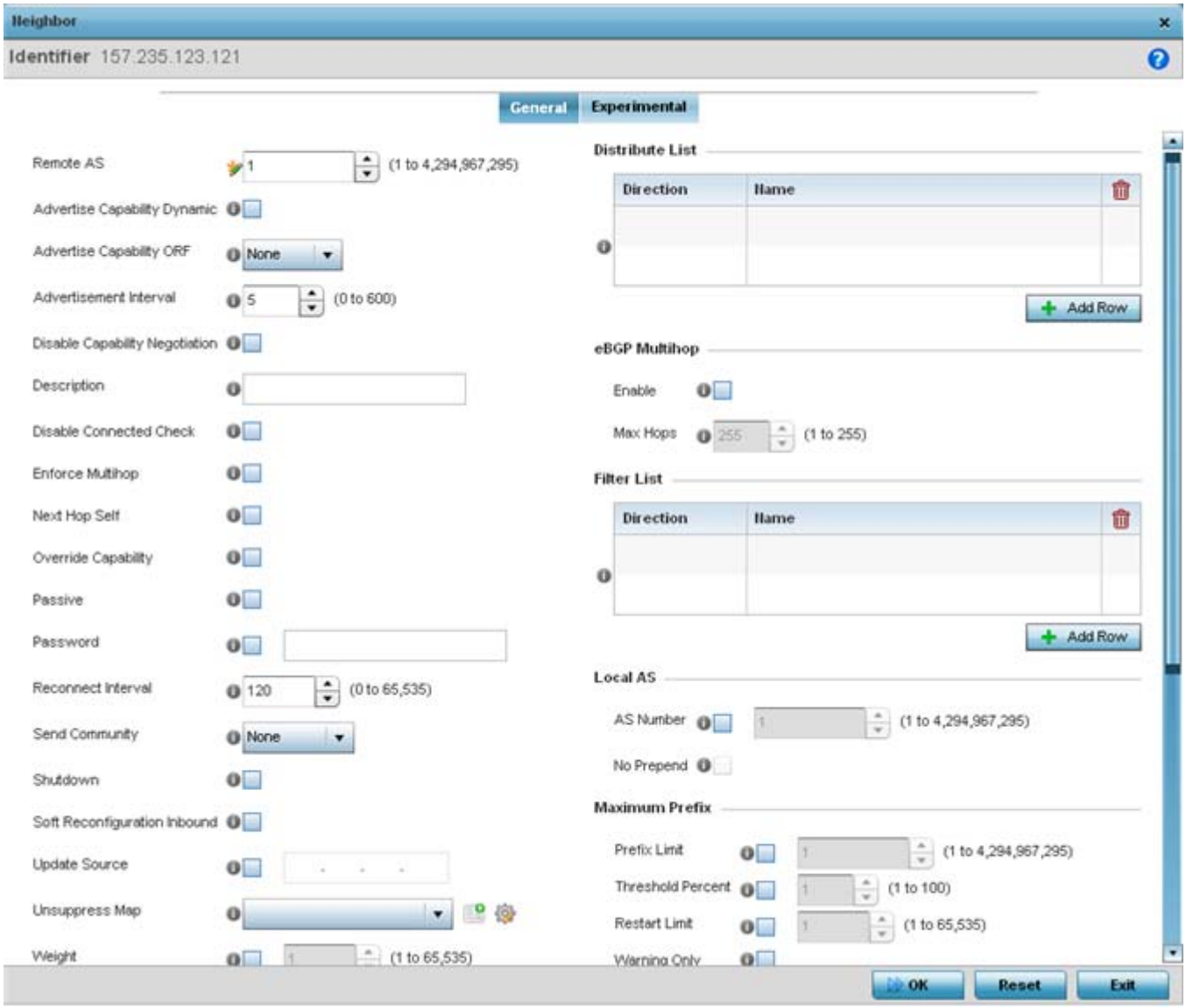


Figure 8-74 *Border Gateway Protocol - Neighbor tab - General screen*

The **General** tab displays the different configuration parameters for the neighbor BGP device.

16 Configure the following common parameters:

Remote AS	Define the *Autonomous System Number* (ASN) for the neighbor BGP device. ASN is a set of routers under the same administration that use *Interior Gateway Protocol* (IGP) and common metrics to define how to route packets within the AS. Set a value from 1 - 4,294,967,295.
Advertise Capability Dynamic	Select this option to show a neighbor device's capability to advertise or withdraw and address capability to other peers in a non-disruptive manner. This setting is disabled by default.

Advertise Capability ORF	Select this option to enable *Outbound Router Filtering* (ORF) and advertise this capability to peer devices. ORFs send and receive capabilities to lessen the number of updates exchanged between BGP peers. By filtering updates, ORF minimizes update generation and exchange overhead. The local BGP device advertises ORF in the *send* mode. The peer BGP device receives the ORF capability in *receive* mode. The two devices exchange updates to maintain the ORF for each router. Only a peer group or an individual BGP router can be configured to be in *receive* or *send* mode. A member of a peer group cannot be configured.
Advertisement Interval	Use the *Advertisement Interval* to set the minimum interval between sending BGP router updates. Sending too many router updates creates flapping of routes leading to possible disruptions. Set a minimum interval so that the BGP routing updates are sent after the set interval in seconds. The default is 5 seconds.
Disable Capability Negotiation	Select to disable capability negotiation with BGP neighbors. This is to allow compatibility with older BGP versions that have no capability parameters used in the *open* messages between peers. This setting id disabled by default.
Description	Provide a 80 character maximum description for this BGP neighbor device.
Disable Connected Check	If utilizing loopback interfaces to connect single-hop BGP peers, enable the neighbor disable connected check before establishing a the BGP peering session.This setting is disabled by default.
Enforce Multihop	A *multihop* route is a route to external peers on indirectly connected networks. Select to enforce neighbors to perform multi-hop check. This setting is disabled by default.
Next Hop Self	Select to enable *Next Hop Self*. Use this to configure this device as the next hop for a BGP speaking neighbor or peer group. This allows the BGP device to change the next hop information that is sent to iBGP peers. The next hop address is set to the IP address of the interface used to communicate with the eBGP neighbor. This setting is disabled by default
Override Capability	Select this to enable the ability to override capability negotiation result. This setting is disabled by default.
Passive	Select this option to set this BGP neighbor as passive. When a neighbor is set as passive, the local device should not attempt to open a connection to this device. This setting is disabled by default.
Password	Select this option to set a password for this BGP neighbor. Use the text-box to enter the password to use for this neighbor.
Reconnect Interval	Set a reconnection interval for peer BGP devices from 0 - 65,535 seconds. The default setting is 120 seconds.
Send Community	Select this option to ensure the community attribute is sent to the BGP neighbor. The community attribute groups destinations in a certain community and applies routing decisions based on the community. On receiving community attribute, the BGP router announces it to the neighbor.
Shutdown	Select this option to administratively shutdown this BGP neighbor. This setting is disabled by default.

Soft Reconfiguration Inbound	Select this option to store updates for inbound soft reconfiguration. Soft-reconfiguration can be used in lieu of BGP route refresh capability. Selecting this option enables local storage of all received routes and their attributes. This requires additional memory on the BGP device. When a soft reset (inbound) is performed on the neighbor device, the locally stored routes are reprocessed according to the inbound policy. The BGP neighbor connection is not affected.
Update Source	Select this option to allow internal BGP sessions to use any operational interface for TCP connections. Use *Update Source* in conjunction with any specified interface on the router. The loopback interface is the interface that is most commonly used with this command. The use of loopback interface eliminates a dependency and BGP does not have to rely on the availability of a particular interface for making TCP connections. This setting is disabled by default.
Unsuppress Map	Enable *Unsuppress Map* to selectively advertise more precise routing information to this neighbor. Use this in conjunction with the *Route Aggregate* command. The Route Aggregate command creates a route map with a IP/mask address that consolidates the subnets under it. This enables a reduction in number of route maps on the BGP device to one entry that encompasses all the different subnets. Use Unsuppress Map to selectively allow/deny a subnet or a set of subnets. Use the *Create* icon to create a new route map. Use the *Edit* icon to edit an existing route map list after selecting it.
Weight	Select to set the weight of all routes learned from this BGP neighbor. Weight is used to decide the preferred route when the same route is learned from multiple neighbors. The highest weight is always chosen.

17 Configure or set the following **Default Originate** parameters. Default originate is used by the local BGP router to send the default route 0.0.0.0 to its neighbor for use as a default route.

Enable	Select to enable *Default* Originate on this BGP neighbor. This setting is disabled by default.
Route Map	Use the drop-down menu to select a route map to use as the *Default Originate* route.

18 Configure or set the following **Route Map** parameters by selecting **Add Row**. This configures how route maps are applied for this BGP neighbor.

Direction	Use the drop-down menu to configure the direction on which the selected route map is applied. Select one from *in*, *out*, *export* or *import*.
Route Map	Use the drop-down menu to select the route map to use with this BGP neighbor. Use the *Create* icon to create a new route map. Use the *Edit* icon to edit an existing route map after selecting it.

19 Configure or set the following **Distribute List** parameters by selecting **Add Row**. Up to 2 distribute list entries can be created.

Direction	Use the drop-down menu to configure the direction on which the selected IP access list is applied. Select either *in* or *out*.

Name	Use the drop-down menu to select the route map to use with this BGP neighbor. Use the *Create* icon to create a new IP Access list. Use the *Edit* icon to edit an existing IP Access list after selecting it.

20 Configure or set the following **eBGP Multihop** parameters. This configures the maximum number of hops that can be between eBGP neighbors not directly connected to each other.

Enable	Select to enable *eBGP Multihop* on this BGP neighbor.
Max Hops	Set the maximum number of hops between eBGP neighbors not connected directly. Select a value from 1 - 255.

21 Configure or set the following **Filter List** parameters by selecting **Add Row**. Up to 2 filter list entries can be created.be created.

Direction	Use the drop-down menu to configure the direction on which the selected AS Path list is applied. Select either *in* or *out.*
Name	Use the drop-down menu to select the AS Path list to use with this BGP neighbor. Use the *Create* icon to create a new AS Path list. Use the *Edit* icon to edit an existing AS Path list after selecting it.

22 Configure or set the following **Local AS** parameters.

CAUTION: This is an experimental feature and its actual operation may be unpredictable.

AS Number	Specify the local *Autonomous System* (AS) number. Select from 1 - 4,294,967,295.
No Prepend	Select to enable. When enabled, the local AS number is not prepended to route updates from eBGP peers.

23 Configure or set the following **Maximum Prefix** value. This configures the maximum number of prefix that can be received from a BGP neighbor.

Prefix Limit	Sets the maximum number of prefix that can be received from a BGP neighbor. Select from 1 - 4,294,967,295. Once this threshold is reached, the BGP peer connection is reset.
Threshold Percent	Sets the threshold limit for generating a log message. When this percent of the *Prefix Limit* is reached, a log entry is generated. For example if the *Prefix Limit* is set to 100 and *Threshold Percent* is set to 65, then after receiving 65 prefixes, a log entry is created.
Restart Limit	Sets the number of times a reset BGP peer connection is restarted. Select a value from 1 - 65535
Warning Only	Select to enable. When the number of prefixes specified in *Prefix Limit* field is exceeded, the connection is reset. However, when this option is enabled, the connection is not reset and an event is generated instead. This setting is disabled by default.

24 Configure or set the following **Prefix List** parameters. Up to 2 prefix list entries can be created.

Direction	Use the drop-down menu to configure the direction on which the selected IP prefix list is applied. Select either *in* or *out.*

Name	Use the drop-down menu to select the IP prefix list to use with this BGP neighbor. Use the *Create* icon to create a new IP prefix list or select the *Edit* icon to edit an existing IP prefix list after selecting it.

25 Set the following **Timers** for this BGP neighbor:

Keepalive	Set the time duration in seconds for keepalive. The keep alive timer is used to maintain connections between BGP neighbors. Set a value from 1 - 65,535 seconds.
Holdtime	Set the time duration in seconds for hold time.

26 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

27 Select the **Experimental** tab.

CAUTION: This is an experimental feature and its actual operation may be unpredictable.

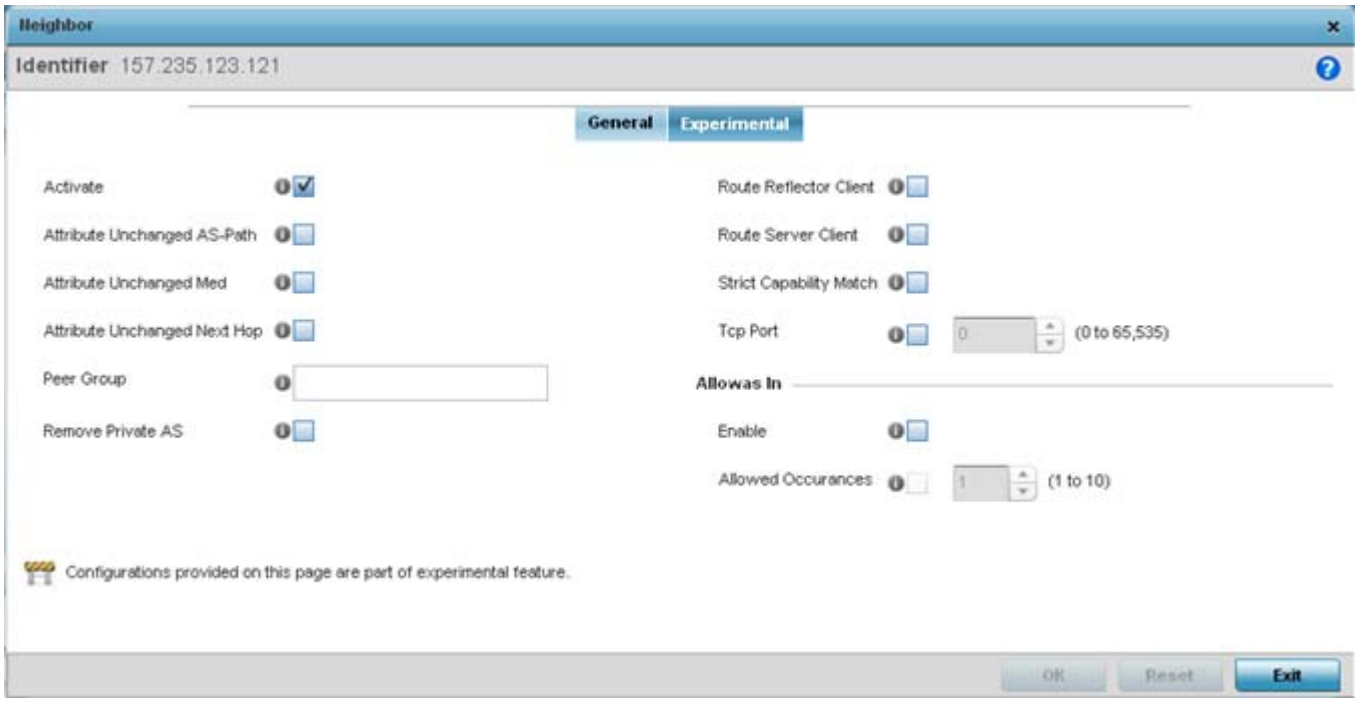


Figure 8-75 *Border Gateway Protocol - Neighbor tab - Experimental tab*

28 Set the following **Experimental** BGP parameters:

Activate	Enable an address family for this neighbor. This setting is enabled by default.
Attribute Unchanged AS-Path	Select to enable propagating AS path BGP attribute unchanged to this neighbor BGP device. This setting is enabled by default.
Attribute Unchanged Med	Select to enable propagating MED BGP attribute unchanged to this neighbor BGP device. This setting is enabled by default.

Attribute Unchanged Next Hop	Select to enable propagating the next hop BGP attribute value unchanged to this neighbor BGP device. This setting is enabled by default.
Peer Group	Set the peer group for this BGP neighbor device. Peer groups are a set of BGP neighbors with the same update policies. This facilitates the updates of various policies, such as, distribute lists and filter lists. The peer group can be configured as a single entity. Any changes made to the peer group is propagated to all members.
Remove Private AS	Select this option to remove the private *Autonomous System* (AS) number from outbound updates. Private AS numbers are not advertised to the Internet. This option is used with external BGP (eBGP) peers only. The router removes the AS numbers only if the update includes private AS numbers. If the update includes both private and public AS numbers, the system treats it as an error.
Route Reflector Client	Select this option to enable this BGP neighbor as a route reflector client for the local router. Route reflectors control large numbers of iBGP peering.Using route reflection, the number of iBGP peers is reduced. This option configures the local BGP device as a route reflector and the neighbor as its route reflector client. This setting is disabled by default.
Route Server Client	Select this option to enable this neighbor BGP device to act as a route server client. This setting is disabled by default.
Strict Capability Match	Select this option to enable a strict capability match before allowing a neighbor BGP peer to open a connection. When capabilities do not match, the BGP connection is closed. This setting is disabled by default.
TCP Port	Select to enable configuration of non-standard BGP port for this BGP neighbor. By default the BGP port number is 179. To configure a non standard port for this BGP neighbor, use the control to set the port number. Select a value from 1 - 65535.

29 Configure or set the following **Allowas In** parameters. This configures the *Provider Edge* (PE) routers to allow the re-advertisement of all prefixes containing duplicate *Autonomous System Numbers* (ASN). This creates a pair of *VPN Routing/Forwarding* (VRF) instances on each PE router to receive and re-advertise prefixes. The PE router receives prefixes with ASNs from all PE routers and advertises to its neighbor PE routers on one VRF. The other VRF receives prefixes with ASNs from the *Customer Edge* (CE) routers and re-advertises them to all PE routers in the configuration.

Enable	Select this option to enable re-advertisement of all prefixes containing duplicate ASNs.
Allowed Occurrences	Set the maximum number of times an ASN is advertised. Select a value in the rage 1 - 10.

30 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration. Select **Exit** to close this window and go back to the main screen.

31 Select the **Experimental** tab from the BGP main screen.

CAUTION: This is an experimental feature and its actual operation may be unpredictable.

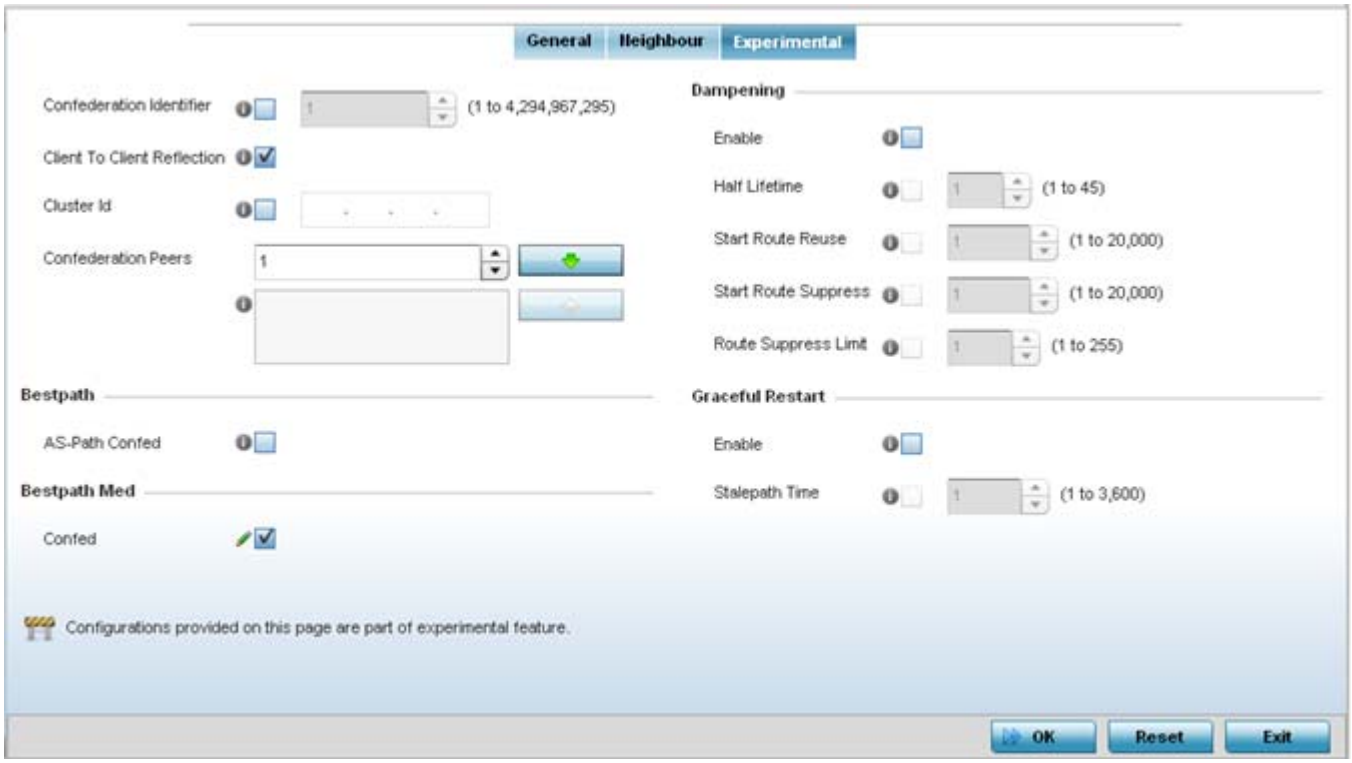


Figure 8-76 *Border Gateway Protocol - Experimental tab*

32 Set the following **Experimental** BGP features:

Confederation Identifier	Enable and set a *confederation identifier* to allow an AS to be divided into several ASs. This confederation is visible to external routers as a single AS. Select a value from 1 - 4,294,967,295.
Client to Client Reflection	Select to enable client-to-client route reflection. Route reflectors are used when all iBGP speakers are not fully meshed. If the clients are fully meshed, the route-reflectors are not required. The default is enabled.
Cluster ID	Select to enable and set a Cluster ID if the BGP cluster has more than one route-reflectors. A cluster generally consists of a single route-reflector and its clients. The cluster is usually identified by the router ID of this single route-reflector. Sometimes, to increase the redundancy, a cluster might have more than one route-reflectors configured. In this case, all route-reflectors in the cluster are identified by the Cluster ID. Select a value from 1 - 4,294,967,295.
Confederation Peers	Use this spinner to select the confederation members. Once selected, select the *Down Arrow* button next to this control to add the AS as a confederation member. Multiple AS configurations can be added to the list of confederation members. To remove an AS as a confederation member, select the AS from the list and select the *Up Arrow* button next to the list.

33 Configure or set the following **Bestpath** parameter:

AS-Path Confed	Select this option to allow the comparison of the confederation AS path length when selecting the best route. This indicates the AS confederation path length must be used, if available, in the BGP path when deciding the best path.

34 Configure or set the following **Bestpath MED** parameter:

Confed	Select to enable. Use this option to allow comparing MED when selecting the best route when learned from confederation peers. This indicates that MED must be used, when available, in the BGP best path when deciding the best path between routes from different confederation peers.

35 Configure or set the following **Dampening** parameters. Dampening minimizes the instability caused by route flapping. A penalty is added for every flap in the flapping route. As soon as the total penalty reaches the *Route Suppress Limit* value, the advertisement of this route is suppressed. This penalty is delayed when the time specified in *Half Lifetime* occurs. Once the penalty becomes lower than the value specified in *Start Route Reuse*, the advertisement of the route is un-suppressed.

Enable	Select to enable dampening on advertised routes. When this option is selected, other configuration fields in this Dampening field are enabled. This setting is disabled by default.
Half Lifetime	Select to enable and configure the half lifetime value. A penalty is imposed on a route that flaps. This is the time for the penalty to decrease to half its current value. Set a value from 1 - 45 in minutes. The default is 1 second.
Start Route Reuse	Select to enable and configure the route reuse value. When the penalty for a suppressed route decays below the value specified in *Start Route Reuse* field, the route is un-suppressed. Set a value from 1 - 20000.
Start Route Suppress	Select to enable and configure the route suppress value. When a route flaps, a penalty is added to the route. When the penalty reaches or exceeds the value specified in *Route Suppress Limit*, the route is suppressed. Set a value from 1 - 20000.
Route Suppress Limit	Select to enable and configure the maximum duration in minutes a suppressed route is suppressed. This is the maximum duration for which a route remains suppressed before it is reused. Set a value from 1 - 255 minutes.

36 Configure or set the **Graceful Restart** parameters. This provides a graceful restart mechanism for a BGP session reset in which the BGP daemon is not restarted, so that any changes in network configuration that caused the BGP reset does not affect packet forwarding.

Enable	Select to enable a graceful restart on this BGP router. This section is disabled by default.
Stalepath Time	Configure the maximum time to retain stale paths from restarting neighbor. This is the time the paths from a restarting neighbor is preserved. All stale paths, unless reinstated by the neighbor after re-establishment, are deleted at the expiry of this timer value. Set a value from 1 - 3600 seconds.

37 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration. Select **Exit** to close this window and go back to the main screen.

8.8.12 Setting a Profile's Forwarding Database Configuration

Profile Network Configuration

A *Forwarding Database* is used by a bridge to forward or filter packets. The bridge reads the packet's destination MAC address and decides to either forward the packet or drop (filter) it. If it is determined the destination MAC is

on a different network segment, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered). As nodes transmit packets through the bridge, the bridge updates its forwarding database with known MAC addresses and their locations on the network. This information is then used to filter or forward the packet.

To define a forwarding database configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **Forwarding Database**.

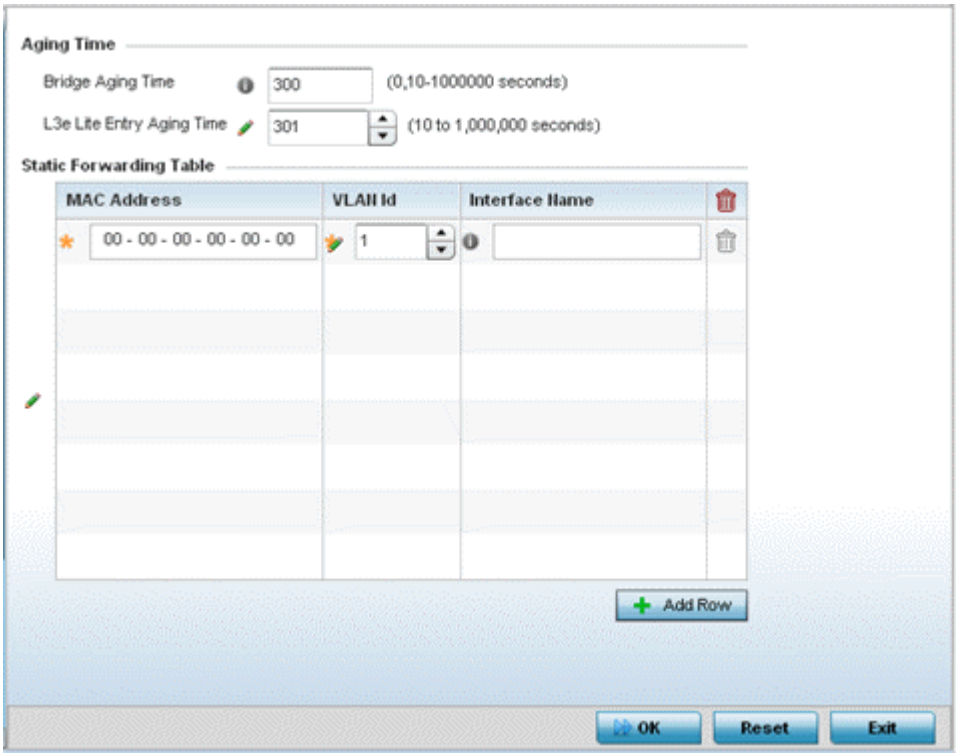


Figure 8-77 *Forwarding Database screen*

4 Define a **Bridge Aging Time** between 0, 10-1,000,000 seconds.

The aging time defines the length of time an entry remains in the a bridge's forwarding table before being deleted due to inactivity. If an entry replenishments a destination generating continuous traffic, this timeout value will never be invoked. However, if the destination becomes idle, the timeout value represents the length of time that must be exceeded before an entry is deleted from the forwarding table. The default setting is 300 seconds.

5 Define a **L3e Lite Entry Aging Time** between 10-1,000,000 seconds.

The default setting is 300 seconds.

6 Use the **+ Add Row** button to create a new row within the MAC address table.

7 Set a destination MAC Address address. The bridge reads the packet's destination MAC address and decides to forward the packet or drop (filter) it. If it's determined the destination MAC is on a different network, it forwards the packet to the segment. If the destination MAC is on the same network segment, the packet is dropped (filtered)

8 Define the target **VLAN ID** if the destination MAC is on a different network segment.

9 Provide an **Interface Name** used as the target destination interface for the target MAC address.

10 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

8.8.13 Setting a Profile's Bridge VLAN Configuration

Profile Network Configuration

A *Virtual LAN* (VLAN) is separately administrated virtual network within the same physical managed network. VLANs are broadcast domains defined to allow control of broadcast, multicast, unicast, and unknown unicast within a Layer 2 device.

Administrators often need to route traffic to interoperate between different VLANs. Bridging VLANs are only for non-routable traffic, like tagged VLAN frames destined to some other device which will untag it. When a data frame is received on a port, the VLAN bridge determines the associated VLAN based on the port of reception. Using forwarding database information, the Bridge VLAN forwards the data frame on the appropriate port(s). VLAN's are useful to set separate networks to isolate some computers from others, without actually having to have separate cabling and Ethernet switches. Controllers and service platforms can do this on their own, without the need to know what VLAN it's on (this is called port-based VLAN, since it's assigned by port). Another common use is to put specialized devices like VoIP Phones on a separate network for easier configuration, administration, security or service quality.

To define a bridge VLAN configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **Bridge VLAN**.

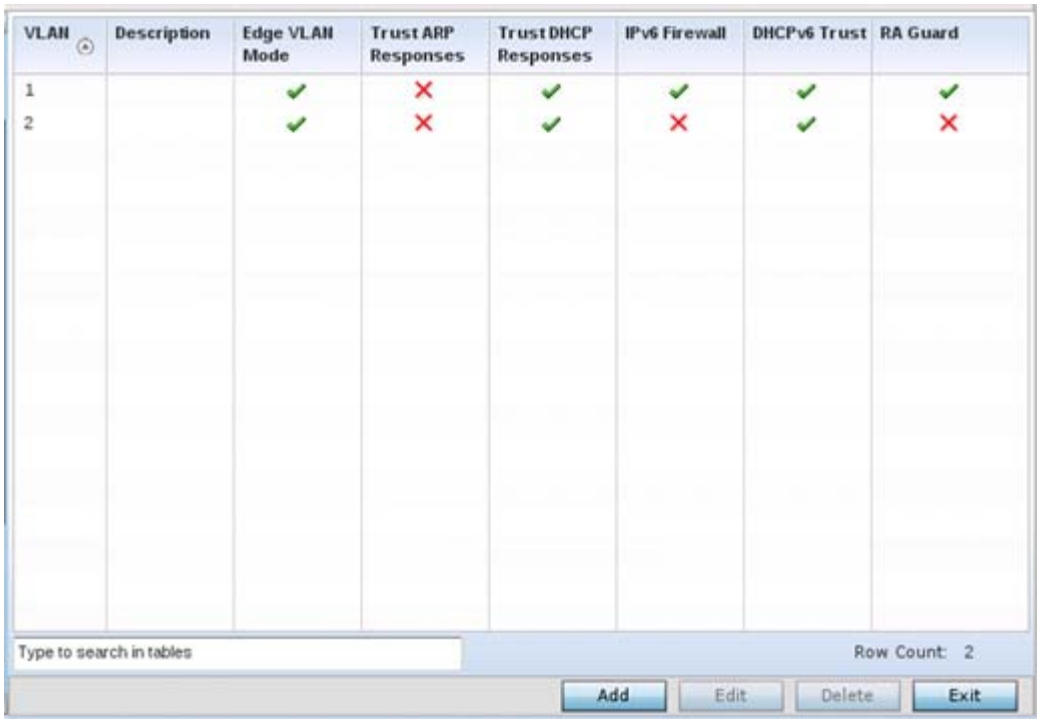


Figure 8-78 *Profile - Network Bridge VLAN screen*

4 Review the following VLAN configuration parameters to determine whether an update is warranted:

VLAN	Lists the numerical identifier defined for the Bridge VLAN when initially created. The available range is from 1 - 4095. This value cannot be modified during the edit process.
Description	Lists a description of the VLAN assigned when it was created or modified. The description should be unique to the VLAN's specific configuration and help differentiate it from other VLANs with similar configurations.
Edge VLAN Mode	Defines whether the VLAN is currently in edge VLAN mode. A green checkmark defines the VLAN as extended. An edge VLAN is the VLAN where hosts are connected. For example, if VLAN 10 is denied with wireless clients, and VLAN 20 is where the default gateway resides, VLAN 10 should be marked as an edge VLAN and VLAN 20 shouldn't. When defining a VLAN as an edge VLAN, the firewall enforces additional checks on hosts in that VLAN. For example, a host cannot move from an edge VLAN to another VLAN and still keep firewall flows active.
Trust ARP Responses	When ARP trust is enabled, a green checkmark displays. When disabled, a red "X" displays. Trusted ARP packets are used to update the IP-MAC Table to prevent IP spoof and arp-cache poisoning attacks.
Trust DHCP Responses	When DHCP trust is enabled, a green checkmark displays. When disabled, a red "X" displays. When enabled, DHCP packets from a DHCP server are considered trusted and permissible. DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks.
IPv6 Firewall	Lists whether an IPv6 firewall is enabled on this bridge VLAN. A green checkmark defines this setting as enabled. A red X defines this setting as disabled. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. These hosts require firewall packet protection unique to IPv6 traffic, as IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the *neighbor discovery* (ND) protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters.
DHCPv6 Trust	Lists whether DHCPv6 responses are trusted on this bridge VLAN. A green checkmark defines this setting as enabled. A red X defines this setting as disabled. If enabled, only DHCPv6 responses are trusted and forwarded over the bridge VLAN.
RA Guard	Lists whether *router advertisements* (RA) are allowed on this bridge VLAN. A green checkmark defines this setting as enabled. A red X defines this setting as disabled. RAs are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes (address abbreviations) and other subnet and host information.

5 Select **Add** to define a new bridge VLAN configuration, **Edit** to modify an existing bridge VLAN configuration or **Delete** to remove a VLAN configuration.

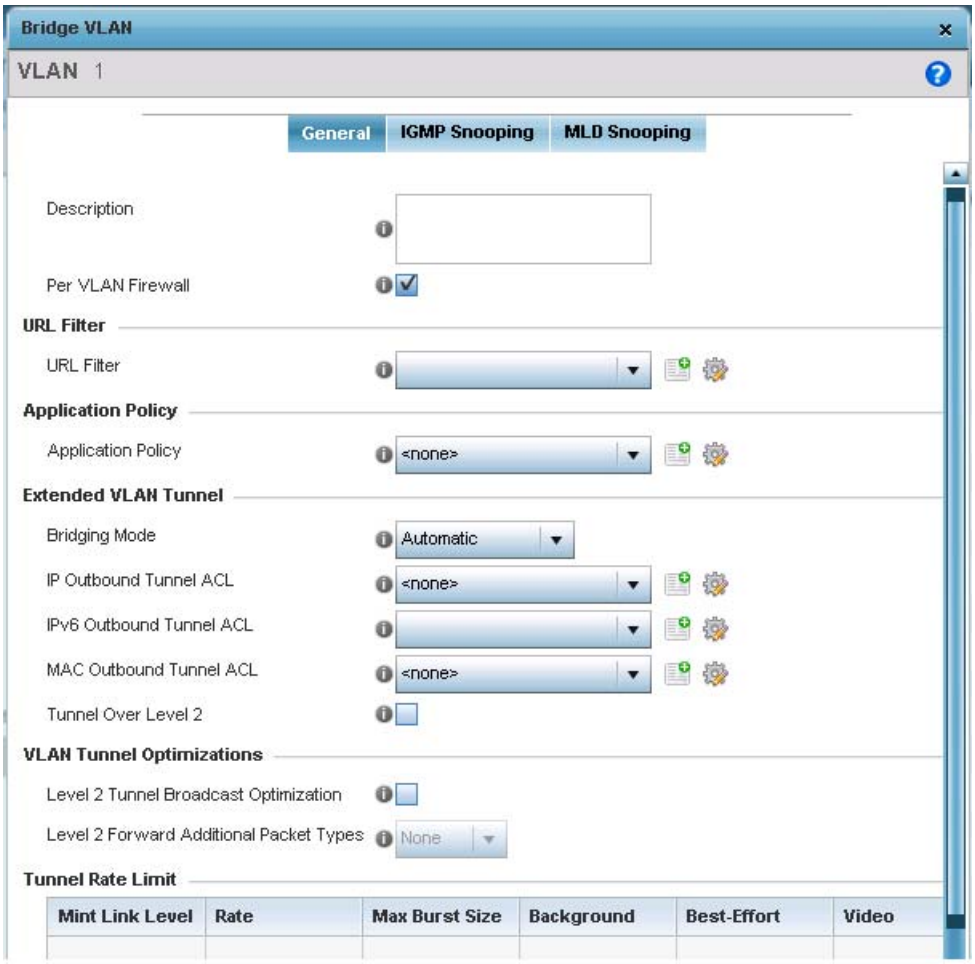


Figure 8-79 *Bridge VLAN - General tab*

The **General** tab displays by default.

6 If adding a new Bridge VLAN configuration, use the spinner control to define a **VLAN** ID between 1 - 4094. This value must be defined and saved before the General tab can become enabled and the remainder of the settings defined. VLAN IDs 0 and 4095 are reserved and unavailable.

7 Set the following **General** bridge VLAN parameters:

Description	If creating a new Bridge VLAN, provide a description (up to 64 characters) unique to the VLAN's specific configuration to help differentiate it from other VLANs with similar configurations.
Per VLAN Firewall	Enable this setting to provide firewall allow and deny conditions over the bridge VLAN. This setting is enabled by default.

8 Set or override the following **URL Filter** parameters. Web filters are used to control the access to resources on the Internet

URL Filter	Use the drop-down menu to select a URL filter to use with this Bridge VLAN.

9 Set or override the following **Application Policy** parameters. Use the drop-down to select the appropriate Application Policy to use with this Bridge VLAN configuration.

10 Set the following **Extended VLAN Tunnel** parameters:

Bridging Mode	Specify one of the following bridging modes for the VLAN. *Automatic* - Select automatic to let the controller or service platform determine the best bridging mode for the VLAN. *Local* - Select Local to use local bridging mode for bridging traffic on the VLAN. *Tunnel* - Select Tunnel to use a shared tunnel for bridging traffic on the VLAN. *Isolated-Tunnel* - Uses a dedicated tunnel for bridging traffic on the VLAN.
IP Outbound Tunnel ACL	Select an IP Outbound Tunnel ACL for outbound traffic from the drop-down menu. If an appropriate outbound IP ACL is not available, select the *Create* button to make a new one.
IPv6 Outbound Tunnel ACL	Select an IPv6 Outbound Tunnel ACL for outbound traffic from the drop-down menu. If an appropriate outbound IP ACL is not available, select the Create button to make a new one.
MAC Outbound Tunnel ACL	Select a MAC Outbound Tunnel ACL for outbound traffic from the drop-down menu. If an appropriate outbound MAC ACL is not available click the Create button to make a new one.
Tunnel Over Level 2	Select this option to allow VLAN traffic to be tunneled over level 2 links. This setting is disabled by default.

NOTE: Local and Automatic bridging modes do not work with ACLs. ACLs can only be used with tunnel or isolated-tunnel modes.

11 Select the **Level 2 Tunnel Broadcast Optimization** checkbox to enable broadcast optimization on this bridge VLAN. L2 Tunnel Broadcast Optimization prevents flooding of ARP packets over the virtual interface. Based on the learned information, ARP packets are filtered at the wireless controller level. This option is enabled by default.

If enabling L2 tunnel broadcast optimization, set the **Level 2 Forward Additional Packet Types** as *None* or *WNMP* to specify if additional packet types are forwarded or not across the L2 tunnel. By default, L2 tunnel broadcast optimization disables *Wireless Network Management Protocol* (WNMP) packet forwarding also across the L2 tunnel. Use this option to enable the forwarding of only WNMP packets. The default value is None.

12 Select **+ Add Row** to set the following **Tunnel Rate Limit** parameters:

Mint Link Level	Select the MINT link level from the drop-down menu.
Rate	Define a transmit rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received over the bridge VLAN. Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5,000 kbps.
Max Burst Size	Set a maximum burst size between 0 - 1024 kbytes. The smaller the burst, the less likely the receive packet transmission will result in congestion. The default burst size is 320 kbytes.

Background	Set the random early detection threshold in % for low priority background traffic. Set a value from 1 - 100%. The default is 50%.
Best-Effort	Set the random early detection threshold in % for low priority best-effort traffic. Set a value from 1 - 100%. The default is 50%.
Video	Set the random early detection threshold in % for high priority video traffic. Set a value from 1 - 100%. The default is 25%.
Voice	Set the random early detection threshold in % for high priority voice traffic. Set a value from 1 - 100%. The default is 25%.

13 Set the following **Layer 2 Firewall** parameters:

Trust ARP Response	Select this option to use trusted ARP packets to update the DHCP Snoop Table to prevent IP spoof and arp-cache poisoning attacks. This feature is disabled by default.
Trust DHCP Responses	Select this option to use DHCP packets from a DHCP server as trusted and permissible within the managed network. DHCP packets are used to update the DHCP Snoop Table to prevent IP spoof attacks. This feature is disabled by default.
Enable Edge VLAN Mode	Select this option to enable edge VLAN mode. When selected, the edge controller or service platform's IP address in the VLAN is not used, and is now designated to isolate devices and prevent connectivity. This feature is enabled by default.

14 Set the following **IPv6 Settings**:

IPv6 Firewall	Select this option to enable an IPv6 firewall on this bridge VLAN. This setting is enabled by default.
DHCPv6 Trust	Select this option to enable the trust all DHCPv6 responses on this bridge VLAN. DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. This setting is enabled by default.
RA Guard	Select this option to enable router advertisements or ICMPv6 redirects on this bridge VLAN. This setting is enabled by default.

15 Refer to the **Captive Portal** field to select an existing captive portal configuration to apply access restrictions to the bridge VLAN configuration.

A captive portal is an access policy for providing temporary and restrictive access using a standard Web browser. Captive portals provides authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Once logged into the captive portal, additional *Terms and Agreement*, *Welcome*, *Fail* and *No Service* pages provide the administrator with a number of options on captive portal screen flow and user appearance.

If an existing captive portal does not suite the bridge VLAN configuration, either select the **Edit** icon to modify an existing configuration or select the **Create** icon to define a new configuration that can be applied to the bridge VLAN. For information on configuring a captive portal policy, see *Configuring Captive Portal Policies on page 11-1*.

16 Refer to the **Captive Portal Snoop Subnet** field to configure the IPv4 clients to be excluded when snooping an IPv4 subnet for static wired captive portal clients. In the **Subnet** field, provide the subnet to snoop on. In the **Exclude IP** provide one (1) IP address in the subnet that can be excluded from snooping.

17 Refer to the **Captive Portal Snoop IPv6 Subnet** field to configure the IPv6 clients to be excluded when snooping an IPv6 subnet for static wired captive portal clients. Multiple rows can be added to this field.

Subnet	Use this field to provide an IPv6 subnet to snoop on.
Exclude IP	Use this field to provide the IPv6 address in the subnet that can be excluded from snooping.

18 Select the **OK** button to save the changes to the General tab. Select **Reset** to revert to the last saved configuration.

19 Select the **IGMP Snooping** tab to define the VLAN's IGMP configuration.

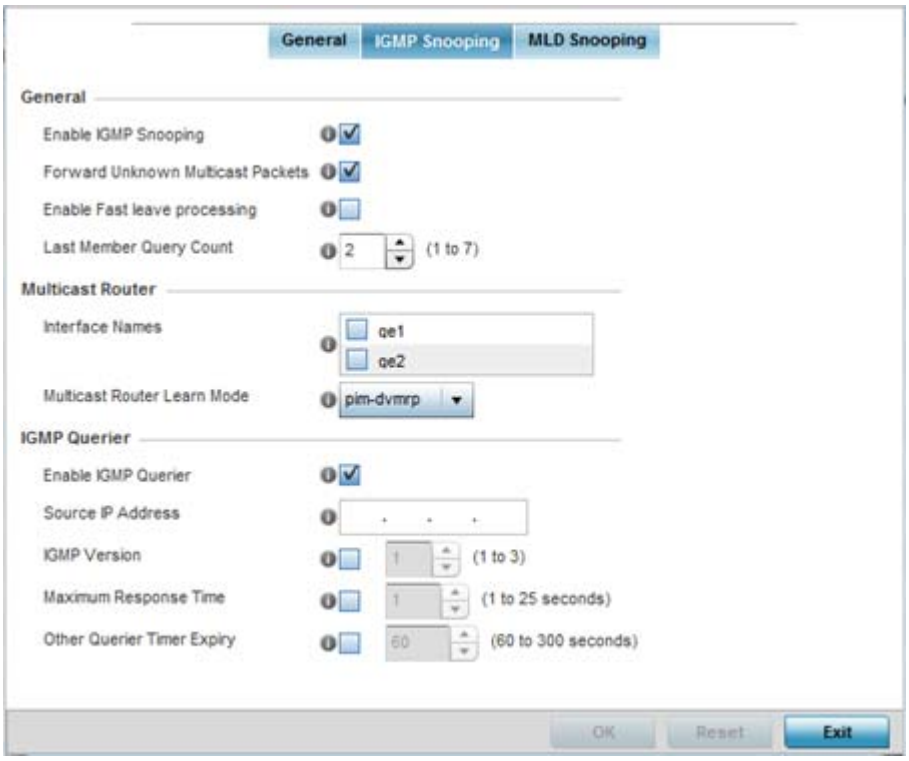


Figure 8-80 *Bridge VLAN - IGMP Snooping Tab*

20 Define the following **General** IGMP parameters for the bridge VLAN configuration:

The *Internet Group Management Protocol* (IGMP) is a protocol used for managing members of IP multicast groups. Controller and service platforms listen to IGMP network traffic and forward IGMP multicast packets to radios on which the interested hosts are connected. On the wired side of the network, the wired interfaces are flooded. This feature reduces the unnecessary flooding of multicast traffic in the network.

Enable IGMP Snooping	Select the check box to enable IGMP snooping. If disabled, snooping on a per VLAN basis is also disabled. This feature is enabled by default. If disabled, the settings under bridge configuration are overridden. For example, if IGMP snooping is disabled, but the bridge VLAN is enabled, the effective setting is disabled.
Forward Unknown Unicast Packets	Select the check box to enable to forward unicast packets from unregistered multicast groups. If disabled (the default setting), the unknown unicast forward feature is also disabled for individual VLANs.

Enable Fast leave processing	Select this option to remove a Layer 2 LAN interface from the IGMP snooping forwarding table entry without initially sending IGMP group-specific queries to the interface. When receiving a group specific IGMPv2 leave message, IGMP snooping removes the interface from the Layer 2 forwarding table entry for that multicast group, unless a multicast router was learned on the port. Fast-leave processing enhances bandwidth management for all hosts on the network. This setting is disabled by default.
Last Member Query Count	Specify the number (1 - 7) of group specific queries sent before removing an IGMP snooping entry. The default settings is 2.

21 Define the following **Multicast Router** settings:

Interface Names	Select the ge1 or radio interfaces used to IGMP snooping over a multicast router.
Multicast Router Learn Mode	Set the pim-dvmrp or static multicast routing learn mode.

22 Set the following **IGMP Querier** parameters for the profile's bridge VLAN configuration:

Enable IGMP Querier	IGMP snoop querier is used to keep host memberships alive. It's primarily used in a network where there's a multicast streaming server, hosts subscribed to the server and no IGMP querier present. An IGMP querier sends out periodic IGMP query packets. Interested hosts reply with an IGMP report packet. IGMP snooping is only conducted on wireless radios. IGMP multicast packets are flooded on wired ports. IGMP multicast packet are not flooded on the wired port. IGMP membership is also learnt on it and only if present, then it is forwarded on that port.
Source IP Address	Define an IP address applied as the source address in the IGMP query packet. This address is used as the default VLAN querier IP address.
IGMP Version	Use the spinner control to set the IGMP version compatibility to either version *1*, *2* or *3*. The default setting is 3.
Maximum Response Time	Specify the maximum time (from 1 - 25 seconds) before sending a responding report. When no reports are received from a radio, radio information is removed from the snooping table. For IGMP reports from wired ports, reports are only forwarded to the multicast router ports. The default setting is 10 seconds.
Other Querier Timer Expiry	Specify an interval in either *Seconds* (60 - 300) or *Minutes* (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute.

23 Select the **OK** button located at the bottom right of the screen to save the changes to the IGMP Snooping tab. Select **Reset** to revert to the last saved configuration.

24 Select the **MLD Snooping** tab.

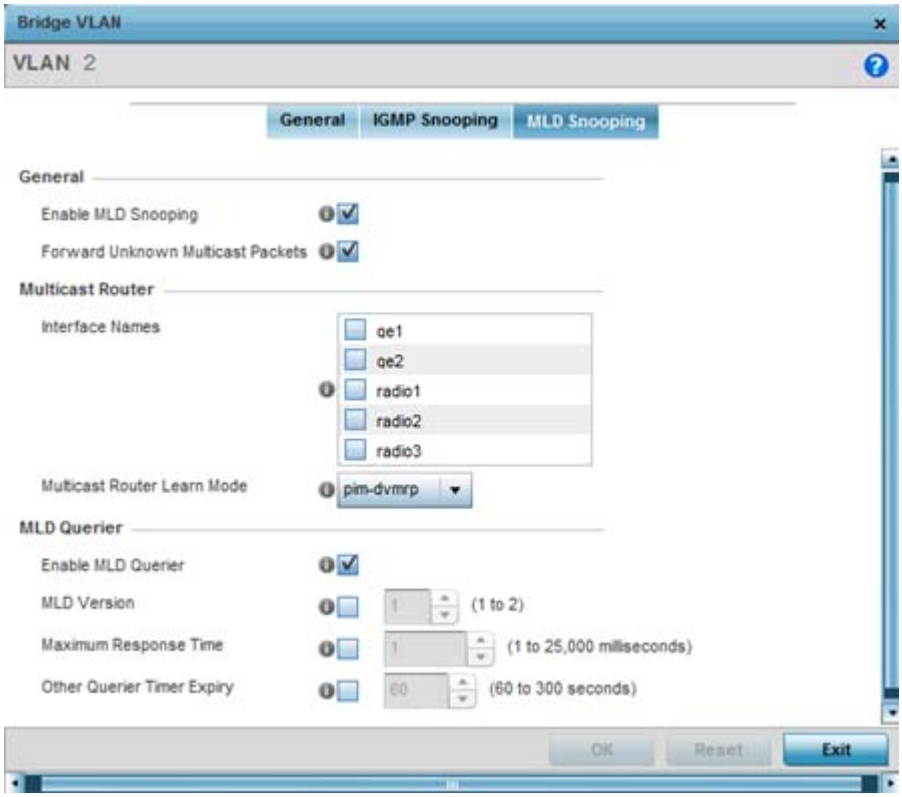


Figure 8-81 *Bridge VLAN - MLD Snooping Tab*

Define the following **General** MLD snooping parameters for the bridge VLAN configuration

Multicast Listener Discovery (MLD) snooping enables a controller, service platform or Access Point to examine MLD packets and make forwarding decisions based on content. MLD is used by IPv6 devices to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups.

MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or Access Point VLANs. When enabled, MLD messages are examined between hosts and multicast routers and to discern which hosts are receiving multicast group traffic. The controller, service platform or Access Point then forwards multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces.

Enable MLD Snooping	Enable MLD snooping to examine MLD packets and support content forwarding on this bridge VLAN. Packets delivered are identified by a single multicast group address. Multicast packets are delivered using best-effort reliability, just like IPv6 unicast. MLD snooping is enabled by default.
Forward Unknown Unicast Packets	Use this option to either *enable* or *disable* IPv6 unknown unicast forwarding. Unicast addresses identify a single network interface, whereas a multicast address is used by multiple hosts. This setting is enabled by default.

25 Define the following **Multicast Router** settings:

Interface Names	Select the physical ge port or radio interfaces used for MLD snooping.

Multicast Router Learn Mode	Set the *pim-dvmrp* or *static* multicast routing learn mode. DVMRP builds a parent-child database using a constrained multicast model to build a forwarding tree rooted at the source of the multicast packets. Multicast packets are initially flooded down this source tree. If redundant paths are on the source tree, packets are not forwarded along those paths.

26 Set the following **MLD Querier** parameters for the profile's bridge VLAN configuration:

Enable MLD Querier	Select the option to enable MLD querier on the controller, service platform or Access Point. When enabled, the device sends query messages to discover which network devices are members of a given multicast group. This setting is enabled by default.
MLD Version	Define whether MLD version *1* or *2* is utilized with the MLD querier. MLD version 1 is based on IGMP version 2 for IPv4. MLD version 2 is based on IGMP version 3 for IPv4 and is fully backward compatible. IPv6 multicast uses MLD version 2. The default MLD version is 2.
Maximum Response Time	Specify the maximum response time (from 1 - 25,000 milliseconds) before sending a responding report. Queriers use MLD reports to join and leave multicast groups and receive group traffic. The default setting is 1 milliseconds.
Other Querier Timer Expiry	Specify an interval in either *Seconds* (60 - 300) or *Minutes* (1 - 5) used as a timeout interval for other querier resources. The default setting is 60 seconds.

27 Select the **OK** button located at the bottom right of the screen to save the changes. Select **Reset** to revert to the last saved configuration.

8.8.14 Setting a Profile's Cisco Discovery Protocol Configuration

Profile Network Configuration

The *Cisco Discovery Protocol* (CDP) is a proprietary data link layer network protocol implemented in Cisco networking equipment and used to share information about network devices.

To set a profile's CDP configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **Cisco Discovery Protocol (CDP)**.

Figure 8-82 *Profile - Network Cisco Discovery Protocol screen*

4 Check the **Enable CDP** box to enable the Cisco Discovery Protocol on the device.

5 Refer to the **Hold Time** field and use the spinner control to define a hold time between 10 - 1800 seconds for transmitted CDP Packets. The default value is 180 seconds.

6 Refer to the **Timer** field and use the spinner control to define a interval between 5 - 900 seconds to transmit CDP Packets. The default value is 60 seconds.

7 Select the **OK** button to save the changes. Select **Reset** to revert to the last saved configuration.

8.8.15 Setting a Profile's Link Layer Discovery Protocol Configuration

Profile Network Configuration

The *Link Layer Discovery Protocol* (LLDP) or IEEE 802.1AB is a vendor-neutral Data Link Layer protocol used by network devices for advertising of (announcing) identity, capabilities and interconnections on a IEEE 802 LAN network. The protocol is formally referred to by the IEEE as Station and Media Access Control Connectivity Discovery. Both LLDP snooping and ability to generate and transmit LLDP packets is provided.

Information obtained via CDP and LLDP snooping is available in the UI. Information obtained using LLDP is provided by an Access Point during the adoption process, so the layer 2 device detected by the Access Point can be used as a criteria in the provisioning policy.

To set a profile's LLDP configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **Link Layer Discovery Protocol**.

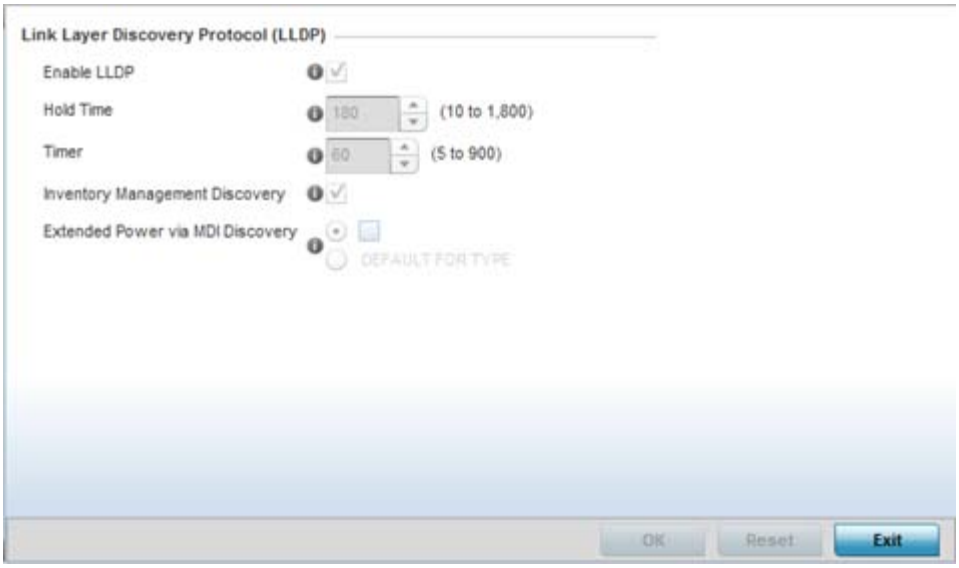


Figure 8-83 *Profile - Network Link Layer Discovery Protocol screen*

4 Check the **Enable LLDP** box to enable Link Layer Discovery Protocol on the device.

5 Refer to the **Hold Time** field and use the spinner control to define a hold time from 10 - 1800 seconds for transmitted LLDP packets. The default value is 180 seconds.

6 Refer to the **Timer** field and use the spinner control to define the interval between 5 - 900 seconds to transmit LLDP packets. The default value is 60 seconds.

7 Enable **Inventory Management Discovery** to track and identify inventory attributes including manufacturer, model or software version.

8 Extended Power via MDI Discovery provides detailed power information through end points and other connected devices. Select the **Extended Power via MDI Discovery** box to enable this feature. or select the **Default for Type** option to use a WiNG internal default value.

9 Select the **OK** button to save the changes. Select **Reset** to revert to the last saved configuration.

8.8.16 Setting a Profile's Miscellaneous Network Configuration

Profile Network Configuration

A profile can be configured to include a hostname in a DHCP lease for a requesting device and its profile. This helps an administrator track the leased DHCP IP address by hostname for the supported device profile. When numerous DHCP leases are assigned, an administrator can better track the leases when hostnames are used instead of devices.

To include a hostnames in DHCP request:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **Miscellaneous**.

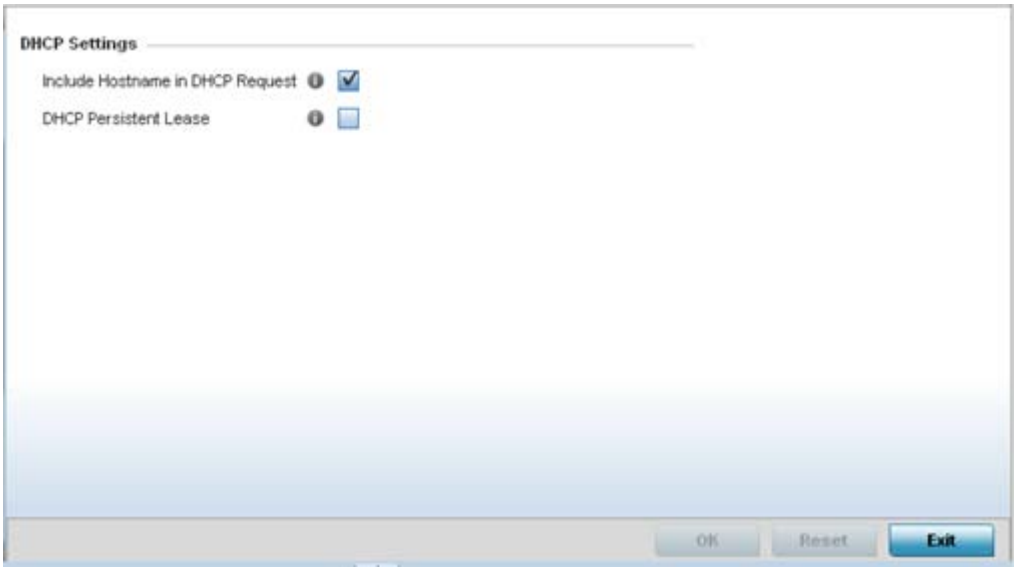


Figure 8-84 *Profile Miscellaneous screen*

4 Refer to the DHCP Settings section to configure miscellaneous DHCP Settings.

Include Hostname in DHCP Request	Select *Include Hostname in DHCP Request* to include a hostname in a DHCP lease for a requesting device. This feature is disabled by default.
DHCP Persistent Lease	Enables a persistent DHCP lease for a requesting device. A persistent DHCP lease assigns the same IP Address and other network information to the device each time it renews its DHCP lease.

5 Select the **OK** button located at the bottom right of the screen to save the changes. Select **Reset** to revert to the last saved configuration.

8.8.17 Setting a Profile's Alias Configuration

Profile Network Configuration

With large deployments, the configuration of remote sites utilizes a set of shared attributes, of which a small set of attributes are unique for each location. For such deployments, maintaining separate configuration (WLANs, profiles, policies and ACLs) for each remote site is complex. Migrating any global change to a particular configuration item to all the remote sites is a complex and time consuming operation.

- Also, this practice does not scale gracefully for quick growing deployments.
- An alias enables an administrator to define a configuration item, such as a hostname, as an alias once and use the defined alias across different configuration items such as multiple ACLs.
- Once a configuration item, such as an ACL, is utilized across remote locations, the Alias used in the configuration item (ACL) is modified to meet local deployment requirement. Any other ACL or other configuration items using the modified alias also get modified, simplifying maintenance at the remote deployment.
- Aliases have scope depending on where the Alias is defined. Alias are defined with the following scopes:
- *Global aliases* are defined from the **Configuration** > **Network** > **Alias** screen. Global aliases are available for use globally across all devices, profiles and RF Domains in the system.
- *Profiles aliases* are defined from the **Configuration** > **Devices** > **System Profile** > **Network** > **Alias** screen. Profile aliases are available for use to a specific group of wireless controllers or Access Points. Alias values defined in a profile override the alias values defined within global aliases.

- *RF Domain aliases* are defined from the **Configuration** > **Devices** > **RF Domain** > **Alias** screen. RF Domain aliases are available for use for a site as a RF Domain is site specific. RF Domain alias values override alias values defined in a global alias or a profile alias configuration.
- *Device aliases* are defined from the **Configuration** > **Devices** > **Device Overrides** > **Network** > **Alias** screen. Device aliases are utilized by a singular device only. Device alias values override global, profile or RF Domain alias configurations.

Using an alias, configuration changes made at a remote location override any updates at the management center. For example, if an network alias defines a network range as 192.168.10.0/24 for the entire network, and at a remote deployment location, the local network range is 172.16.10.0/24, the network alias can be overridden at the deployment location to suit the local requirement. For the remote deployment location, the network alias work with the 172.16.10.0/24 network. Existing ACLs using this network alias need not be modified and will work with the local network for the deployment location. This simplifies ACL definition and management while taking care of specific local deployment requirements.

For more information, refer to the following:

- *Basic Alias*
- *Network Group Alias*
- *Network Service Alias*

8.8.17.1 Basic Alias

Setting a Profile's Alias Configuration

A *basic alias* is a set of configurations consisting of *VLAN*, *Host*, *Network* and *Address Range* alias configurations. A VLAN alias is a configuration for optimal VLAN re-use and management for local and remote deployments. A host alias configuration is for a particular host device's IP address. A network alias configuration is utilized for an IP address on a particular network. An address range alias is a configuration for a range of IP addresses.

To set a network basic alias configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **Alias**.
The Alias screen displays with the Basic Alias tab displayed by default.

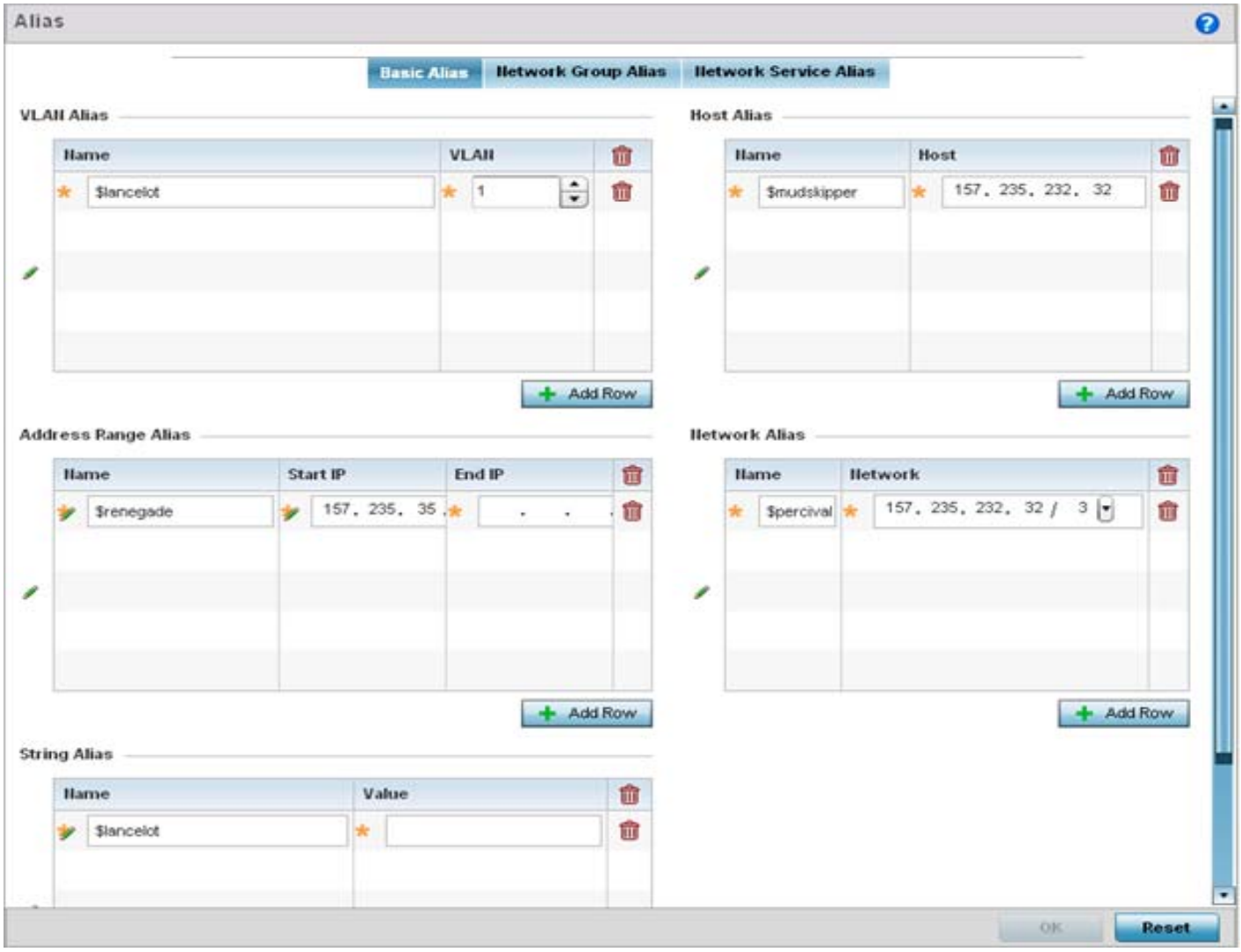


Figure 8-85 *Basic Alias screen*

4 Select **+ Add Row** to define **VLAN Alias** settings:

Use the **Vlan Alias** field to create unique aliases for VLANs that can be utilized at different deployments. For example, if a VLAN ID is set as 10 for the central network, and the VLAN is set as 26 at a remote location, the VLAN can be overridden at the remote location using an alias. At the remote location, the network is functional with an ID of 26, but utilizes the name defined at the central local network. A new VLAN need not be created specifically at the remote location.

Name	If adding a new *VLAN Alias,* provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Vlan	Use the spinner control to set a numeric VLAN ID from 1 - 4094.

5 Select **+ Add Row** to define **Address Range Alias** settings:

Use the **Address Range Alias** field to create aliases for IP address ranges that can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110,

the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.

Name	If adding a new *Address Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Start IP	Set a starting IP address used with a range of addresses utilized with the address range alias.
End IP	Set an ending IP address used with a range of addresses utilized with the address range alias.

6 Select **+ Add Row** to define **String Alias** settings:

Use the **String Alias** field to create aliases for hosts that can be utilized at different deployments. For example, if the main domain at a remote location is called loc1.domain.com and at another deployment location it is called loc2.domain.com, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the loc1.domain.com domain and at the other with the loc2.domain.com domain.

Name	If adding a new *String Alias,* provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Value	Provide a string value to use in the alias.

7 Select **+ Add Row** to define **Host Alias** settings:

Use the **Host Alias** field to create aliases for hosts that can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.

Name	If adding a new *Host Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Host	Set the IP address of the host machine.

8 Select **+ Add Row** to define **Network Alias** settings:

Use the **Network Alias** field to create aliases for IP networks that can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

Name	If adding a new *Network Alias,* provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Network	Provide a network address in the form of *host/mask*.

9 Select **OK** when completed to update the set of basic alias rules. Select **Reset** to revert the screen back to its last saved configuration.

8.8.17.2 Network Group Alias

A *network group alias* is a set of configurations consisting of host and network configurations. Network configurations are complete networks in the form of 192.168.10.0/24 or an IP address range in the form of 192.168.10.10-192.168.10.20. Host configurations are in the form of a single IP address, 192.168.10.23.

A network group alias can contain multiple definitions for a host, network, and IP address range. A maximum of eight (8) Host entries, eight (8) network entries and eight (8) IP addresses range entries can be configured inside a network group alias. A maximum of 32 network group alias entries can be created.

To set a network group alias configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **Alias**.

4 Select the **Network Group Alias** tab. The screen displays the attributes of existing network group alias configurations.

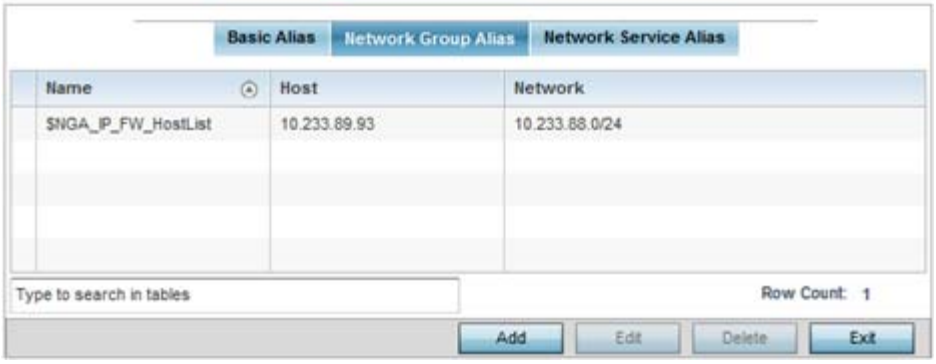


Figure 8-86 *Network Group Alias screen*

Name	Displays the administrator assigned name used with the network group alias.
Host	Displays all the host aliases configured in the listed network group alias. Displays a blank column if no host alias is defined.
Network	Displays all network aliases configured in the listed network group alias. Displays a blank column if no network alias is defined.

5 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies.

6 Select the added row to expand it into configurable parameters for defining the network alias rule.

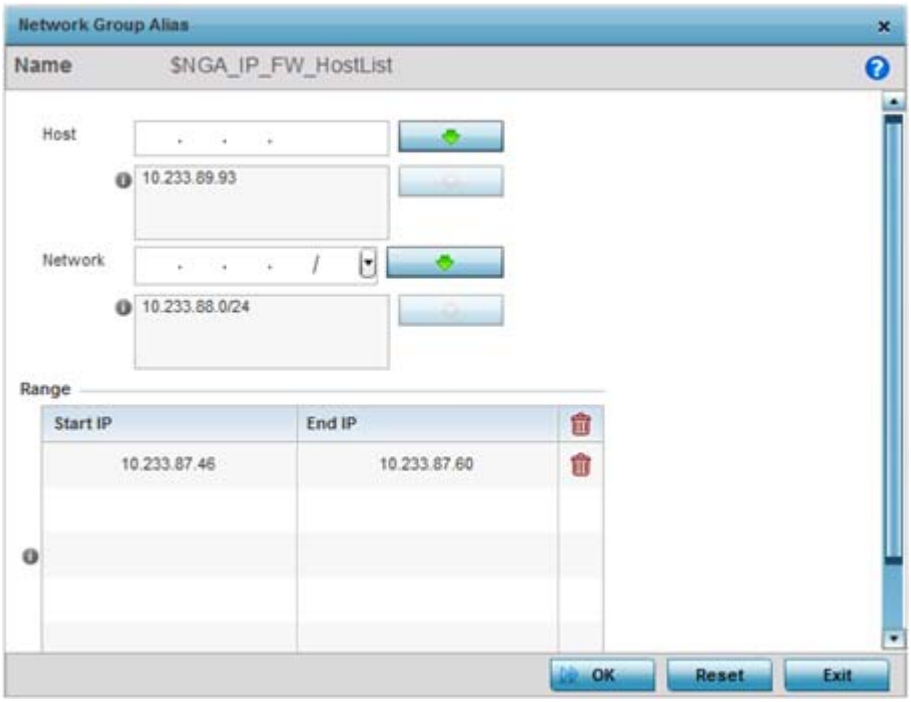


Figure 8-87 *Network Group Alias Add screen*

7 If adding a new **Network Alias Rule,** provide it a name up to 32 characters. The network group alias name always starts with a dollar sign ($).

8 Define the following network group alias parameters:

Host	Specify the Host IP address for up to eight IP addresses supporting network aliasing. Select the down arrow to add the IP address to the table.
Network	Specify the netmask for up to eight IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Select the down arrow to add the mask to the table.

9 Within the **Range** table, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the alias range or double-click on an existing an alias range entry to edit it.

10 Select **OK** when completed to update the network alias rules. Select **Reset** to revert the screen back to its last saved configuration.

8.8.17.3 Network Service Alias

A *network service alias* is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per network service alias.

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

To define a service alias configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the Network menu to display its submenu options.

3 Select **Alias**.

4 Select the **Network Service Alias** tab. The screen displays existing network service alias configurations.

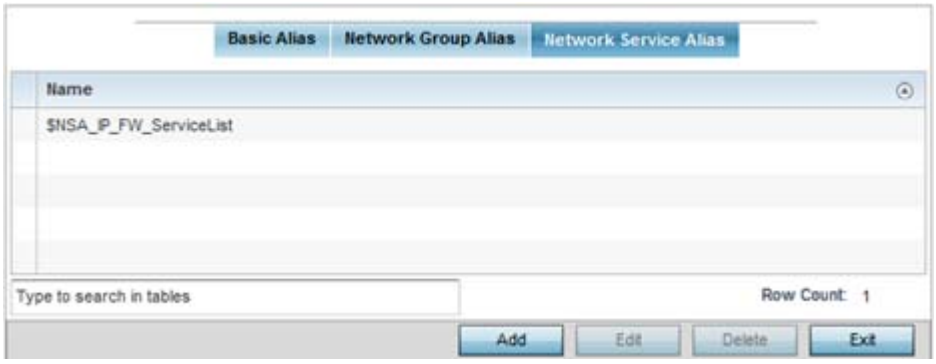


Figure 8-88 *Network Service Alias screen*

5 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies.

6 Select the added row to expand it into configurable parameters for defining the service alias rule.

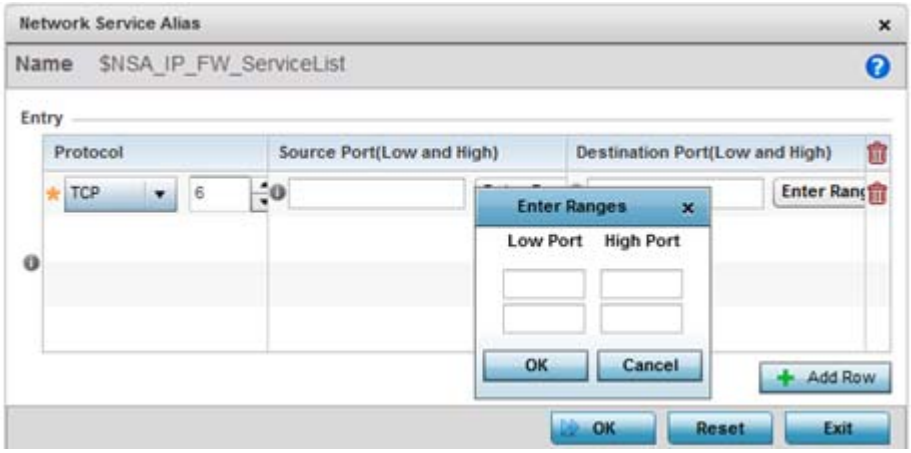


Figure 8-89 *Network Service Alias Add screen*

7 If adding a new **Network Service Alias Rule,** provide it a name up to 32 characters. Ensure a $ precedes the name.

8 Select **+ Add Row** and provide the following configuration parameters:

Protocol	Specify the protocol for which the alias has to be created. Use the drop down to select the protocol from *eigrp, gre, icmp, igmp, ip, vrrp, igp, ospf, tcp* and *udp.* Select *other* if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected.
Source Port (Low and High)	This field is only relevant if the protocol is either *tcp* or *udp.* Specify the source ports for this protocol entry. A range of ports can be specified. Select the *Enter Ranges* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

Destination Port (Low and High)	This field is only relevant if the protocol is either *tcp* or *udp*. Specify the destination ports for this protocol entry. A range of ports can be specified. Select the *Enter Ranges* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

9 Within the **Range** field, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the service alias range or double-click on an existing service alias range entry to edit it.

10 Select **OK** when completed to update the service alias rules. Select **Reset** to revert the screen back to its last saved configuration.

8.8.18 Setting a Profile's IPv6 Neighbor Configuration

Profile Network Configuration

IPv6 neighbor discovery uses ICMP messages and solicited multicast addresses to find the link layer address of a neighbor on the same local network, verify the neighbor's reachability and track neighboring devices.

Upon receiving a neighbor solicitation message, the destination replies with *neighbor advertisement* (NA). The source address in the advertisement is the IPv6 address of the device sending the message. The destination address in the advertisement message is the IPv6 address of the device sending the neighbor solicitation. The data portion of the NA includes the link layer address of the node sending the neighbor advertisement.

Neighbor solicitation messages also verify the availability of a neighbor once its the link layer address is identified. When a node wants to verify the reachability of a neighbor, the destination address in a neighbor solicitation message is the unicast address of the neighbor.

A neighbor is interpreted as reachable when an acknowledgment is returned indicating packets have been received and processed. If packets are reaching the device, they're also reaching the next hop neighbor, providing a confirmation the next hop is reachable.

To set an IPv6 neighbor discovery configuration:

1 Select **Configuration** > **Profiles** > **Network**.

2 Expand the **Network** menu to display its submenu options.

3 Select **IPv6 Neighbor**.

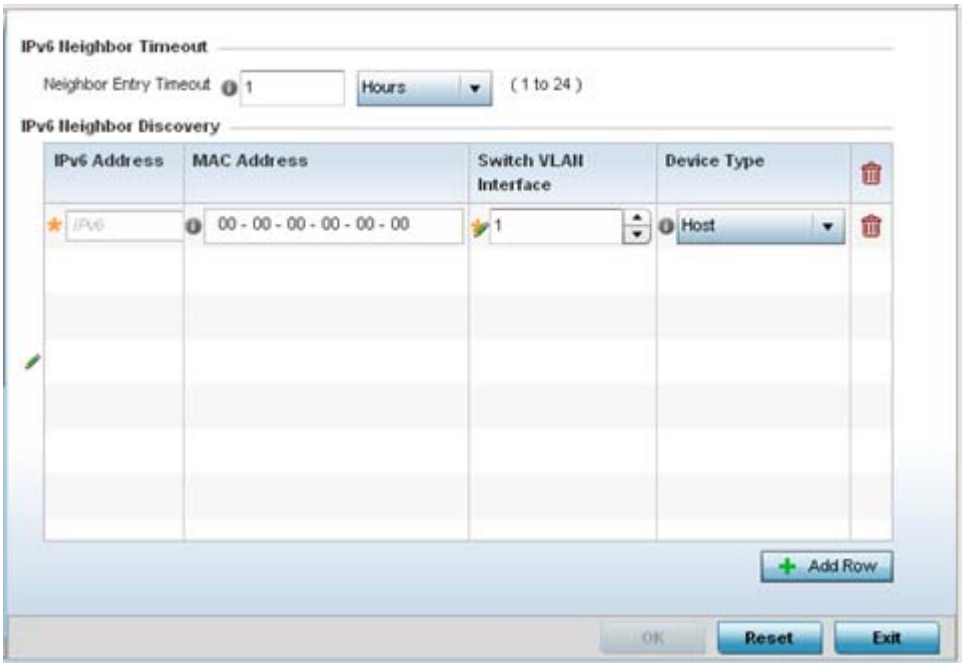


Figure 8-90 *IPv6 Neighbor screen*

4 Set an **IPv6 Neighbor Entry Timeout** in either *Seconds* (15 - 86,400), *Minutes* (1 - 1,440), *Hours* (1 - 24) or *Days* (1). The default setting is 1 hour.

5 Select **+ Add Row** to define the configuration of **IPv6 Neighbor Discovery** configurations. A maximum of 256 neighbor entries can be defined.

IPv6 Address	Provide a static IPv6 IP address for neighbor discovery. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via CMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
MAC Address	Enter the hardware encoded MAC addresses of up to 256 IPv6 neighbor devices. A neighbor is interpreted as reachable when an acknowledgment is returned indicating packets have been received and processed. If packets are reaching the device, they're also reaching the next hop neighbor, providing a confirmation the next hop is reachable.
Switch VLAN Interface	Use the spinner control to set the virtual interface (from 1 - 4094) used for neighbor advertisements and solicitation messages.
Device Type	Specify the device type for this neighbor solicitation. Neighbor solicitations request the link layer address of a target node while providing the sender's own link layer address to the target. Neighbor solicitations are multicast when the node needs to resolve an address and unicast when the node seeks to verify the reachability of a neighbor. Options include *Host, Router* and *DHCP Server.* The default setting is Host.

6 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

8.8.19 Profile Network Configuration and Deployment Considerations

Profile Network Configuration

Before defining a profile's network configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- Administrators often need to route traffic between different VLANs. Bridging VLANs are only for non-routable traffic, like tagged VLAN frames destined to some other device which will untag it. When a data frame is received on a port, the VLAN bridge determines the associated VLAN based on the port of reception.
- Static routes, while easy, can be overwhelming within a large or complicated network. Each time there is a change, someone must manually make changes to reflect the new route. If a link goes down, even if there is a second path, the router would ignore it and consider the link down.
- Static routes require extensive planning and have a high management overhead. The more routers in a network, the more routes need that to be configured. If you have *N* number of routers and a route between each router is needed, then you must configure *N* x *N* routes. Thus, for a network with nine routers, you'll need a minimum of 81 routes (9 x 9 = 81).

8.9 Profile Security Configuration

A profile can have its own firewall policy, wireless client role policy, WEP shared key authentication, NAT policy and VPN policy applied. If an existing firewall, client role or NAT policy is unavailable, an administrator can navigate from **Configuration** > **Profiles** to **Configuration** > **Security** to create the required security policy configuration. Once created, separate policies can be applied to the profile to best support the data protection and security requirements of the device model supported by the profile.

For more information, refer to the following sections:

- *Setting the Profile's Security Settings*
- *Setting the Profile's Certificate Revocation List (CRL) Configuration*
- *Setting the Profile's Trustpoint Configuration*
- *Setting the Profile's VPN Configuration*
- *Setting the Profile's Auto IPSec Tunnel Configuration*
- *Setting the Profile's NAT Configuration*
- *Setting the Profile's Bridge NAT Configuration*
- *Setting the Profile's Application Visibility (AVC) Configuration*

8.9.1 Setting the Profile's Security Settings

Profile Security Configuration

A profile can leverage existing firewall, wireless client role and WIPS policies and apply them to the profile's configuration. This affords each profile a truly unique combination of data protection policies best meeting the data protection requirements of the profile's supported device model.

To define a profile's security settings:

1 Select the Configuration tab from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu.

4 Select **Security.**

5 Select **Settings**.

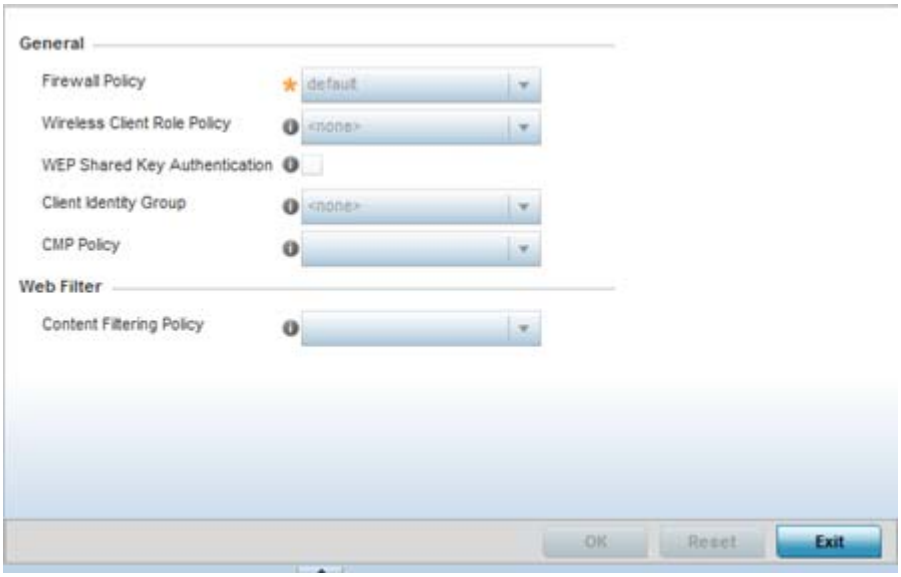


Figure 8-91 *Security - Settings screen*

6 Refer to the **General** field to assign or create the following security policy's to the profile:

Firewall Policy	Use the drop-down menu to select an existing Firewall Policy to use as an additional security mechanism with this profile. All devices using this profile must meet the requirements of the firewall policy to access the network. A firewall is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms both blocking and permitting data traffic within the network. If an existing Firewall policy does not meet your requirements, select the *Create* icon to create a new firewall policy that can be applied to this profile. An existing policy can also be selected and edited as needed using the *Edit* icon.
Wireless Client Role Policy	Use the drop-down menu to select a client role policy used to strategically filter client connections based on a pre-defined set of filter rules and connection criteria. If an existing Wireless Client Role policy does not meet your requirements, select the *Create* icon to create a new configuration that can be applied to this profile. An existing policy can also be selected and edited as needed using the *Edit* icon.
WEP Shared Key Authentication	Select this option to require devices to use a WEP key to access the network using this profile. The controller or service platform use the key algorithm to convert an ASCII string to the same hexadecimal number. Clients without adapters need to use WEP keys manually configured as hexadecimal numbers. This option is disabled by default.

Client Identity Group	Select the client identity group to apply to this device profile. Client identity is a set of unique fingerprints used to identify a class of devices. A *Client identity group* is a set of client attributes that identify devices and apply specific permissions and restrictions on them.The information is used to configure permissions and access rules for that device class and can assist administrators by applying permissions and rules to multiple devices simultaneously. For information on setting a client identity group configuration that can be selected and applied to a device profile, see *Device Fingerprinting on page 10-47*.
CMP Policy	Use the drop down-menu to assign a CMP policy to allow a device to communicate to a CMP supported CA server, initiate a certificate request and download the required certificates from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting the certificates from the server. It can also auto update the certificates which are about to expire.

7 Use the **Content Filtering Policy** drop-down menu to select or override the **URL Filter** configuration applied to this virtual interface.

URL filtering is used to restrict access to specific resources (by category) on the Internet.

8 Select **OK** to save the changes made within the Settings screen. Select **Reset** to revert to the last saved configuration.

8.9.2 Setting the Profile's Certificate Revocation List (CRL) Configuration

Profile Security Configuration

A *certificate revocation list* (CRL) is a list of certificates that have been revoked or are no longer valid. A certificate can be revoked if the *certificate authority* (CA) had improperly issued a certificate, or if a private-key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.

To define a CRL configuration that can be applied to a profile:

1 Select the **Configuration** tab from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu.

4 Select **Security**.

5 Select **Certificate Revocation**.

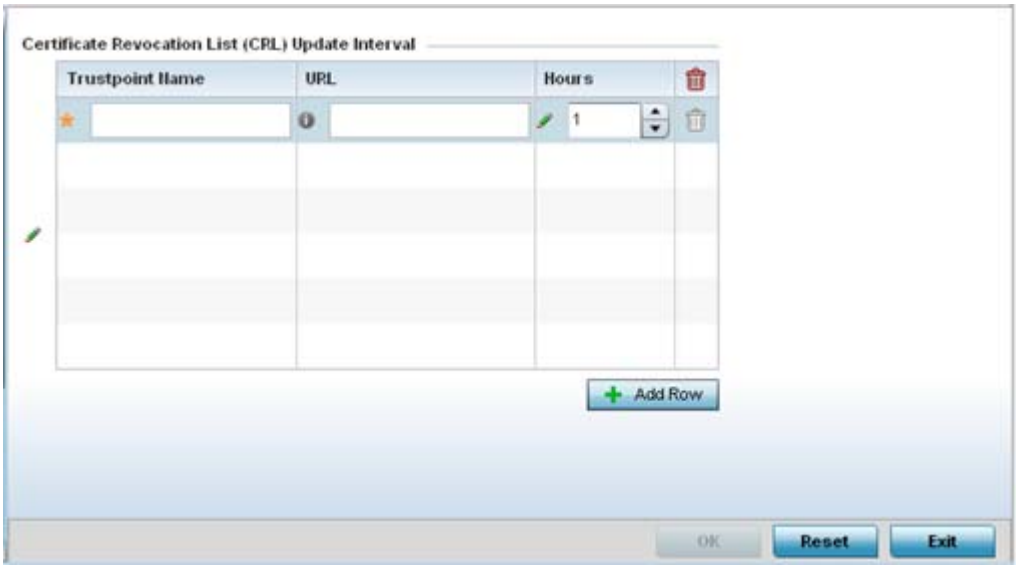


Figure 8-92 *Security - Certificate Revocation screen*

6 Select the **+ Add Row** button to add a column within the **Certificate Revocation List (CRL) Update Interval** table to quarantine certificates from use in the network.

Additionally, a certificate can be placed on hold for a defined period. If, for instance, a private key was found and nobody had access to it, its status could be reinstated.

a Provide the name of the trustpoint in question within the **Trustpoint Name** field. The name cannot exceed 32 characters.

b Enter the resource ensuring the trustpoint's legitimacy within the **URL** field.

c Use the spinner control to specify an interval (in hours) after which a device copies a CRL file from an external server and associates it with a trustpoint.

7 Select **OK** to save the changes made within the Certificate Revocation screen. Select **Reset** to revert to the last saved configuration.

8.9.3 Setting the Profile's Trustpoint Configuration

Profile Security Configuration

A RADIUS certificate links identity information with a public key enclosed in the certificate. A *certificate authority* (CA) is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate.

To define a RADIUS Trustpoint configuration that can be applied to a profile:

1 Select the **Configuration** tab from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu.

4 Select **Security**.

5 Select **Trustpoints**.

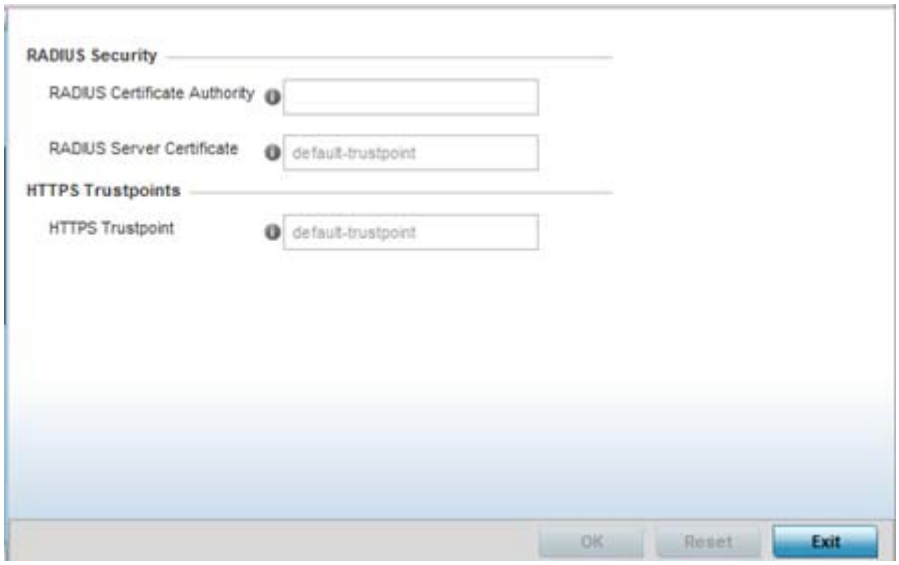


Figure 8-93 *Security - Trustpoint screen*

6 Set the following **RADIUS Security** certificate settings:

RADIUS Certificate Authority	Either use the default-trustpoint or select an existing certificate.
RADIUS Server Certificate	Either use the default-trustpoint or select an existing certificate/trustpoint.

7 Set the following **HTTPS Trustpoints** settings:

HTTPS Trustpoint	Either use the default trustpoint or select the Stored radio button to enable a drop-down menu where an existing certificate/trustpoint can be utilized. For more information, see *Certificate Management on page 5-12*.

8 Select **OK** to save the changes made within the RADIUS Trustpoints screen. Select **Reset** to revert to the last saved configuration,

8.9.4 Setting the Profile's VPN Configuration

Profile Security Configuration

IPSec VPN provides a secure tunnel between two networked peer controllers or service platforms. Administrators can define which packets are sent within the tunnel, and how they're protected. When a tunnelled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination.

Tunnels are sets of *security associations* (SA) between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunnelled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (*AH* or *ESP*).

Use *crypto maps* to configure IPSec VPN SAs. Crypto maps combine the elements comprising IPSec SAs. Crypto maps also include *transform sets*. A transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic. One crypto map is utilized for each IPsec peer, however for remote VPN deployments one crypto map is used for all the remote IPsec peers.

Internet Key Exchange (IKE) protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs, and enables secure communications without time consuming manual pre-configuration.

To define a profile's VPN settings:

1 Select the **Configuration** tab from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu.

4 Select **Security**.

5 Select **VPN Configuration.**

The **Basic Settings** tab displays by default. Refer to the Peer Settings table to add peer addresses and keys for VPN tunnel destinations. Use the **+ Add Row** function as needed to add additional destinations and keys.

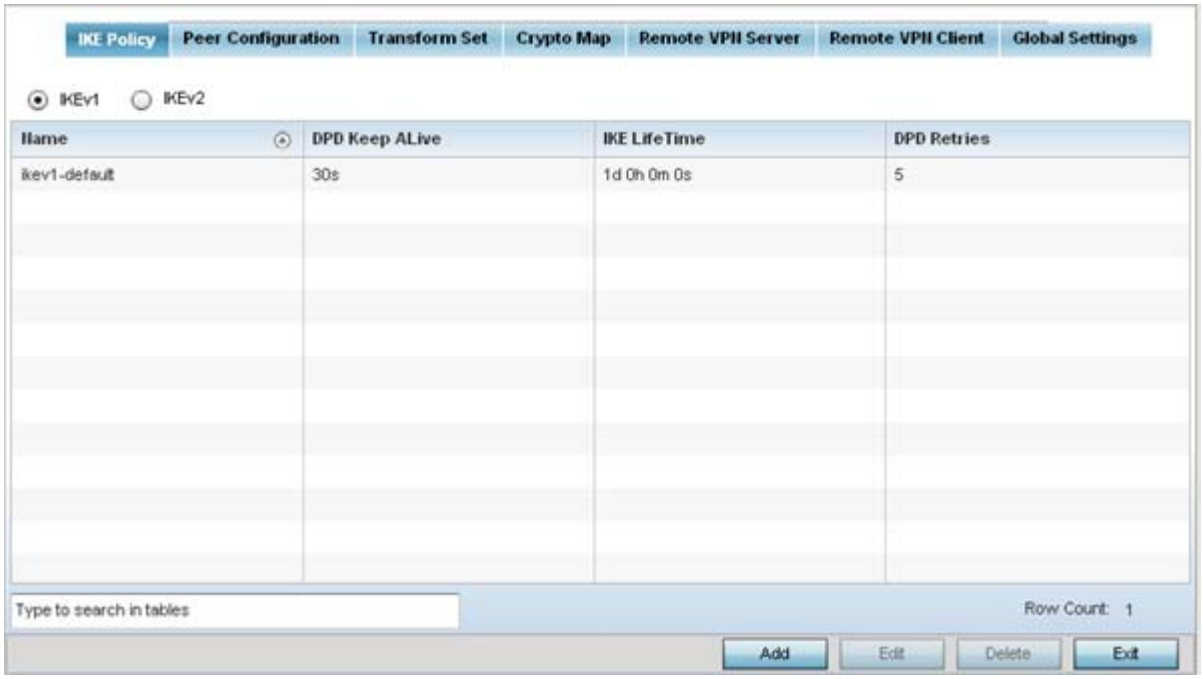


Figure 8-94 *Profile Security - VPN IKE Policy screen*

6 Select either the **IKEv1** or **IKEv2** radio button to enforce VPN peer key exchanges using either *IKEv1* or *IKEv2*.

IKEv2 provides improvements from the original IKEv1 design (improved cryptographic mechanisms, NAT and firewall traversal, attack resistance etc.) and is recommended in most deployments. The appearance of the IKE Policy screens differ depending on the selected IKEv1 or IKEv2 mode.

7 Refer to the following to determine whether an IKE Policy requires creation, modification or removal:

Name	Displays the 32 character maximum name assigned to the IKE policy.
DPD Keep Alive	Lists each policy's IKE keep alive message interval defined for IKE VPN tunnel dead peer detection.

IKE LifeTime	Displays each policy's lifetime for an IKE SA. The lifetime defines how long a connection (encryption/authentication keys) should last, from successful key negotiation to expiration. Two peers need not exactly agree on the lifetime, though if they do not, there is some clutter for a superseded connection on the peer defining the lifetime as longer.
DPD Retries	Lists each policy's number maximum number of keep alive messages sent before a VPN tunnel connection is defined as dead by the peer. This screen only appears when IKEv1 is selected.

8 Select **Add** to define a new IKE Policy configuration, **Edit** to modify an existing configuration or **Delete** to remove an existing configuration.

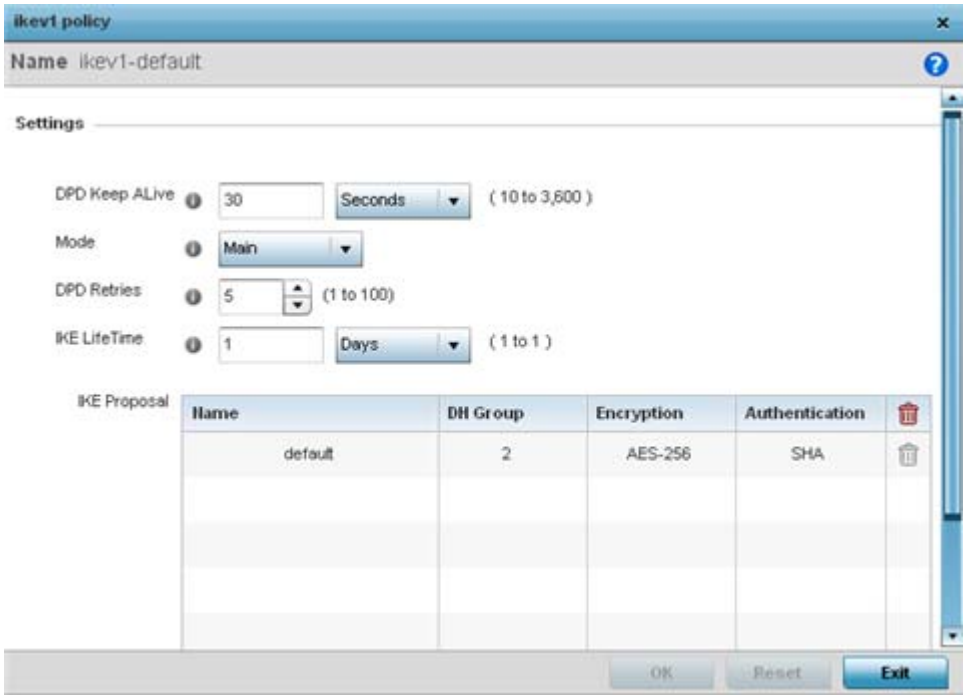


Figure 8-95 *Profile Security - IKE Policy - Add/Edit screen*

Name	If creating a new IKE policy, assign it a 32 character maximum name to help differentiate this IKE configuration from others with similar parameters.
DPD Keep Alive	Configure the IKE keep alive message interval used for dead peer detection on the remote end of the IPSec VPN tunnel. Set this value in either *Seconds* (10 - 3,600), *Minutes* (1 - 60) or *Hours* (1). The default setting is 30 seconds. This setting is required for both IKEv1 and IKEV2.
Mode	If using IKEv1, use the drop-down menu to define the IKE mode as either *Main* or *Aggressive*. IPSEC has two modes in IKEv1 for key exchanges. Aggressive mode requires 3 messages be exchanged between the IPSEC peers to setup the SA, Main requires 6 messages. The default setting is Main.
DPD Retries	Use the spinner control to set the maximum number of keep alive messages sent before a VPN tunnel connection is defined as dead. The available range is from 1 - 100. The default setting is 5.

IKE LifeTime	Set the lifetime defining how long a connection (encryption/ authentication keys) should last from successful key negotiation to expiration. Set this value in either *Seconds* (600 - 86,400), *Minutes* (10 - 1,440), *Hours* (1 - 24) or *Days* (1). This setting is required for both IKEv1 and IKEV2.

9 Select **+ Add Row** to define the network address of a target peer and its security settings.

Name	If creating a new IKE policy, assign the target peer (tunnel destination) a 32 character maximum name to distinguish it from others with a similar configuration.
DH Group	Use the drop-down menu to define a *Diffie-Hellman* (DH) identifier used by the VPN peers to derive a shared secret password without having to transmit. DH groups determine the strength of the key used in key exchanges. The higher the group number, the stronger and more secure the key. Options include *2*, *5* and *14*. The default setting is 5.
Encryption	Select an encryption method used by the tunnelled peers to securely interoperate. Options include *3DES*, *AES*, *AES-192* and *AES-256*. The default setting is AES-256.
Authentication	Select an authentication hash algorithm used by the peers to exchange credential information. Options include *SHA*, *SHA256*, *AES-XCBC-HMAC-128* and *MD5*. The default setting is SHA.

10 Select **OK** to save the changes made within the IKE Policy screen. Select **Reset** to revert to the last saved configuration. Select the **Delete Row** icon as needed to remove a peer configuration.

11 Select the **Peer Configuration** tab to assign additional network address and IKE settings to the an intended VPN tunnel peer destination.

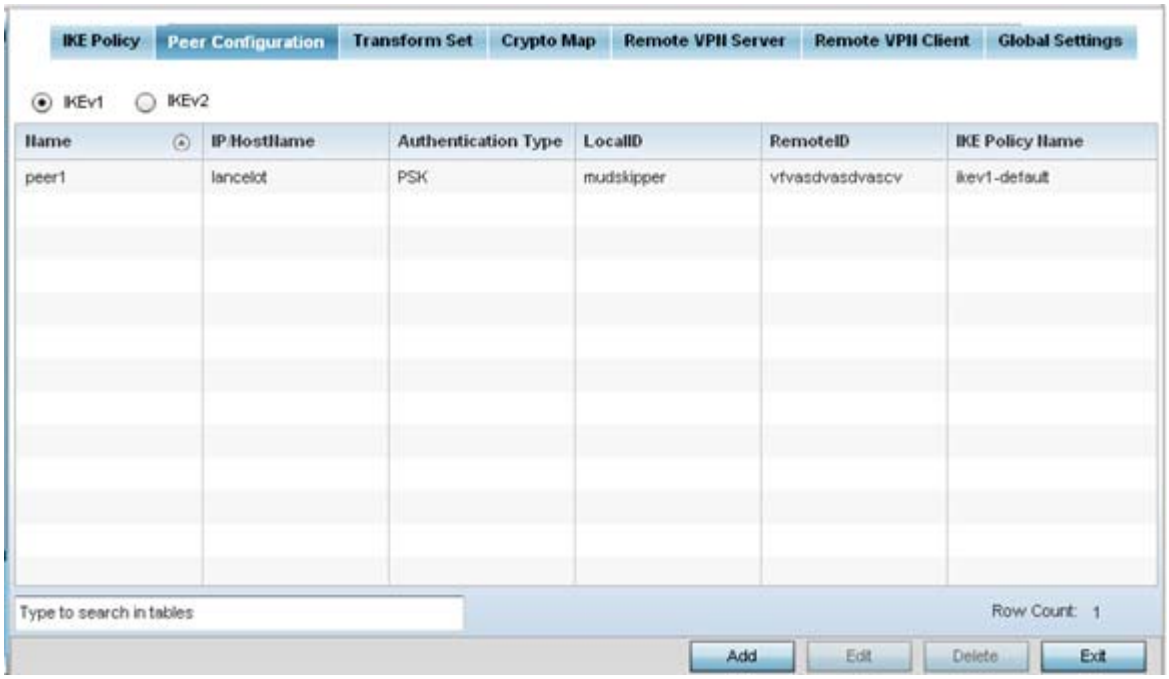


Figure 8-96 *Profile Security - VPN Peer Destination screen (IKEv1 example)*

12 Select either the **IKEv1** or **IKEv2** radio button to enforce VPN key exchanges using either *IKEv1* or *IKEv2.*

13 Refer to the following to determine whether a new VPN **Peer Configuration** requires creation, an existing configuration requires modification or a configuration requires removal.

Name	Lists the 32 character maximum name assigned to each listed peer configuration upon creation.
IP/Hostname	Displays the IP address (or host address FQDN) of the IPSec VPN peer targeted for secure tunnel connection and data transfer.
Authentication Type	Lists whether the peer configuration has been defined to use *pre-shared key* (PSK) or RSA. *Rivest, Shamir, and Adleman* (RSA) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for both signing and encryption. If using IKEv2, this screen displays both *local* and *remote* authentication, as both ends of the VPN connection require authentication.
LocalID	Lists the local identifier used within this peer configuration for an IKE exchange with the target VPN IPSec peer.
RemoteID	Displays the means the target remote peer is to be identified (string, FQDN etc.) within the VPN tunnel.
IKE Policy Name	Lists the IKEv1 or IKE v2 policy used with each listed peer configuration. If a policy requires creation, select the *Create* button.

14 Select **Add** to define a new peer configuration, **Edit** to modify an existing configuration or **Delete** to remove an existing peer configuration. The parameters that can de defined for the peer configuration vary depending on whether IKEv1 or IKEv2 was selected.

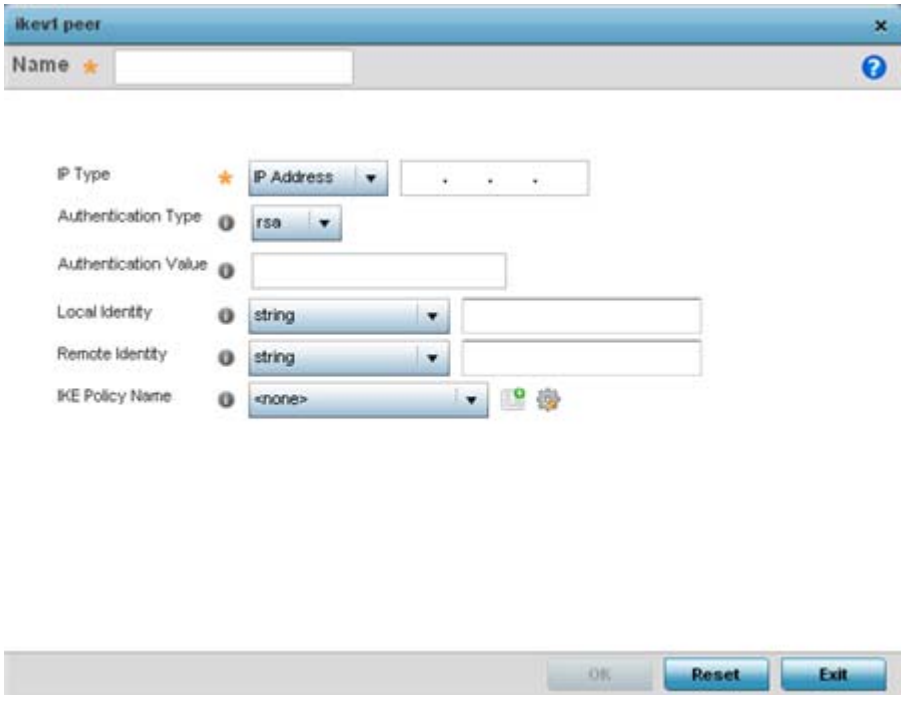


Figure 8-97 *Profile Security - VPN IKE Policy - Add IKE Peer screen*

Name	If creating a new peer configuration (remote gateway) for VPN tunnel connection, assign it a 32 character maximum name to distinguish it from other with similar attributes.

IP Type or Select IP/Hostname	Enter either the *IP address* or FQDN *hostname* of the IPSec VPN peer used in the tunnel setup. If IKEv1 is used, this value is titled *IP Type*, if IKEv2 is used, this parameter is titled *Select IP/Hostname*. A Hostname cannot exceed 64 characters.
Authentication Type	Select either *pre-shared key* (PSK) or RSA. *Rivest, Shamir, and Adleman* (RSA) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing and encryption If using IKEv2, this screen displays both *local* and *remote* authentication options, as both ends of the VPN connection require authentication. RSA is the default value for both local and remote authentication (regardless of IKEv1 or IKEv2).
Authentication Value	Define the authentication string (shared secret) shared by both ends of the VPN tunnel connection. The string must be between 8 - 21 characters long. If using IKEv2, both a local and remote string must be specified for handshake validation at both ends (local and remote) of the VPN connection.
Local Identity	Select the local identifier used with this peer configuration for an IKE exchange with the target VPN IPSec peer. Options include I*P Address*, *Distinguished Name*, *FQDN*, *email* and *string*. The default setting is string.
Remote Identity	Select the remote identifier used with this peer configuration for an IKE exchange with the target VPN IPSec peer. Options include I*P Address*, *Distinguished Name*, *FQDN*, *email* and *string*. The default setting is string.
IKE Policy Name	Select the IKEv1 or IKE v2 policy name (and settings) to apply to this peer configuration. If a policy requires creation, select the *Create* icon.

15 Select **OK** to save the changes made within the peer configuration screen. Select **Reset** to revert to the last saved configuration.

16 Select the **Transform Set** tab.

Create or modify *Transform Set* configurations to specify how traffic is protected.

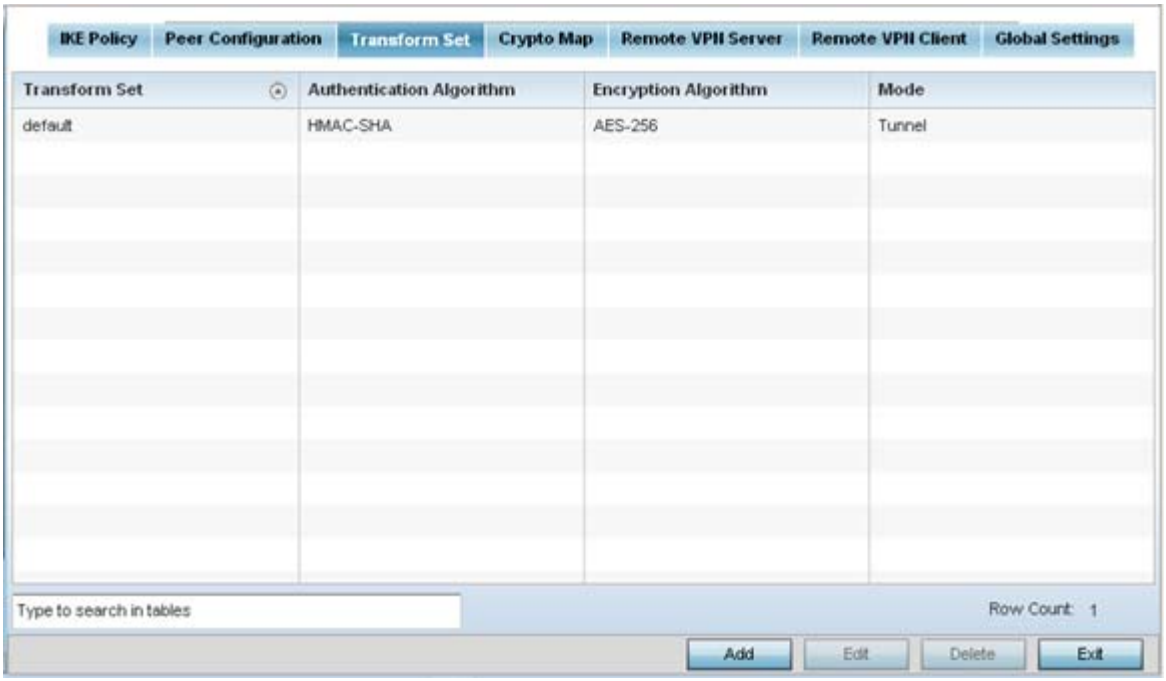


Figure 8-98 *Profile Security - VPN Transform Set screen*

17 Review the following attributes of existing **Transform Set** configurations:

Name	Lists the 32 character maximum name assigned to each listed transform set upon creation. Again, a transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic.
Authentication Algorithm	Lists each transform sets's authentication scheme used to validate identity credentials. The authentication scheme is either *HMAC-SHA* or *HMAC-MD5*.
Encryption Algorithm	Displays each transform set's encryption method for protecting transmitted traffic.
Mode	Displays either *Tunnel* or *Transport* as the IPSec tunnel type used with the transform set. Tunnel is used for site-to-site VPN and Transport should be used for remote VPN deployments.

18 Select **Add** to define a new transform set configuration, **Edit** to modify an existing configuration or **Delete** to remove an existing transform set.

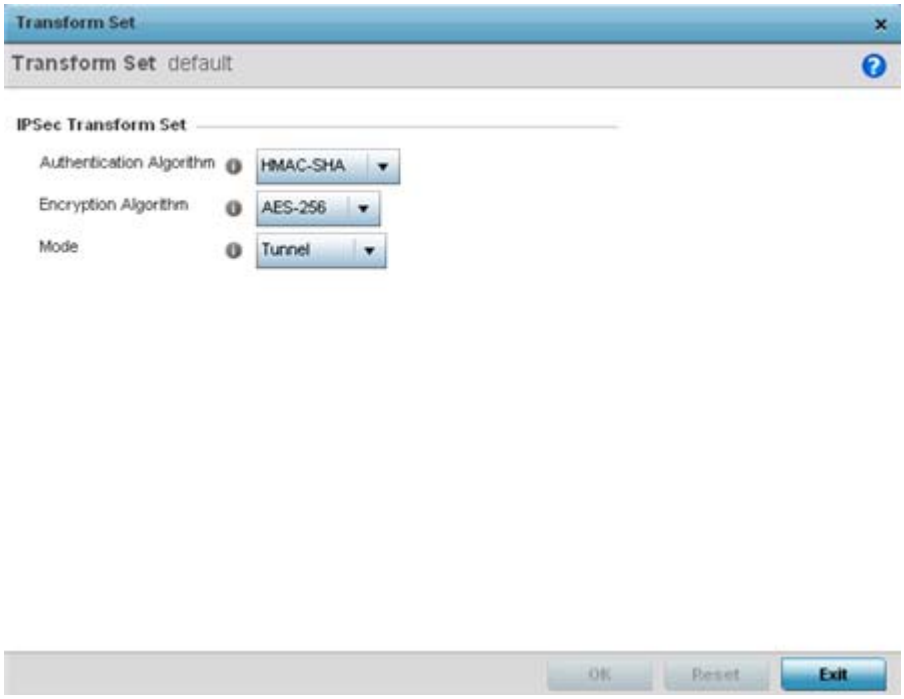


Figure 8-99 *Profile Security - VPN Transform Set create/modify screen*

19 Define the following settings for the new or modified transform set configuration:

Name	If creating a new transform set, define a 32 character maximum name to differentiate this configuration from others with similar attributes.
Authentication Algorithm	Set the transform sets's authentication scheme used to validate identity credentials. Use the drop-down menu to select either *HMAC-SHA* or *HMAC-MD5*. The default setting is HMAC-SHA.
Encryption Algorithm	Set the transform set encryption method for protecting transmitted traffic. Options include *DES*, *3DES*, *AES*, *AES-192* and *AES-256*. The default setting is AES-256.
Mode	Use the drop-down menu to select either *Tunnel* or *Transport* as the IPSec tunnel type used with the transform set. Tunnel is used for site-to-site VPN and Transport should be used for remote VPN deployments.

20 Select **OK** to save the changes made within the Transform Set screen. Select **Reset** to revert to the last saved configuration.

21 Select the **Crypto Map** tab.

Use crypto maps (as applied to IPSec VPN) to combine the elements used to create IPSec SAs (including transform sets).

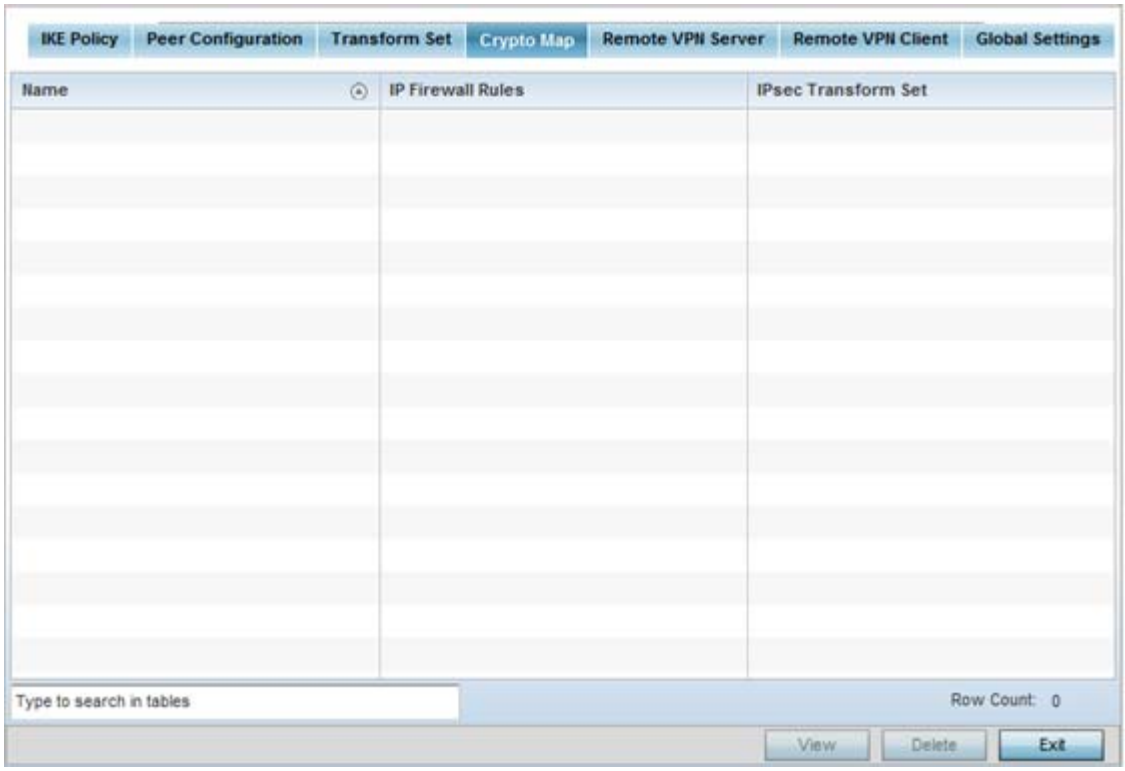


Figure 8-100 *Profile Security - VPN Crypto Map screen*

22 Review the following **Crypto Map** configuration parameters to assess their relevance:

Name	Lists the 32 character maximum name assigned for each crypto map upon creation. This name cannot be modified as part of the edit process.
IP Firewall Rules	Lists the IP firewall rules defined for each displayed crypto map configuration. Each firewall policy contains a unique set of access/deny permissions applied to the VPN tunnel and its peer connection.
IPSec Transform Set	Displays the transform set (encryption and has algorithms) applied to each listed crypto map configuration. Thus, each crypto map can be customized with its own data protection and peer authentication schemes.

23 If requiring a new crypto map configuration, select the **Add** button. If updating the configuration of an existing crypto map, select it from amongst those available and select the **Edit** button.

24 If adding a new crypto map, assign it a name up to 32 characters in length as a unique identifier. Select the **Continue** button to proceed to the **VPN Crypto Map** screen.

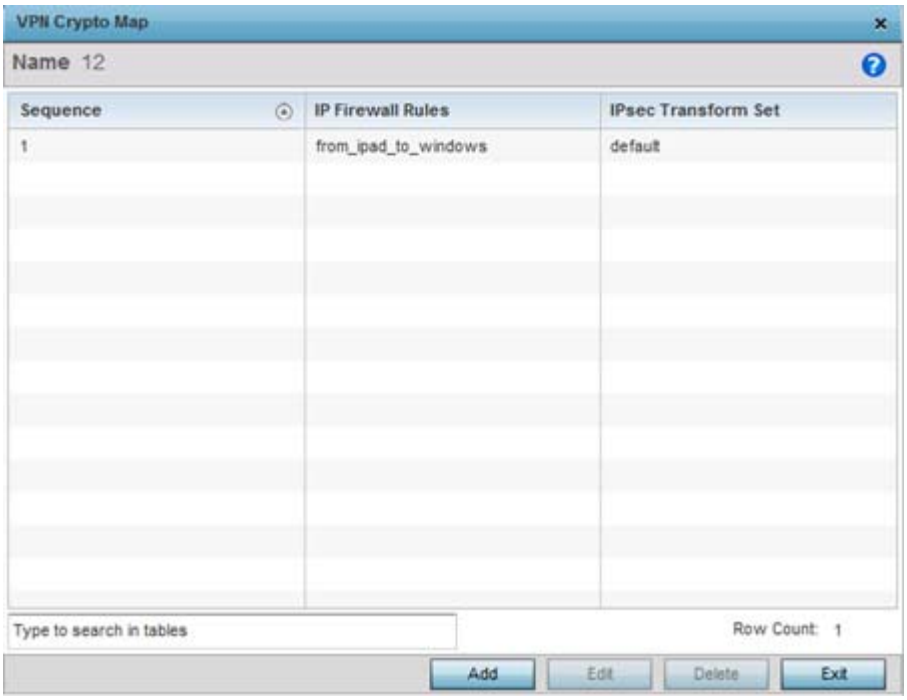


Figure 8-101 *Profile Security - VPN Crypto Map Add / Edit screen*

25 Review the following before determining whether to add or modify a crypto map configuration.

Sequence	Each crypto map configuration uses a list of entries based on a sequence number. Specifying multiple sequence numbers within the same crypto map, provides the flexibility to connect to multiple peers from the same interface, based on the sequence number (from 1 - 1,000).
IP Firewall Rules	Lists the IP firewall rules defined for each displayed crypto map configuration. Each firewall policy contains a unique set of access/deny permissions applied to the VPN tunnel and its peer connection.
IPSec Transform Set	Displays the transform set (encryption and hash algorithms) applied to each listed crypto map configuration. Thus, each crypto map can be customized with its own data protection and peer authentication schemes.

26 If requiring a new crypto map configuration, select the **Add** button. If updating the configuration of an existing crypto map, select it from amongst those available and select the **Edit** button.

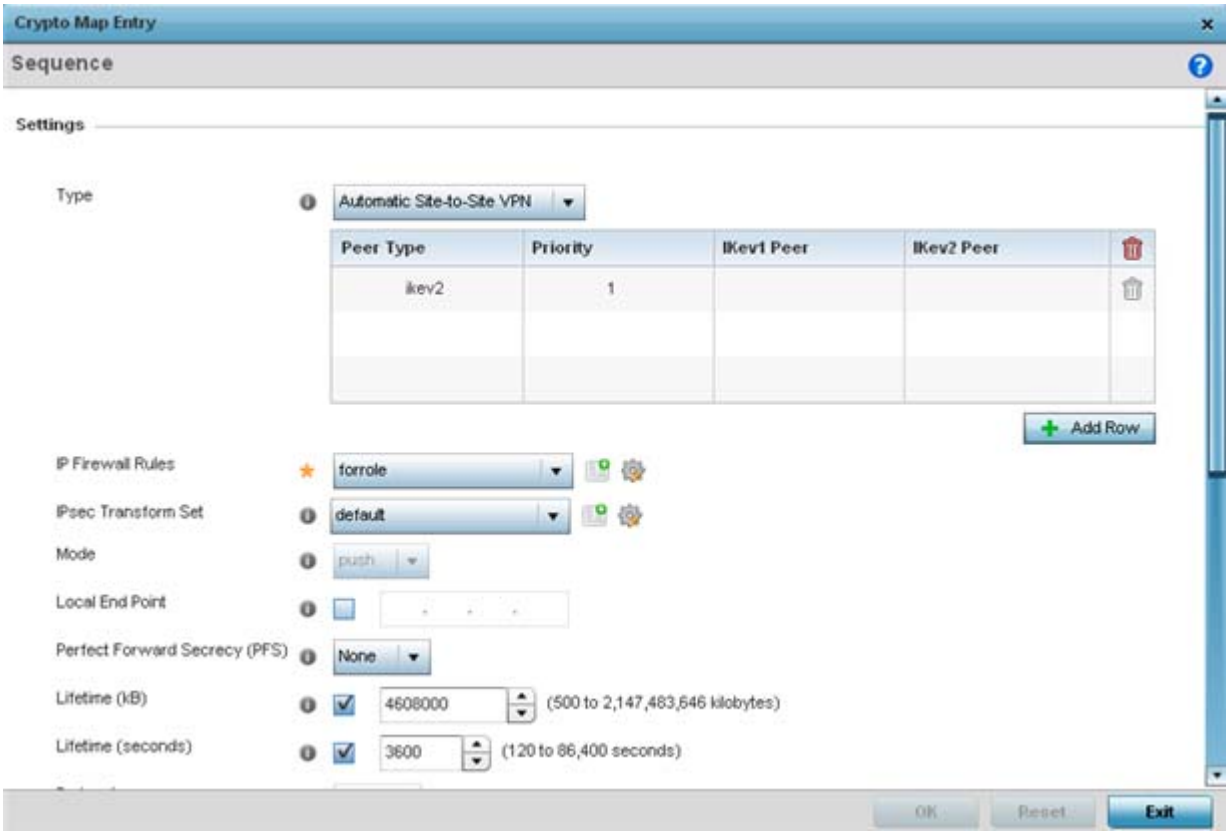


Figure 8-102 *Profile Security - VPN Crypto Map Entry screen*

27 Define the following **Settings** to set the crypto map configuration:

Sequence	Each crypto map configuration uses a list of entries based on a sequence number. Specifying multiple sequence numbers within the same crypto map extends connection flexibility to multiple peers on the same interface, based on this selected sequence number (from 1 - 1,000).
Type	Define the *site-to-site-manual*, *site-to-site-auto* or *remote VPN* configuration defined for each listed crypto map configuration.
IP Firewall Rules	Use the drop-down menu to select the ACL used to protect IPSec VPN traffic. New access/deny rules can be defined for the crypto map by selecting the *Create* icon, or an existing set of firewall rules can be modified by selecting the *Edit* icon.
IPSec Transform Set	Select the transform set (encryption and hash algorithms) to apply to this crypto map configuration.
Mode	Use the drop-down menu to define which mode (*pull* or *push*) is used to assign a virtual IP. This setting is relevant for IKEv1 only, since IKEv2 always uses the configuration payload in pull mode. The default setting is push.
Local End Point	Select this radio button to define an IP address as a local tunnel end point address. This setting represents an alternative to an interface IP address.

Perfect Forward Secrecy (PFS)	PFS is key-establishment protocol, used to secure VPN communications. If one encryption key is compromised, only data encrypted by that specific key is compromised. For PFS to exist, the key used to protect data transmissions must *not* be used to derive any additional keys. Options include *None*, *2*, *5* and *14*. The default setting is None.
Lifetime (kB)	Select this option to define a connection volume lifetime (in kilobytes) for the duration of an IPSec VPN security association. Once the set volume is exceeded, the association is timed out. Use the spinner control to set the volume from 500 - 2,147,483,646 kilobytes.
Lifetime (seconds)	Select this option to define a lifetime (in seconds) for the duration of an IPSec VPN security association. Once the set value is exceeded, the association is timed out. The available range is from 120 - 86,400 seconds. The default setting is 120 seconds.
Protocol	Select the security protocol used with the VPN IPSec tunnel connection. SAs are unidirectional, existing in each direction and established per security protocol. Options include *ESP* and *AH*. The default setting is ESP.
Remote VPN Type	Define the remote VPN type as either *None* or *XAuth*. XAuth (extended authentication) provides additional authentication validation by permitting an edge device to request extended authentication information from an IPSec host. This forces the host to respond with additional authentication credentials. The edge device responds with a failed or passed message. The default setting is XAuth.
Manual Peer IP	Select this option to define the IP address of an additional encryption/ decryption peer.
Time Out	Set an IPSec *security association* (SA) timeout in either *Seconds* (120 - 86,400), *Minutes* (2 - 1,440), *Hours* (1 - 24) or *Days* (1). The default setting is 15 minutes.
Enable NAT after IPSec	Enable this setting to utilize IP/Port NAT on the VPN tunnel. This setting is disabled by default.

28 Select **OK** to save the updates made to the Crypto Map Entry screen. Selecting **Reset** reverts the screen to its last saved setting.

29 Select **Remote VPN Server**.

Use this screen to define the server resources used to secure (authenticate) a remote VPN connection with a target peer.

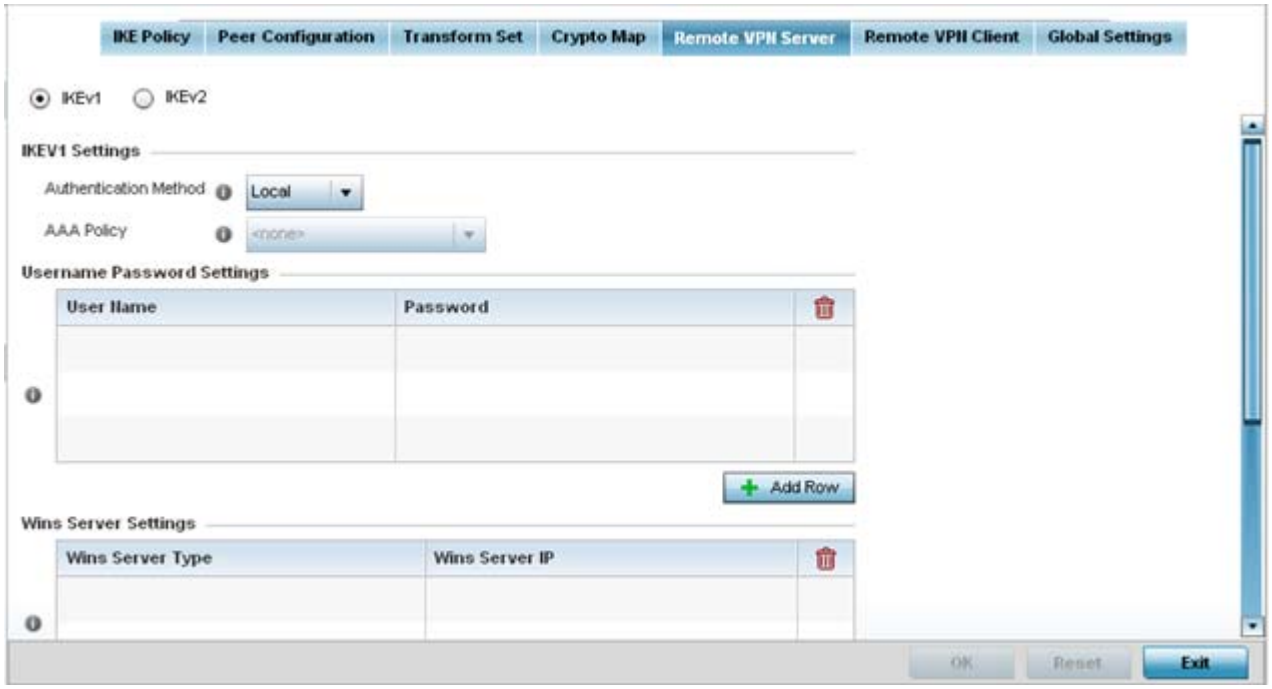


Figure 8-103 *Profile Security - Remote VPN Server screen (IKEv1 example)*

30 Select either the **IKEv1** or **IKEv2** radio button to enforce peer key exchanges over the remote VPN server using either IKEv1 or IKEv2.

IKEv2 provides improvements from the original IKEv1 design (improved cryptographic mechanisms, NAT and firewall traversal, attack resistance etc.) and is recommended in most deployments. The appearance of the screen differs depending on the selected IKEv1 or IKEv2 mode.

31 Set the following **IKEv1** or **IKEv2 Settings**:

Authentication Method	Use the drop-down menu to specify the authentication method used to validate the credentials of the remote VPN client. Options include *Local* (on board RADIUS resource if supported) and *RADIUS* (designated external RADIUS resource). If selecting Local, select the *+ Add Row* button and specify a *User Name* and *Password* for authenticating remote VPN client connections with the local RADIUS resource. The default setting is Local. AP6521 model Access Point does not have a local RADIUS resource and must use an external RADIUS server resource.
AAA Policy	Select the AAA policy used with the remote VPN client. AAA policies define RADIUS authentication and accounting parameters. The Access Point can optionally use AAA server resources (when using RADIUS as the authentication method) to provide user database and authentication data.

32 Refer to the **Username Password Settings** field and specify local user database user name and password credentials required for user validation when conducting authentication locally.

33 Refer to the **Wins Server Settings** field and specify *primary* and *secondary* server resources for validating RADIUS authentication requests on behalf of a remote VPN client. These external WINS server resources are available to validate RADIUS resource requests.

34 Refer to the **Name Server Settings** field and specify *primary* and *secondary* server resources for validating RADIUS authentication requests on behalf of a remote VPN client. These external name server resources are available to validate RADIUS resource requests.

35 Select the **IP Local Pool** option to define an IP address and mask for a virtual IP pool used to IP addresses to remote VPN clients.

36 If using IKEv2, specify these additional DHCP settings (required for IKEv2 only):

DHCP Server Type	Specify whether the DHCP server is specified as an *IP address*, *Hostname (FQDN)* or *None* (a different classification will be defined). *Dynamic Host Configuration Protocol* (DHCP) allows hosts on an IP network to request and be assigned IP addresses and discover information about the network where they reside.
DHCP Server	Depending on the DHCP server type selected, enter either the numerical IP address, hostname or other (if None is selected as the server type). A Hostname cannot exceed 64 characters.
IP Local Pool	Define an IP address and mask for a virtual IP pool used to assign IP addresses to requesting remote VPN clients.
Relay Agent IP Address	Select this option to define a DHCP relay agent IP address. DHCP relays exchange messages between a DHCPv6 server and client. A client and relay agent exist on the same link. When A DHCP request is received from the client, the relay agent creates a relay forward message and sends it to a specified server address. If no addresses are specified, the relay agent forwards the message to all DHCP server relay multicast addresses. The server creates a relay reply and sends it back to the relay agent. The relay agent then sends back the response to the client.

37 Select **OK** to save the updates made to the Remote VPN Server screen. Selecting **Reset** reverts the screen to its last saved configuration.

38 Select the **Remote VPN Client** tab.

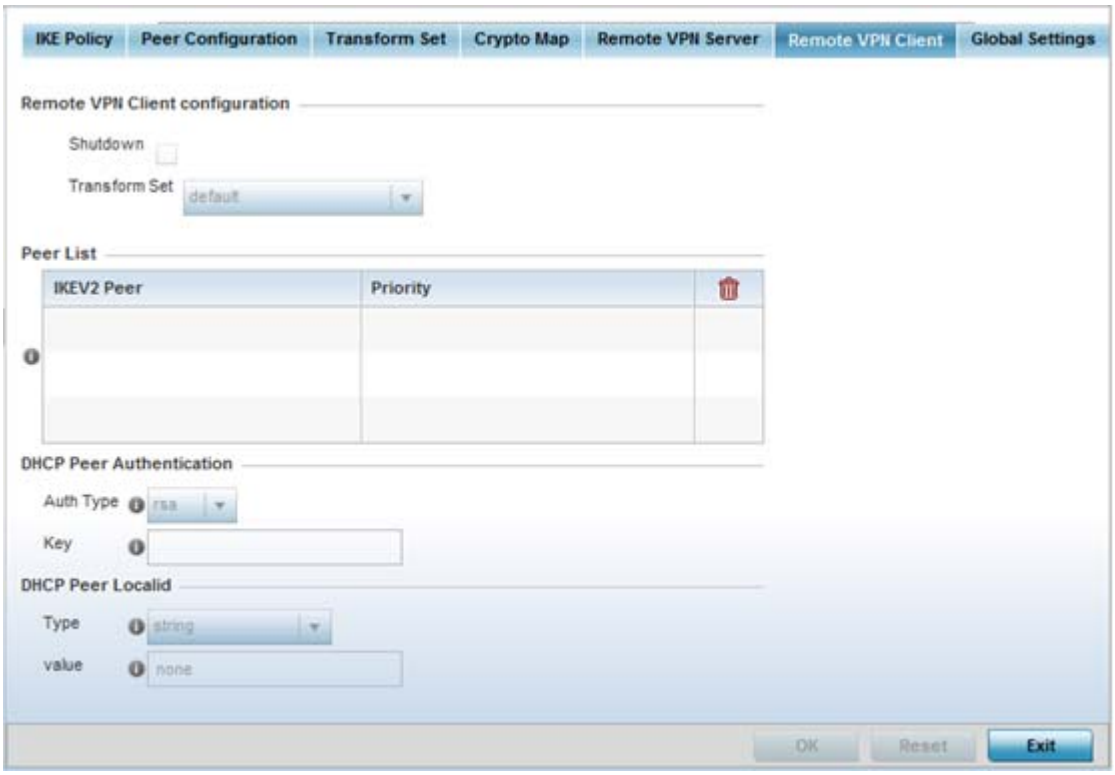


Figure 8-104 *Profile Security - Remote VPN Client screen*

39 Set the following **Remote VPN Client configuration** settings:

Shutdown	Select this option to shutdown the remote VPN client.
Transform Set	Select the transform set configuration to apply to remote client VPN connections. A transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected client traffic.

40 Refer to the **Peer List** to select IKEV2 peer configurations and assign them priorities for utilization with Remote VPN client connections.

IKEv2 uses an initial handshake in which VPN peers negotiate cryptographic algorithms, mutually authenticate, and establish a session key, creating an IKE-SA. Additionally, a first IPsec SA is established during the initial SA creation. All IKEv2 messages are request/response pairs. It is the responsibility of the side sending the request to retransmit if it does not receive a timely response.

41 Set the following **DHCP Peer Authentication** settings:

Auth Type	Use the drop-down menu to specify the DHCP peer authentication type. Options include *PSK* and *rsa*. The default setting is rsa.
Key	Provide a 8 - 21 character shared key password for DHCP peer authentication.

42 Set the following **DHCP Peer Localid** settings:

Type	Select the DHCP peer local ID type. Options include *string* and *autogen-uniqueid*. The default setting is string.
value	Set the DHCP peer local ID. The ID cannot exceed 128 characters.

43 Select **OK** to save the updates made to the Remote VPN Client screen. Selecting **Reset** reverts the screen to its last saved configuration.

44 Select the **Global Settings** tab.

The Global Settings screen provides options for *Dead Peer Detection* (DPD). DPD represents the actions taken upon the detection of a dead peer within the IPSec VPN tunnel connection.

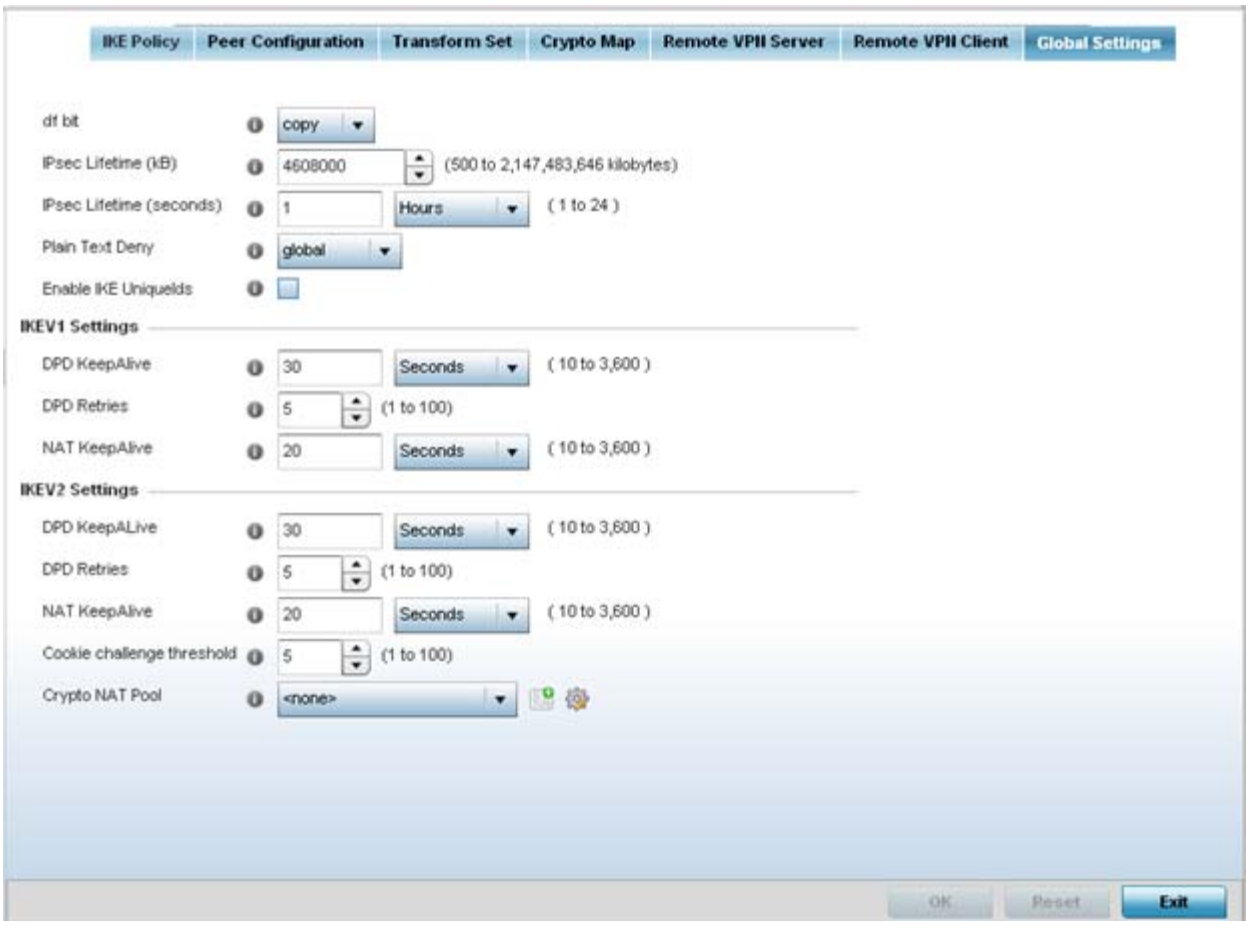


Figure 8-105 *Profile Security - Global VPN Settings screen*

45 Define the following **IPSec Global** settings:

df bit	Select the DF bit handling technique used for the ESP encapsulating header. Options include *Clear*, *set* and *copy*. The default setting is Copy.
IPsec Lifetime (kB)	Set a connection volume lifetime (in kilobytes) for the duration of an IPSec VPN security association. Once the set volume is exceeded, the association is timed out. Use the spinner control to set the volume from 500 - 2,147,483,646 kilobytes. The default settings is 4,608,000 kilobytes.
IPsec Lifetime (seconds)	Set a lifetime (in seconds) for the duration of an IPSec VPN security association. Once the set value is exceeded, the association is timed out. The available range either *Seconds* (120 - 86,400), *Minutes* (2 - 1,440), *Hours* (1 - 24) or *Days* (1). The default setting is 3,600 seconds.
Plain Text Deny	Select *global* or *interface* to set the scope of the ACL. The default setting is global, expanding the rules of the ACL beyond just the interface.

Enable IKE UniqueIds	Select this option to initiate a unique ID check. This setting is disabled by default.

46 Set the following **IKEV1 Settings**:

DPD KeepAlive	Define the interval (or frequency) for IKE keep alive messages for dead peer detection. Options include *Seconds* (10 - 3,600), *Minutes* (1 - 60) and *Hours* (1). The default setting is 30 seconds.
DPD Retries	Use the spinner control to define the number of keep alive messages sent to an IPSec VPN client before the tunnel connection is defined as dead. The available range is from 1 - 100. The default number of messages is 5.
NAT KeepAlive	Define the interval (or frequency) for NAT keep alive messages for dead peer detection. Options include *Seconds* (10 - 3,600), *Minutes* (1 - 60) and *Hours* (1). The default setting is 20 seconds.

47 Set the following **IKEV2 Settings**:

DPD KeepAlive	Define the interval (or frequency) for IKE keep alive messages for dead peer detection. Options include *Seconds* (10 - 3,600), *Minutes* (1 - 60) and *Hours* (1). The default setting is 30 seconds.
DPD Retries	Use the spinner control to define the number of keep alive messages sent to an IPSec VPN client before the tunnel connection is defined as dead. The available range is from 1 - 100. The default number of messages is 5.
NAT KeepAlive	Define the interval (or frequency) for NAT keep alive messages for dead peer detection. Options include *Seconds* (10 - 3,600), *Minutes* (1 - 60) and *Hours* (1). The default setting is 20 seconds.
Cookie Challenge Threshold	Use the spinner control to define the number of half open IKE *security associations* (SAs) (from 1 - 100) that, when exceeded, enables the cookie challenge mechanism. The is setting applies exclusively to IKEV2. The default setting is 5.
Crypto NAT Pool	Select the NAT pool used for internal source NAT on IPSec tunnels. NAT is used as an IP masquerading technique to hide private IP addresses behind a single, public facing, IP address.

48 Select **OK** to save the updates made to the screen. Selecting **Reset** reverts the screen to its last saved configuration.

8.9.5 Setting the Profile's Auto IPSec Tunnel Configuration

Profile Security Configuration

Auto IPSec tunneling provides a secure tunnel between two networked peer controllers or service platforms and associated Access Points. Administrators can define which packets are sent within the tunnel, and how they're protected. When a tunnelled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination or associated Access Point.

Tunnels are sets of *security associations* (SA) between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunnelled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (*AH* or *ESP*).

Internet Key Exchange (IKE) protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE enables secure communications without time consuming manual pre-configuration for auto IPSec tunneling.

To define an Auto IPsec Tunnel configuration that can be applied to a profile:

1 Select the **Configuration** tab from the Web UI

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu.

4 Select **Security**.

5 Select **Auto IPSec Tunnel**.

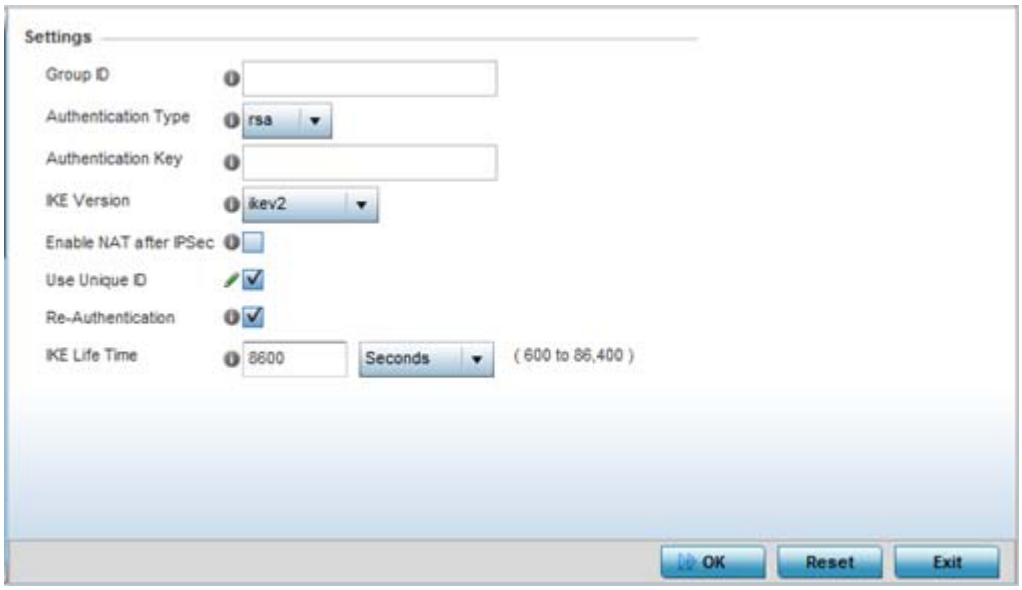


Figure 8-106 *Security Auto IPSec Tunnel screen*

6 The **Auto IPSec Tunnel** screen displays by default. Refer to the **Settings** field to set an Auto IPSec Tunnel configuration for use with this profile.

Group ID	Define a 1 - 64 character group identifier for an IKE exchange supporting auto IPSec tunnel secure peers.
Authentication Type	Use the drop-down menu to select either RSA or PSK (Pre Shared Key) as the authentication type for secure peer authentication on the auto IPSec secure tunnel. *Rivest, Shamir, and Adleman* (RSA) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing, as well as encryption. The default setting is RSA.
Authentication Key	Enter the 8 - 21 character shared key (password) used for auto IPSec tunnel secure peer authentication.
IKE Version	Use the drop-down menu to select the IKE version used for auto IPSec tunnel secure authentication with the IPSec gateway.
Enable NAT after IPSec	Select this option to enable internal source port NAT on the auto IPSec secure tunnel.
Use Unique ID	Select this option to use a unique ID with auto IPSec secure authentication for the IPSec remote gateway (appending the MiNT ID). This setting is disabled by default.

Re-Authentication	Select this option to re-authenticate the key on an IKE rekey. This setting is enabled by default.
IKE Lifetime	Set a lifetime in either *Seconds* (600 - 86,400), *Minutes* (10 - 1,440), *Hours* (1 - 24) or *Days* (1) for IKE security association duration. The default is 8600 seconds.

7 Select **OK** to save the changes made to the auto IPSec tunnel configuration. Select **Reset** to revert to the last saved configuration.

8.9.6 Setting the Profile's NAT Configuration

Profile Security Configuration

Network Address Translation (NAT) is a technique to modify network address information within IP packet headers in transit across a traffic routing device. This enables mapping one IP address to another to protect network address credentials. With typical deployments, NAT is used as an IP masquerading technique to hide private IP addresses behind a single, public facing, IP address.

NAT is a process of modifying network address information in IP packet headers while in transit across a traffic routing device for the purpose of remapping one IP address to another. In most deployments NAT is used in conjunction with IP masquerading which hides RFC1918 private IP addresses behind a single public IP address.

NAT can provide an profile outbound Internet access to wired and wireless hosts connected to either an Access Point or a wireless controller. Many-to-one NAT is the most common NAT technique for outbound Internet access. Many-to-one NAT allows an Access Point or wireless controller to translate one or more internal private IP addresses to a single, public facing, IP address assigned to a 10/100/1000 Ethernet port or 3G card.

To define a NAT configuration that can be applied to a profile:

1 Select the Configuration tab from the Web UI

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu.

4 Select **Security**.

5 Select **NAT**.

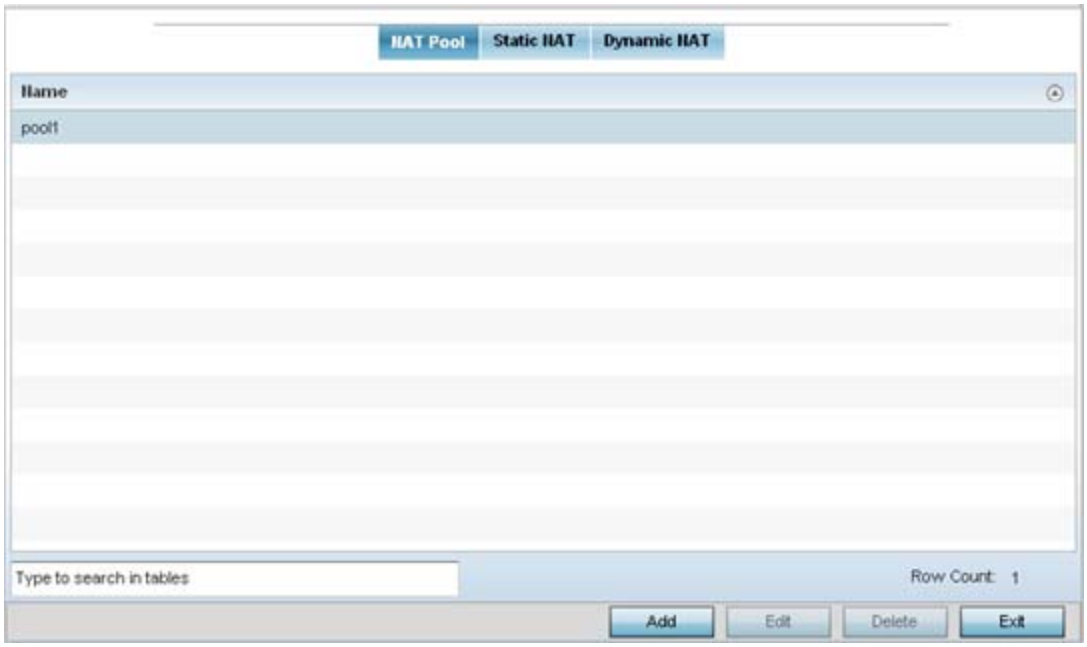


Figure 8-107 *Security NAT screen - NAT Pool tab*

The **NAT Pool** displays by default. The NAT Pool screen lists those NAT policies created thus far. Any of these policies can be selected and applied to a profile.

6 Select **Add** to create a new NAT policy that can be applied to a profile. Select **Edit** to modify the attributes of a existing policy or select **Delete** to remove obsolete NAT policies from the list of those available to a profile.

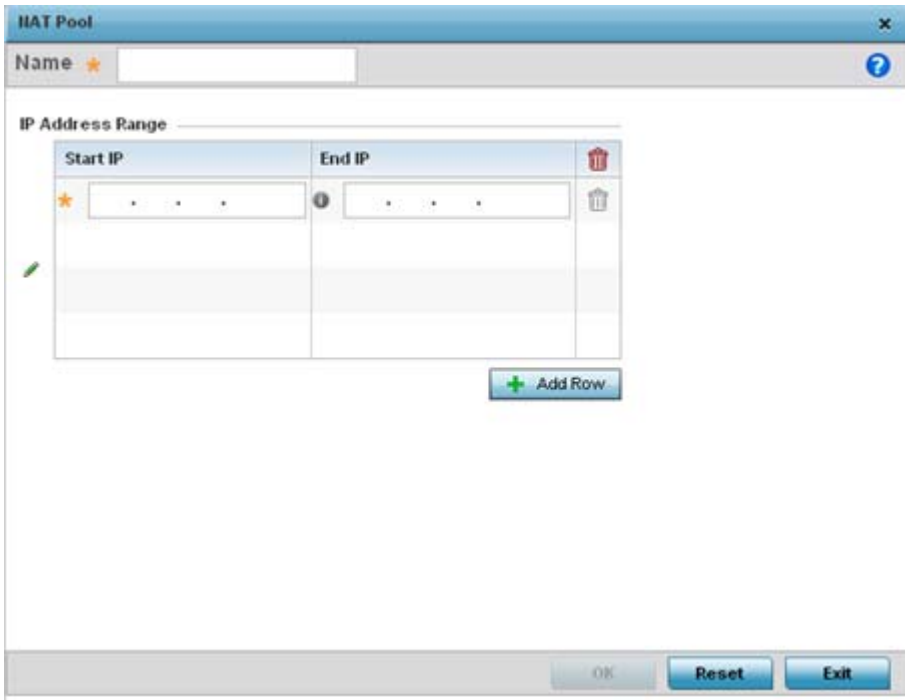


Figure 8-108 *Security NAT Pool screen*

7 If adding a new NAT policy or editing the configuration of an existing policy, define the following parameters:

Name	If adding a new NAT policy, provide a name to help distinguish it from others with similar configurations. The length cannot exceed 64 characters.
IP Address Range	Define a range of IP addresses hidden from the public Internet. NAT modifies network address information in the defined IP range while in transit across a traffic routing device. NAT only provides IP address translation and does not provide a firewall. A branch deployment with NAT by itself will not block traffic from being potentially routed through a NAT device. Consequently, NAT should be deployed with a stateful firewall.

8 Select the **+ Add Row** button as needed to append additional rows to the IP Address Range table.

9 Select **OK** to save the changes made to the profile's NAT Pool configuration. Select **Reset** to revert to the last saved configuration.

10 Select the **Static NAT** tab.

The **Source** tab displays by default and lists existing static NAT configurations. Existing static NAT configurations are not editable, but new configurations can be added or existing ones deleted as they become obsolete.

Static NAT creates a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a Web server on a perimeter interface with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host.

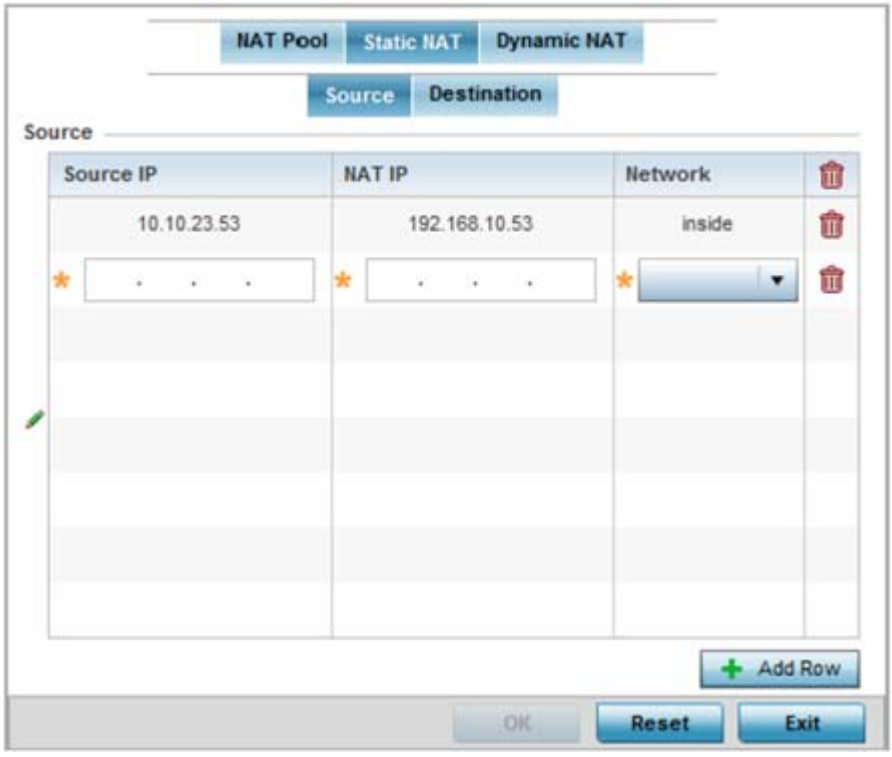


Figure 8-109 *Static NAT screen*

11 Select **+ Add Row** to create a new static NAT configuration. Existing NAT source configurations are not editable.

12 Set or override the following **Source** configuration parameters:

Source IP	Enter the local address used at the origination of the static NAT configuration. This address (once translated) is not exposed to the outside world when the translation address is used to interact with the remote destination.
NAT IP	Enter the IP address of the matching packet to the specified value. The IP address modified can be either source or destination based on the direction specified.
Network	Select *Inside* or *Outside* NAT as the network direction. Select Inside to create a permanent, one-to-one mapping between an address on an internal network and a perimeter or external network. To share a Web server on a perimeter interface with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual address of the server from users on insecure interfaces. Casual access by unauthorized users becomes much more difficult. Static NAT requires a dedicated address on the outside network for each host. Inside NAT is the default setting.Inside is the default setting.

13 Select the **Destination** tab to view destination NAT configurations and ensure packets passing through the NAT back to the managed LAN are searched against the records kept by the NAT engine. The destination IP address is changed back to the specific internal private class IP address to reach the LAN over the network.

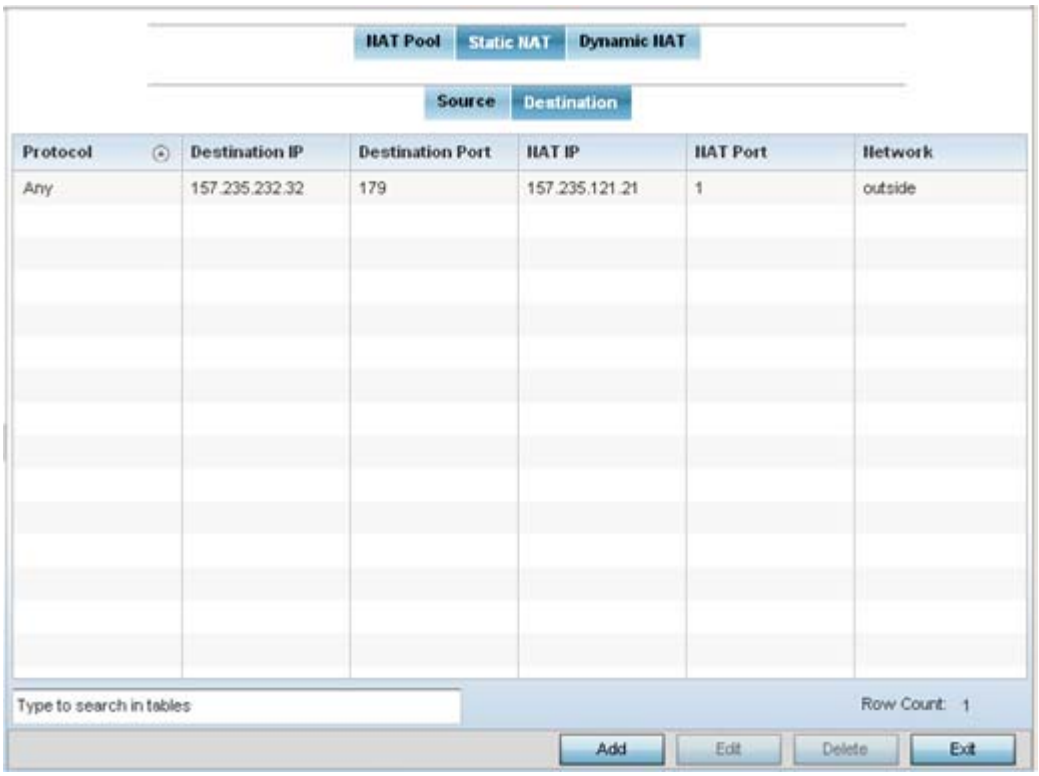


Figure 8-110 *NAT Destination screen*

14 Select **Add** to create a new NAT destination configuration. Existing NAT destination configurations are not editable.

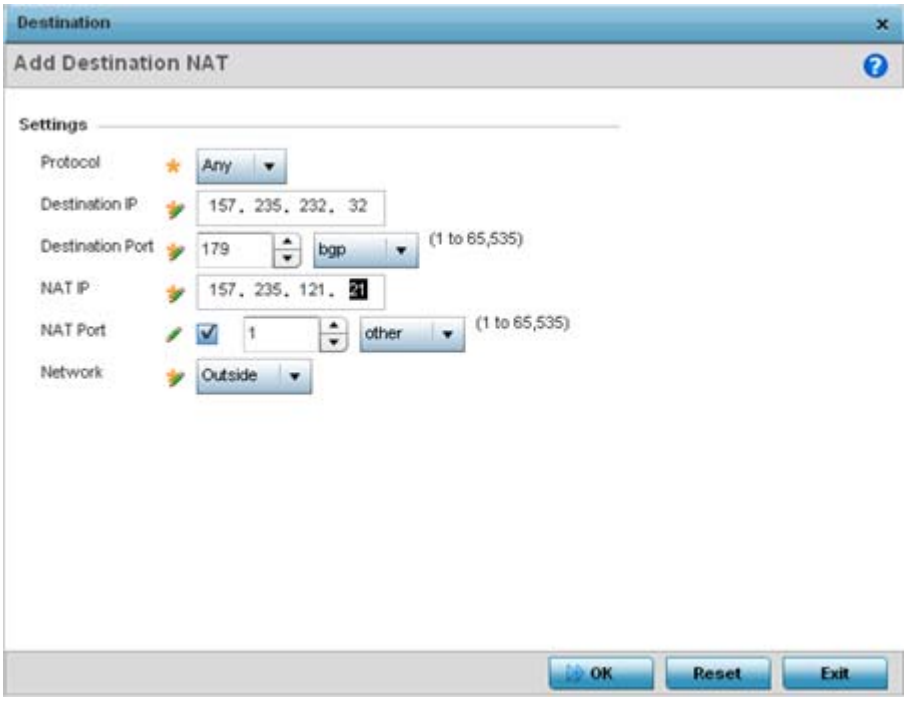


Figure 8-111 *NAT Destination Add screen*

15 Set the following **Destination** configuration parameters:

Protocol	Select the protocol for use with static translation. *TCP, UDP* and *Any* are available options. TCP is a transport layer protocol used by applications requiring guaranteed delivery. It's a sliding window protocol handling both timeouts and retransmissions. TCP establishes a full duplex virtual connection between two endpoints. Each endpoint is defined by an IP address and a TCP port number. The *User Datagram Protocol* (UDP) offers only a minimal transport service, non-guaranteed datagram delivery, and provides applications direct access to the datagram service of the IP layer. UDP is used by applications not requiring the level of service of TCP or are using communications services (multicast or broadcast delivery) not available from TCP. The default setting is Any.
Destination IP	Enter the local address used at the (source) end of the static NAT configuration. This address (once translated) is not be exposed to the outside world when the translation address is used to interact with the remote destination.
Destination Port	Use the spinner control to set the local port used at the (source) end of the static NAT configuration. The default port is 1.
NAT IP	Enter the IP address of the matching packet to the specified value. The IP address modified can be either *source* or *destination* based on the direction specified.
NAT Port	Set the port number of the matching packet to the specified value. This option is valid only if the direction specified is destination.
Network	Select *Inside* or *Outside* NAT as the network direction. Inside is the default setting.

16 Select **OK** to save the changes made to the static NAT configuration. Select **Reset** to revert to the last saved configuration.

17 Select the **Dynamic NAT** tab.

Dynamic NAT translates the IP address of packets from one interface to another interface based on configured conditions. Dynamic NAT requires packets be switched through a NAT router to generate translations in the translation table.

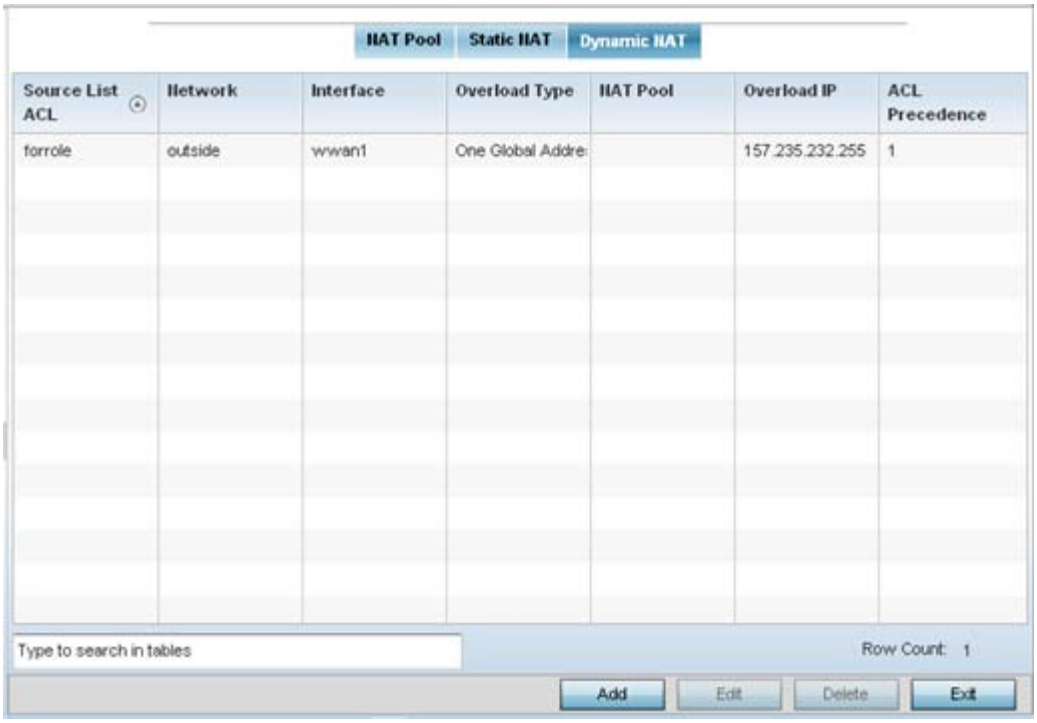


Figure 8-112 *Dynamic NAT screen*

18 Refer to the following to determine whether a new Dynamic NAT configuration requires creation, edit or deletion:

Source List ACL	Lists an ACL name to define the packet selection criteria for the NAT configuration. NAT is applied only on packets which match a rule defined in the access list. These addresses (once translated) are not exposed to the outside world when the translation address is used to interact with the remote destination.
Network	Displays *Inside* or *Outside* NAT as the network direction for the dynamic NAT configuration.
Interface	Lists the VLAN (between 1 - 4094) used as the communication medium between the source and destination points within the NAT configuration.
Overload Type	Lists the Overload Type used with the listed IP ACL rule. Options include *NAT Pool*, *One Global Address* and *Interface IP Address*. Interface IP Address is the default setting.
NAT Pool	Displays the name of an existing NAT pool used with the dynamic NAT configuration.
Overload IP	Enables the use of one global address for numerous local addresses.
ACL Precedence	Lists the administrator assigned priority set for the listed source list ACL. The lower the value listed the higher the priority assigned to these ACL rules.

19 Select **Add** to create a new Dynamic NAT configuration, **Edit** to modify an existing configuration or **Delete** to permanently remove a configuration.

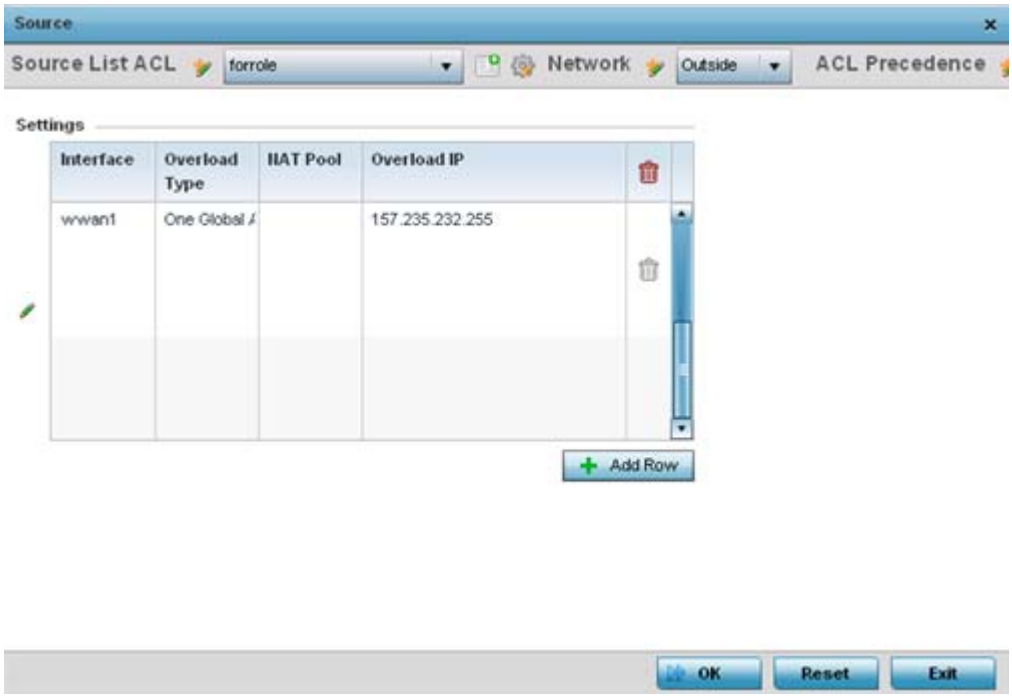


Figure 8-113 *Source ACL List screen*

20 Set the following to define the Dynamic NAT configuration:

Source List ACL	Use the drop-down menu to select an ACL name to define the packet selection criteria for NAT. NAT is applied only on packets which match a rule defined in the access list. These addresses (once translated) are not exposed to the outside world when the translation address is used to interact with the remote destination.
Network	Select *Inside* or *Outside* NAT as the network direction for the dynamic NAT configuration. Inside is the default setting.
ACL Precedence	Set the priority (from 1 - 5000) for the source list ACL. The lower the value, the higher the priority assigned to these ACL rules.
Interface	Use the drop-down menu to select the VLAN (between 1 - 4094) used as the communication medium between the source and destination points within the NAT configuration. Ensure the VLAN selected represents the intended network traffic within the NAT supported configuration. VLAN1 is available by default.
Overload Type	Select the check box of Overload Type used with the listed IP ACL rule. Options include *NAT Pool*, *One Global Address* and *Interface IP Address*. Interface IP Address is the default setting.
NAT Pool	Provide the name of an existing NAT pool for use with the dynamic NAT configuration.
Overload IP	Enables the use of one global address for numerous local addresses.

21 Select **OK** to save the changes made to the dynamic NAT configuration. Select **Reset** to revert to the last saved configuration.

8.9.7 Setting the Profile's Bridge NAT Configuration

Profile Security Configuration

Use *Bridge NAT* to manage Internet traffic originating at a remote site. In addition to traditional NAT functionality, Bridge NAT provides a means of configuring NAT for bridged traffic through an Access Point. NAT rules are applied to bridged traffic through the Access Point, and matching packets are NATed to the WAN link instead of being bridged on their way to the router.

Using Bridge NAT, a tunneled VLAN (extended VLAN) is created between the NoC and a remote location. When a remote client needs to access the Internet, Internet traffic is routed to the NoC, and from there routed to the Internet. This increases the access time for the end user on the client.

To resolve latency issues, Bridge NAT identifies and segregates traffic heading towards the NoC and outwards towards the Internet. Traffic towards the NoC is allowed over the secure tunnel. Traffic towards the Internet is switched to a local WLAN link with access to the Internet.

To define a NAT configuration that can be applied to a profile:

1 Select the Configuration tab from the Web UI

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu

4 Select **Security**.

5 Select **Bridge NAT**.

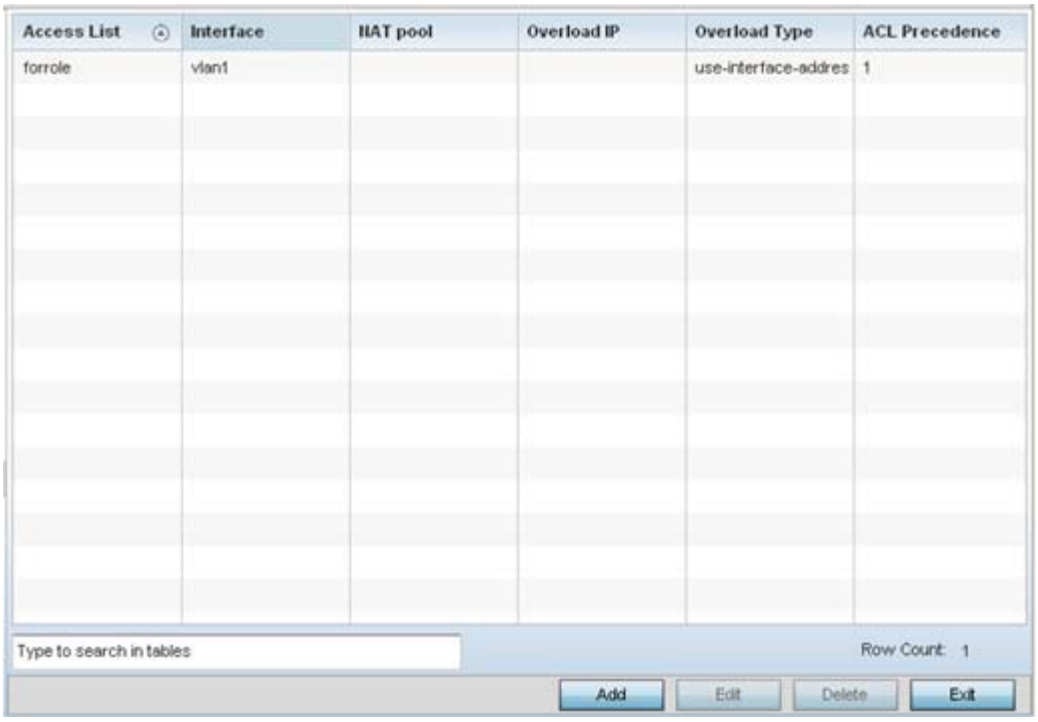


Figure 8-114 *Security Bridge NAT screen*

6 Review the following Bridge NAT configurations to determine whether a new Bridge NAT configuration requires creation or an existing configuration be modified or removed.

Access List	Lists the ACL applying IP address access/deny permission rules to the Bridge NAT configuration.
Interface	Lists the communication medium (outgoing layer 3 interface) between source and destination points. This is either the Access Point's *pppoe1* or *wwan1* interface or the VLAN used as the redirection interface between the source and destination.
NAT Pool	Lists the names of existing NAT pools used with the Bridge NAT configuration. This displays only when the *Overload Type* is NAT Pool.
Overload IP	Lists the address used globally and collectively for numerous local addresses.
Overload Type	Lists the overload type used with the listed IP ACL rule. Set as either *NAT Pool*, *One Global Address* or *Interface IP Address*.
ACL Precedence	Lists the administrator assigned priority set for the ACL. The lower the value listed the higher the priority assigned to these ACL rules.

7 Select **Add** to create a new Bridge VLAN configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.

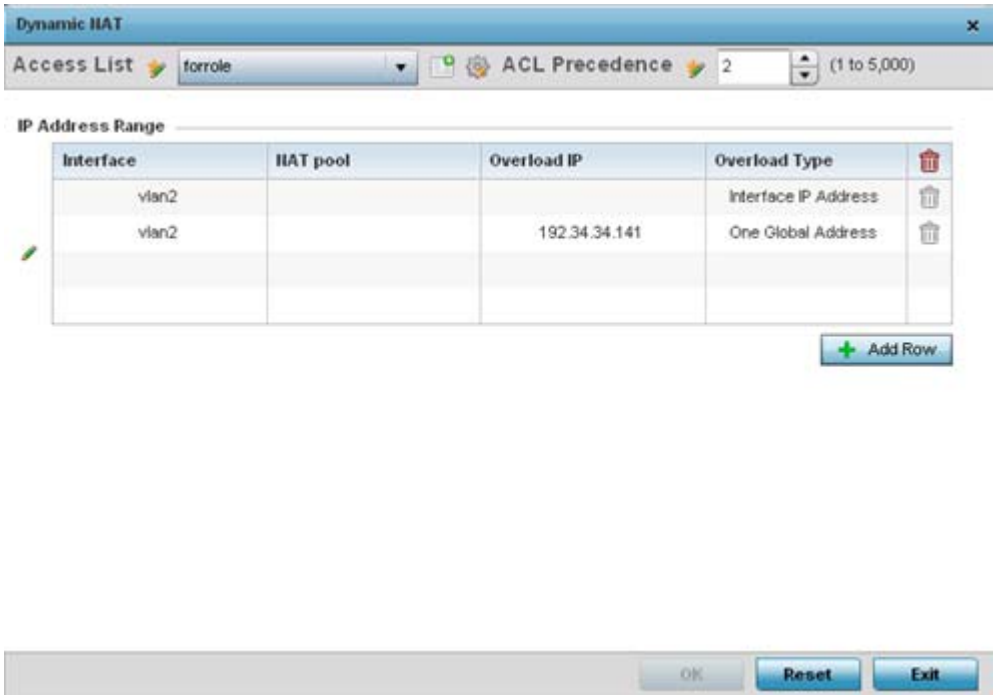


Figure 8-115 *Security Source Dynamic NAT screen*

8 Select the **Access List** whose IP rules are applied to this policy based forwarding rule. A new ACL can be defined by selecting the **Create** icon, or an existing set of IP ACL rules can be modified by selecting the **Edit** icon.

9 Use the **IP Address Range** table to configure IP addresses and address ranges used to access the Internet.

ACL Precedence	Set the priority (from 1 - 5000) for the ACL. The lower the value, the higher the priority assigned to these ACL rules.

Interface	Lists the outgoing layer 3 interface on which traffic is re-directed. The interface can be an Access Point *wwan1* or *pppoe1* interface. Traffic can also be redirected to a designated VLAN.
NAT Pool	Displays the NAT pool used by this Bridge NAT entry. A value is only displayed only when Overload Type has been set to *NAT Pool*.
Overload IP	Lists whether a single global address collectively supports numerous local addresses.
Overload Type	Displays the override type for this policy based forwarding rule.

10 Select **+ Add Row** to set IP address range settings for the Bridge NAT configuration.

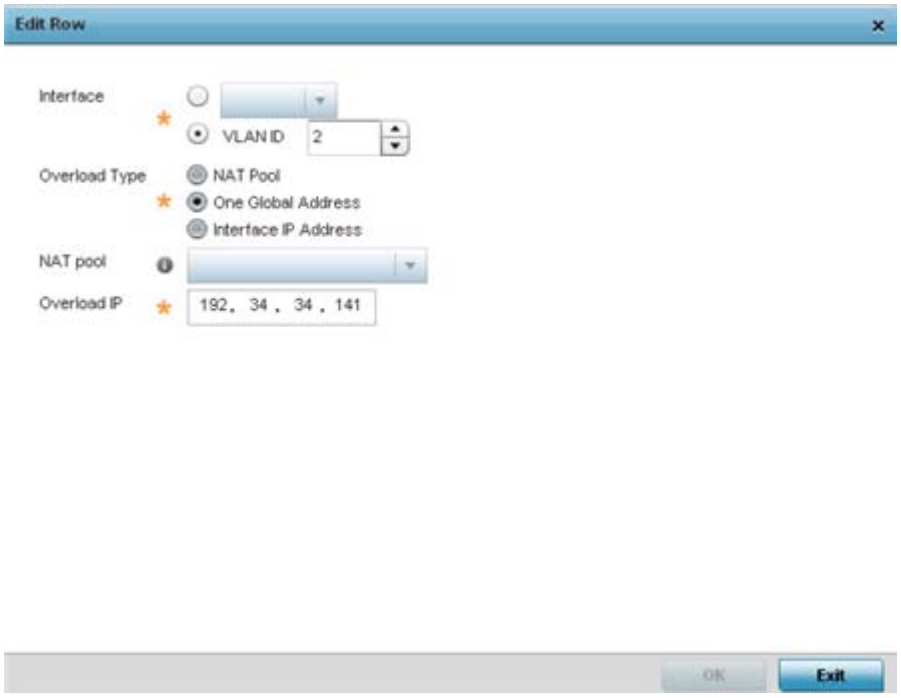


Figure 8-116 *Security Source Dynamic NAT screen*

11 Select **OK** to save the changes made within the Add Row and Source Dynamic NAT screen. Select **Reset** to revert to the last saved configuration.

8.9.8 Setting the Profile's Application Visibility (AVC) Configuration

Profile Security Configuration

Deep packet inspection (DPI) is an advanced packet analysis technique, which analyzes packet and packet content headers to determine the nature of network traffic. When DPI is enabled, packets of all flows are subjected to DPI to get accurate results. DPI identifies applications (such as, Netflix, Twitter, Facebook, etc.) and extracts metadata (such as, host name, server name, TCP-RTT, etc.) for further use by the WiNG firewall.

To configure a profile's application visibility settings and overrides:

1 Select the Configuration tab from the Web UI

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu

4 Select **Security**.

5 Select **Application Visibility.**

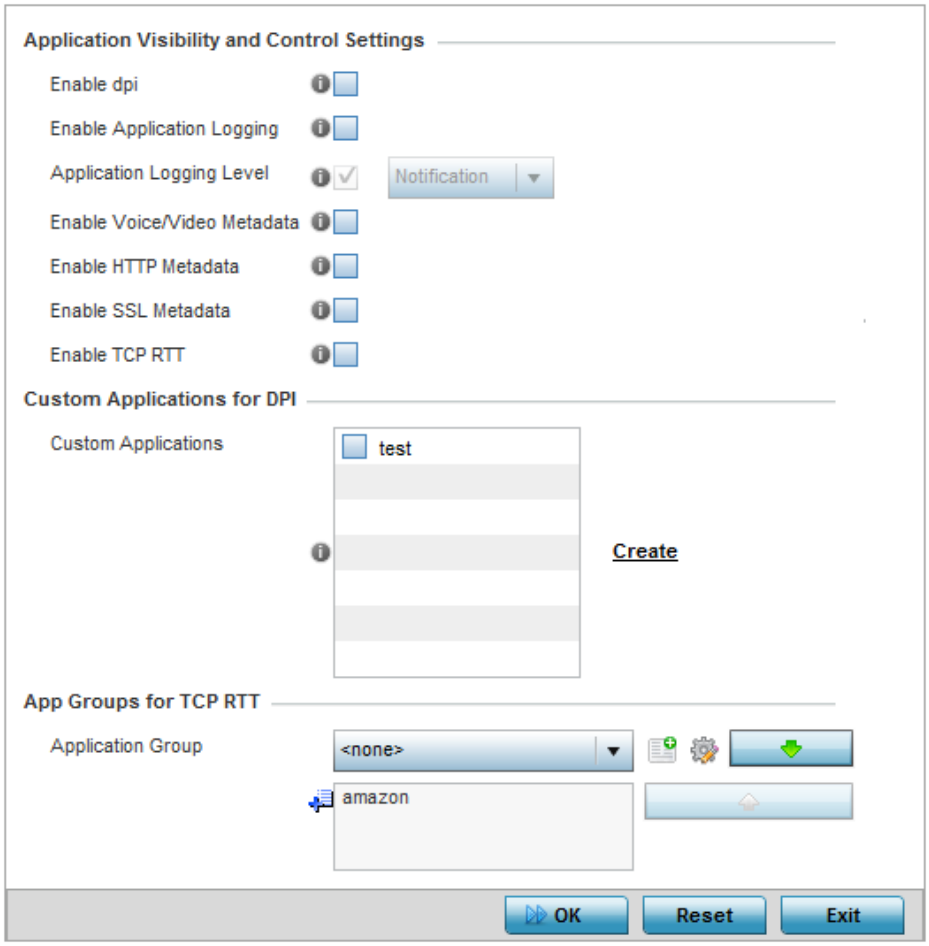


Figure 8-117 *Profile - Security - Application Visibility screen*

6 Refer the following **Application Visibility and Control Settings**:

Enable dpi	Enable this setting to provide deep-packet inspection. When enabled, network flows are inspected at a granular level to identify applications (such as, Netflix, Twitter, Facebook, etc.) and extract metadata (such as, host name, server name, TCP-RTT, etc.) for further use by the WiNG firewall.
Enable Applications Logging	Select this option to enable event logging for DPI application recognition. This setting is disabled by default.
Application Logging Level	If enabling DPI application recognition, set the logging level. Severity levels include *Emergency, Alert, Critical, Errors, Warning, Notice, Info* and *Debug*. The default logging level is Notification.
Enable Voice/Video Metadata	Select this option to enable the metadata extraction from voice and video classified flows. The default setting is disabled.
Enable HTTP Metadata	Select this option to enable the metadata extraction from HTTP flows. The default setting is disabled.

Enable SSL Metadata	Select this option to enable the metadata extraction from SSL flows. The default setting is disabled.
Enable TCP RTT	Select this option to enable extraction of RTT information from TCP flows. The default setting is disabled.

7 Review the **Custom Applications for DPI** field to select the custom applications available for this device profile. For information on creating custom applications and their categories, see *Application on page 7-58*.

If enabling TCP-RTT metadata collection, in the **App Groups for TCP RTT** field, specify the application groups for which TCP-RTT metadata collection is to be enabled. Select the *Application Groups* from the drop-down menu and use the green, down arrow to move the selection to the box below. Note, you can add maximum of 8 (eight) groups to the list. If the desired application group is not available, select the **Create** icon to define a new application group configuration or select the **Edit** icon to modify an existing application group. For information on creating custom application groups, see *Application Group on page 7-60*.

8 Select **OK** to save the changes or overrides. Select **Reset** to revert to the last saved configuration.

8.9.9 Profile Security Configuration and Deployment Considerations

Profile Security Configuration

Before defining a profile's security configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- Make sure the contents of the certificate revocation list are periodically audited to ensure revoked certificates remain quarantined or validated certificates are reinstated.
- A RFS4000 model wireless controller ships with a baseline configuration supporting many-to-one NAT between devices connected to GE1 - GE5 ports on VLAN 1, and the UP1 port assigned to VLAN 2100. A RFS4000 can be deployed within a small site using its default configuration, and then be connected to a Internet service providing instant access to the Internet.
- NAT alone does not provide a firewall. If deploying NAT on a controller or service platform profile, add a firewall on the profile to block undesirable traffic from being routed. For outbound Internet access, a stateful firewall can be configured to deny all traffic. If port address translation is required, a stateful firewall should be configured to only permit the TCP or UDP ports being translated.
- A RFS6000 model wireless controller ships with a minimum baseline configuration without NAT enabled. A RFS6000 wireless controller requires VLAN configuration, IP addressing and NAT rules be created before many-to-one NAT services can be defined.
- RFS4000 and RFS6000 model wireless controllers can provide outbound NAT services for hosts connected to multiple VLANs. For small deployments, VLANs should be terminated within a RFS4000 wireless controller providing site routing services. For medium-scale deployments, VLANs are typically terminated on a L3 (IP layer) or L2 (Ethernet layer).

8.10 Profile VRRP Configuration

A default gateway is a critical resource for connectivity. However, it's prone to a single point of failure. Thus, redundancy for the default gateway is required. If WAN backhaul is available, and a router failure occurs, then the Access Point should act as a router and forward traffic on to its WAN link.

Define an external *Virtual Router Redundancy Protocol* (VRRP) configuration when router redundancy is required in a network requiring high availability.

Central to the configuration of VRRP is the election of a VRRP master. A VRRP master (once elected) performs the following functions:

- *Responds to ARP requests*
- *Forwards packets with a destination link layer MAC address equal to the virtual router MAC address*
- *Rejects packets addressed to the IP address associated with the virtual router, if it is not the IP address owner*
- *Accepts packets addressed to the IP address associated with the virtual router, if it is the IP address owner or accept mode is true.*

Those nodes that lose the election process enter a backup state. In the backup state they monitor the master for any failures, and in case of a failure one of the backups, in turn, becomes the master and assumes the management of the designated virtual IPs. A backup does not respond to an ARP request, and discards packets destined for a virtual IP resource.

To define the configuration of a VRRP group:

1 Select **Configuration** > **Profiles**.

2 Select **VRRP.**

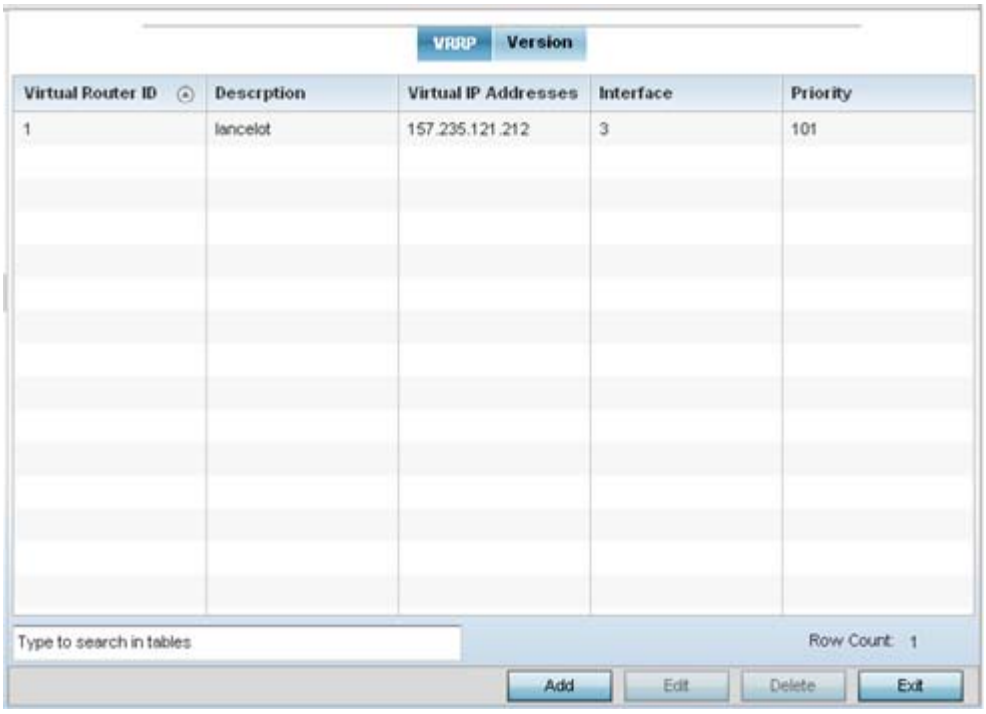


Figure 8-118 *Profile - VRRP screen*

3 Review the following VRRP configuration data to assess if a new VRRP configuration is required or if an existing VRRP configuration requires modification or removal:

Virtual Router ID	Lists a numerical index (1 - 254) used to differentiate VRRP configurations. The index is assigned when a VRRP configuration is initially defined. This ID identifies the virtual router a packet is reporting status for.
Description	Displays a description assigned to the VRRP configuration when it was either created or modified. The description is implemented to provide additional differentiation beyond the numerical virtual router ID.
Virtual IP Addresses	Lists the virtual interface IP address used as the redundant gateway address for the virtual route.

Interface	Displays the interfaces selected on the Access Point to supply VRRP redundancy failover support.
Priority	Lists a numerical value (1 - 254) used for the virtual router master election process. The higher the numerical value, the higher the priority in the election process.

4 Select the **Version** tab to define the VRRP version scheme used with the configuration.

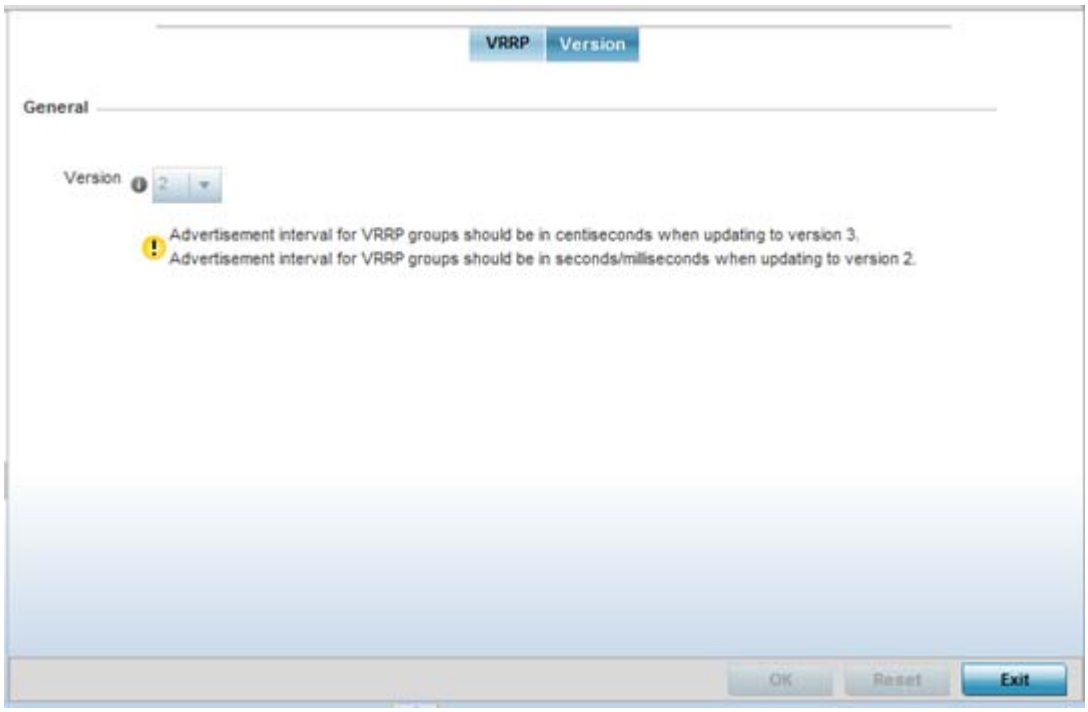


Figure 8-119 *VRRP screen - Version tab*

VRRP version 3 (RFC 5798) and 2 (RFC 3768) are options for router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP. For more information on the VRRP protocol specifications (available publicly) refer to *http://www.ietf.org/rfc/rfc3768.txt* (version 2) and *http://www.ietf.org/rfc/rfc5798.txt* (version 3).

5 From within VRRP tab, select **Add** to create a new VRRP configuration or **Edit** to modify the attributes of an existing VRRP configuration. If necessary, existing VRRP configurations can be selected and permanently removed by selecting **Delete**.

If adding or editing a VRRP configuration, the following screen displays:

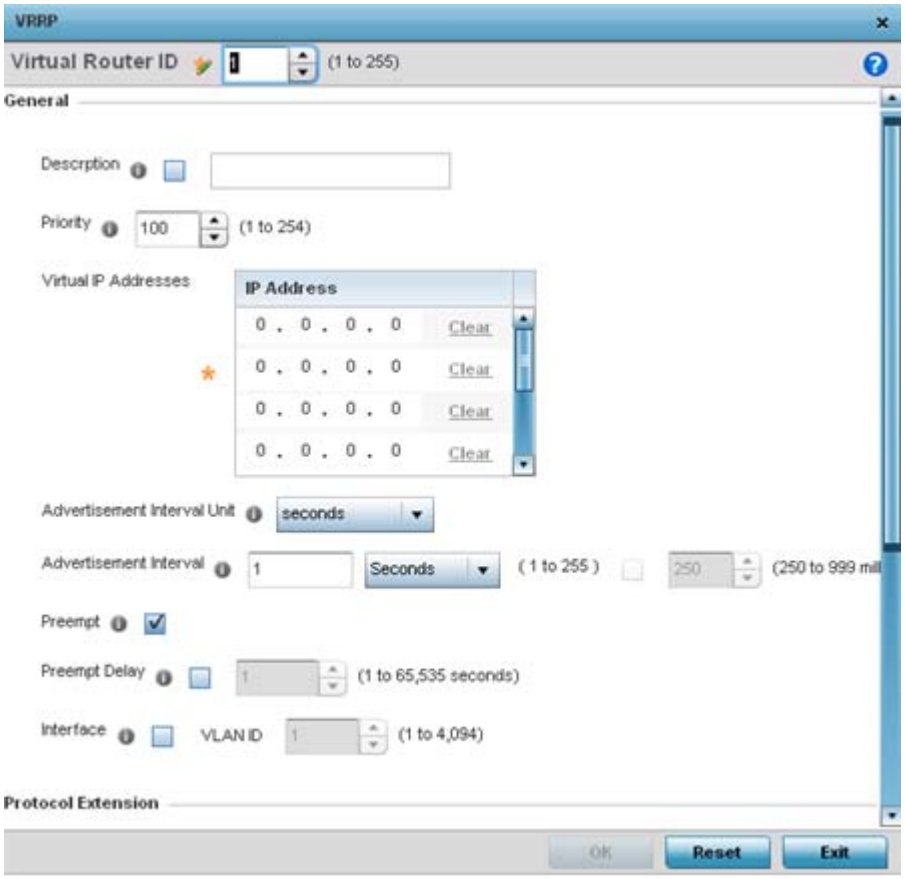


Figure 8-120 *VRRP screen*

6 If creating a new VRRP configuration, assign a **Virtual Router ID** from (1 - 255). In addition to functioning as numerical identifier, the ID identifies the Access Point's virtual router a packet is reporting status for.

7 Define the following VRRP **General** parameters:

Description	In addition to an ID assignment, a virtual router configuration can be assigned a textual description (up to 64 characters) to further distinguish it from others with a similar configuration.
Priority	Use the spinner control to set a VRRP priority setting from 1 - 254. The Access Point uses the defined setting as criteria in selection of a virtual router master. The higher the value, the greater the likelihood of this virtual router ID being selected as the master.
Virtual IP Addresses	Provide up to 8 IP addresses representing Ethernet switches, routers or security appliances defined as virtual routing resources.
Advertisement Interval Unit	Select either *seconds*, *milliseconds* or *centiseconds* as the unit used to define VRRP advertisements. Once an option is selected, the spinner control becomes enabled for that *Advertisement Interval* option. The default interval unit is seconds. If changing the VRRP group version from 2 to 3, ensure the advertisement interval is in centiseconds. Use VRRP group version 2 when the advertisement interval is either in seconds or milliseconds.

Advertisement Interval	Once a Advertisement Interval Unit has been selected, use the spinner control to set the Interval at which the VRRP master sends out advertisements on each of its configured VLANs. The default setting is 1 second.
Preempt	Select this option to ensure a high priority backup router is available to preempt a lower priority backup router resource. The default setting is enabled. When selected, the *Preempt Delay* option becomes enabled to set the actual delay interval for pre-emption. This setting determines if a node with a higher priority can takeover all the Virtual IPs from the nodes with a lower priority.
Preempt Delay	If the Preempt option is selected, use the spinner control to set the delay interval (in seconds) for pre-emption.
Interface	Select this value to enable/disable VRRP operation and define the VLAN (1 - 4,094) interface where VRRP is running. These are the interfaces monitored to detect a link failure.

8 Refer to the **Protocol Extension** field to define the following:

Sync Group	Select the option to assign a VRRP sync group to this VRRP ID's group of virtual IP addresses. This triggers VRRP failover if an advertisement is not received from the virtual masters that are part of this VRRP sync group. This setting is disabled b y default.
Network Monitoring: Local Interface	Select the *wwan1*, *pppoe1* and *VLAN ID(s)* as needed to extend VRRP monitoring to these local interfaces. Once selected, these interfaces can be assigned an *increasing* or *decreasing* level or priority for virtual routing within the VRRP group.
Network Monitoring: Critical Resource Name	Assign the priority level for the selected local interfaces. Backup virtual routers can *increase* or *decrease* their priority in case the critical resources connected to the master router fail, and transition to the master state. Additionally, the master virtual router can lower its priority if the critical resources connected to it fails, so the backup can transition to the master state. This value can only be set on the backup or master router resource, not both. Options include *None*, *increment-priority* and *decrement priority*.
Network Monitoring: Delta Priority	Use this setting to decrement the configured priority (by the set value) when the monitored interface is down. When critical resource monitoring, the configured value is incremented by the value defined.

9 Select **OK** to save the changes made to the VRRP configuration. Select **Reset** to revert to the last saved configuration.

8.11 Profile Critical Resources Configuration

Critical resources are device IP addresses or interface destinations on the network defined as critical to the health of the network. The critical resource feature allows for the continuous monitoring of these addresses. A critical resource, if not available, can result in the network suffering performance degradation. A critical resource can be a gateway, AAA server, WAN interface or any hardware or service on which the stability of the network depends. Critical resources are pinged regularly. If there's a connectivity issue, an event is generated stating a critical resource is unavailable. By default, there's no enabled critical resource policy and one needs to be created and implemented.

Critical resources can be monitored directly through the interfaces on which they're discovered. For example, a critical resource on the same subnet as an Access Point can be monitored by its IP address. However, a critical resource located on a VLAN must continue to monitored on that VLAN.

Critical resources can be configured for Access Points and wireless controllers using their respective profiles.

To define critical resources:

1 Select **Configuration** > **Profiles**.

2 Select **Critical Resources.**

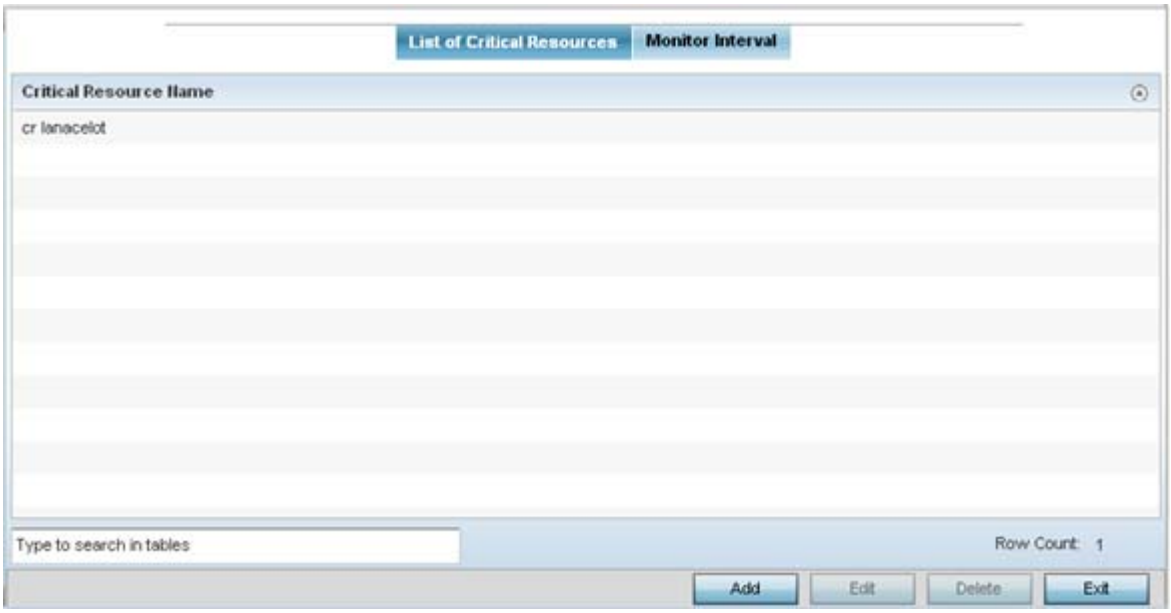


Figure 8-121 *Critical Resources screen - List of Critical Resources tab*

The screen lists the destination IP addresses or interfaces (VLAN, WWAN, or PPPoE) used for critical resource connection. IP addresses can be monitored directly by the controller or service platform, whereas a VLAN, WWAN or PPPoE must be monitored behind an interface.

3 Click the **Add** button at the bottom of the screen to add a new critical resource and connection method, or select and existing resource and select **Edit** to update the resource's configuration.

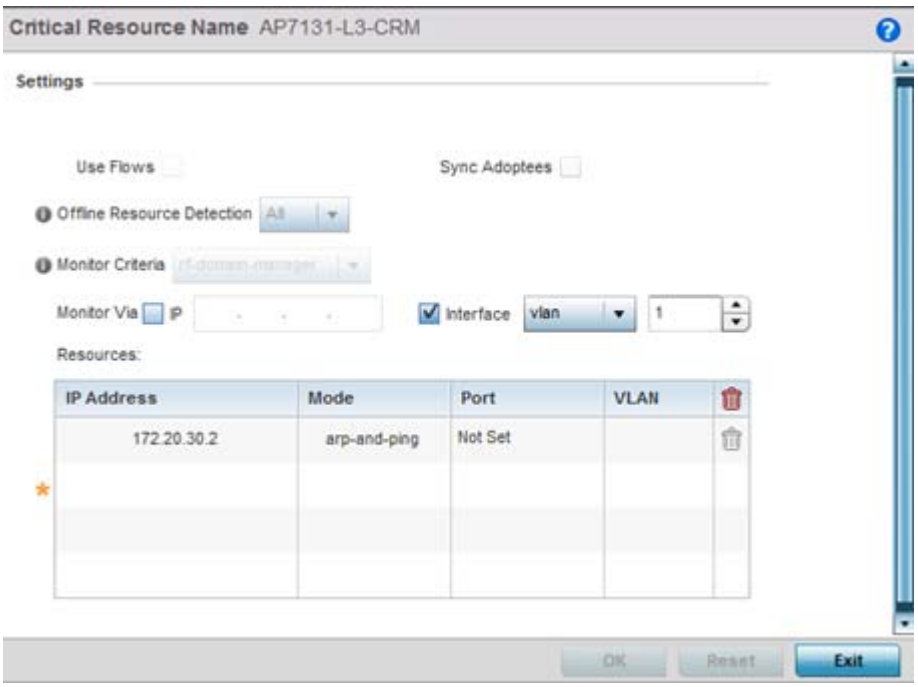


Figure 8-122 *Critical Resources screen - Adding a Critical Resource*

4 Select **Use Flows** to configure the critical resource to monitor using firewall flows for DHCP or DNS instead of ICMP or ARP packets to reduce the amount of traffic on the network. Select **Sync Adoptees** to sync adopted devices to state changes with a resource-state change message. These settings are disabled by default.

5 Use the **Offline Resource Detection** drop-down menu to define how critical resource event messages are generated. Options include *Any* and *All*. If selecting **Any**, an event is generated when the state of any single critical resource changes. If selecting **All**, an event is generated when the state of all monitored critical resources change.

6 Use the **Monitor Criteria** drop-down menu to select either *rf-domain-manager*, *cluster-master* or *All* as the resource for monitoring critical resources by one device and updating the rest of the devices in a group.

If selecting **rf-domain-manager**, the current rf-domain manager performs resource monitoring, and the rest of the devices do not. The RF-domain-manager updates any state changes to the rest of the devices in the RF Domain. With the **cluster-master** option, the cluster master performs resource monitoring and updates the cluster members with state changes. With a controller managed RF Domain, Monitoring Criteria should be set tor **All**, since the controller might not know the VLAN bridged locally by the devices in the RF Domain monitoring DHCP.

7 Select the **IP** option (within the **Monitor Via** field at the top of the screen) to monitor a critical resource directly (within the same subnet) using the provided IP address as a network identifier.

8 Select the **Interface** checkbox (within the **Monitor Via** field at the top of the screen) to monitor a critical resource using either the critical resource's VLAN, WWAN1 or PPPoE1 interface. If VLAN is selected, a spinner control is enabled to define the destination VLAN ID used as the interface for the critical resource.

9 Select **+ Add Row** to define the following for critical resource configurations:

IP Address	Provide the IP address of the critical resource. This is the address used to ensure the critical resource is available. Up to four addresses can be defined.

Mode	Set the ping mode used when the availability of a critical resource is validated. Select from: *arp-only* – Use the *Address Resolution Protocol* (ARP) for only pinging the critical resource. ARP is used to resolve hardware addresses when only the network layer address is known. *arp-and-ping* – Use both ARP and *Internet Control Message Protocol* (ICMP) for pining the critical resource and sending control messages (device not reachable, requested service not available, etc.).
Port	Use the drop-down menu to provide the physical port for each critical resource. The ports available depend on the device in use.
VLAN	Define the VLAN on which the critical resource is available using the spinner control.

10 Select the **Monitor Interval** tab.

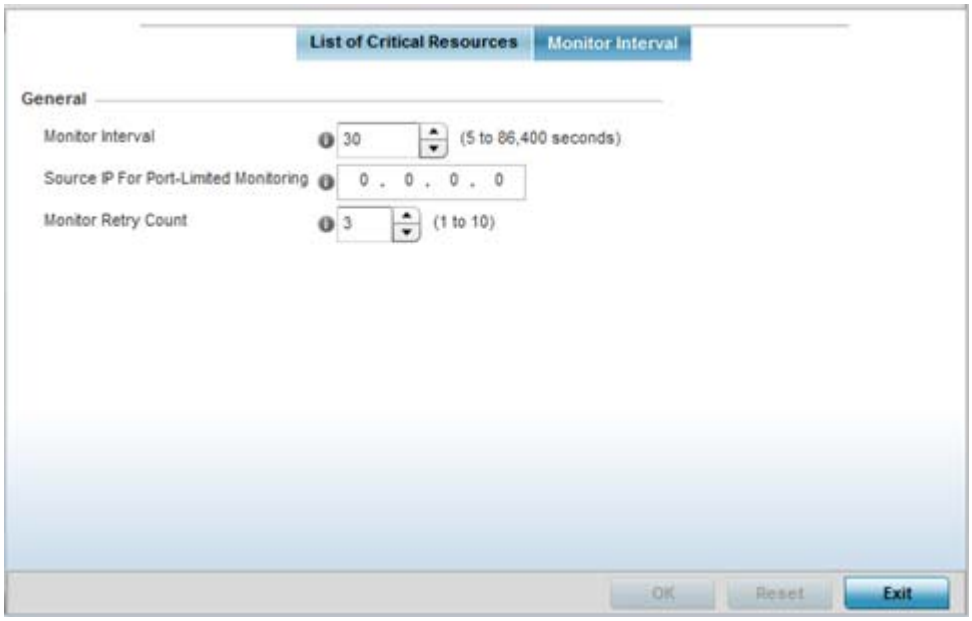


Figure 8-123 *Critical Resources screen - Monitor Interval tab*

11 Set **Monitor Interval** as the duration between two successive pings to the critical resource. Define this value in seconds from 5 - 86,400. The default setting is 30 seconds.

12 Set the **Source IP for Port-Limited Monitoring** to define the IP address used as the source address in ARP packets used to detect a critical resource on a layer 2 interface. Generally, the source address 0.0.0.0 is used in the APR packets used to detect critical resources. However, some devices do not support the above IP address and drop the ARP packets. Use this field to provide an IP address specifically used for this purpose. The IP address used for Port-Limited Monitoring must be different from the IP address configured on the device.

13 Set the **Monitoring Retries before Marking Resource as DOWN** for the number of retry connection attempts (1 - 10) permitted before this device connection is defined as down (offline). The default setting is three connection attempts.

14 Select **OK** to save the changes to the monitor interval. Select **Reset** to revert to the last saved configuration.

8.12 Profile Services Configuration

A profile can contain specific captive portal, DHCP server and RADIUS server configurations supported by the controller or service platform's own internal resources. These captive portal, IP assignment and user authorization resources can be defined uniquely as profile requirements dictate.

To define a profile's services configuration:

1 Select the **Configuration t**ab from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu.

4 Select **Services.**

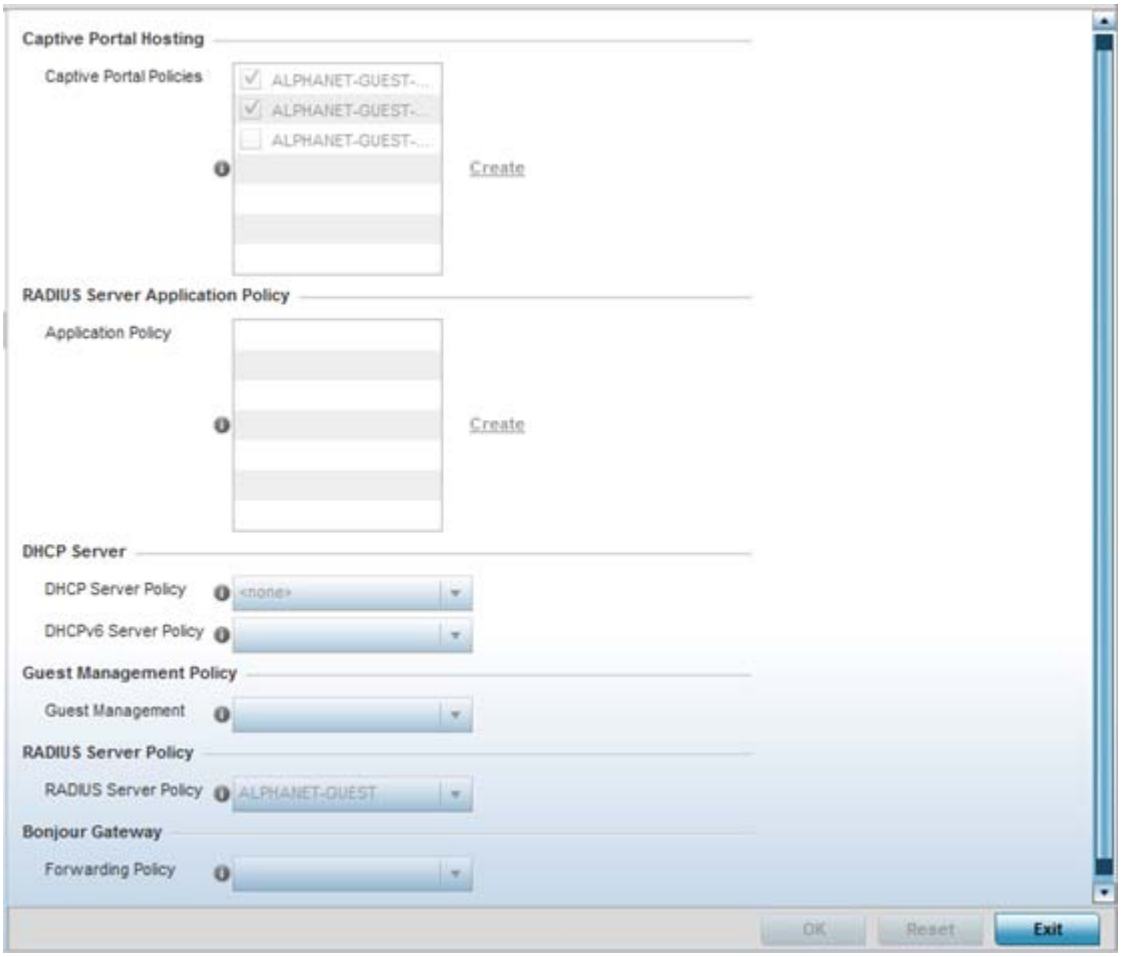


Figure 8-124 *Profile Services screen*

5 Refer to the **Captive Portal Hosting** section to select or set a guest access configuration (captive portal) for use with this profile.

A *captive portal* is guest access policy for providing guests temporary and restrictive access to the network.

A captive portal provides secure authenticated access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Once logged into the captive

portal, additional *Agreement*, *Welcome* and *Fail* pages provide the administrator with a number of options on screen flow and user appearance.

Either select an existing captive portal policy, use the default captive portal policy or select the **Create** link to create a new captive portal that can be applied to the profile. For morel information, see, *Configuring Captive Portal Policies*.

6 Select a **RADIUS Server Application Policy** policy to authenticate users and authorize access to the network. A RADIUS policy provides the centralized management of authentication data (usernames and passwords). When an client attempts to associate, the controller or service platform sends the authentication request to the RADIUS server. If no existing policies are available select the **Create** link.

7 Use the **DHCP Server Policy** drop-down menu assign this profile a DHCP or DHCPv6 server policy. If an existing DHCP or DHCPv6 policy does not meet the profile's requirements, select the **Create** button to create a new policy configuration that can be applied to this profile.

Dynamic Host Configuration Protocol (DHCP) allows hosts on an IP network to request and be assigned IP addresses as well as discover information about the network where they reside. Each subnet can be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool. When the onboard DHCP server allocates an address for a DHCP client, the client is assigned a lease, which expires after an pre-determined interval. Before a lease expires, wireless clients (to which leases are assigned) are expected to renew them to continue to use the addresses. Once the lease expires, the client is no longer permitted to use the leased IP address. The profile's DHCP server policy ensures all IP addresses are unique, and no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired).

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. DHCP in IPv6 works in with IPv6 router discovery. With the proper RA flags, DHCPv6 works like DHCP for IPv4. The central difference is the way a device identifies itself if assigning addresses manually instead of selecting addresses dynamically from a pool.

8 Use the **Guest Management Policy** drop-down menu to select an existing Guest Management policy to use as a mechanism to manage guest users with this profile.

9 Use the **RADIUS Server Policy** drop-down menu to select an existing RADIUS server policy to use as a user validation security mechanism with this profile.

A profile can have its own unique RADIUS server policy to authenticate users and authorize access to the network. A profile's RADIUS policy provides the centralized management of controller or service platform authentication data (usernames and passwords). When an client attempts to associate, an authentication request is sent to the RADIUS server.

For more information, see *Setting the RADIUS Configuration*.

10 From the **Forwarding Policy** drop-down, select the **Bonjour Gateway** forwarding policy. Select the **Create** icon to define a new Bonjour Gateway forwarding policy configuration or select the **Edit** icon to modify an existing Bonjour Gateway forwarding policy configuration.

Bonjour is Apple's implementation of *zero-configuration networking* (Zeroconf). Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates devices such as printers, other computers and services that these computers offer over a local network.

Bonjour provides a general method to discover services on a *local area network* (LAN). It allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with special DNS configuration, it can be extended to find services across broadcast domains.

11 Select **OK** to save the changes made to the profile's services configuration. Select **Reset** to revert to the last saved configuration.

8.12.1 Profil

Profile Services Configuration

Before defining a profile's captive portal, DHCP and RADIUS services configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- A profile plan should consider the number of wireless clients allowed on the captive portal and the services provided, or if the profile should support captive portal access at all.
- Profile configurations supporting a captive portal should include firewall policies to ensure logical separation is provided between guest and internal networks so internal networks and hosts are not reachable from captive portals.
- DHCP's lack of an authentication mechanism means a DHCP server supported profile cannot check if a client or user is authorized to use a given user class. This introduces a vulnerability when using user class options. Ensure a profile using an internal DHCP resource is also provisioned with a strong user authorization and validation configuration.

8.13 Profile Management Configuration

Controllers and service platforms have mechanisms to allow/deny management access to the network for separate interfaces and protocols (*HTTP*, *HTTPS*, *Telnet*, *SSH* or *SNMP*). These management access configurations can be applied strategically to profiles as resource permissions dictate.

Additionally, an administrator can define a profile with unique configuration file and device firmware upgrade support. In a clustered environment, these operations can be performed on one controller or service platform, then propagated to each member of the cluster and onwards to the devices managed by each cluster member.

To define a profile's management configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu.

4 Select **Management.**

5 Expand the Management menu item to display its sub menu options.

6 Select **Settings** from the Management menu.

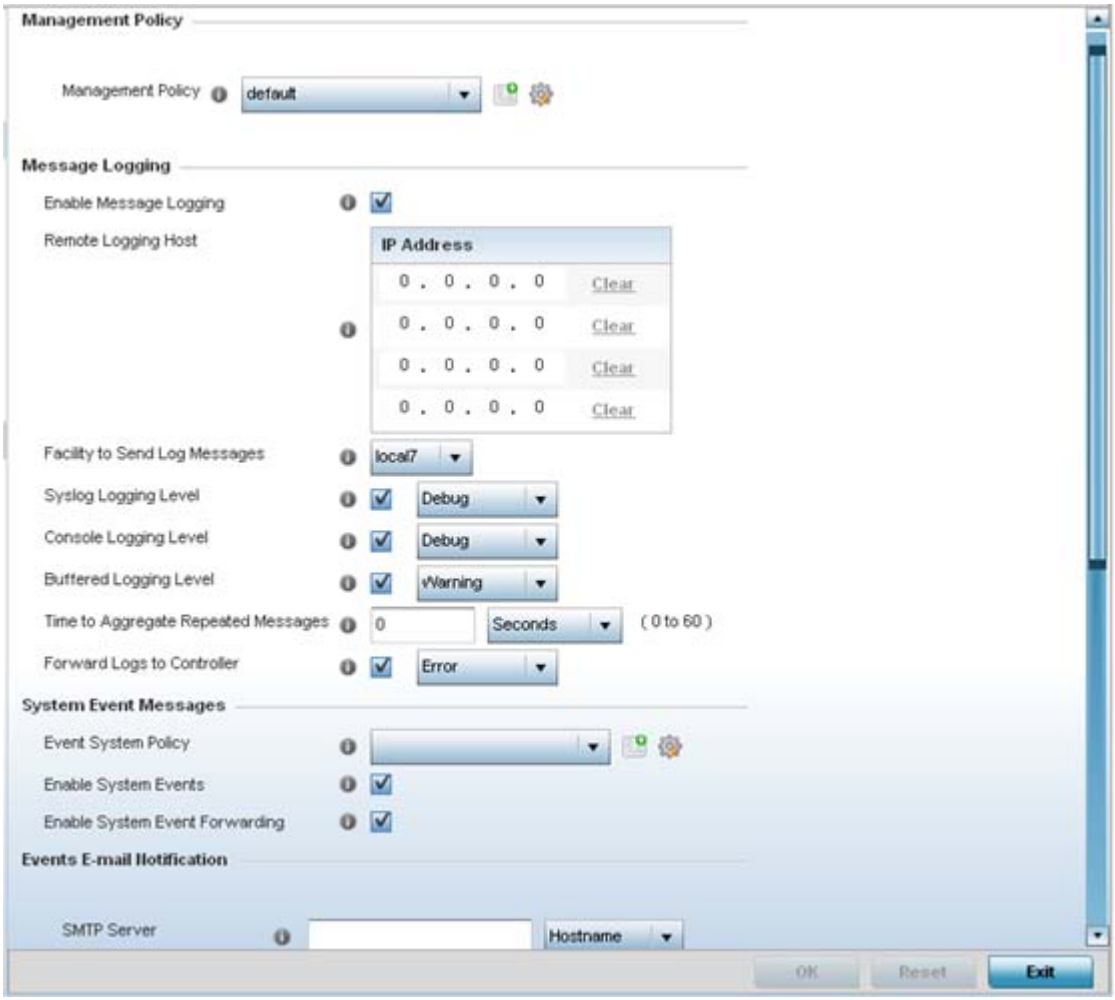


Figure 8-125 *Profile Management Settings screen*

7 Refer to the **Management Policy** field to select or set a management configuration for use with this profile. A default management policy is also available if no existing policies are usable.

Use the drop-down menu to select an existing management policy to apply to this profile. If no management policies exist meeting the data access requirements of this profile, select the **Create** icon to access a series of screens used to define administration, access control and SNMP configurations. Select an existing policy and select the **Edit** icon to modify the configuration of an existing management policy. For more information, see *Viewing Management Access Policies*.

8 Refer to the **Message Logging** field to define how the profile logs system events. It's important to log individual events to discern an overall pattern that may be negatively impacting performance using the configuration defined for this profile.

Enable Message Logging	Select this option to enable the profile to log system events to a user defined log file or a syslog server. Selecting this check box enables the rest of the parameters required to define the profile's logging configuration. This option is disabled by default.
Remote Logging Host	Use this table to define numerical (non DNS) IP addresses for up to three external resources where logged system events can be sent on behalf of the profile. Select *Clear* as needed to remove an IP address.

Facility to Send Log Messages	Use the drop-down menu to specify the local server facility (if used) for the profile's syslog event log transfer.
Syslog Logging Level	Event severity coincides with the syslog logging level defined for the profile. Assign an identifier to log events based on criticality. Severity levels include 0 - *Emergency,* 1 - *Alert*, 2 - *Critical*, 3 - *Errors*, 4 - *Warning*, 5 - *Notice*, 6 - *Info* and 7 - *Debug*. The default logging level is 4.
Console Logging Level	Event severity coincides with the syslog logging level defined for the profile. Assign an identifier to log events based on criticality. Severity levels include 0 - *Emergency,* 1 - *Alert*, 2 - *Critical*, 3 - *Errors*, 4 - *Warning*, 5 - *Notice*, 6 - *Info* and 7 - *Debug*. The default logging level is 4.
Buffered Logging Level	Event severity coincides with the syslog logging level defined for the profile. Assign an identifier to log events based on criticality. Severity levels include 0 - *Emergency,* 1 - *Alert*, 2 - *Critical*, 3 - *Errors*, 4 - *Warning*, 5 - *Notice*, 6 - *Info* and 7 - *Debug*. The default logging level is 4.
Time to Aggregate Repeated Messages	Define the increment (or interval) system events are logged on behalf of this profile. The shorter the interval, the sooner the event is logged. Either define an interval in *Seconds* (0 - 60) or *Minutes* (0 -1). The default value is 0 seconds.
Forward Logs to Controller	Select the checkbox to define a log level for forwarding event logs. Log levels include *Emergency, Alert*, *Critical*, *Error*, *Warning*, *Notice*, *Info* and *Debug*. The default logging level is Error.

9 Refer to the **System Event Messages** section to define how system messages are logged and forwarded on behalf of the profile.

Event System Policy	Select an Event System Policy from the drop-down menu. If an appropriate policy does not exist click the *Create* button to make a new policy.
Enable System Events	Select this option to allow the profile to capture system events and append them to a log file. It's important to log individual events to discern an overall pattern that may be negatively impacting system performance. This setting is enabled by default.
Enable System Event Forwarding	Select the *Enable System Event Forwarding* box to enable the forwarding of system events to another cluster member. This setting is enabled by default.

10 Refer to the **Events E-mail Notification** section to define how system event notification emails are sent.

SMTP Server	Specify either the *Hostname* or *IP Address* of the outgoing SMTP server where notification emails will be originated. A Hostname cannot exceed 64 characters.
Port of SMTP	If a non-standard SMTP port is used on the outgoing SMTP server check this box and specify a port between 1 and 65,535 for the outgoing SMTP server to use.
Sender Email Address	Specify the 64 character maximum email address from which notification emails are originated. This is the *from* address on notification emails.
Recipient's E-mail Address	Specify up to 6 Email addresses to be the recipient's of event Email notifications.

Username for SMTP Server	Specify the username of the sender on the outgoing SMTP server. Many SMTP servers require users to authenticate with a *username* and *password* before sending email through the server.
Password for SMTP Server	Specify the password associated with the username of the sender on the outgoing SMTP server. Many SMTP servers require users to authenticate with a *username* and *password* before sending email through the server.

11 Refer to the **Persist Configurations Across Reloads** field to define or override how configuration settings are handled after reloads.

Persist Configurations Across Reloads	Use the drop-down menu to configure whether configuration overrides should persist when the device configuration is reloaded. Available options are *Enabled*, *Disabled* and *Secure*.

12 Refer to the **HTTP Analytics** field to define analytic compression settings and update intervals.

Compress	Select this option to use compression to when sending updates to the controller. This option is disabled by default.
Update Interval	Define an interval in either *Seconds* (1 - 3,600), *Minutes* (1 - 60) or *Hours* (1) for interval to push buffered packets. The default setting in 1 minute.

13 Refer to the **External Analytics Engine** section to define or override analytics engine login information for an external host.

The Guest Access & Analytics software module is a site-wide Enterprise License available only on the NX9000 service platforms. When a customer visits a store, they connect to the Wireless LAN via guest access using a mobile device. The user needs to authenticate only on their first visit, and will automatically connect to the network for subsequent visits. The Analytics module helps gather data about customer behavior such as web sites visited, search terms used, mobile device types, number of new users vs. repeat users. This data provides a better understanding of pricing strategies and promotions being run by competitors. The data can be exported for additional in-depth analysis.

Controller	Select this option to provide service platform analytics to a local device. This setting is enabled by default.
URL	When using an external analytics engine with a NX9000 series service platform, enter the IP address or *uniform resource locator* (URL) for the system providing external analytics functions.
User Name	Enter the user name needed to access the external analytics engine.
Password	Enter the password associated with the username on the external analytics engine.
Update Interval	Set the interval in either *Seconds* (1 - 3,600), *Minutes* (1 - 60) or *Hours* (1) to forward buffered information to an external server resource, even when the buffers are not full. The default setting in 1 minute.

14 Select **OK** to save the changes made to the profile's management settings. Select **Reset** to revert to the last saved configuration.

15 Select **Firmware** from the Management menu.

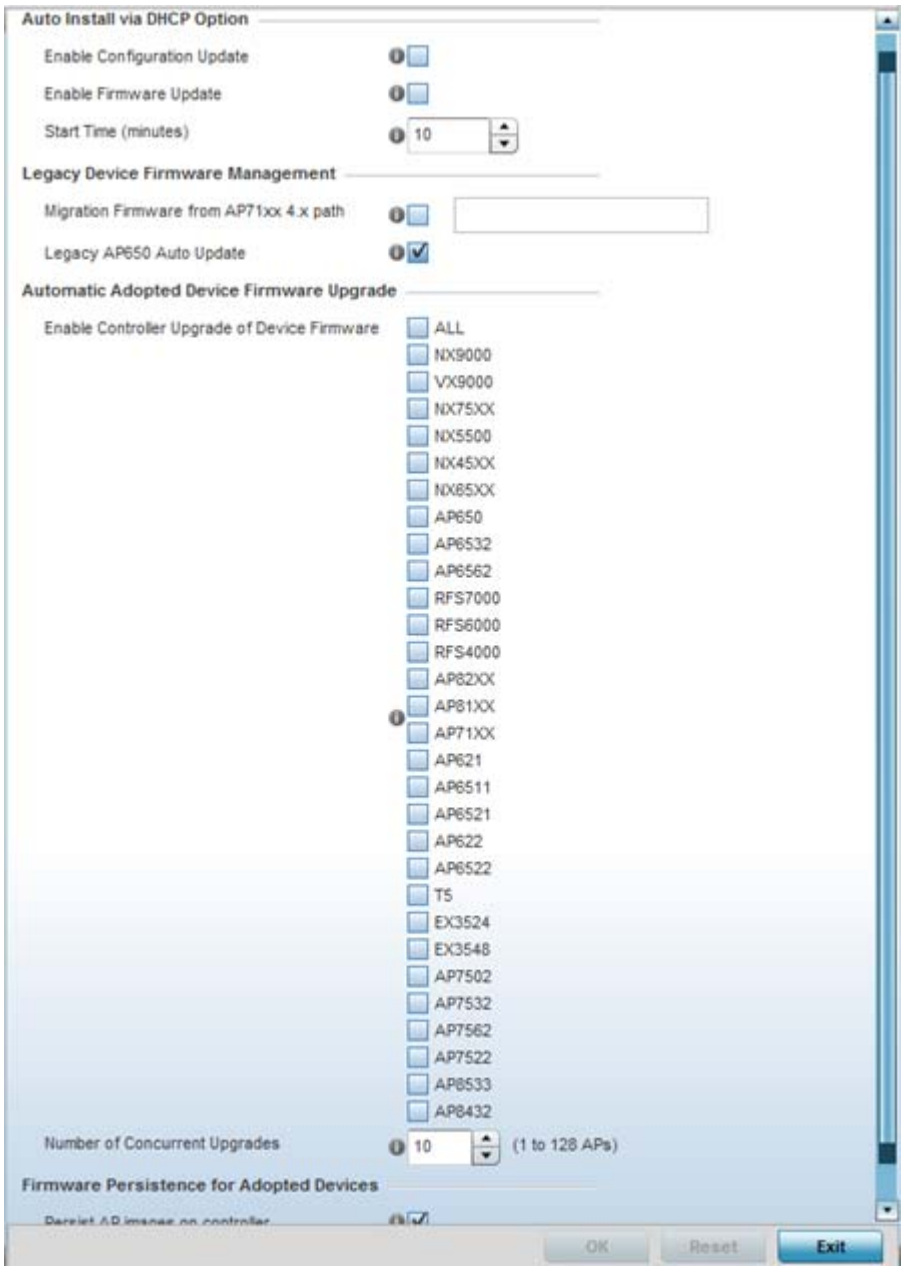


Figure 8-126 *Profile Management Firmware screen*

16 Refer to the **Auto Install via DHCP Option** section to configure automatic configuration file and firmware updates.

Enable Configuration Update	Select the *Enable Configuration Update* radio button (from within the Automatic Configuration Update field) to enable automatic configuration file updates for the profile from an external location. If enabled (the setting is disabled by default), provide a complete path to the target configuration file used in the update.
Enable Firmware Upgrade	Select this option to enable automatic firmware upgrades (for this profile) from a user defined remote location. This value is disabled by default.

Start Time (minutes)	Use the spinner control to set the number of minutes to delay the start of an auto upgrade operation. Stagger the start of an upgrade operation as needed in respect to allowing an Access Point to complete its current client support activity before being rendered offline during the update operation. The default setting is 10 minutes.

17 Refer to the parameters within the **Legacy Device Firmware Management** field to set legacy Access Point firmware provisions:

Migration Firmware from AP71xx 4.x path	Provide a path to a firmware image used to provision AP71xx model Access Points currently utilizing a 4.x version legacy firmware file. Once a valid path is provided, the update is enabled to the version maintained locally for AP71xx models.
Legacy AP650 Auto Update	Select this option to provision AP650 model Access Points from their legacy firmware versions to the version maintained locally for that model. This setting is enabled by default, making updates to AP650 models automatic if a newer AP650 image is maintained locally.

18 Use the parameters within the **Automatic Adopted Device Firmware Upgrade** section to define an automatic firmware upgrade from a local file.

Enable Controller Upgrade of Device Firmware	Select this radio button to enable adopted devices to upgrade to a newer firmware version using its associated controller or service platform's most recent resident firmware file for that specific model. This parameter is disabled by default.
Number of Concurrent Upgrades.	Use the spinner control to define the maximum number (1 - 20) of adopted Access Points that can receive a firmware upgrade at the same time. Keep in mind, during a firmware upgrade, the Access Point is offline and unable to perform its normal wireless client support function until the upgrade process is complete.

19 Select the **Persist AP images on Controller** button (from within the **Firmware Persistence for Adopted Devices** field) to enable the RF domain manager to retain and store the new image of an Access Point selected for a firmware update. The image is only stored on the RF domain manager when there's space to accommodate it.

The upgrade sequence is different depending on whether the designated RF domain manager is a controller/ service platform or Access Point.

- *When the RF domain manager is an Access Point* - The NOC uploads a provisions an Access Point model's firmware on to the Access Point RF domain manager. The NOC initiates an auto-update for Access Points using that model's firmware. If the **Persist Image on Controller** option is selected, the RF domain manager retains the image for that model. The NOC then provisions the firmware of the next Access Point type to the RF domain manager. The auto-update process is then repeated for that model. Once all the selected models have been updated, the RF domain manager's model is updated last.
- *When the RF domain manager is a controller or service platform* - The NOC adopts controllers to the NOC's cluster within its RF domain. The NOC triggers an update on active controllers or service platforms and reboots them as soon as the update is complete. As soon as the active nodes come back up, the NOC triggers an update on standby controllers or service platforms and reboots them as soon as the update is complete. When the standby controllers or service platforms come back up:
  - *If the reboot is not scheduled* - The Access Points adopted to RF domain members are not updated.It's expected the controllers and service platforms have auto-upgrade enabled which will update the Access Points when re-adopted.
  - *If the reboot is scheduled* - The NOC pushes the first Access Point model's firmware to the RF domain manager. The NOC initiates an Access Point upgrade on all Access Points on the RF domain manager for that model. If the **Persist Image on Controller** option is selected, the RF domain manager retains the image for

that model. The NOC then provisions the firmware of the next Access Point type to the RF domain manager. This process is repeated until each selected Access Point model is updated.

The Firmware Persistence feature is *enabled* for all controller and service platform RF domain managers with the flash memory capacity to store firmware images for the selected Access Point models they provision. This feature is *disabled* for Access Point RF domain managers that do not typically have the required flash memory capacity.

20 Select **Heartbeat** from the Management menu. Select the **Service Watchdog** option to implement heartbeat messages to ensure associated devices are up and running and capable of effectively interoperating. The Service Watchdog is enabled by default.

21 Select **OK** to save the changes made to the profile maintenance Heartbeat tab. Select **Reset** to revert to the last saved configuration.

8.13.1 Profile Management Configuration and Deployment Considerations

Profile Management Configuration

Before defining a profile's management configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- Define profile management access configurations providing both encryption and authentication. Management services like HTTPS, SSH and SNMPv3 should be used when possible, as they provide data privacy and authentication.
- SNMPv3 should be used for management profile configurations, as it provides both encryption and authentication and SNMPv1 and v2 do not.

8.14 Profile Mesh Point Configuration

Mesh points are Access Points dedicated to mesh network support. Mesh networking enables users to access broadband applications anywhere (including moving vehicles).

To review a profile's mesh point configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu.

4 Select **Mesh Point.**

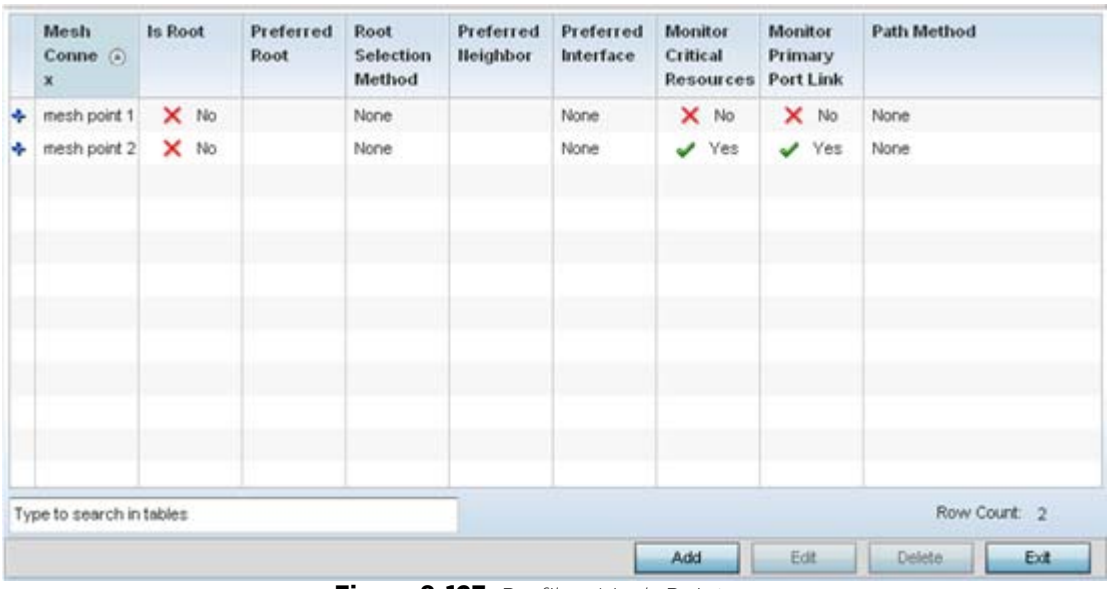


Figure 8-127 *Profile - Mesh Point screen*

5 Refer to the **Mesh Point** screen to view existing Mesh Points. If an existing Mesh Point configuration does not meet your requirements, select the **Add** button to create a new mesh point configuration or the **Edit** button to modify the parameters of an existing mesh point configuration. The Mesh Point screen displays the **Settings** tab by default.

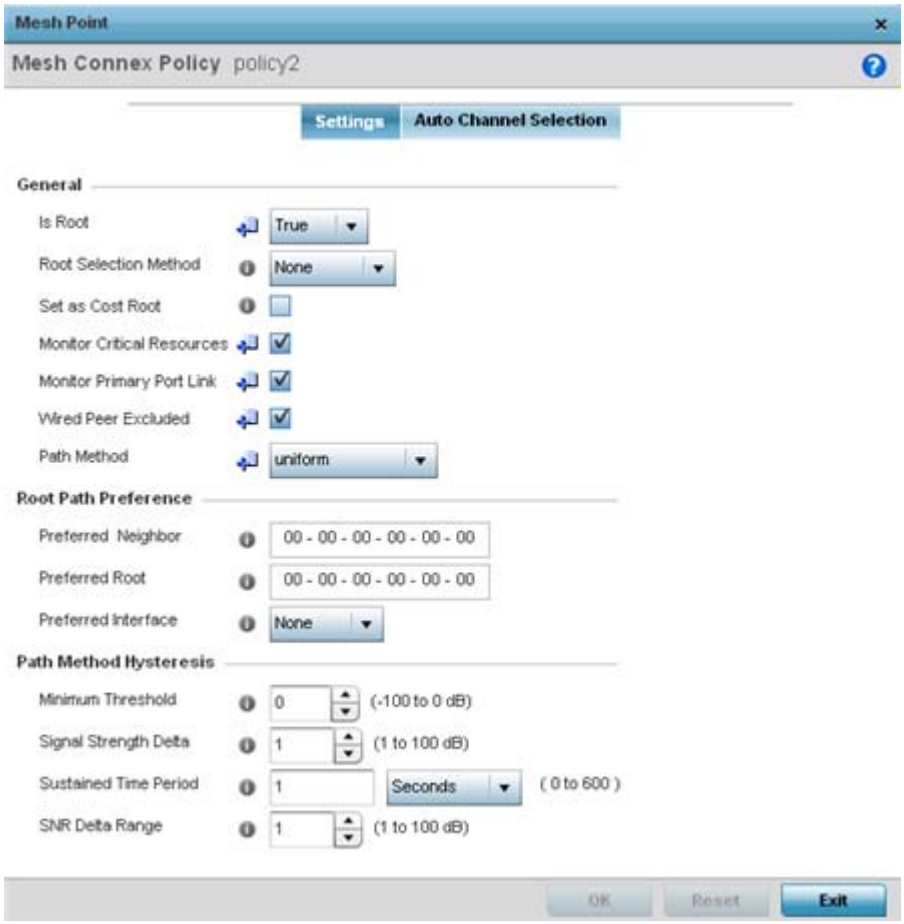


Figure 8-128 *Mesh Point - Settings Screen*

6 Define the following **Settings**:

MeshConnex Policy	If adding a new policy, specify a name for the MeshConnex Policy. The name cannot be edited later with other configuration parameters. Until a viable name is provided, the Settings tab cannot be enabled for configuration.
Is Root	Select the root behavior of this mesh point. Select *True* to indicate this mesh point is a root node for this mesh network. Select *False* to indicate this mesh point is not a root node for this mesh network.
Root Selection Method	Use the drop-down menu to determine whether this meshpoint is the root or non-root meshpoint. Select either *None, auto-mint* or *auto-proximity*. The default setting is None. When auto-mint is selected, root selection is based on the total cost to the root. Cost to the root is measured as total cost through hops to the root node. Root selection occurs for the root with the least path cost. When auto-proximity is selected, root selection is based on signal strength of candidate roots. None indicates no preference in root selection.
Set as Cost Root	Select this option to set the mesh point as the cost root for meshpoint root selection. This setting is disabled by default.
Monitor Critical Resources	Enable this feature to allow dynamic conversion of a mesh point from root to non-root when there is a critical resource failure. This option is disabled by default.

Monitor Primary Port Link	Enable this feature to allow dynamic conversion of a mesh point from root to non-root during a link down event. This option is disabled by default.
Wired Peer Excluded	Select this option to exclude a mesh from forming a link with another mesh device that's a wired peer. This option is disabled by default.
Path Method	Use the drop-down menu to select the method (criteria) used for selecting the root path. The following options are available: *None* – Select this to indicate no criteria used in root path selection. *uniform* – Select this to indicate that the path selection method is uniform. When selected, two paths will be considered equivalent if the average value is the same for these paths. *mobile-snr-leaf* – Select this option if the Access Point is mounted on a vehicle or a mobile platform (AP7161 models only). When selected, the path to the route will be selected based on the *Signal To Noise Ratio* (SNR) to the neighbor device. *snr-leaf* – Select this to indicate the path with the best signal to noise ratio is always selected. *bound-pair* – Select this option to bind one mesh point connection at a time. Once established, other mesh point connection requests are denied.

NOTE: An AP7161 model Access Point can be deployed as a *vehicular mounted modem* (VMM) to provide wireless network access to a mobile vehicle (car, train etc.). A VMM provides layer 2 mobility for connected devices. VMM does not provide layer 3 services, such as IP mobility. For VMM deployment considerations, see *Vehicle Mounted Modem (VMM) Deployment Considerations on page 8-221*.

NOTE: When using 4.9GHz, the root preferences selection for the radio's preferred interface still displays as 5GHz.

7 Set the following **Root Path Preference**:

Preferred Neighbor	Specify the MAC address of a preferred mesh point neighbor.
Preferred Root	Specify the MAC address of a a preferred root device.
Preferred Interface	Use the drop-down menu to set the preferred mesh point interface to *2.4GHz*, *4.9 GHz* or *5.0GHz*. Selecting *None* makes all mesh point interfaces of equal priority for root path preference.

8 Set the following **Path Method Hysteresis**:

Minimum Threshold	Enter the minimum value for SNR above which a candidate for the next hop in a dynamic mesh network is considered for selection. This field along with *Signal Strength Delta* and *Sustained Time Period* are used to dynamically select the next hop in a dynamic mesh network. The default setting is 0 dB.
Signal Strength Delta	Enter a delta value in dB. A candidate for selection as a next hop in a dynamic mesh network must have a SNR value higher than the set value. This field, along with the *Minimum Threshold* and *Sustained Time Period,* are used to dynamically select the next hop in a dynamic mesh network. The default setting is 1 dB.

Sustained Time Period	Enter the duration (in seconds or minutes) for the duration a signal must sustain the constraints specified in the *Minimum Threshold* and *Signal Strength Delta* path hysteresis value. These values are used to dynamically select the next hop in a dynamic mesh network. The default setting is 1 second.
SNR Delta Range	Select the root selection method hysteresis (from 1 - 100dB) SNR delta range a candidate must sustain. The default setting is 1 dB.

9 Select the **Auto Channel Selection** tab.

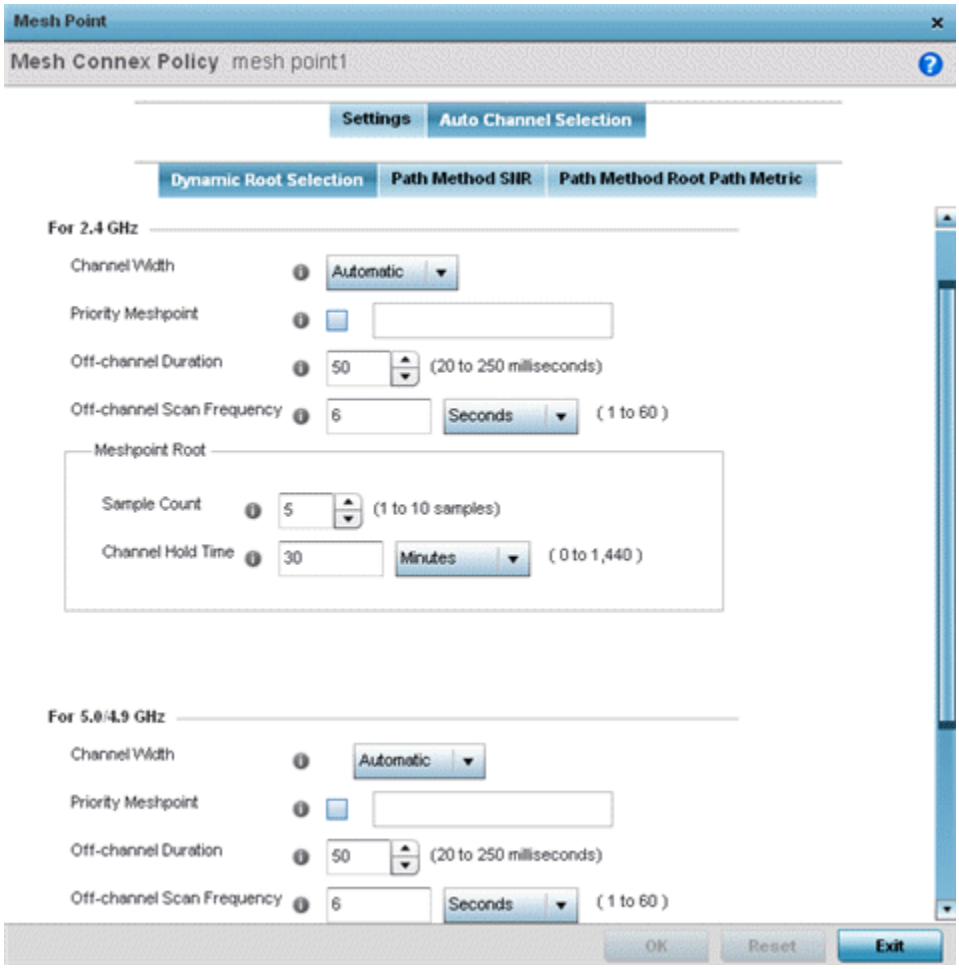


Figure 8-129 *Mesh Point Auto Channel Selection - Dynamic Root Selection screen*

The **Dynamic Root Selection** screen displays by default. The Dynamic Root Selection screen provides configuration options for the 2.4 GHz and 5.0/4.9 GHz frequencies.

10 Set the following values (common to both 2.4 GHZ and 5.0/4.9 GHz):

Channel Width	Set the channel width the meshpoint's automatic channel scan assigns to the selected radio. Available options include: *Automatic* – Defines the channel width is calculated automatically. This is the default value. *20 MHz* – Sets the width between two adjacent channels as 20 MHz. *40 MHz* – Sets the width between two adjacent channels as 40 MHz. *80 MHz* – Sets the width between two adjacent channels as 80 MHz for 802.11ac Access Points.
Priority Meshpoint	Configure the meshpoint monitored for automatic channel scans. This is the meshpoint assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a meshpoint is automatically selected. This setting is disabled by default.
Off-channel Duration	Set the duration (from 20 - 250 milliseconds) the scan dwells on each channel when performing an off channel scan. The default is 50 milliseconds.
Off-channel Scan Frequency	Set the duration (from 1- 60 seconds) between two consecutive off channel scans. The default is 6 seconds.
Meshpoint Root - Sample Count	Configure the number of scan samples (from 1- 10) performed for data collection before a mesh channel is selected. The default is 5.
Meshpoint Root - Channel Hold Time	Configure the duration (from 0 - 1440 minutes) to remain on a channel before channel conditions are reassessed for a possible channel change. Set this value to zero (0) to prevent an automatic channel selection from occurring. The default setting is 30 minutes.

11 Select the **Path Method SNR** tab to configure *signal to noise* (SNR) ratio values when selecting the path to the meshpoint root.

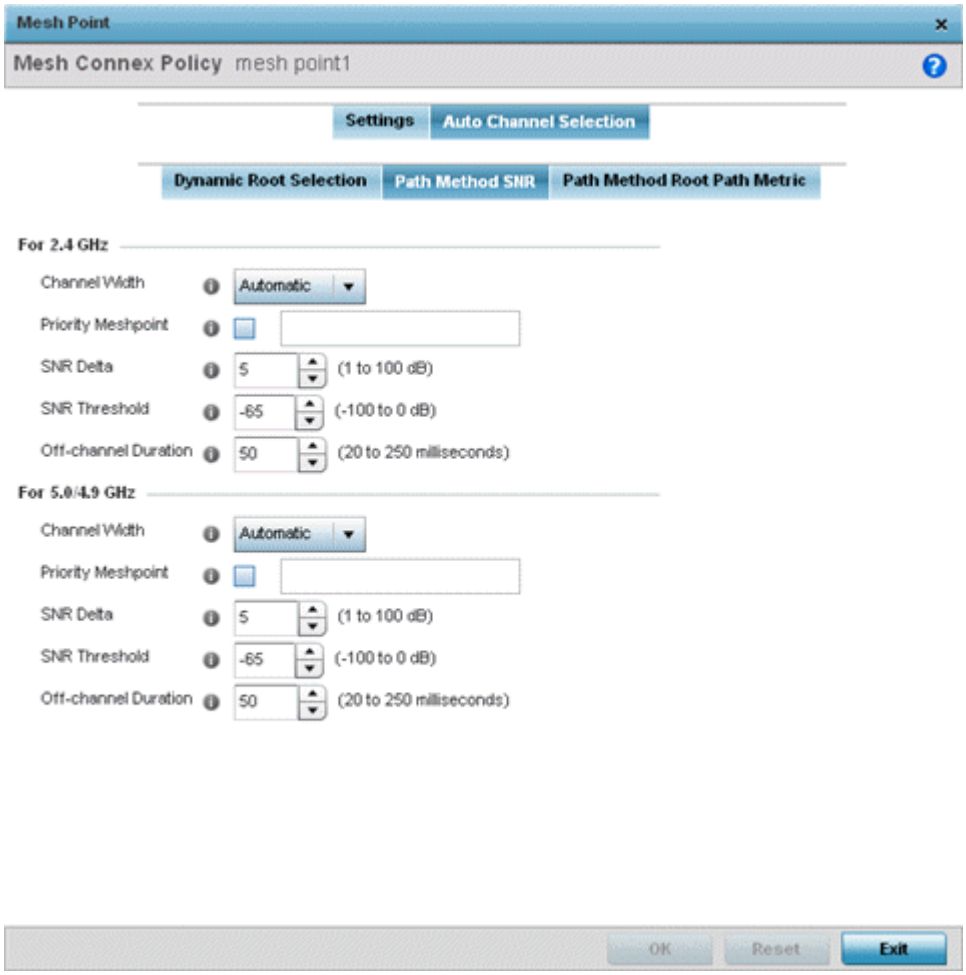


Figure 8-130 *Mesh Point Auto Channel Selection - Path Method SNR screen*

12 Set the following 2.4 GHz and 5.0/4.9 GHz path method SNR data:

Channel Width	Set the channel width the meshpoint automatic channel scan assigns to the selected radio. Available options include: *Automatic* – Defines the channel width calculation automatically. This is the default value. *20 MHz* – Sets the width between two adjacent channels as 20 MHz. *40 MHz* – Sets the width between two adjacent channels as 40 MHz. *80 MHz* – Sets the width between two adjacent channels as 80 MHz for 802.11ac Access Points.
Priority Meshpoint	Set the meshpoint monitored for automatic channel scans. This is the meshpoint assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a meshpoint is automatically selected. This setting is disabled by default.

SNR Delta	Set the *signal to noise* (SNR) ratio delta (from 1 - 100 dB) for mesh path selections. When path selection occurs, the defined value is utilized for selecting the optimal path. A better candidate, on a different channel, must have a signal strength that exceeds this delta value when compared to the signal strength of the next hop in the mesh network. The default setting is 5 dB.
SNR Threshold	Set the SNR threshold for mesh path selections (from -100 to 0 dB). If the signal strength of the next mesh hop falls below this set value, a scan is triggered to select a better next hop. the default setting is -65 dB.
Off-channel Duration	Configure the duration (from 20 - 250 milliseconds) for scan dwells on each channel, when performing an off channel scan. The default setting is 50 milliseconds.

13 Select the **Path Method Root Path Metric** tab to calculate root path metrics for a mesh point.

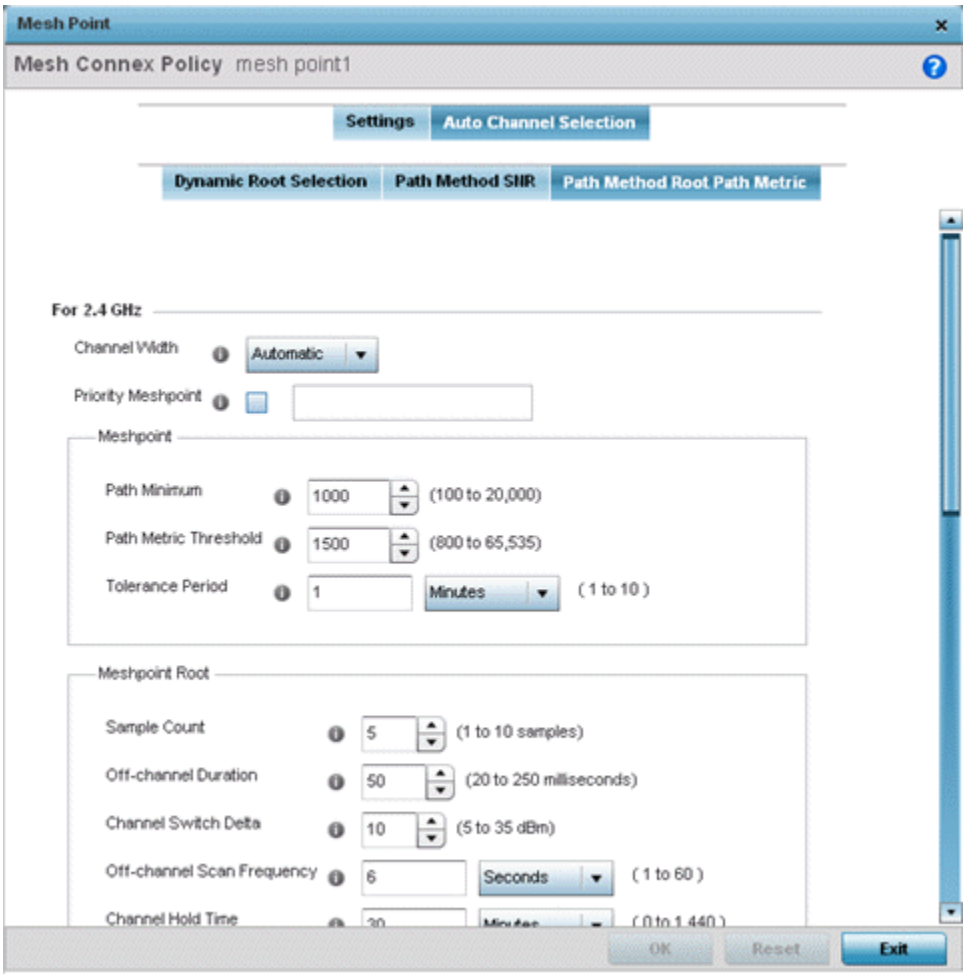


Figure 8-131 *Mesh Point Auto Channel Selection - Root Path Metric screen*

14 Set the following **Path Method Root Path Metrics** (applying to both the 2.4 GHz and 5.0/4.9 GHz frequencies):

Channel Width	Set the channel width meshpoint automatic channel scan should assign to the selected radio. The available options are: *Automatic* – Defines the channel width as calculated automatically. This is the default value. *20 MHz* – Set the width between two adjacent channels as 20 MHz. *40 MHz* – Set the width between two adjacent channels as 40 MHz. *80 MHz* – Sets the width between two adjacent channels as 80 MHz for 802.11ac Access Points.
Priority Meshpoint	Define the meshpoint assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a meshpoint is automatically selected.
Meshpoint: Path Minimum	Set the minimum path metric (from 100 - 20,000) for mesh connection establishment. The default setting is 1000.
Meshpoint: Path Metric Threshold	Configure a minimum threshold (from 800 - 65535) for triggering an automatic channel selection for meshpoint selection. The default is 1500.
Meshpoint: Tolerance Period	Configure a duration to wait before triggering an automatic channel selection for the next mesh hop. The default is one minute.
Meshpoint Root: Sample Count	Set the number of scans (from 1- 10) for data collection before a mesh point root is selected. The default is 5.
Meshpoint Root: Off-channel Scan Frequency	Configure the duration (from 1 -60 seconds) between two consecutive off channel scans for meshpoint root. The default is 6 seconds.
Meshpoint Root: Channel Hold Time	Set the minimum duration (from 0 - 1440 minutes) to remain on a selected channel before channel conditions are reassessed for a possible channel change. Set this value to zero (0) to prevent an automatic channel selection from occurring. The default is 30 minutes.
Meshpoint Root: Channel Switch Delta	Configure the delta (from 5 - 35 dBm) that triggers a meshpoint root automatic channel selection when exceeded. The default is 10 dBm.

15 Select **OK** to save the updates to the Mesh Point configuration. Select **Reset** to revert to the last saved configuration.

8.14.1 Vehicle Mounted Modem (VMM) Deployment Considerations

Before defining a VMM configuration (mounting an AP7161 mesh point on a moving vehicle), refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Disable layer 2 stateful packet inspection from the firewall policy. For more information, see *Firewall Policy Advanced Settings on page 10-10*.
- Set the RTS threshold value to 1 on all mesh devices. The default is 2347. For more information on defining radio settings, refer to *Access Point Radio Configuration on page 8-55*.
- Use Opportunistic as the rate selection setting for the AP7161 radio. The default is Standard.
- Disable Dynamic Chain Selection (radio setting). The default is enabled. This setting can be disabled in the CLI using the dynamic-chain-selection command, or in the UI.
- Disable A-MPDU Aggregation if the intended vehicular speed is greater than 30 mph.

- Setting a misconfiguration recovery time for the non-root AP profile is recommended. This should delay the rejection of the newest configuration push from the controller, potentially causing adoption loss.
- The additional delay is to support cases when the new configuration from the controller causes the root AP to move from current channel to other channels, resulting in a mesh link going down, and in turn non-root APs losing adoption. This delay accommodates the time needed for the non-root AP to scan all channels and finding the best root node. The non-root AP can begin operating on the new channel, and establish the mesh link re-adopt to the controller. (For countries using DFS, the scan time is also factored in for the configured value). If the AP fails to find a suitable root node within this time, this new config is a misconfiguration and the device would reject the latest config.
- For outdoor APs, it is recommended the misconfiguration-recovery-time be disabled. This can be accomplished by setting the value to 0. Update non root ap71xx profiles on the controller to include this change.

  Using an appropriate console terminal and or connection to your device log on to the CLI and follow these steps:

```
rfs6000-xxxxxx>enable
rfs6000-xxxxxx #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
rfs6000-xxxxxx (config)#profile ap71xx Non-Root AP71xx
rfs6000-xxxxxx (config-profile-Non-Root-AP71xx)#misconfiguration-recovery-time
0
rfs6000-xxxxxx (config-profile-Non-Root-AP71xx)#
```

8.15 Profile Environmental Sensor Configuration *(AP8132 Only)*

A sensor module is a USB environmental sensor extension to either an AP8132 or AP8232 model Access Point. It provides a variety of sensing mechanisms, allowing the monitoring and reporting of the Access Point's radio coverage area. The output of the sensor's detection mechanisms are viewable using either the Environmental Sensor screen.

To set or override an environmental sensor configuration for an AP8132 model Access Point:

1 Select the **Configuration** tab from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu.

4 Select **Environmental Sensor**.

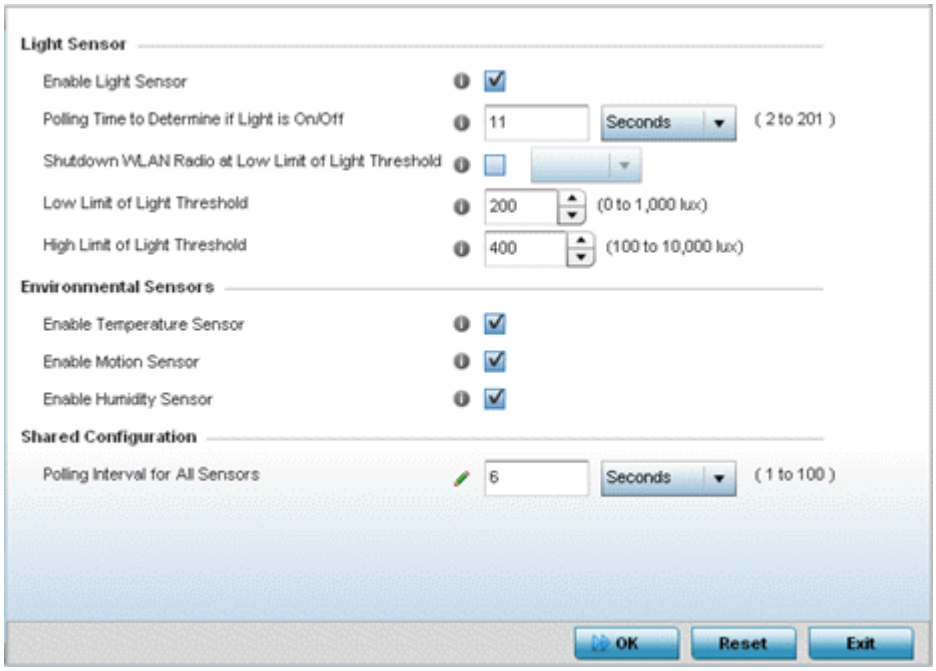


Figure 8-132 *Profile - Environmental Sensor screen*

5 Set the following **Light Sensor** settings for the sensor module:

Enable Light Sensor	Select this option to enable the light sensor on the module. This setting is enabled by default. The light sensor reports whether the deployment location has its lights powered on or off.
Polling Time to Determine if Light is On/Off	Define an interval in *Seconds* (2 - 201) or *Minutes* (1 - 4) for the sensor module to poll its environment to assess light intensity to determine whether lighting is on or off. The default polling interval is 10 seconds. Light intensity is used to determine whether the Access Point's deployment location is currently populated with clients.
Shutdown WLAN Radio at Low Limit of Light Threshold	Select this option to power off the Access Point's radio if the light intensity dims below the set threshold. If enabled, select All (both radios), radio-1 or radio-2.
Low Limit of Light Threshold	Set the low threshold limit (from 0 - 1,000 lux) to determine whether the lighting is off in the Access Point's deployment location. The default is 200. In daytime, the light sensor's value is between 350-450. The default values for the low threshold is 200, i.e., the radio is turned off if the average reading value is lower than 200.
High Limit of Light Threshold	Set the upper threshold limit (from 100 - 10,000 lux) to determine whether the lighting is on in the Access Point's deployment location. The default high threshold is 400. The radios are turned on when the average value is higher than 400.

6 Enable or disable the following **Environmental Sensors**:

Enable Temperature Sensor	Select this option to enable the module's temperature sensor. Results are reported back to the Access Point's Environment screens within the Statistics node. This setting is enabled by default.

Enable Motion Sensor	Select this option to enable the module's motion sensor. Results are reported back to the Access Point's Environment screens within the Statistics node. This setting is enabled by default.
Enable Humidity Sensor	Select this option to enable the module's humidity sensor. Results are reported back to the Access Point's Environment screens within the Statistics node. This setting is enabled by default.

7 Define or override the following **Shared Configuration** setting:

Polling Interval for All Sensors	Set an interval in either *Seconds* (1 - 100) or *Minutes* (1 - 2) for the time between all environmental polling (both light and environment). The default setting is 5 seconds.

8 Select **OK** to save the changes made to the environmental sensor screen. Select **Reset** to revert to the last saved configuration.

8.16 Advanced Profile Configuration

A profile's advanced configuration is comprised of defining its MINT protocol configuration and the profile's NAS identifier and port ID attributes. MINT provides secure profile communications at the transport layer. Using MINT, a device can be configured to only communicate with other authorized (MINT enabled) devices. Therefore, MINT is well designed for profile support, wherein a group of managed devices share the same configuration attributes.

Refer to the advanced profile's Miscellaneous menu item to set the profile's NAS configuration. The profile database on the RADIUS server consists of user profiles for each connected *network access server* (NAS) port.

To set a profile's advanced configuration:

1 Select the **Configuration** tab from the Web UI.

2 Select **Profiles** from the Configuration tab.

3 Select **Manage Profiles** from the Configuration > Profiles menu.

4 Select **Advanced** and expand the menu item.
The following sub menu items are available as advanced profile configuration options:
- *Client Load Balance Configuration*
- *Configuring MINT Protocol*
- *Advanced Profile Miscellaneous Configuration*

8.16.1 Client Load Balance Configuration

Advanced Profile Configuration

Set a the ratios and calculation values used by Access Points to distribute client loads both amongst neighbor devices and the 2.4 and 5 GHz radio bands.

To define Access Point client load balance algorithms:

1 Select **Client Load Balancing** from the Advanced menu item.

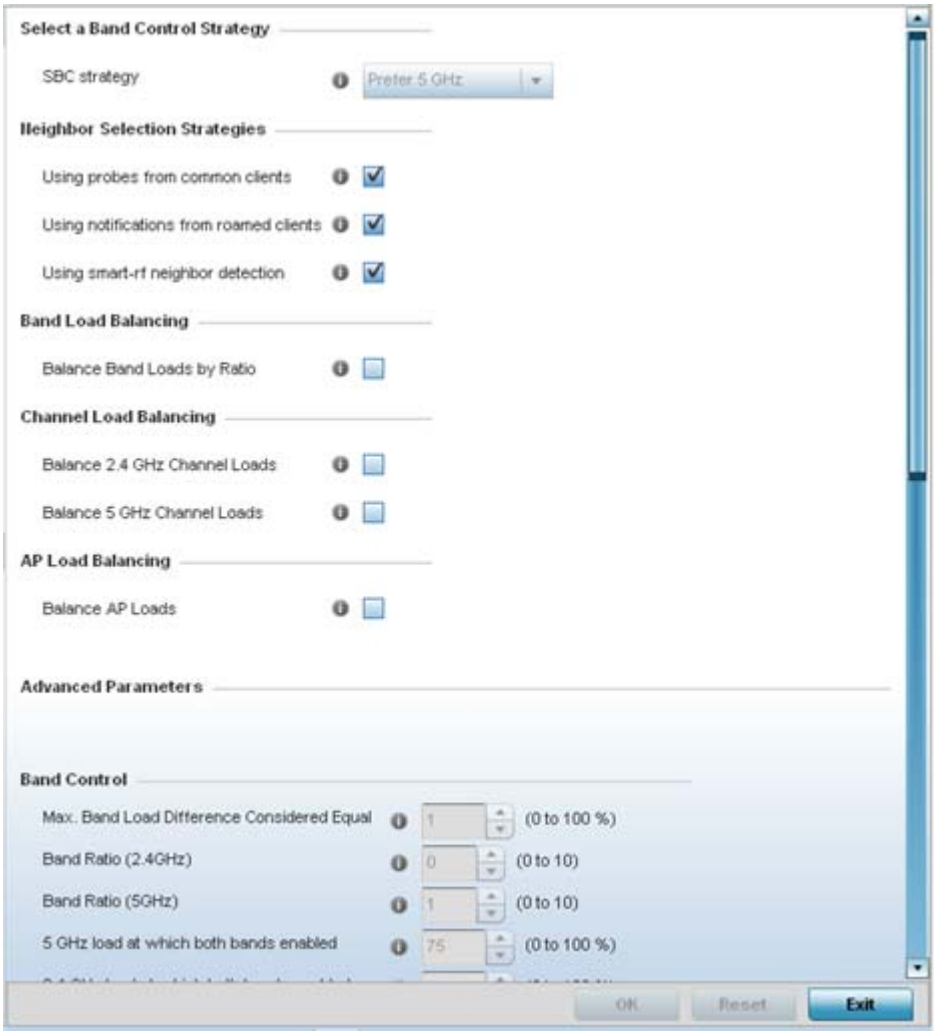


Figure 8-133 *Advanced Profile - Client Load Balancing screen*

2 Use the **Group ID** field to define a group ID of up to 32 characters to differentiate the ID from others with similar configurations.

3 Select the **SBC strategy** from the drop-down menu to determine how band steering is conducted.

Band steering directs 5 GHz-capable clients to that band. When an Access Point hears a request from a client to associate on both the 2.4 GHz and 5 GHz bands, it knows the client is capable of operation in 5 GHz. Band steering steers the client by responding only to the 5 GHz association request and not the 2.4 GHz request. The client only associates in the 5 GHz band.

4 Set the following **Neighbor Selection Strategies**:

Using Probes from common clients	Select this option to select neighbors (peer devices) using probes from common clients. This setting is enabled by default.
Using Notifications from roamed clients	Select this option to select neighbors (peer devices) using roam notifications from roamed clients. This setting is enabled by default.
Using smart-rf neighbor detection	Select this option to select neighbors (peer devices) using Smart RF. This setting is enabled by default.

5 Enable **Balance Band Loads by Radio** to distribute an Access Points client traffic load across both the 2.4 and 5 GHz radio bands.

6 Set the following **Channel Load Balancing** settings:

Balance 2.4 GHz Channel Loads	Select this option to balance an Access Point's 2.4 GHz client load across all channels available to that model SKU. This setting is enabled by default.
Balance 5 GHz Channel Loads	Select this option to balance an Access Point's 5 GHz client load across all channels available to that model SKU. This setting is enabled by default.

7 Enable **Balance AP Loads** (from within the **AP Load Balance** field) to distribute client traffic evenly amongst neighbor Access Points. This setting is enabled by default.

8 Set the following **Band Control** values:

Max. Band Load Difference Considered Equal	Set the maximum load difference (from 1 - 100%) considered equal when comparing band loads. The default setting is 1%.
Band Ratio (2.4 GHz)	Set the relative load for the 2.4 GHz radio band as a leveled ratio from 1 - 10. The default setting is 0.
Band Ratio (5 GHz)	Set the relative load for the 5 GHz radio band as a leveled ratio from 1 - 10. The default setting is 0.
5 GHz load at which both bands enabled	Define the 5 GHz radio load value (from 1 - 100%) above which the 5 GHz radio is equally preferred in the overall load balance distribution. The default is 75%.
2.4 GHz load at which both bands enabled	Define the 2.4 GHz radio load value (from 1 - 100%) above which the 2.4 GHz radio is equally preferred in the overall load balance distribution. The default is 75%.

9 Define the following **Neighbor Selection** settings:

Minimal signal strength for common clients	Define the minimum signal strength value (from -100 to 30 dBm) that must be exceeded for an Access Point's detected client to be considered a common client. the default setting is -100 dBi.
Minimum number of clients seen	Set the minimum number of clients (from 0 - 256) that must be common to two or more Access Points for the Access Points to regard one another as neighbors using the common client neighbor detection strategy. The default setting is 0.
Max confirmed neighbors	Set the maximum number (from 1 - 16) of neighbor Access Points that must be detected amongst peer Access Point to initiate load balancing. The default setting is 16.
Minimum signal strength for smart-rf neighbors	Set the minimal signal strength value (from -100 to 30 dBm) for an Access Point detected using Smart RF to qualify as a neighbor Access Point. the default setting is - 65 dBm.

10 Set the following **Advanced Parameters** for client load balancing:

Max. 2.4 GHz Difference Considered Equal	Set the maximum load difference (from 1 - 100%) considered equal when comparing 2.4 GHz client loads. The default setting is 1%.

Min. Value to Trigger 2.4 Ghz Channel Balancing	Set the threshold (from 1 - 100%) beyond which channel load balancing is triggered in the 2.4 GHz radio band. The default setting is 5%.
Weightage given to Client Count	Set the weightage (from 1- 100%) applied to client count calculations in the 2.4 GHz radio band. The default setting is 90%.
Weightage given to Throughput	Set the weightage (from 1- 100%) applied to client throughput calculations in the 2.4 GHz radio band. The default setting is 10%.
Max. 5 GHz Difference Considered Equal	Set the maximum load difference (from 1 - 100%) considered equal when comparing 5 GHz client loads. The default setting is 1%.
Min. Value to Trigger 5 Ghz Channel Balancing	Set the threshold (from 1 - 100%) beyond which channel load balancing is triggered in the 5 GHz radio band. The default setting is 5%.
Weightage given to Client Count	Set the weightage (from 1- 100%) applied to client count calculations in the 5 GHz radio band. The default setting is 90%.
Weightage given to Throughput	Set the weightage (from 1- 100%) applied to client throughput calculations in the 5 GHz radio band. The default setting is 10%.

11 Define the following **AP Load Balancing** settings:

Min. Value to Trigger Balancing	Set a value (from 1 - 100%) used to trigger client load balancing when exceeded. The default setting is 5%.
Max. AP Load Difference Considered Equal	Set the maximum load balance differential (from 1 - 100%) considered equal when comparing neighbor Access Point client loads. The default setting is 1%.
Weightage Given to Client Count	Set the weightage (from 1- 100%) applied to client count in an Access Point's overall load calculation. The default setting is 90%.
Weightage Given to Throughout	Set the weightage (from 1- 100%) applied to client throughput in an Access Point's overall load calculation. The default setting is 10%.

12 Select **OK** to save the changes made to the profile's client load balance configuration. Select **Reset** to revert to the last saved configuration.

8.16.2 Configuring MINT Protocol

Advanced Profile Configuration

MINT provides the means to secure profile communications at the transport layer. Using MINT, a device can be configured to only communicate with other authorized (MINT enabled) devices.

Keys can be generated externally using any application (like openssl). These keys must be present on the managed device managing the domain for key signing to be integrated with the UI. A MAP device that needs to communicate with another first negotiates a security context with that device. The security context contains the transient keys used for encryption and authentication. A secure network requires users to know about certificates and PKI. However, administrators do not need to define security parameters for Access Points to be adopted (secure WISPe being an exception, but that isn't a commonly used feature). Also, users can replace any device on the network or move devices around and they continue to work. Default security parameters for MiNT are such that these scenarios continue to function as expected, with minimal user intervention required only when a new network is deployed.

To define a profile's MINT configuration:

1 Select **MINT Protocol** from the Advanced profile menu item.

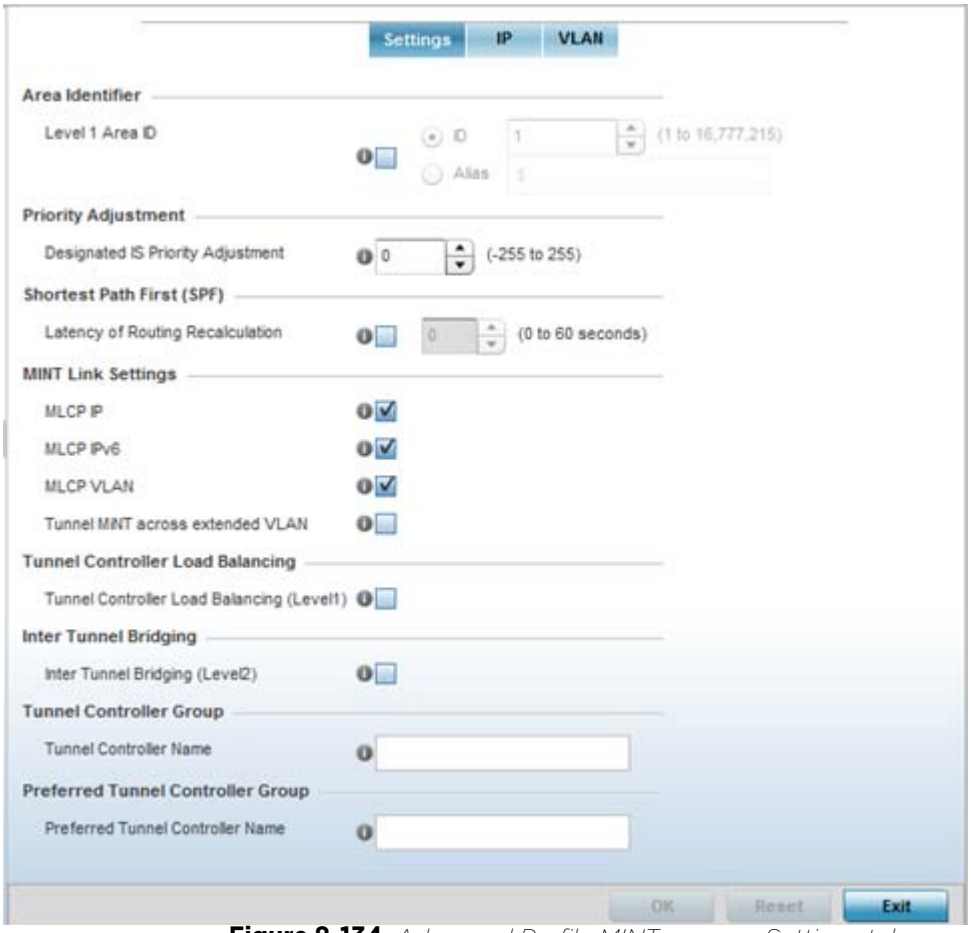


Figure 8-134 *Advanced Profile MINT screen - Settings tab*

The **Settings** tab displays by default.

2 Refer to the **Area Identifier** field to define the Level 1 and Level 2 Area IDs used by the profile's MINT configuration.

Level 1 Area ID	Select this option to either use a spinner control for setting the Level 1 Area ID (1 - 16,777,215) or create an alias for the ID. An alias enables an administrator to define a configuration item, such as a this area ID, as an alias once and use the alias across different configuration items. The default value is disabled.

3 Define the following **Priority Adjustment** in respect to devices supported by the profile:

Designated IS Priority Adjustment	Set a **Designated IS Priority Adjustment** setting from -255 and 255. This is the value added to the base level DIS priority to influence the *Designated IS* (DIS) election. A value of +1 or greater increases DISiness. The default setting is 0.

4 Select the **Latency of Routing Recalculation** check box (within the **Shortest Path First (SPF)** field) to enable the spinner control used for defining a latency period from 0 - 60 seconds. The default setting has the check box disabled.

5 Define the following **MINT Link Settings** in respect to devices supported by the profile:

MLCP IP	Check this box to enable *MINT Link Creation Protocol* (MLCP) by IP Address. MLCP is used to create one UDP/IP link from the device to a neighbor. The neighboring device does not need to be a controller or service platform, it can be another Access Point with a path to the controller or service platform.
MLCP IPv6	Check this box to enable MLCP for automated MiNT UDP/IP link creation. This setting is enabled by default.
MLCP VLAN	Check this box to enable MLCP by VLAN. MLCP is used to create one VLAN link from the device to a neighbor. That neighboring device does not need to be a controller or service platform, it can be another Access Point with a path to the controller or service platform.
Tunnel MiNT across extended VLAN	Select this option to tunnel MiNT protocol packets across an extended VLAN. This setting is disabled by default.

6 Select **Tunnel Controller Load Balancing (Level 1)** to enable load balance distribution via a WLAN tunnel controller. This setting is disabled by default.

7 Select **Inter Tunnel Bridging (Level 2)** to enable inter tunnel bridging. This setting is disabled by default.

8 Enter a 64 character maximum **Tunnel Controller Name** for this tunneled-WLAN-controller interface.

9 Enter a 64 character maximum **Preferred Tunnel Controller Name** this Access Point prefers to tunnel traffic to via an extended VLAN.

10 Select the **IP** tab to display the link IP network address information shared by the devices managed by the MINT configuration.

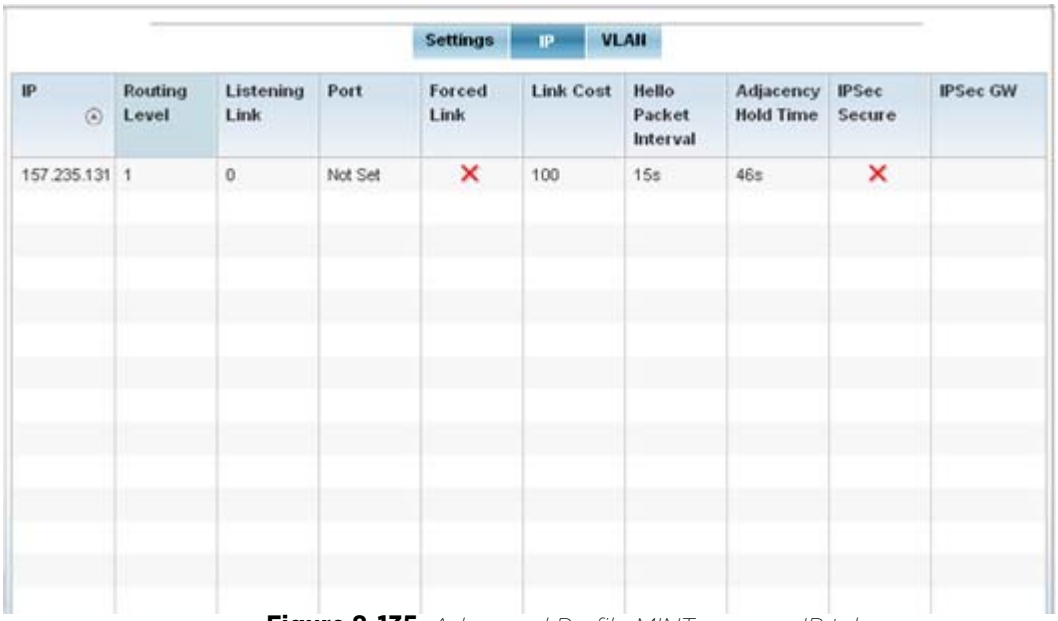


Figure 8-135 *Advanced Profile MINT screen - IP tab*

11 The IP tab displays the IP address, routing level, link cost, hello packet interval and Adjacency Hold Time managed devices use to securely communicate amongst one another within the managed network. Select **Add** to create a new Link IP configuration or **Edit** to modify an existing MINT configuration.

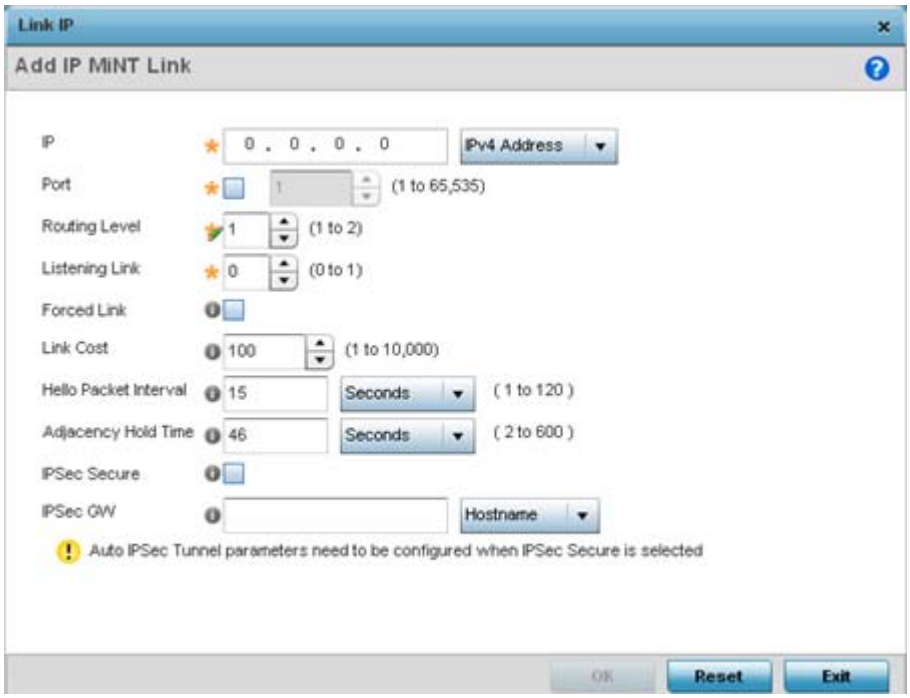


Figure 8-136 *Advanced Profile MINT screen - IP Add tab*

12 Set the following **Link IP** parameters to complete the MINT network address configuration:

IP	Define or override the IP address used by peers for interoperation when supporting the MINT protocol. Use the drop-down to select the type of IP address provided. The available choices are *IPv4 Address* and *IPv6 Address*.
Port	To specify a custom port for MiNT links, select this option and use the spinner control to define the port number between 1 and 65,535.
Routing Level	Use the spinner control to define a routing level of either 1 or 2.
Listening Link	Specify a listening link of either 0 or 1. UDP/IP links can be created by configuring a matching pair of links, one on each end point. However, that is error prone and doesn't scale. So UDP/IP links can also listen (in the TCP sense), and dynamically create connected UDP/IP links when contacted.
Forced Link	Check this box to specify the MiNT link as a forced link.
Link Cost	Use the spinner control to define a link cost between 1 - 10,000. The default value is 100.
Hello Packet Interval	Set an interval in either *Seconds* (1 - 120) or *Minutes* (1 - 2) for the transmission of hello packets. The default interval is 15 seconds.
Adjacency Hold Time	Set a hold time interval in either *Seconds* (2 - 600) or *Minutes* (1 - 10) for the transmission of hello packets. The default interval is 46 seconds.
IPSec Secure	Enable this option to provide IPSec secure peer authentication on the MiNT connection (link). This option is disabled by default.
IPSec GW	Select the numerical IP address or administrator defined hostname of the IPSec gateway.

13 Select the **VLAN** tab to display the link IP VLAN information shared by the devices managed by the MINT configuration.

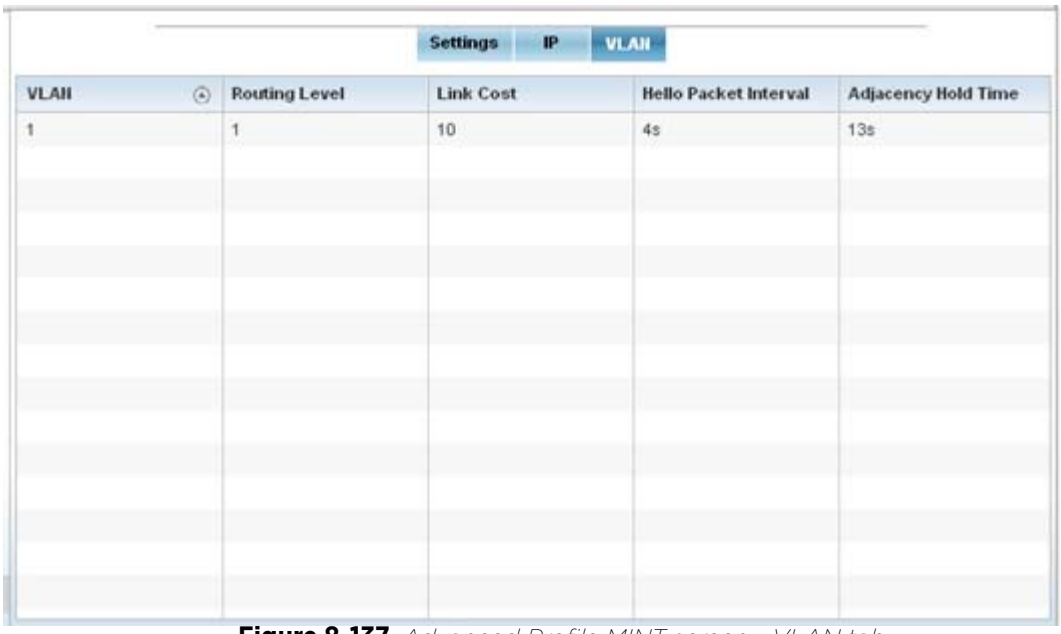


Figure 8-137 *Advanced Profile MINT screen - VLAN tab*

14 The VLAN tab displays the **VLAN**, **Routing Level**, **Link Cost**, **Hello Packet Interval** and **Adjacency Hold Time** managed devices use to securely communicate amongst one another. Select **Add** to create a new VLAN link configuration or **Edit** to modify an existing MINT configuration.

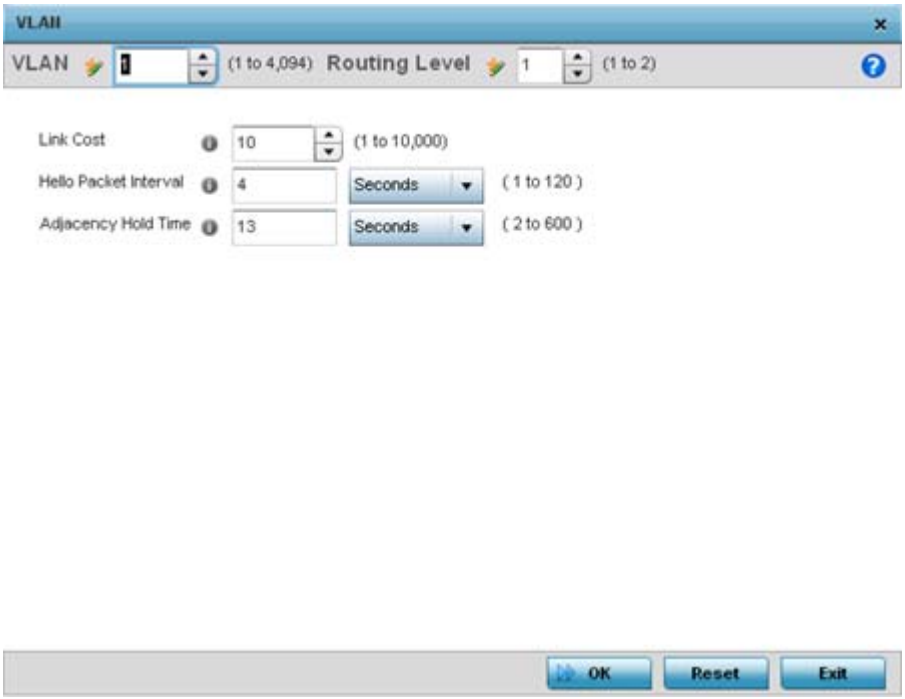


Figure 8-138 *Advanced Profile MINT screen - VLAN tab*

15 Set the following **VLAN** parameters for the MINT configuration:

VLAN	Define a VLAN ID between 1 - 4,094 used by peers for interoperation when supporting the MINT protocol.
Routing Level	Use the spinner control to define a routing level of either *1* or *2*.
Link Cost	Use the spinner control to define a link cost between 1 - 10,000. The default value is 100.
Hello Packet Interval	Set an interval in either *Seconds* (1 - 120) or *Minutes* (1 - 2) for the transmission of hello packets. The default interval is 15 seconds.
Adjacency Hold Time	Set a hold time interval in either *Seconds* (2 - 600) or *Minutes* (1 - 10) for the transmission of hello packets. The default interval is 46 seconds.

16 Select **OK** to save the updates and overrides to the MINT Protocol's VLAN configuration. Select **Reset** to revert to the last saved configuration.

17 Select the **Rate Limits** tab to display data rate limits configured on extended VLANs and optionally add or edit rate limit configurations.

Excessive traffic can cause performance issues on an extended VLAN. Excessive traffic can be caused by numerous sources including network loops, faulty devices or malicious software such as a worm or virus that has infected on one or more devices. Rate limiting reduces the maximum rate sent or received per wireless client. It prevents any single user from overwhelming the wireless network. It can also provide differential service for service providers. Uplink and downlink rate limits are usually configured on a RADIUS server using vendor specific attributes. Rate limits are extracted from the RADIUS server's response. When such attributes are not present, the settings defined on the controller, service platform or Access Point are applied. An administrator can set separate QoS rate limit configurations for data types transmitted from the network (upstream) and data transmitted from a wireless clients back to associated radios (downstream).

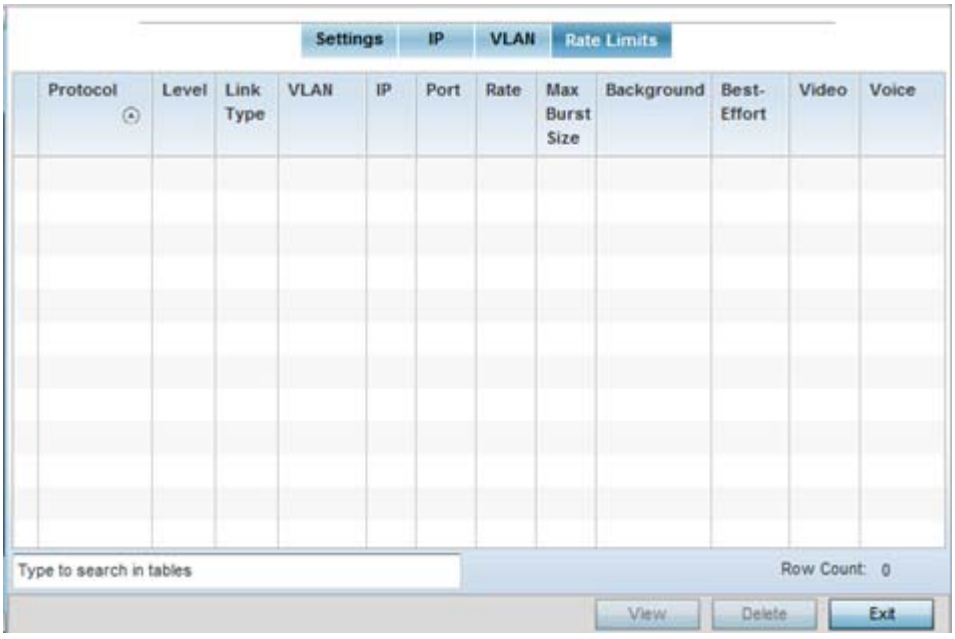


Figure 8-139 *Advanced Profile MINT screen - Rate Limit tab*

Existing rate limit configurations display along with their virtual connection protocols and data traffic QoS customizations.

18 Select **Add** to create a new rate limit configuration.

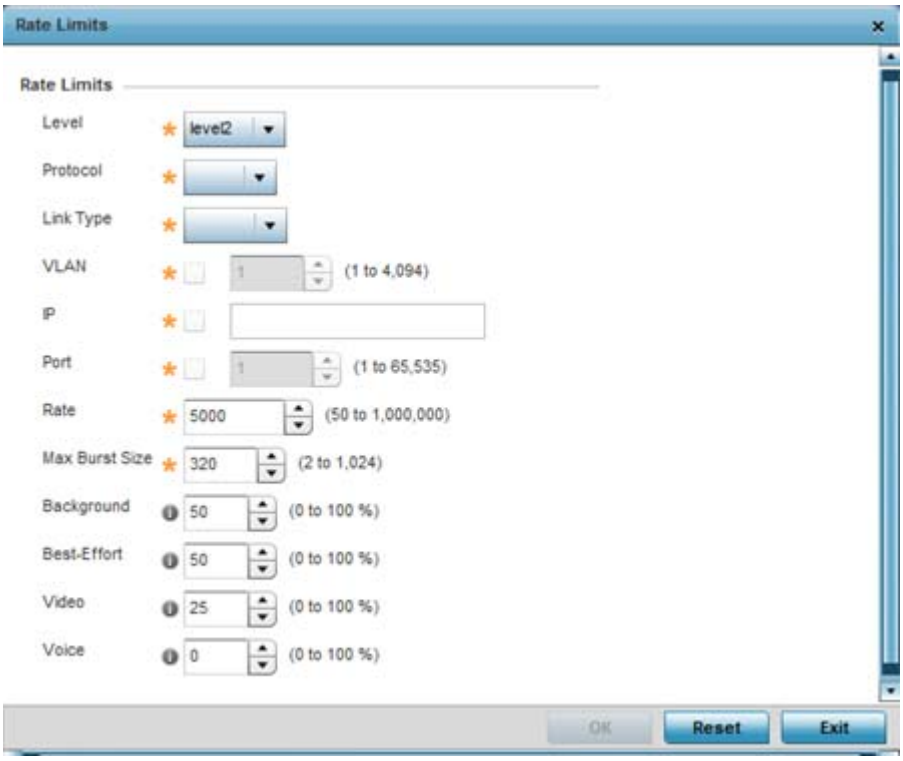


Figure 8-140 *Advanced Profile MINT screen - Add Rate Limit*

19 Set the following **Rate Limits** to complete the MINT configuration:

Level	Select *level2* to apply rate limiting for all links on level2.
Protocol	Select either *mlcp* or *link* as this configuration's rate limit protocol. *Mint Link Creation Protocol* (MLCP) creates a UDP/IP link from the device to a neighbor. The neighboring device does not need to be a controller or service platform, it can be an Access Point with a path to the controller or service platform. Select *link* to rate limit using statically configured MiNT links.
Link Type	Select either *VLAN*, to configure a rate limit configuration on a specific virtual LAN, or *IP* to set rate limits on a static IP address/Port configuration.
VLAN	When the Protocol is set to *link* and the Link Type is set to *VLAN*, use the spinner control to select a virtual LAN from 1 - 4094 to refine the rate limiting configuration to a specific VLAN.
IP	When the Protocol is set to *link* and the Link Type is set to *VLAN*, enter the IP address as the network target for rate limiting.
Port	When the Protocol is set to *link* and the Link Type is set to *VLAN*, use the spinner control to set the virtual port (1 - 65,535) used for rate limiting traffic.
Rate	Define a rate limit between 50 - 1,000,000 kbps. This limit constitutes a threshold for the maximum the number of packets transmitted or received (from all access categories). Traffic that exceeds the defined rate is dropped and a log message is generated. The default setting is 5000 kbps.

Max Burst Size	Use the spinner to set the maximum burst size from 0 - 1024 kb. The smaller the burst, the less likely the upstream packet transmission will result in congestion for the WLAN's client destinations. By trending the typical number of ARP, broadcast, multicast and unknown unicast packets over a period of time, the average rate for each access category can be obtained. Once a baseline is obtained, administrators should add a 10% margin (minimally) to allow for traffic bursts. The default burst size is 320 kbytes.
Background	Configures the random early detection threshold (as a percentage) for low priority background traffic. Background packets are dropped and a log message generated if the rate exceeds the set value. Background traffic consumes the least bandwidth of any access category, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis). The default setting is 50%.
Best-Effort	Configures the random early detection threshold (as a percentage) for low priority best-effort traffic. Best-effort packets are dropped and a log message generated if the rate exceeds the set value. Best effort traffic consumes little bandwidth, so this value can be set to a lower value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 50%.
Video	Configures the random early detection threshold (as a percentage) for high priority video traffic. Video packets are dropped and a log message generated if the rate exceeds the set value. Video traffic consumes significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 25%.
Voice	Configures the random early detection threshold (as a percentage) for high priority voice traffic. Voice packets are dropped and a log message generated if the rate exceeds the set value. Voice applications consume significant bandwidth, so this value can be set to a higher value once a general upstream rate is known by the network administrator (using a time trend analysis).The default setting is 0%.

20 Select **OK** to save the updates and overrides to the MINT Protocol's rate limit configuration. Select **Reset** to revert to the last saved configuration.

8.16.3 Advanced Profile Miscellaneous Configuration

Advanced Profile Configuration

Refer to the advanced profile's Miscellaneous menu item to set the profile's NAS configuration. The profile database on the RADIUS server consists of user profiles for each connected *network access server* (NAS) port. Each profile is matched to a username representing a physical port. When users are authorized, it queries the user profile database using a username representative of the physical NAS port making the connection.

1 Select **Miscellaneous** from the Advanced Profile's menu item.

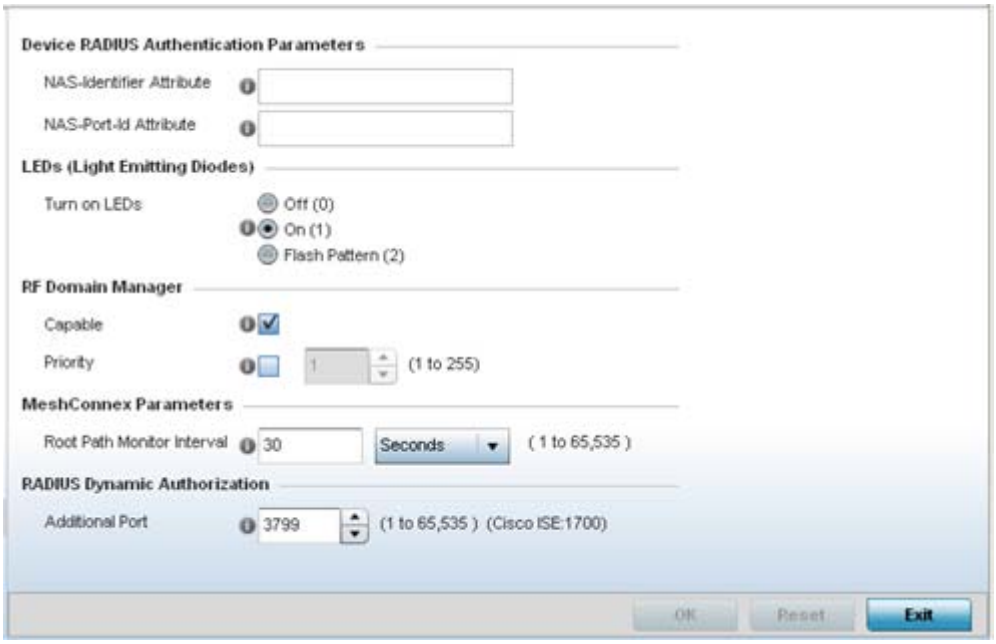


Figure 8-141 *Advanced Profile Miscellaneous screen*

2 Set a **NAS-Identifier Attribute** up to 253 characters.

This is the RADIUS NAS-Identifier attribute that typically identifies the controller or service platform where a RADIUS message originates.

3 Set a **NAS-Port-Id Attribute** up to 253 characters in length.

This is the RADIUS NAS port ID attribute which identifies the device port where a RADIUS message originates.

4 Select the **Turn on LEDs** option (within the **LEDs (Light Emitting Diodes)** section) to enable the LEDs on Access Point. This parameter is not available for controllers or service platforms.

Select the **Flash Pattern(2)** option (within the **LEDs (Light Emitting Diodes)** field) to flash an Access Point's LED's in a distinct manner (different from its operational LED behavior) to allow an administrator to validate an Access Point has received its configuration from its managing controller or service platform.

Enabling this feature allows an administrator to validate an Access Point has received its configuration (perhaps remotely at the site of deployment) without having to log into the managing controller or service platform. This feature is disabled by default.

5 Select the **Capable** option (within the **RF Domain Manager** section) to designate this specific profile managed device as being capable of being the RF Domain manager. The default value is enabled.

6 Select the **Priority** check box (within the **RF Domain Manager** section) to set a priority value for this specific profile managed device. Once enabled, use the spinner control to set a device priority between 1 - 255. The higher the number set, the higher the priority in the RF Domain manager election process.

7 Configure a **Root Path Monitor Interval**, between 1 and 65,535 seconds, to specify how often to check if the meshpoint is up or down.

Set the **Additional Port** value (within the **RADIUS Dynamic Authorization** field) between 1 and 65,535 seconds, or to 1700 to enable a CISCO *Identity Services Engine* (ISE) *Authentication, Authorization and Accounting* (AAA) server to dynamically authenticate a client.

When a client requests access to a CISCO ISE RADIUS server supported network, the server presents the client with a URL where a device's compliance is checked for definition file validity (this form of file validity checking is called *posture*). If the client device complies, it is allowed access to the network.

8 Select **OK** to save the changes made to the profile's advanced miscellaneous configuration. Select **Reset** to revert to the last saved configuration.

9 RF Domains

About RF Domains

A controller or service platform's configuration is composed of numerous elements including RF Domains, profiles, policies, WLANs and device specific configurations. RF Domains are used to assign regulatory, location and relevant policies to controllers and service platforms. RF Domains are required, and each controller or service platform must be assigned at least one default RF Domain.

RF Domains allow administrators to assign configuration data to multiple devices deployed in a common coverage area, such as in a floor, building or site. Each RF Domain contains policies that can determine a Smart RF or WIPS configuration.

RF Domains enable administrators to override WLAN SSID name and VLAN assignments. This enables the deployment of a global WLAN across multiple sites and unique SSID name or VLAN assignments to groups of Access Points servicing the global WLAN. This WLAN override technique eliminates the requirement for defining and managing a large number of individual WLANs and profiles.

A configuration contains (at a minimum) one default RF Domain and can optionally use additional user defined RF Domains:

- *Default RF Domain* - Automatically assigned to each controller or service platform and associated Access Point by default.
- *User Defined RF Domains* - Created by administrators and manually assigned to individual controller or service platforms, but can be automatically assigned to Access Points using adoption policies.

Each controller and service platform is assigned to only one RF Domain at a time. However, a user defined RF Domain can be assigned to multiple controllers or service platforms as required. User defined RF Domains can be manually assigned or automatically assigned to Access Points using an AP provisioning policy.

Default RF Domains

Each controller and service platform utilizes a default RF Domain. Access Points are assigned to this default RF Domain as they are discovered by the controller or service platform. The default RF Domain can be used for single site deployments, where regional, regulatory and RF policies are common between devices. When regional, regulatory or RF policies need to be device specific, user defined RF Domains are recommended.

A default RF Domain can also omit configuration parameters to prohibit regulatory configuration from automatically being inherited by devices as they are discovered by the controller or service platform. This is desirable in multi-site deployments with devices spanning multiple countries. Omitting specific configuration parameters eliminates the risk of an incorrect country code from being automatically assigned to a device.

User Defined RF Domains

Configure and deploy user defined RF Domains for single or multiple sites when controllers or service platforms require unique regulatory and regional configurations, or unique Smart RF and WIPS policies. User defined RF Domains can be used to:

- Assign unique Smart RF or WIPS policies to Access Points deployed on different floors or buildings within a site.
- Assign unique regional or regulatory configurations to Access Points deployed in different states or countries.

- Assign unique WLAN SSIDs and/or VLAN IDs to sites assigned a common WLAN without having to define individual WLANs for each site.

User defined RF Domains must be manually assigned to controllers or service platforms, but can be manually or automatically assigned to Access Points. Manual RF Domain assignment can be performed using the CLI or UI by modifying each device's individual configuration and assigning a specific RF Domain to the device. Automatic RF Domain assignments can be made using an AP provisioning policy which can assign specific RF Domains to Access Points based on an Access Point's model, serial number, VLAN, DHCP option, IP address or MAC address.

Automatic RF Domain assignments are useful in large deployments, as they enable plug-n-play Access Point deployments by automatically applying RF Domains to remote Access Points.

9.1 Managing RF Domains

Managing RF Domains entails configuring individual RF Domains as required and managing them as a collective set.

To review the configurations of existing RF Domains:

1 Select **Configuration** > **RF Domains** from the Web UI

The **RF Domain** screen displays within the main portion of the Web UI, and the **RF Domain Browser** displays in the lower, left-hand, portion of the Web UI.

2 Refer to the RF Domain screen to review high-level configuration data for existing RF Domain policies.

Figure 9-1 *RF Domains screen*

3 Use the following (read only) information to determine whether a new RF Domain policy requires creation, or an existing RF Domain requires edit or deletion:

RF Domain	Lists each policy's name, as assigned when it was created. The RF Domain name cannot be changed as part of the edit process. Only one RF Domain can be assigned to a controller or service platform.

Location	Displays the physical location assigned to the RF Domain. The name could be as specific as the floor of a building, or as generic as an entire site. The location defines the physical area where a common set of devices are deployed using the policy's RF Domain configuration.
Contact	Lists the contact (or administrator) assigned to respond to events created by, or impacting, RF Domain member devices.
Time Zone	Displays the geographic time zone set for each RF Domain policy. RF Domains can be assigned unique country codes and time zone information for upload by devices deployed and managed across different states or countries, thus making them ideal for configurations across different geographical areas.
Country	Displays the two-digit country code set for the policy. The country code must be set accurately to avoid illegal operation, as device radios transmit in specific channels unique to their country of operation.

4 Refer to the **RF Domain Browser** to expand each existing RF Domain policy and review the device MAC addresses operating within the location defined and are using the configuration defined for the policy.

Figure 9-2 *RF Domain Browser*

5 Once the data within the RF Domain screen and RF Domain Browser is reviewed, determine whether a new policy requires creation, or if an existing policy requires edit or deletion. The management of RF Domains entails the following:

- *RF Domain Basic Configuration*
- *RF Domain Sensor Configuration*
- *RF Client Name Configuration*
- *RF Domain Overrides*
- *RF Domain Network Alias*

9.1.1 RF Domain Basic Configuration

To set a RD Domain basic configuration:

1 Select **Configuration** > **RF Domains** from the Web UI.

2 From the RF Domain screen, either select the **Add** button or highlight an existing RF Domain and select **Edit**. An RF Domain configuration can be permanently removed by highlighting it from the list and selecting **Delete**.

An existing RF Domain can also be modified by selecting it directly from the RF Domain Browser.

If adding or modifying an existing RF Domain, the RF Domain **Basic Configuration** screen displays by default.

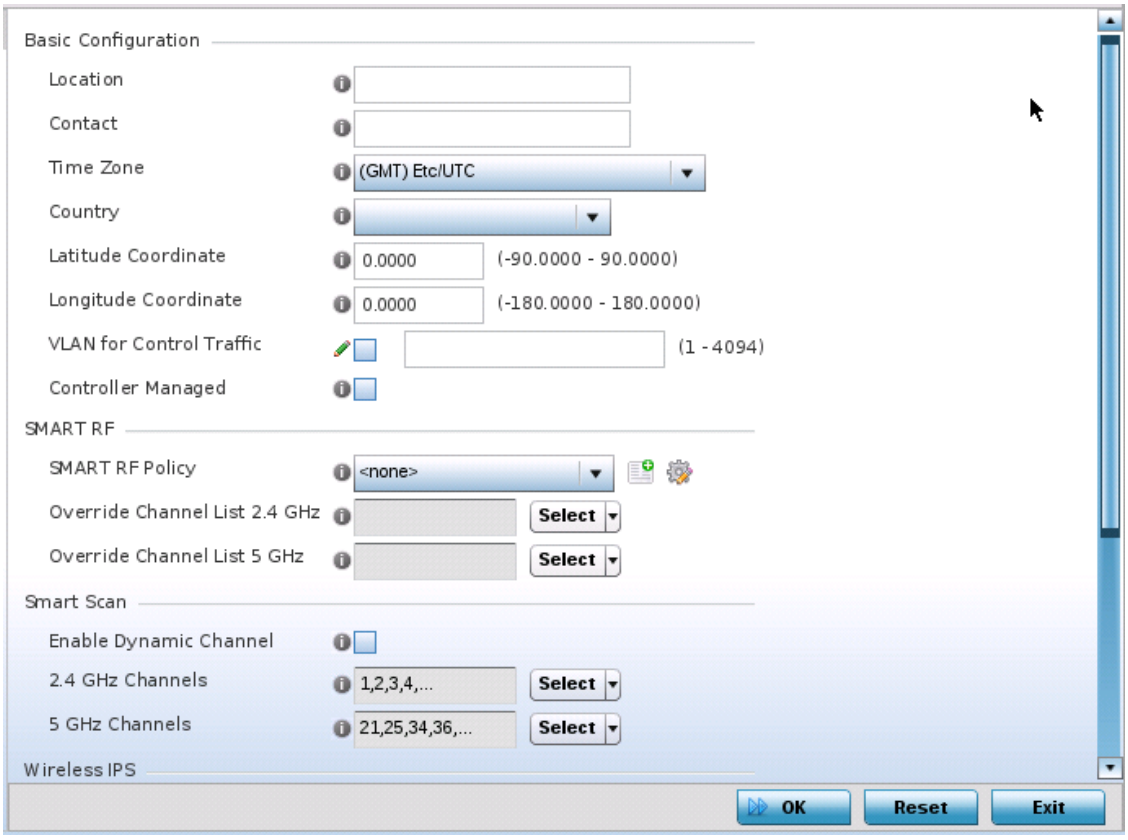


Figure 9-3 *RF Domain - Basic Configuration screen*

3 Define the following **Basic Configuration** parameters for the RF Domain:

RF Domain	If creating a new RF Domain, assign it a name representative of its intended function. The name cannot exceed 32 characters. The name cannot be changed as part of the edit process.
Location	Assign the physical location of the controller or service platform RF Domain. This name could be as specific as the floor of a building, or as generic as an entire site. The location defines the physical area where a common set of device configurations are deployed and managed by the RF Domain policy.
Contact	Provide the name of the contact (or administrator) assigned to respond to events created by or impacting the RF Domain.
Time Zone	Set the geographic time zone set for the RF Domain. RF Domains can be assigned unique country codes and time zone information for upload by devices deployed and managed across different states or countries, thus making them ideal for configurations across different geographical areas.
Country	Define the two-digit country code set for the RF Domain. The country code must be set accurately to avoid a device's illegal operation, as device radios transmit in specific channels unique to the country of operation.
Latitude Coordinate	Configures the of the RF Domain's latitude in order to fix its exact geographical location on a map. Use this option to define the geographical area where a common set of device configurations are deployed and managed by this RF Domain policy.

Longitude Coordinate	Configures the of the RF Domain's longitude in order to fix its exact geographical location on a map. Use this option to define the geographical area where a common set of device configurations are deployed and managed by this RF Domain policy.
VLAN for Traffic Control	Select the check box to enable a spinner control used for specifying the VLAN (within a range of 1 - 4,094) used for traffic control within this RF Domain.
Controller Managed	Select the check box to enable management of the RF Domain for adopted wireless clients by the controller or service platform.This option is disabled by default.

When a radio fails or is faulty, a Smart RF policy can used provide automatic recovery by instructing neighboring Access Points to increase their transmit power to compensate for the coverage loss.

Once correct Access Point placement has been established, Smart-RF can optionally be leveraged for automatic detector radio selection. Smart-RF uses detector radios to monitor RF events and can be used to ensure adequate detector coverage is available.

For an overview of Smart RF and instructions on how to create a Smart RF policy that can be used with a RF Domain, see *Smart RF Policy on page 6-79*.

4 Define the following **SMART RF** parameters for the RF Domain:

SMART RF Policy	Assign an existing Smart RF Policy to the RF Domain, or if none exist create a new one. Use the Smart RF Policy drop-down menu to navigate to existing Smart RF policies and select the one best suited to the function of the RF Domain. If none exist, select the *Create* icon and provide the required parameters to define a Smart RF configuration that can be used with the RF Domain. An existing policy can be edited by selecting the policy from the drop-down menu and selecting the *Edit* icon.
Override Channel List 2.4 GHz	Select an override list of channels Smart RF can use for channel compensations on 2.4 GHz radios.
Override Channel List 5 GHz	Select an override list of channels Smart RF can use for channel compensations on 5 GHz radios.

5 Define the following **Smart Scan** values:

Enable Dynamic Channel	Enable this setting to configuration the dynamic channel listing mode for smart scans in the 2.4 and 5 GHz bands. This setting is disabled by default.
2.4 GHz Channels	Set the list of 2.4 GHz mode channels sent in smart scans responses to clients.
5 GHz Channels	Set the list of 5 GHz mode channels sent in smart scans responses to clients.

6 Assign an existing **Wireless IPS** (WIPS) policy to the RF Domain, or if none exist create a new one.

Use the **WIPS Policy** drop-down menu to navigate to existing WIPS policies and select the one best suited to the function of the RF Domain. If none exist, select the **Create** icon and provide the required parameters to define a WIPS configuration that can be used with the RF Domain. An existing policy can be edited by selecting the policy from the drop-down menu and selecting the **Edit** icon.

A WIPS policy provides protection against wireless threats and acts as a key layer of security complementing wireless VPNs, encryption and authentication. a WIPS policy uses a dedicated sensor for actively detecting and

locating rogue AP devices. After detection, WIPS uses mitigation techniques to block the devices by manual termination, air lockdown, or port suppression.

For an overview of WIPS and instructions on how to create a WIPS policy that can be used with a RF Domain, see *Configuring a WIPS Policy on page 10-52*.

7 Refer to the **Statistics** field to define the **Update Interval** (from 0, 5 - 300 seconds) used to statistics update interval for this specific RF Domain. A value of zero is permissible to enable *auto mode*. Use auto mode, the update interval is automatically set by the RF Domain manager based on the RF Domain's current load.

8 Use the **Licenses** drop-down menu to obtain and leverage feature licenses from RF Domain member devices.

9 Select **OK** to save the changes to the Basic Configuration, or select **Reset** to revert to the last saved configuration.

9.1.2 RF Domain Sensor Configuration

The *Wireless Intrusion Protection System* (WIPS) protects the network, wireless clients and Access Point radio traffic from attacks and unauthorized access. WIPS provides tools for standards compliance and around-the-clock wireless network security in a distributed environment. WIPS allows administrators to identify and accurately locate attacks, rogue devices and network vulnerabilities in real time and permits both a wired and wireless lockdown of wireless device connections upon acknowledgment of a threat.

In addition to AirDefense sensors, an Access Point radio can function as a sensor and upload data to an external WIPS server. Unique WIPS server configurations are used by RF Domains to ensure a WIPS server is available to support the unique data protection needs of individual RF Domains.

WIPS is not supported on a WLAN basis, rather sensor functionality is supported on the Access Point radio(s) available to each managed WLAN. When an Access Point radio is functioning as a WIPS sensor, it's able to scan in sensor mode across all legal channels within 2.4 and 5.0 GHz. Sensor support requires an AirDefense WIPS Server on the network. Sensor functionality is not provided by the Access Point alone. The Access Point works in conjunction with a dedicated WIPS server.

The AP7522, AP7532, AP7562, AP8432 and AP8533 model Access Points can also function as L-Sense sensors. L-Sense is a highly scalable indoor locationing platform that gathers location-related analytics, such as visitor trends, peak and off-peak times, dwell time, heat-maps, etc. to enable entrepreneurs deeper visibility at a venue. To enable the location tracking system, the L-Sense server should be up and running and the RF Domain Sensor configuration should point to the L-sense server.

To define a sensor configuration for an RF Domain's group of member devices:

1 From the RF Domain screen, either select the **Add** button or highlight an existing policy and select **Edit**.

An existing policy can also be modified by selecting it directly from the RF Domain Browser.

2 Select the **Sensor** item from within the RF Domain screen.

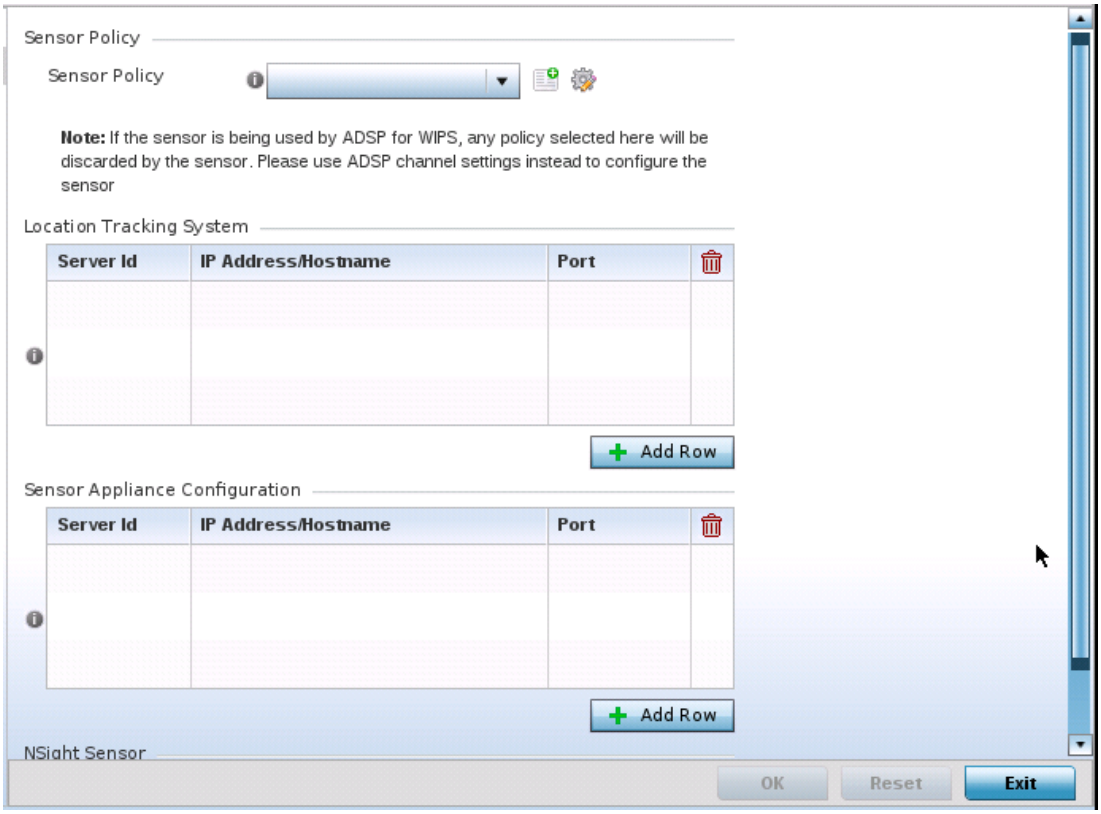


Figure 9-4 *RF Domain - Sensor screen*

3 Select the **+ Add Row** button to populate the **Location Tracking System** table with up to one L-Sense server credentials.

Server Id	Use the spinner control to assign a numerical ID for the *Location Tracking Sensor* (L-Sense) resource. As of now only one (1) L-Sense sever can be configured.
IP Address/Hostname	Provide the numerical (non DNS) IP address or hostname of the L-Sense server used by the RF Domain member devices. A hostname cannot exceed 64 characters or contain an underscore. When configured, Access Points (supporting L-Sense) post location-related analytics to the L-Sense server.
Port	Use the spinner control to specify the port for the L-Sense server. This is the port on which the L-Sense server is reachable. The default port is 443.

4 Select the **+ Add Row** button to populate the **ADSP Appliance Configuration** table with up to three rows for ADSP server credentials:

Server Id	Use the spinner control to assign a numerical ID for up to three WIPS server resources. The server with the lowest defined ID is the first reached by the controller or service platform. The default ID is 1.
IP Address/Hostname	Provide the numerical (non DNS) IP address or hostname of each server used as a WIPS sensor server by RF Domain member devices. A hostname cannot exceed 64 characters or contain an underscore.
Port	Use the spinner control to specify the port of each WIPS sensor server utilized by RF member devices. The default port is 443.

5 Select the **Enable NSight Sensor** option, within the **NSight Sensor** field, to enable the sensor module. This option is disabled by default.

6 Select **OK** to save the changes to the ADSP appliance sensor configuration, or select **Reset** to revert to the last saved configuration.

9.1.3 RF Client Name Configuration

The **Client Name Configuration** screen displays clients connected to RF Domain member Access Points adopted by networked controllers or service platforms. Use the screen to associate administrator assigned client names to specific connected client MAC addresses for improved client management.

To define a client name configuration used with RF Domain member devices:

1 From the RF Domain screen, either select the **Add** button or highlight an existing policy and select **Edit**.
An existing policy can also be modified by selecting it directly from the RF Domain browser.

2 Select the **Client Name Configuration** item from within the RF Domain screen.

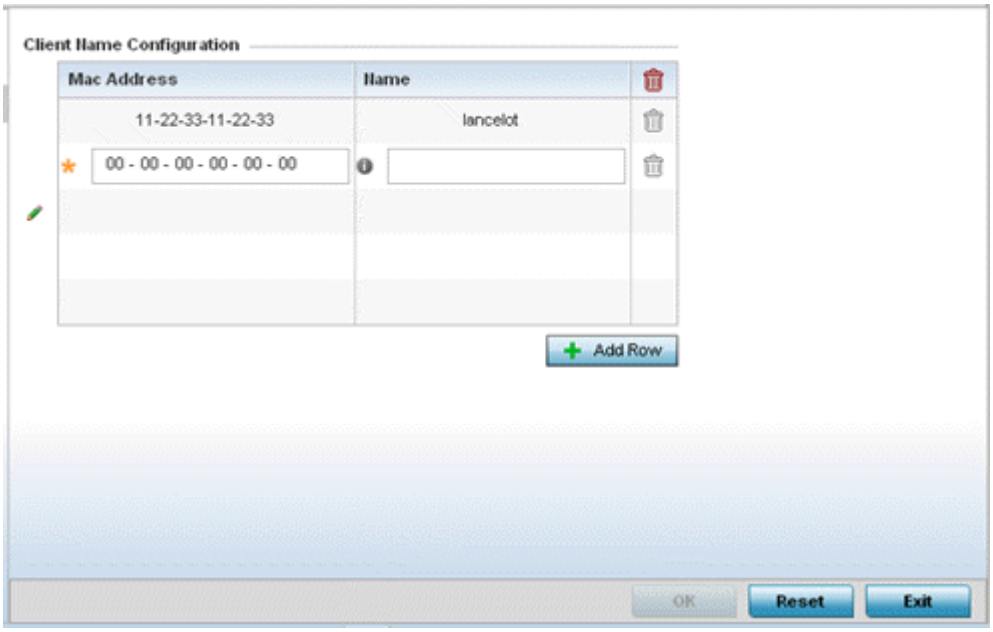


Figure 9-5 *RF Domain Client Configuration screen*

3 Either select the **+ Add Row** button to create a new client configuration or highlight an existing configuration and select the **Delete** icon to remove it.

4 Enter the client's factory coded MAC address.

5 Assign a **Name** to the RF Domain member Access Point's connected client to assist in its easy recognition.

6 Select **OK** to save the changes to the configuration, or select **Reset** to revert to the last saved configuration.

9.1.4 RF Domain Overrides

Each WLAN provides associated wireless clients with a *Service Set Identifier* (SSID). This has limitations, because it requires wireless clients associate with different SSIDs to obtain QoS and security policies. However, a WiNG managed RF Domain can have WLANs assigned and advertise a single SSID, but allow users to inherit different QoS or security policies. Use the Override SSID screen to assign WLANs an override SSID as needed for the RF Domain.

Controllers and service platforms allow the mapping of a WLAN to more than one VLAN. When a wireless client associates with a WLAN, it is assigned a VLAN in such a way that users are load balanced across VLANs. The VLAN is assigned from the pool representative of the WLAN. Clients are tracked per VLAN, and assigned to the least used/loaded VLAN. Client VLAN usage is tracked on a per-WLAN basis.

To define an override SSID and override VLAN configuration used with a RF Domain:

1 From the RF Domain screen, either select the **Add** button or highlight an existing policy and select **Edit**.

An existing policy can also be modified by selecting it directly from the RF Domain Browser.

2 Select the **Overrides** item from within the RF Domain screen.

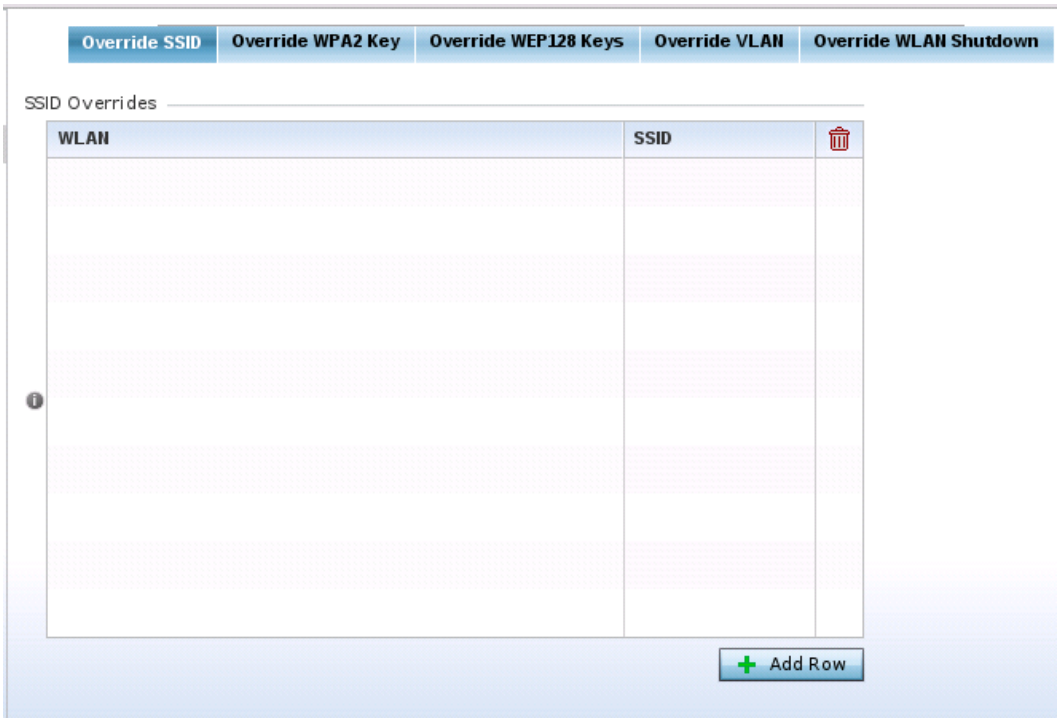


Figure 9-6 *RF Domain Override SSID screen*

The Overrides screen is partitioned into two tabs, with the **Override SSID** screen displayed by default.

3 Either select the **+ Add Row** button to create a new Override SSID configuration. Highlight an existing Sensor Server Configuration and select the Delete icon to remove it from the table.

4 Use the **WLAN** drop-down menu to select an existing WLAN to be supplied an override SSID.

If a WLAN configuration has not been defined, you'll need to select the **Create** button and define at least one complete WLAN configuration. For detailed information on the steps required to create a WLAN, see *Wireless LAN Policy on page 6-2*.

5 Enter the name of the **SSID** to use with this WLAN.

6 Select **OK** to save the changes to the Override SSID configuration, or select **Reset** to Revert to the last saved configuration.

7 Select the **Override WPA2 Key** tab.

The Override WPA2 Key screen enables an administrator to override a WLAN's existing WPA2 PSK at the RF Domain level (not the profile level). WPA2 is a newer 802.11i standard that provides even stronger wireless security than *Wi-Fi Protected Access* (WPA) and WEP.

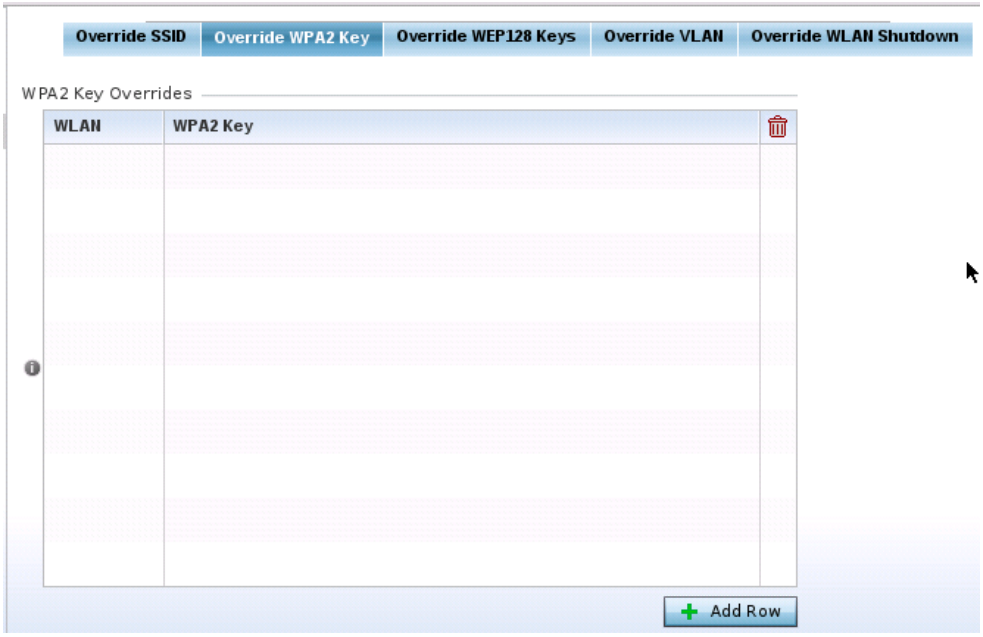


Figure 9-7 *RF Domain Override WPA2 PSK screen*

8 Select the **+ Add Row** button to populate the screen with a row for selecting an existing WLAN to override with a new WPA2 key.

WLAN	Use the drop-down menu to selecting an existing WLAN whose key is to be overridden at the RF Domain level. A new WLAN configuration can be defined by selecting the *Create* icon, or an existing WLAN configuration can be modified by selecting the *Edit* icon.
WPA2 Key	Enter either an alphanumeric string of 8 to 64 ASCII characters or 64 HEX characters as the primary string both transmitting and receiving authenticators must share in this new override PSK. The alphanumeric string allows character spaces. The string is converted to a numeric value. This passphrase saves the administrator from entering the 256-bit key each time keys are generated.

9 Select **OK** to save the changes to the Override WPA2 Key configuration, or select **Reset** to Revert to the last saved configuration.

10 Select the **Override WEP128 Keys** tab.

The Override WEP128 Keys screen enables an administrator to override a WLAN's existing WEP128 Keys at the RF Domain level (not the profile level). WEP 128 uses a 104 bit key which is concatenated with a 24-bit *initialization vector* (IV) to form the RC4 traffic key. WEP may be all a small-business user needs for the simple encryption of wireless data on the WLAN. However, networks that require more security are at risk from a WEP flaw. WEP is only recommended if there are client devices incapable of using higher forms of security. The existing 802.11 standard alone offers administrators no effective method to update keys.

The screen displays existing WLAN's whose WEP128 key configuration can be overridden at the RF Domain level. Either select **Add** to create a new WEP128 key configuration, or select an existing WEP128 Key and the **Edit** button to modify the selected key's existing key algorithm. The screen populates with the parameters required to override a WEP 128 configuration for the selected WLAN.

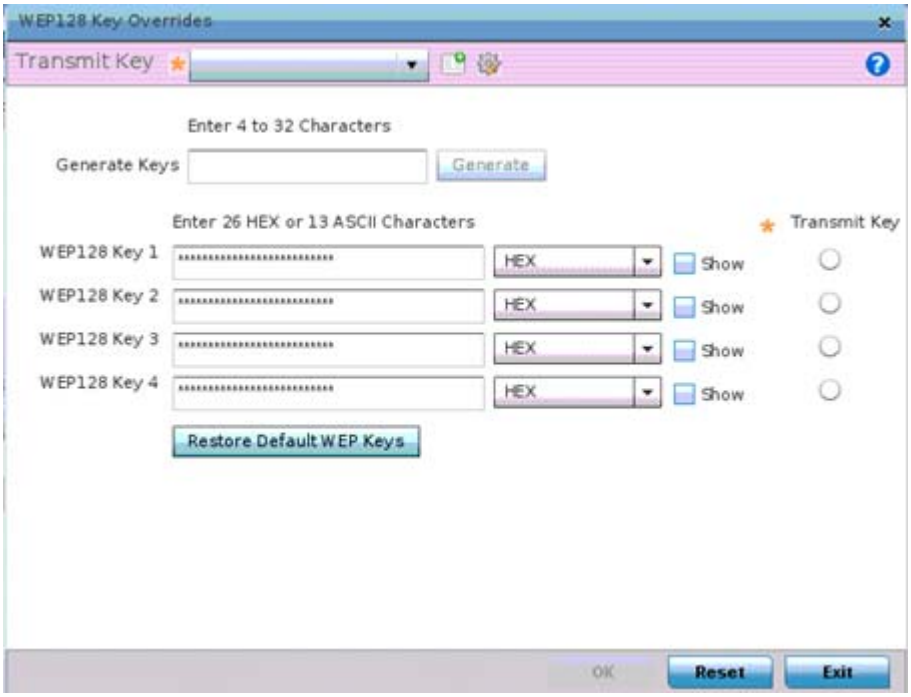


Figure 9-8 *RF Domain Override WEP128 Keys screen*

11 Define the following settings for the WEP 128 key override:

Generate Keys	Specify a 4 to 32 character RF Domain override Pass Key and click the *Generate* button. The pass key can be any alphanumeric string. Wireless devices and their connected clients use the algorithm to convert an ASCII string to the same hexadecimal number. Clients without adapters need to use WEP keys manually configured as hexadecimal numbers.
Keys 1-4	Use the Key #1-4 areas to specify key numbers. For WEP 128 (104-bit key), the keys are 26 hexadecimal characters in length. Select one of these keys for default activation by clicking its radio button. Selecting *Show* displays a key in exposed plain text.
Restore Default WEP Keys	If you feel it necessary to restore the WEP algorithm back to its default settings, click the *Restore Default WEP Keys* button. Default WEP 128 keys are as follows: *Key 1* 101112131415161718191A1B1C *Key 2* 202122232425262728292A2B2C *Key 3* 303132333435363738393A3B3C *Key 4* 404142434445464748494A4B4C

12 Select **OK** to save the changes to the Override WEP128 Key configuration, or select **Reset** to Revert to the last saved configuration.

13 Select the **Override VLAN** tab.

The Override VLAN screen lists those WLANs available for override.

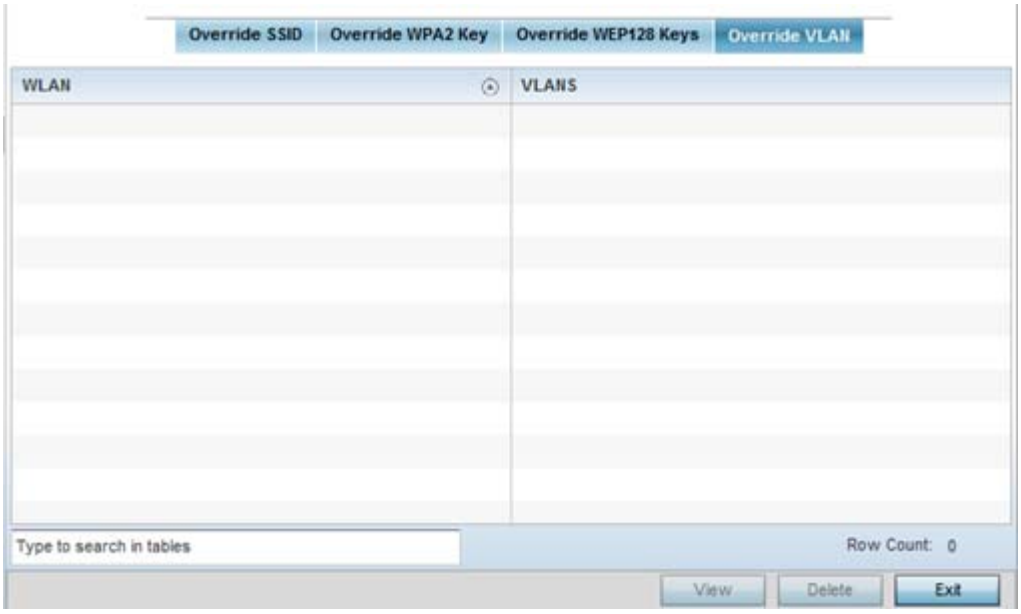


Figure 9-9 *RF Domain Override VLAN screen*

14 Either select **Add** to define a new VLAN override configuration, choose an existing WLAN and select **Edit** to change the override VLAN and limit or select **Delete** to remove a WLAN's override VLAN configuration.

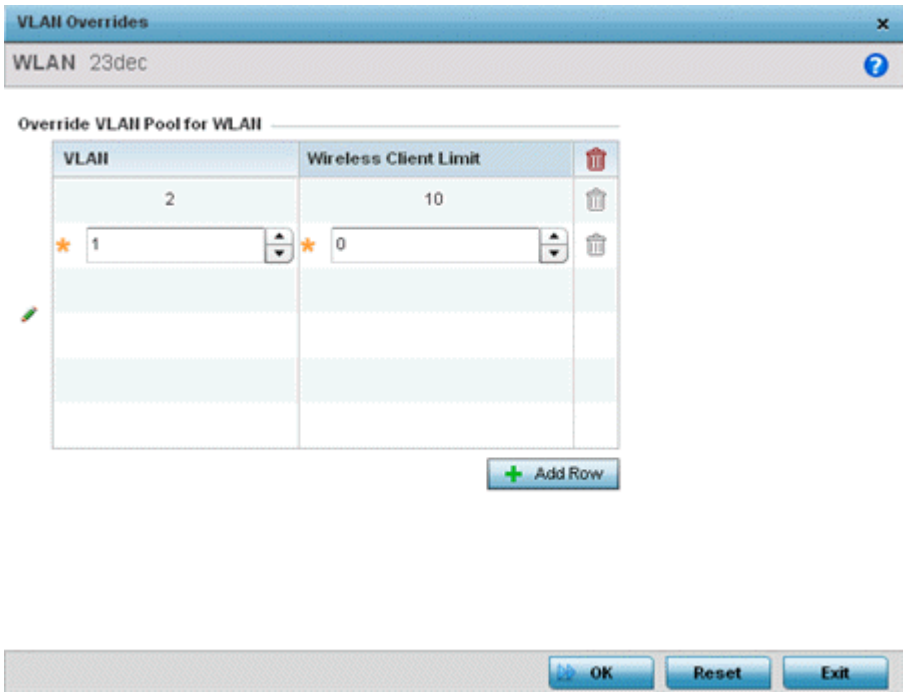


Figure 9-10 *RF Domain Override VLAN Add screen*

15 Use the **VLAN** spinner control to change the VLANs for an existing WLAN client connection or select the **+ Add Row** button to add additional VLANs for WLAN client connection.

16 Use the **Wireless Client Limit** spinner control to set the client user limit for the VLAN. The maximum allowed client limit is 8192 per VLAN. VLANs can be defined from 1 - 4094. The default setting is 0.

17 Select **OK** to save the changes to the Override VLAN configuration, or select **Reset** to Revert to the last saved configuration.

18 Select the **Override WLAN Shutdown** tab.

19 Select the **+ Add Row** button to populate the screen with a row for selecting an existing WLAN to override the WLAN mode of operation.

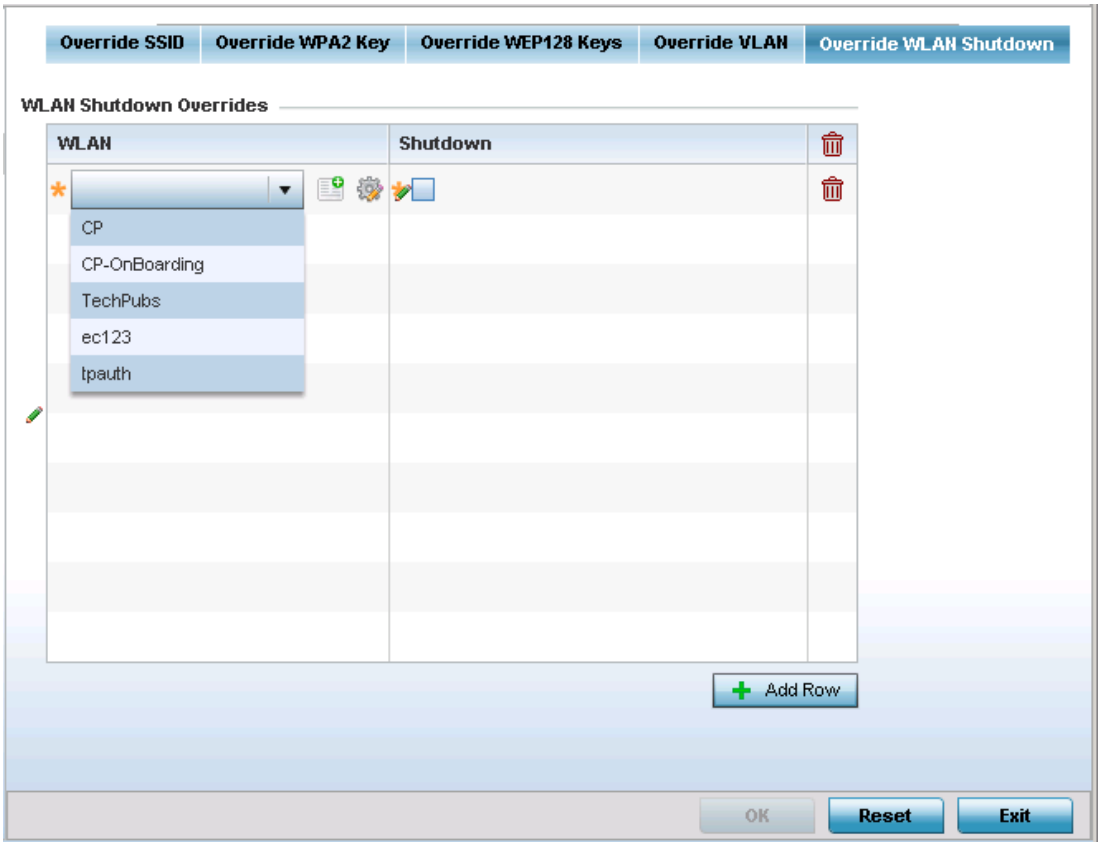


Figure 9-11 *RF Domain Override Override WLAN Shutdown Add screen*

20 Provide the following parameters:

WLAN	Use the drop-down menu to select an existing WLAN whose mode of operation is to be overridden at the RF Domain level.
Shutdown	Select to shut down the WLAN operation on all mapped radios. When selected, the RF Domains Access Points, mapped to the selected WLAN, stop beaconing the WLAN's SSID.

21 Select **OK** to save the changes to the Override WLAN Shutdown configuration, or select **Reset** to Revert to the last saved configuration.

9.1.5 RF Domain Network Alias

With large deployments, the configuration of remote sites utilizes a set of shared attributes, of which a small set of attributes are unique for each location. For such deployments, maintaining separate configuration (WLANs, profiles, policies and ACLs) for each remote site is complex. Migrating any global change to a particular configuration item to all the remote sites is a complex and time consuming operation.

Also, this practice does not scale gracefully for quick growing deployments.

An alias enables an administrator to define a configuration item, such as a hostname, as an alias once and use the defined alias across different configuration items such as multiple ACLs.

Once a configuration item, such as an ACL, is utilized across remote locations, the Alias used in the configuration item (ACL) is modified to meet local deployment requirement. Any other ACL or other configuration items using the modified alias also get modified, simplifying maintenance at the remote deployment.

Aliases have scope depending on where the Alias is defined. Alias are defined with the following scopes:

- *Global aliases* are defined from the **Configuration** > **Network** > **Alias** screen. Global aliases are available for use globally across all devices, profiles and RF Domains in the system.
- *Profiles aliases* are defined from the **Configuration** > **Devices** > **System Profile** > **Network** > **Alias** screen. Profile aliases are available for use to a specific group of wireless controllers or Access Points. Alias values defined in a profile override the alias values defined within global aliases.
- *RF Domain aliases* are defined from the **Configuration** > **Devices** > **RF Domain** > **Alias** screen. RF Domain aliases are available for use for a site as a RF Domain is site specific. RF Domain alias values override alias values defined in a global alias or a profile alias configuration.
- *Device aliases* are defined from the **Configuration** > **Devices** > **Device Overrides** > **Network** > **Alias** screen. Device aliases are utilized by a singular device only. Device alias values override global, profile or RF Domain alias configurations.

Using an alias, configuration changes made at a remote location override any updates at the management center. For example, if an network alias defines a network range as 192.168.10.0/24 for the entire network, and at a remote deployment location, the local network range is 172.16.10.0/24, the network alias can be overridden at the deployment location to suit the local requirement. For the remote deployment location, the network alias work with the 172.16.10.0/24 network. Existing ACLs using this network alias need not be modified and will work with the local network for the deployment location. This simplifies ACL definition and management while taking care of specific local deployment requirements.

For more information, refer to the following:

- *RF Domain Basic Alias*
- *RF Domain Network Group Alias*
- *RF Domain Network Service Alias*

9.1.5.1 RF Domain Basic Alias

A *basic alias* is a set of configurations consisting of *VLAN*, *Host*, *Network* and *Address Range* alias configurations. A VLAN alias is a configuration for optimal VLAN re-use and management for local and remote deployments. A host alias configuration is for a particular host device's IP address. A network alias configuration is utilized for an IP address on a particular network. An address range alias is a configuration for a range of IP addresses.

To set a network basic alias configuration for a RF Domain:

1 Select **Configuration** > **RF Domains** from the Web UI.

The **RF Domain** screen displays within the main portion of the Web UI, and the **RF Domain Browser** displays in the lower, left-hand, portion of the Web UI.

2 From the RF Domain screen, either select the **Add** button or highlight an existing RF Domain and select **Edit**.

An existing policy can also be modified by selecting it directly from the RF Domain browser.

3 Expand the **Network** menu item and select **Alias.**

The Alias screen displays with the **Basic Alias** tab displayed by default.

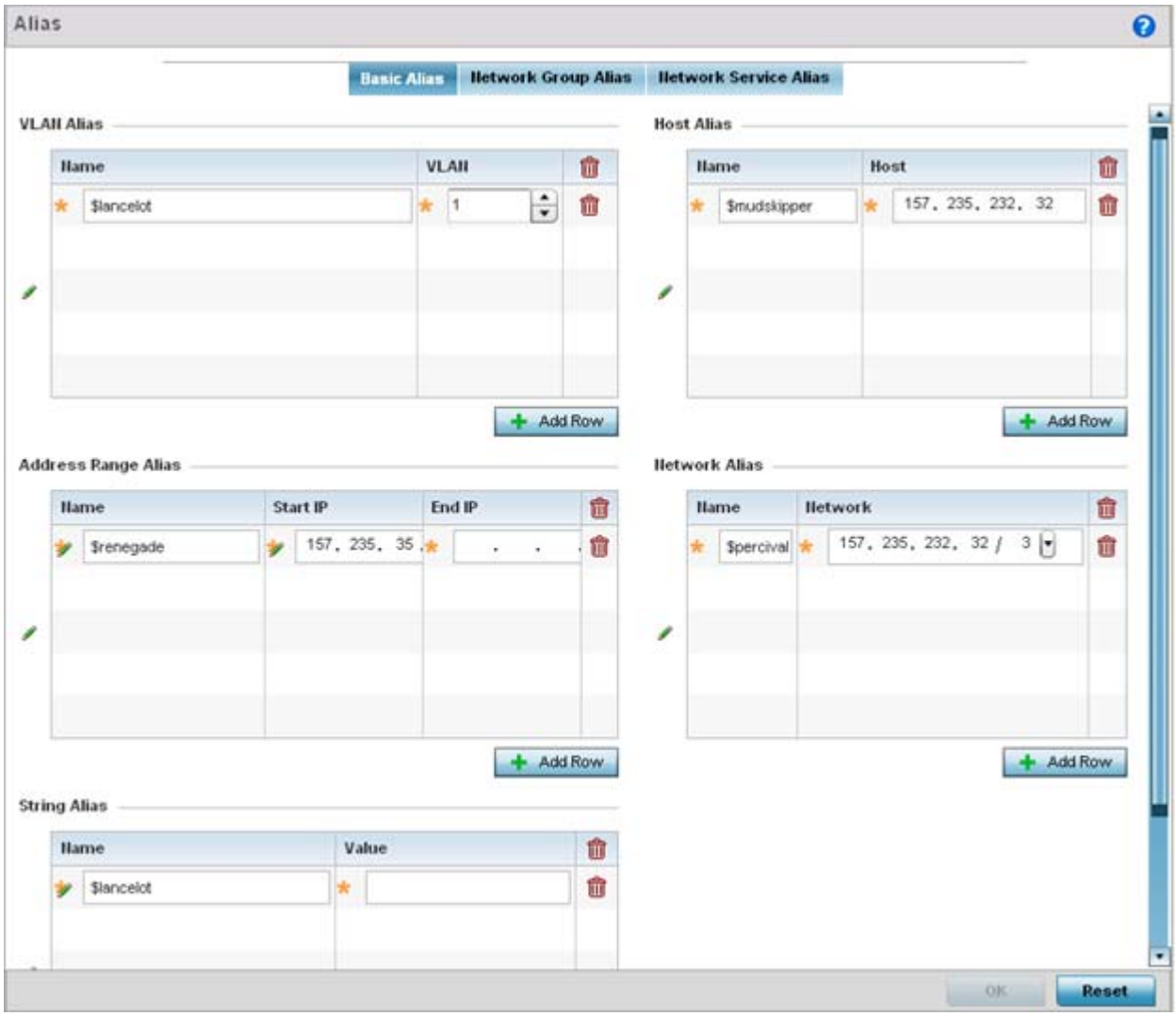


Figure 9-12 *RF Domain Network Basic Alias screen*

4 Select **+ Add Row** to define **VLAN Alias** settings:

Use the **Vlan Alias** field to create unique aliases for VLANs that can be utilized at different deployments. For example, if a VLAN ID is set as 10 for the central network, and the VLAN is set as 26 at a remote location, the VLAN can be overridden at the remote location using an alias. At the remote location, the network is functional with an ID of 26, but utilizes the name defined at the central local network. A new VLAN need not be created specifically at the remote location.

Name	If adding a new *VLAN Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Vlan	Use the spinner control to set a numeric VLAN ID from 1 - 4094.

5 Select **+ Add Row** to define **Address Range Alias** settings:

Use the **Address Range Alias** field to create aliases for IP address ranges that can be utilized at different deployments. For example, if an ACL defines a pool of network addresses as 192.168.10.10 through 192.168.10.100 for an entire network, and a remote location's network range is 172.16.13.20 through 172.16.13.110,

the remote location's ACL can be overridden using an alias. At the remote location, the ACL works with the 172.16.13.20-110 address range. A new ACL need not be created specifically for the remote deployment location.

Name	If adding a new *Address Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Start IP	Set a starting IP address used with a range of addresses utilized with the address range alias.
End IP	Set an ending IP address used with a range of addresses utilized with the address range alias.

6 Select **+ Add Row** to define **String Alias** settings:

Use the **String Alias** field to create aliases for strings that can be utilized at different deployments. For example, if the main domain at a remote location is called loc1.domain.com and at another deployment location it is called loc2.domain.com, the alias can be overridden at the remote location to suit the local (but remote) requirement. At one remote location, the alias functions with the loc1.domain.com domain and at the other with the loc2.domain.com domain.

Name	If adding a new *String Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Value	Provide a 255 character maximum string value to use in the alias.

7 Select **+ Add Row** to define **Host Alias** settings:

Use the **Host Alias** field to create aliases for hosts that can be utilized at different deployments. For example, if a central network DNS server is set a static IP address, and a remote location's local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements.

Name	If adding a new *Host Alias,* provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Host	Set the numeric IP address set for the host.

8 Select **+ Add Row** to define **Network Alias** settings:

Use the **Network Alias** field to create aliases for IP networks that can be utilized at different deployments. For example, if a central network ACL defines a network as 192.168.10.0/24, and a remote location's network range is 172.16.10.0/24, the ACL can be overridden at the remote location to suit their local (but remote) requirement. At the remote location, the ACL functions with the 172.16.10.0/24 network. A new ACL need not be created specifically for the remote deployment. This simplifies ACL definition and allows an administrator to better manage specific local requirements.

Name	If adding a new *Network Alias*, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign ($).
Network	Provide a network address in the form of *host/mask*.

9 Select **OK** when completed to update the set of basic alias rules. Select **Reset** to revert the screen back to its last saved configuration.

9.1.5.2 RF Domain Network Group Alias

A *network group alias* is a set of configurations consisting of host and network configurations. Network configurations are complete networks in the form of 192.168.10.0/24 or an IP address range in the form of 192.168.10.10-192.168.10.20. Host configurations are in the form of a single IP address, 192.168.10.23.

A network group alias can contain multiple definitions for a host, network, and IP address range. A maximum of eight (8) Host entries, eight (8) network entries and eight (8) IP addresses range entries can be configured inside a network group alias. A maximum of 32 network group alias entries can be created.

To set a network group alias configuration for a RF Domain:

1 Select **Configuration** > **RF Domains** from the Web UI.
The **RF Domain** screen displays within the main portion of the Web UI, and the **RF Domain Browser** displays in the lower, left-hand, portion of the Web UI.

2 From the RF Domain screen, either select the **Add** button or highlight an existing RF Domain and select **Edit**.
An existing policy can also be modified by selecting it directly from the RF Domain browser.

3 Expand the **Network** menu item and select **Alias.**

4 Select the **Network Group Alias** tab. The screen displays the attributes of existing network group alias configurations.

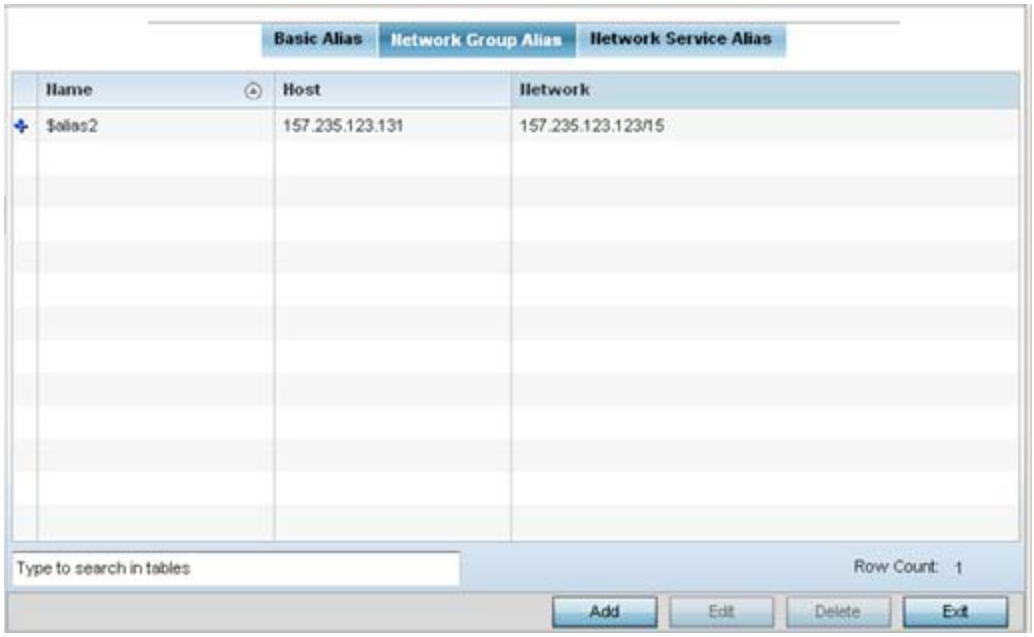


Figure 9-13 *RF Domain Network Group Alias screen*

Name	Displays the administrator assigned name used with the network group alias.
Host	Displays all the host aliases configured in the listed network group alias. Displays a blank column if no host alias is defined.
Network	Displays all network aliases configured in the listed network group alias. Displays a blank column if no network alias is defined.

5 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies.

6 Select the added row to expand it into configurable parameters for defining the network alias rule.

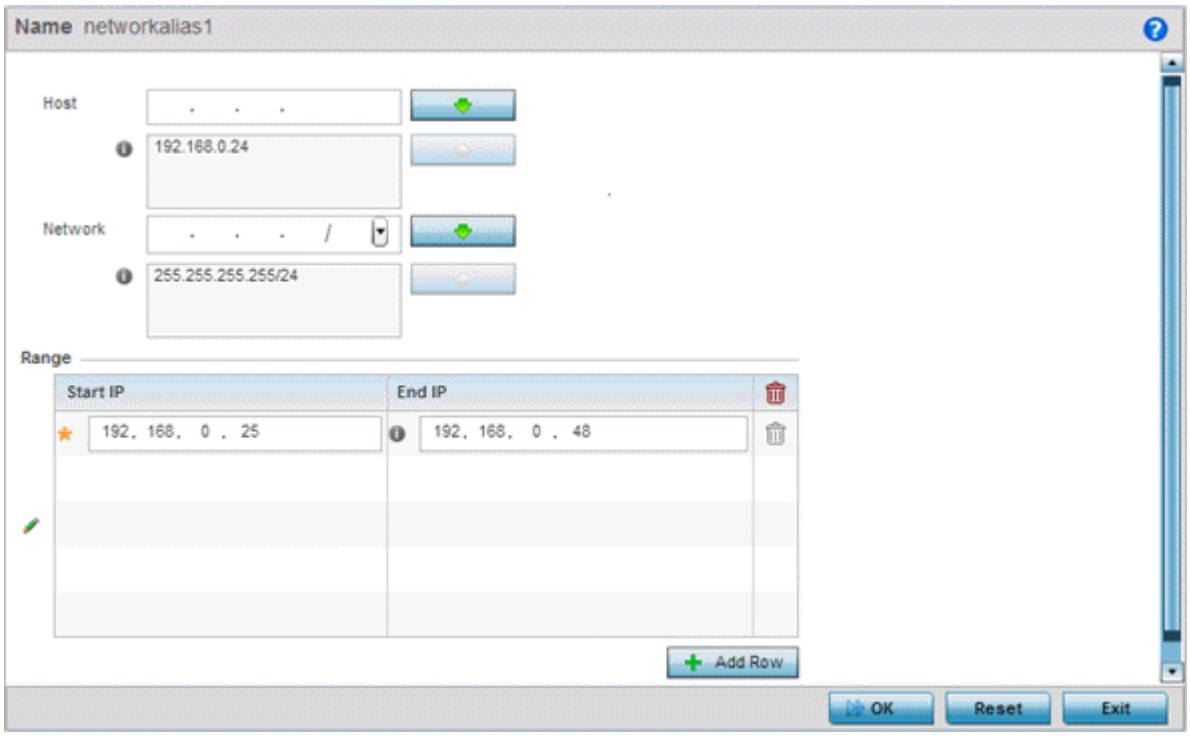


Figure 9-14 *RF Domain Network Group Alias Add screen*

7 If adding a new **Network Alias Rule,** provide it a name up to 32 characters. The network group alias name always starts with a dollar sign ($).

8 Define the following network group alias parameters:

Host	Specify the Host IP address for up to eight IP addresses supporting network aliasing. Select the down arrow to add the IP address to the table.
Network	Specify the netmask for up to eight IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Select the down arrow to add the mask to the table.

9 Within the **Range** table, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the alias range or double-click on an existing an alias range entry to edit it.

10 Select **OK** when completed to update the network alias rules. Select **Reset** to revert the screen back to its last saved configuration.

9.1.5.3 RF Domain Network Service Alias

A *network service alias* is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per network service alias.

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

To define a service alias configuration for a RF Domain:

1 Select **Configuration** > **RF Domains** from the Web UI.

The **RF Domain** screen displays within the main portion of the Web UI, and the **RF Domain Browser** displays in the lower, left-hand, portion of the Web UI.

2 From the RF Domain screen, either select the **Add** button or highlight an existing RF Domain and select **Edit**.

An existing policy can also be modified by selecting it directly from the RF Domain browser.

3 Expand the **Network** menu item and select **Alias.**

4 Select the **Network Service Alias** tab. The screen displays existing network service alias configurations.

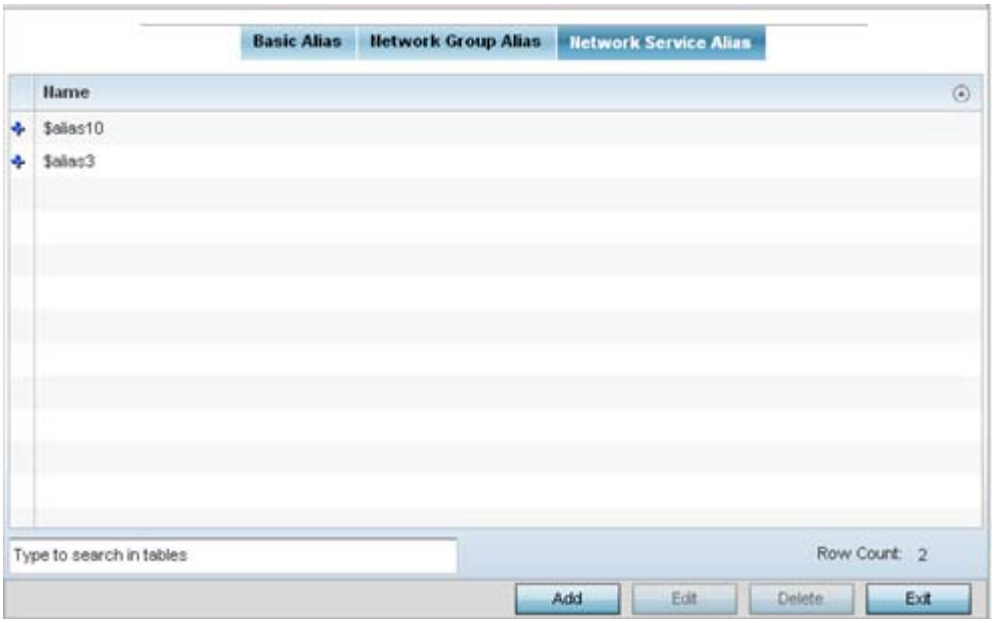


Figure 9-15 *RF Domain Network Service Alias screen*

5 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies.

6 Select the added row to expand it into configurable parameters for defining the service alias rule.

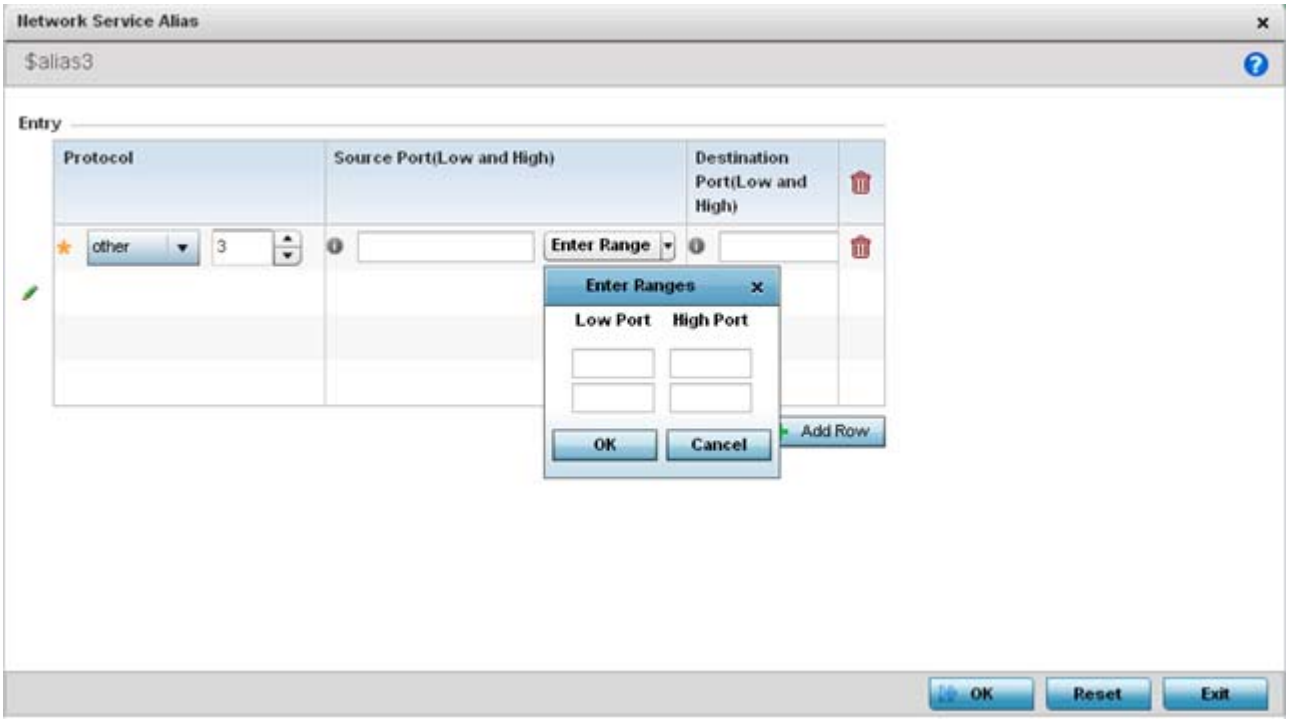


Figure 9-16 *RF Domain Network Service Alias Add screen*

7 If adding a new **Network Service Alias Rule,** provide it a name up to 32 characters. Ensure a $ precedes the name.

8 Select **+ Add Row** and provide the following configuration parameters:

Protocol	Specify the protocol for which the alias has to be created. Use the drop down to select the protocol from *eigrp, gre, icmp, igmp, ip, vrrp, igp, ospf, tcp* and *udp.* Select *other* if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected.
Source Port (Low and High)	This field is only relevant if the protocol is either *tcp* or *udp.* Specify the source ports for this protocol entry. A range of ports can be specified. Select the *Enter Ranges* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.
Destination Port (Low and High)	This field is only relevant if the protocol is either *tcp* or *udp*. Specify the destination ports for this protocol entry. A range of ports can be specified. Select the *Enter Ranges* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

9 Within the **Range** field, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the service alias range or double-click on an existing service alias range entry to edit it.

10 Select **OK** when completed to update the service alias rules. Select **Reset** to revert the screen back to its last saved configuration.

9.1.6 RF Domain Deployment Considerations

Before defining RF Domain policies, refer to the following deployment guidelines to ensure the configurations are optimally effective:

- Controllers or service platforms utilizes a default RF Domain. Access Points are assigned to this default RF Domain as they are discovered. The default RF Domain can be used for single site deployments, where regional, regulatory and RF policies are common between devices.
- User defined RF Domains must be manually assigned to controllers or service platforms, but can be manually or automatically assigned to Access Points.
- A Rogue AP detection configuration is a central component of an RF Domain policy, as it provides the RF Domain policy with the means to filter potentially threatening devices from operating with devices approved within the managed network.
- WIPS is not supported on a WLAN basis, rather sensor functionality is supported on the radio(s) available to each WLAN.
- When planning sensor coverage, a minimum of 1 detector radio is recommended per 4 Access Points. To ensure effective placement, LANPlanner can be used to provide predictive planning services and visualization to ensure adequate radio coverage is provided based on site application and device requirements. LANPlanner provides visualization tools ensuring adequate radio coverage for client radios and sensors. A physical site survey should also be performed to verify client radio coverage, before a final deployment.
- Both default and user defined RF Domains contain policies and configuration parameters. Changes made to policies or configuration parameters are automatically inherited by all the devices assigned to the RF Domain.

10 Security

When protecting wireless traffic to and from a wireless controller or service platform, the administrator should not lose sight of the security solution in it's entirety, since the chain is as weak as its weakest link. A WiNG managed network provides seamless data protection and user validation to protect and secure data at each vulnerable point in the network. WiNG managed wireless devices support a Layer 2 wired/wireless firewall and *Wireless Intrusion Protection System* (WIPS) capabilities at the WLAN, while additionally strengthened with a premium multi-vendor overlay security solution from Air Defense with 24x7 dedicated protection. This security is offered at the most granular level, with role, location and device categorization based network access control available to users based on identity as well as the security posture of the client device. For more information, see:

- *Wireless Firewall*
- *Configuring IP Firewall Rules*
- *Wireless Client Roles*
- *Device Fingerprinting*
- *Intrusion Prevention*
- *EX3500 Time Range*

10.1 Wireless Firewall

A firewall is a mechanism enforcing network access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms both blocking and permitting data traffic within the network. Firewalls implement uniquely defined access control policies, so if you don't have an idea of what kind of access to allow or deny, a firewall is of little value, and in fact could provide a false sense of network security.

With WiNG managed wireless controllers and Access Points, Firewalls are configured to protect against unauthenticated logins from outside the network. This helps prevent hackers from accessing managed wireless clients. Well designed Firewalls block traffic from outside the network, but permit authorized users to communicate freely with outside the network.

Firewalls can be implemented in both hardware and software, or a combination of both. All messages entering or leaving the wireless controller or Access Point pass through the firewall, which examines each message and blocks those not meeting the security criteria (rules) defined.

Firewall rules define the traffic permitted or denied within the network. Rules are processed by a firewall supported device from first to last. When a rule matches the network traffic a controller or service platform is processing, the firewall uses that rule's action to determine whether traffic is allowed or denied.

Rules comprise conditions and actions. A condition describes a traffic stream of packets. Define constraints on the source and destination device, the service (for example, protocols and ports), and the incoming interface. An action describes what should occur to packets matching the conditions set. For example, if the packet stream meets all conditions, traffic is permitted, authenticated and sent to the destination device.

Additionally, MAC rule based firewall filtering can be deployed to apply firewall policies to traffic being bridged by centrally managed radios. MAC filtering can be employed to permit or restrict traffic exchanged between hosts, hosts residing on separate WLANs or hosts forwarding traffic to wired devices.

For more information, refer to the following:

- *Configuring a Firewall Policy*
- *Configuring MAC Firewall Rules*
- *Firewall Deployment Considerations*

10.1.1 Configuring a Firewall Policy

Wireless Firewall

To configure a firewall on the wireless controller or service platform:

1 Select **Configuration** > **Security** > **Wireless Firewall** > **Firewall Policy** to display existing firewall policies.

The **Wireless Firewall** screen lists existing firewall policies. An existing policy can be selected and applied. The user has the option of displaying the configurations of each policy, or referring to the **Wireless Firewall Browser** and selecting individual polices for review.

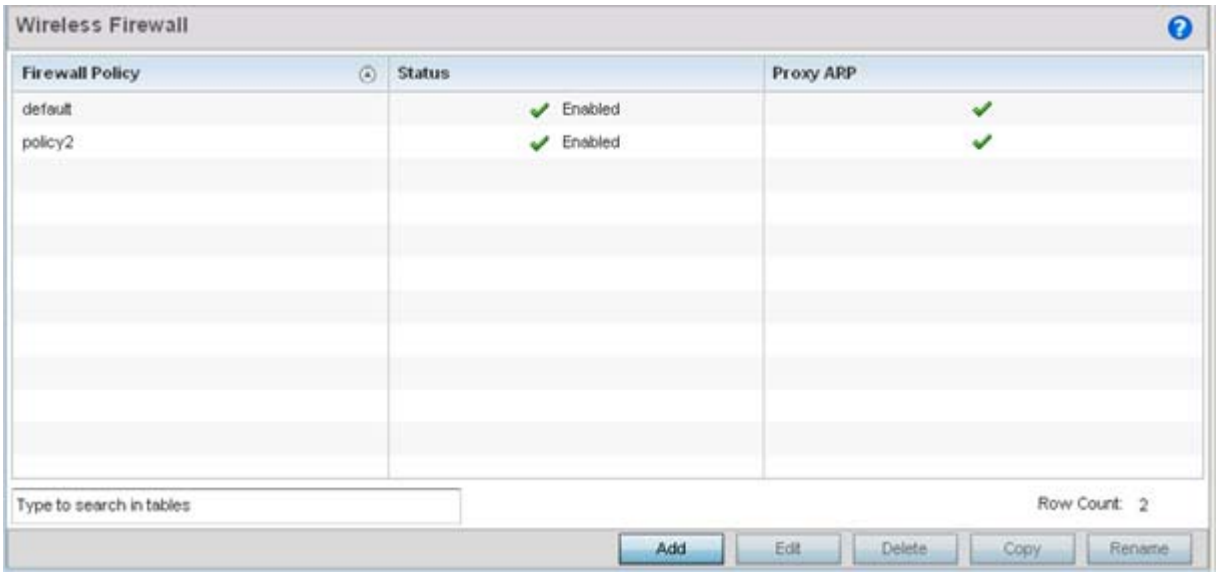


Figure 10-1 *Wireless Firewall Policy screen*

2 Refer to the following configuration data for existing wireless firewall policies:

Firewall Policy	Displays the name assigned to the policy when created. The name cannot be modified as part of the edit process.
Status	Displays a green check mark if the policy has been enabled. A red "X" designates the policy as disabled.
Proxy ARP	Displays a green check mark if Proxy ARP routing has been enabled. A red "X" designates Proxy ARP as disabled.

3 Select **Add** to create a new Wireless Firewall policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available.

For information on adding and editing Wireless Firewall policies, see *Adding and Editing Wireless Firewall Policies on page 10-3*.

10.1.1.1 Adding and Editing Wireless Firewall Policies

Configuring a Firewall Policy

To add or edit a firewall policy:

1 Select **Configuration** > **Security** > **Wireless Firewall** > **Firewall Policy** to display existing firewall policies.

2 Select **Add** to create a new Wireless Firewall policy. Select an existing policy and click **Edit** to modify the attributes of that policy.

The **Denial of Services** tab displays by default.

3 When adding a new policy, first enter a name for the Firewall Policy. The name must not exceed 64 characters. Once a name is specified, click **OK** to enable the other parameters within the screen.

The Wireless Firewall Policy configuration is divided into the following tabs:

- *Firewall Policy Denial of Service*
- *Firewall Policy Storm Control*
- *Firewall Policy Advanced Settings*

10.1.1.1.1 Firewall Policy Denial of Service

Adding and Editing Wireless Firewall Policies

A *denial of service* (DoS) attack is an attempt to make a computer or network resource unavailable to its intended users. Although the means to carry out a DoS attack will vary, it generally consists of a concerted effort of one or more persons attempting to prevent a device, site or service from functioning temporarily or indefinitely.

Most DoS attacks involve saturating the target device with external communications requests so it cannot respond to legitimate traffic or respond so slowly the device becomes unavailable in respect to its defined data rate. DoS attacks are implemented by either forcing targeted devices to reset or consuming the device's resources so it can no longer provide service.

To define a denial of service configuration for a Firewall policy:

1 Select the **Denial of Service** tab from the **Firewall Policy** configuration page.

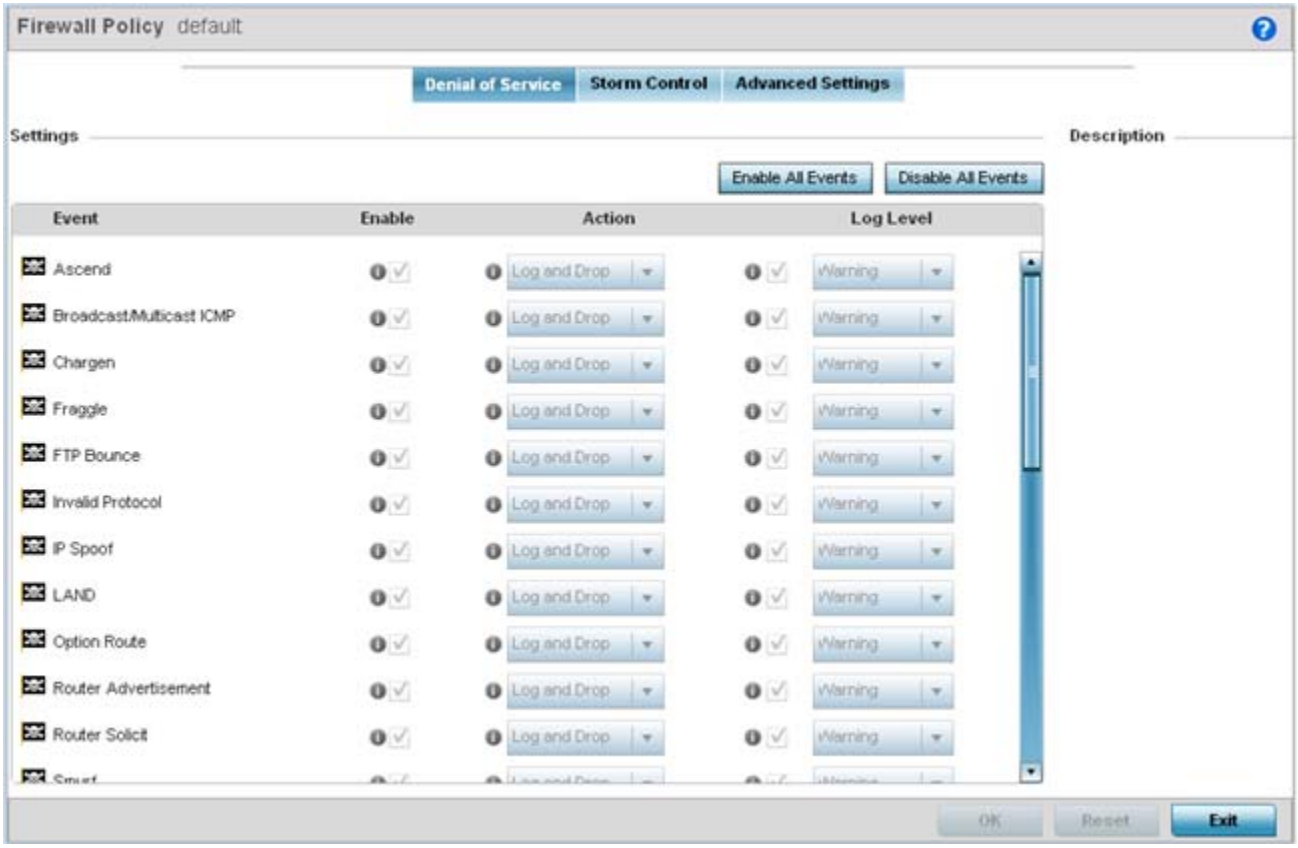


Figure 10-2 *Wireless Firewall Add/Edit Denial of Service screen*

2 The **Settings** window contains a list of all of the *Denial of Service* (DoS) attacks that the wireless controller's firewall has filters for. Each DoS filter contains the following four items:

Event	The *Event* column lists the name of each DoS attack.
Enable	Checking *Enable* box sets the Firewall Policy to filter the associated DoS attack based on the selection in the *Action* column.
Action	If a Denial of Service filter is enabled, chose an action from the drop-down menu to determine how the Firewall Policy treats the associated DoS attack. *Log and Drop* - An entry for the associated DoS attack is added to the log and then the packets are dropped. *Log Only* - An entry for the associated DoS attack is added to the log. No further action is taken. *Drop Only* - The DoS packets is dropped. No further action is taken.
Log Level	To enable logging to the system log, check the box in the *Log Level* column. Then select a standard *Syslog* level from the Log Level drop-down menu.

Denial of Service Event Attacks Table

3 Refer to the following for a summary of each Denial of Service attack the firewall can filter.

Ascend	4 The Ascend DoS attacks are a series of attacks that target known vulnerabilities in various versions of Ascend routers.
Broadcast/Multicast ICMP	Broadcast or Multicast ICMP DoS attacks are a series of attacks that take advantage of ICMP behavior in response to echo replies. These usually involve spoofing the source address of the target and sending ICMP broadcast or multicast echo requests to the rest of the network and in the process flooding the target machine with replies.
Chargen	The *Chargen* attack establishes a Telnet connection to port 19 and attempts to use the character generator service to create a string of characters which is then directed to the DNS service on port 53 to disrupt DNS services.
Fraggle	The Fraggle DoS attack uses a list of broadcast addresses to send spoofed UDP packets to each broadcast address' echo port (port 7). Each of those addresses that have port 7 open will respond to the request generating a lot of traffic on the network. For those that do not have port 7 open they will send an unreachable message back to the originator, further clogging the network with more traffic.
FTP Bounce	The FTP Bounce DoS attack uses a vulnerability in the FTP "PORT" command as a way to scan ports on a target machine by using another machine in the middle.
Invalid Protocol	Attackers may use vulnerability in the endpoint implementation by sending invalid protocol fields, or may misuse the misinterpretation of endpoint software. This can lead to inadvertent leakage of sensitive network topology information, call hijacking, or a DoS attack.
IP Spoof	IP Spoof is a category of DoS attack that sends IP packets with forged source addresses. This can hide the identity of the attacker.
LAND	The LAND DoS attack sends spoofed packets containing the SYN flag to the target destination using the target port and IP address as both the source and destination. This will either crash the target system or result in high resource utilization slowing down all other processes.
Option Route	Enables the IP Option Route denial of service check in the firewall.
Router Advertisement	In this attack, the attacker uses ICMP to redirect the network router function to some other host. If that host can not provide router services, a DoS of network communications occurs as routing stops. This can also be modified to single out a specific system, so that only that system is subject to attack (because only that system sees the 'false' router). By providing router services from a compromised host, the attacker can also place themselves in a *man-in-the-middle* situation and take control of any open channel at will (as mentioned earlier, this is often used with TCP packet forgery and spoofing to intercept and change open TELNET sessions).

Router Solicit	The ICMP Router Solicitation scan is used to actively find routers on a network. Of course, a hacker could set up a protocol analyzer to detect routers as they broadcast routing information on the network. In some instances, however, routers may not send updates. For example, if the local network does not have other routers, the router may be configured to not send routing information packets onto the local network. ICMP offers a method for router discovery. Clients send ICMP router solicitation multicasts onto the network, and routers must respond (as defined in RFC 1122). By sending ICMP router solicitation packets (ICMP type 9) on the network and listening for ICMP router discovery replies (ICMP type 10), hackers can build a list of all of the routers that exist on a network segment. Hackers often use this scan to locate routers that do not reply to ICMP echo requests.
Smurf	The Smurf DoS Attack sends ICMP echo requests to a list of broadcast addresses in a row, and then repeats the requests, thus flooding the network.
Snork	The Snork DoS attack uses UDP packet broadcasts to consume network and system resources.
TCP Bad Sequence	Enables a TCP Bad Sequence denial of service check in the firewall.
TCP FIN Scan	Hackers use the TCP FIN scan to identify listening TCP port numbers based on how the target device reacts to a transaction close request for a TCP port (even though no connection may exist before these close requests are made). This type of scan can get through basic firewalls and boundary routers that filter on incoming TCP packets with the *Finish* (FIN) and ACK flag combination. The TCP packets used in this scan include only the TCP FIN flag setting. If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target device discards the FIN and sends no reply.

TCP Intercept	A SYN-flooding attack occurs when a hacker floods a server with a barrage of requests for connection. Because these messages have unreachable return addresses, the connections cannot be established. The resulting volume of unresolved open connections eventually overwhelms the server and can cause it to deny service to valid requests, thereby preventing legitimate users from connecting to a Web site, accessing email, using FTP service, and so on. The TCP intercept feature helps prevent SYN-flooding attacks by intercepting and validating TCP connection requests. In intercept mode, the TCP intercept software intercepts TCP *synchronization* (SYN) packets from clients to servers that match an extended access list. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and knits the two half-connections together transparently. Thus, connection attempts from unreachable hosts will never reach the server. The software continues to intercept and forward packets throughout the duration of the connection. The number of SYNs per second and the number of concurrent connections proxied depends on the platform, memory, processor, and other factors. In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests. When establishing a security policy using TCP intercept, you can choose to intercept all requests or only those coming from specific networks or destined for specific servers. You can also configure the connection rate and threshold of outstanding connections. Optionally operate TCP intercept in watch mode, as opposed to intercept mode. In watch mode, the software passively watches the connection requests flowing through the router. If a connection fails to get established in a configurable interval, the software intervenes and terminates the connection attempt.
TCP IP TTL Zero	The TCP IP TTL Zero DoS attack sends spoofed multicast packets onto the network which have a *Time To Live* (TTL) of 0. This causes packets to loop back to the spoofed originating machine, and can cause the network to overload.
TCP Null Scan	Hackers use the TCP NULL scan to identify listening TCP ports. This scan also uses a series of strangely configured TCP packets, which contain a sequence number of 0 and no flags. Again, this type of scan can get through some firewalls and boundary routers that filter incoming TCP packets with standard flag settings. If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target discards the TCP NULL scan, sending no reply.
TCP Post SYN	A remote attacker may be attempting to avoid detection by sending a SYN frame with a different sequence number than the original SYN. This can cause an *Intrusion Detection Syste*m (IDS) to become unsynchronized with the data in a connection. Subsequent frames sent during the connection are ignored by the IDS.

TCP Packet Sequence	An attempt to predict the sequence number used to identify packets in a TCP connection, which can be used to counterfeit packets. The attacker hopes to correctly guess the sequence number used by the sending host. If successful, they can send counterfeit packets to the receiving host which will seem to originate from the sending host, even though the counterfeit packets may originate from some third host controlled by the attacker.
TCP XMAS Scan	The TCP XMAS Scan floods the target system with TCP packets including the FIN, URG, and PUSH flags. This is used to determine details about the target system and can crash a system.
TCP Header Fragment	Enables the TCP Header Fragment denial of service check in the firewall.
Twinge	The Twinge DoS attack sends ICMP packets and cycles through using all ICMP types and codes. This can crash some Windows systems.
UDP Short Header	Enables the UDP Short Header denial of service check in the firewall.
WINNUKE	The WINNUKE DoS attack sends a large amount of data to UDP port 137 to crash the NETBIOS service on windows and can also result on high CPU utilization on the target machine.
Hop Limit Zero	Hop limits within IPv6 packets is set to 0 preventing hops as needed.
Multicast ICMPv6	ICMPv6 packets contain multicast L2 DMACs.
TCP Intercept Mobility	Detect IPv6 TCP packet with mobility option *home address option* (HAO) or *route header* (RO) type one set and do not generate syn cookies for such packets.

5 Events can be individually enabled or collectively enabled/disabled using the **Enable All Events** and **Disable All Events** buttons.

6 Select **OK** to update the Denial of Service settings. Select **Reset** to revert to the last saved configuration.

10.1.1.1.2 Firewall Policy Storm Control

Adding and Editing Wireless Firewall Policies

The firewall maintains a facility to control packet storms. Storms are packet bombardments that exceed the high threshold value configured for an interface. During a storm, packets are throttled until the rate falls below the configured rate, severely impacting performance for the RF Domain manager interface. Thresholds are configured in terms of packets per second.

To define a storm control configuration for a Firewall policy:

1 Select the **Storm Control** tab from the **Firewall Policy** configuration page.

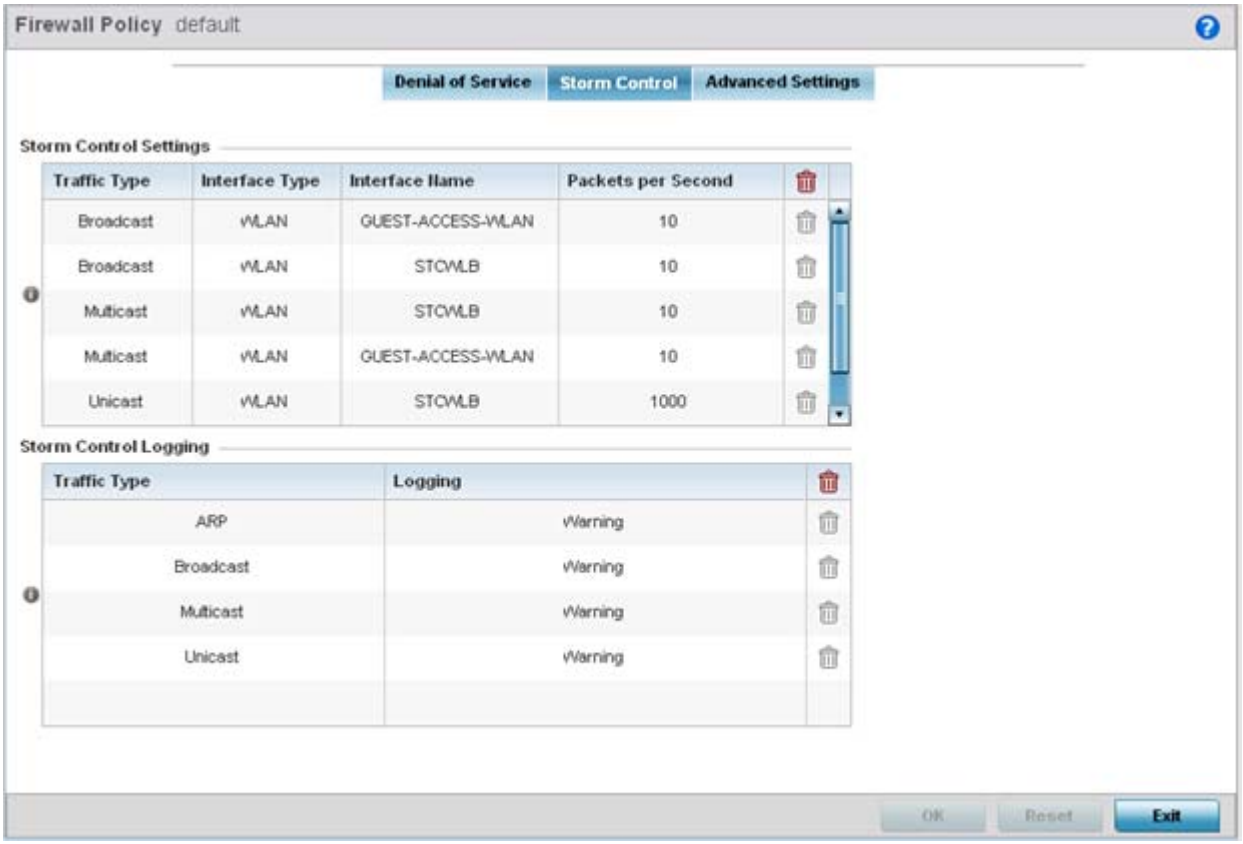


Figure 10-3 *Wireless Firewall Add/Edit Storm Control screen*

2 Refer to the **Storm Control Settings** field to set the following:

Traffic Type	Use the drop-down menu to define the traffic type for which the Storm Control configuration applies. Options include *ARP*, *Broadcast*, *Multicast* and *Unicast*.
Interface Type	Use the drop-down menu to define the interface for which the Storm Control configuration is applied. Only the specified interface uses the defined filtering criteria. Options include *Ethernet*, *WLAN* and *Port Channel*.
Interface Name	Use the drop-down menu to refine the interface selection to a specific WLAN or physical port. This helps with threshold configuration for potentially impacted interfaces.
Packets per Second	Select the check box to activate the spinner control used for specifying the packets per second threshold for activating the Storm Control mechanism.

3 Select **+ Add Row** as needed to add additional Storm Control configurations for other traffic types or interfaces. Select the **Delete** icon as required to remove selected rows.

4 Refer to the **Storm Control Logging** field to define how storm events are logged.

Traffic Type	Use the drop-down menu to define the traffic type for which the Storm Control logging configuration applies. Options include *ARP*, *Broadcast*, *Multicast* and *Unicast*.

Logging	Select the check box to activate the spinner control used for specifying the standard log level used if a Storm Control attack is detected. The default log level is Warning.

5 Select **+ Add Row** as needed to add additional Storm Control log entries for other interfaces. Select the **Delete** icon as required to remove selected rows.

6 Select **OK** to update the Storm Control settings. Select **Reset** to revert to the last saved configuration.

10.1.1.1.3 Firewall Policy Advanced Settings

Adding and Editing Wireless Firewall Policies

To define a firewall policy Advanced Configuration:

1 Select the **Advanced Settings** tab from the **Firewall Policy** configuration page.

The Advanced Settings screen displays **Common** and **IPv6 Settings** tabs with the Common displayed by default. Use these screens to define common IPv4 settings and settings unique to an IPv6 firewall.

IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the *neighbor discovery* (ND) protocol via ICMPv6 router discovery messages. These hosts require firewall packet protection unique to IPv6 traffic, as IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters.

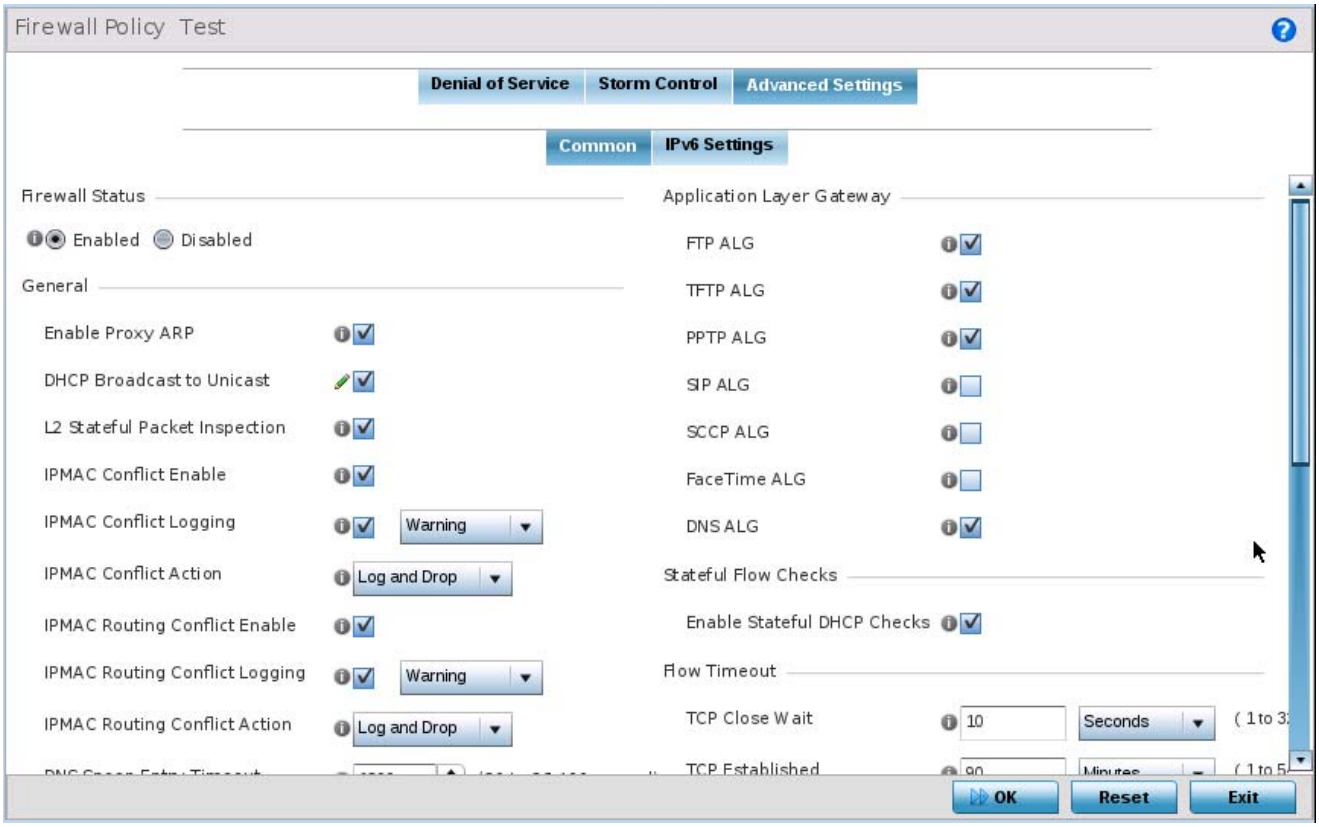


Figure 10-4 *Wireless Firewall Add/Edit Advanced Common Settings screen*

2 Refer to the **Firewall Status** radio buttons to define the firewall as either *Enabled* or *Disabled*. The firewall is enabled by default.

If disabling the firewall, a confirmation prompt displays stating NAT, wireless hotspot, proxy ARP, deny-static-wireless-client and deny-wireless-client sending not permitted traffic excessively will be disabled.

3 Refer to the **General** field to enable or disable the following firewall configuration parameters:

Enable Proxy ARP	Select this check box to allow the Firewall Policy to use Proxy ARP responses for this policy on behalf of another device. Proxy ARP allows the firewall to handle ARP routing requests for devices behind the firewall. This feature is enabled by default.
DHCP Broadcast to Unicast	Select this check box to enable the conversion of broadcast DHCP offers to unicast. Converting DHCP broadcast traffic to unicast traffic can help reduce network traffic loads. This feature is disabled by default.
L2 Stateful Packet Inspection	Select the check box to enable stateful packet inspection for RF Domain manager routed interfaces within the Layer 2 firewall. This feature is disabled by default.
IPMAC Conflict Enable	When multiple devices on the network have the same IP or MAC address this can create routing issues for traffic being passed through the firewall. To avoid these issues, enable Conflict Detection to enable IP and MAC conflict detection. This feature is disabled by default.
IPMAC Conflict Logging	Select this option to enable logging for IP and MAC address conflict detection. This feature is disabled by default.
IPMAC Conflict Action	Use the drop-down menu to set the action taken when an attack is detected. Options include *Log Only*, *Drop Only* or *Log and Drop*. The default setting is Log and Drop.
IPMAC Routing Conflict Enable	Select this option to enable IPMAC Routing Conflict detection. This is also known as a Hole-196 attack in the network. This feature helps to detect if the client is sending routed packets to the correct router-mac-address.
IPMAC Routing Conflict Logging	Select enable logging for IPMAC Routing Conflict detection. This feature is disabled by default.
IPMAC Routing Conflict Action	Use the drop-down menu to set the action taken when an attack is detected. Options include *Log Only*, *Drop Only* or *Log* and *Drop*. The default setting is Log and Drop.
DNS Snoop Entry Timeout	Select this option and set a timeout, in seconds, for DNS Snoop Entry. DNS Snoop Entry stores information such as Client to IP Address and Client to Default Gateway(s) and uses this information to detect if the client is sending routed packets to a wrong MAC address.
IP TCP Adjust MSS	Select this option and adjust the value for the *maximum segment size* (MSS) for TCP segments on the router. Set a value between 472 bytes and 1,460 bytes to adjust the MSS segment size. The default value is 472 bytes.
TCP MSS Clamping	Select this option to enable TCP MSS Clamping. TCP MSS Clamping allows for the configuration of the maximum segment size of packets at a global level.
Max Fragments/ Datagram	Set a value for the maximum number of fragments (between 2 and 8,129) allowed in a datagram before it is dropped. The default value is 140 fragments.
Max Defragmentations/ Host	Set a value for the maximum number of defragmentations, between 1 and 16,384 allowed per host before it is dropped. The default value is 8.

Min Length Required	Select this option and set a minimum length, between 8 bytes and 1,500 bytes, to enforce a minimum packet size before being subject to fragment based attack prevention.
Virtual Defragmentation	Select this option to enable IPv4 and IPv6 virtual defragmentation to help prevent fragment based attacks, such as tiny fragments or large number of fragments.
Virtual Defragmentation Timeout	Set a virtual defragmentation timeout from 1- 60 seconds applicable to both IPv4 and IPv6 packets.

4 Refer to the **Firewall Enhanced Logging** field to set the following parameters:

Log Dropped ICMP Packets	Use the drop-down menu to define how dropped ICMP packets are logged. Logging can be rate limited for one log instance every 20 seconds. Options include *Rate Limited*, *All* or *None*. The default setting is None.
Log Dropped Malformed Packets	Use the drop-down menu to define how dropped malformed packets are logged. Logging can be rate limited for one log instance every 20 seconds. Options include *Rate Limited*, *All* or *None*. The default setting is None.
Enable Verbose Logging	Check this box to enable verbose logging mode for the firewall.

5 The firewall policy allows traffic filtering at the application layer using the **Application Layer Gateway** feature. The Application Layer Gateway provides filters for the following common protocols

FTP ALG	Select this option to allow FTP traffic through the firewall using its default ports. This feature is enabled by default.
TFTP ALG	Select this option to allow TFTP traffic through the firewall using its default ports. This feature is enabled by default.
PPTP ALG	Select this option to allow PPTP traffic through the firewall using its default ports. The *Point-to-Point Tunneling Protocol* (PPTP) is a network protocol that enables the secure transfer of data from a remote client to an enterprise server by creating a VPN across TCP/IP-based data networks. PPTP encapsulates PPP packets into IP datagrams for transmission over the Internet or other public TCP/IP-based networks. This feature is enabled by default.
SIP ALG	Select this option to allow SIP traffic through the firewall using its default ports. This feature is enabled by default.
SCCP ALG	Select this option to allow SCCP traffic through the firewall using its default ports. This feature is enabled by default.
Facetime ALG	Select this option to allow FaceTime traffic through the firewall using its default ports. This feature is enabled by default.
DNS ALG	Enable this option to allow DNS traffic through the firewall using its default ports. This feature is enabled by default.

6 Select the **Enable Stateful DHCP Checks** check box to enable the stateful checks of DHCP packet traffic through the firewall. The default setting is enabled. When enabled, all DHCP traffic flows are inspected.

7 Define **Flow Timeout** intervals for the following flow types impacting the Firewall:

TCP Close Wait	Define a flow timeout value in either *Seconds* (1 - 32,400), *Minutes* (1 - 540) or *Hours* (1 - 9). The default setting is 10 seconds.

TCP Established	Define a flow timeout value in either *Seconds* (1 - 32,400), *Minutes* (1 - 540) or *Hours* (1 - 9). The default setting is 90 minutes.
TCP Reset	Define a flow timeout value in either *Seconds* (1 - 32,400), *Minutes* (1 - 540) or *Hours* (1 - 9). The default setting is 10 seconds.
TCP Setup	Define a flow timeout value in either *Seconds* (1 - 32,400), *Minutes* (1 - 540) or *Hours* (1 - 9). The default setting is 10 seconds.
Stateless TCP Flow	Define a flow timeout value in either *Seconds* (1 - 32,400), *Minutes* (1 - 540) or *Hours* (1 - 9). The default setting is 90 seconds.
Stateless FIN/ RESET Flow	Define a flow timeout value in either *Seconds* (1 - 32,400), *Minutes* (1 - 540) or *Hours* (1 - 9). The default setting is 10 seconds.
ICMP	Define a flow timeout value in either *Seconds* (1 - 32,400), *Minutes* (1 - 540) or *Hours* (1 - 9). The default setting is 30 seconds.
UDP	Define a flow timeout value in either *Seconds* (1 - 32,400), *Minutes* (1 - 540) or *Hours* (1 - 9). The default setting is 30 seconds.
Any Other Flow	Define a flow timeout value in either *Seconds* (1 - 32,400), *Minutes* (1 - 540) or *Hours* (1 - 9). The default setting is 30 seconds.

8 Refer to the **TCP Protocol Checks** field to set the following parameters:

Check TCP states where a SYN packet tears down the flow	Select the check box to allow a SYN packet to delete an old flow in TCP_FIN_FIN_STATE and TCP_CLOSED_STATE and create a new flow. The default setting is enabled.
Check unnecessary resends of TCP packets	Select the check box to enable the checking of unnecessary resends of TCP packets. The default setting is enabled.
Check Sequence Number in ICMP Unreachable error packets	Select the check box to enable sequence number checks in ICMP unreachable error packets when an established TCP flow is aborted. The default setting is enabled.
Check Acknowledgment Number in RST packets	Select the check box to enable the checking of the acknowledgment number in RST packets which aborts a TCP flow in the SYN state. The default setting is enabled.
Check Sequence Number in RST packets	Select the check box to check the sequence number in RST packets which abort an established TCP flow. The default setting is enabled.

9 Select **OK** to update the firewall policy's advanced common settings. Select **Reset** to revert to the last saved configuration.

10 Select the **IPv6 Settings** tab.

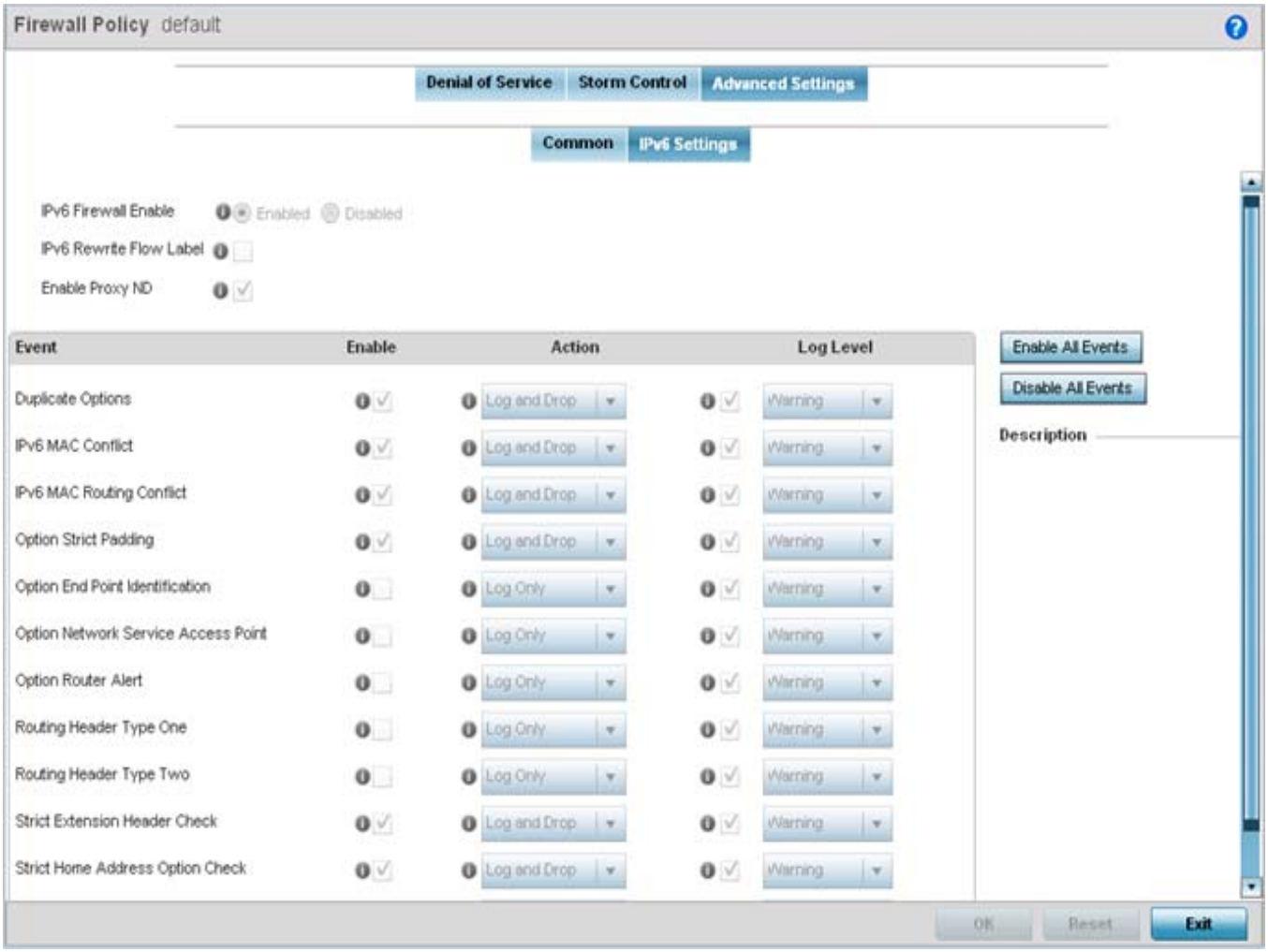


Figure 10-5 *Wireless Firewall Add/Edit Advanced IPv6 Settings screen*

11 Refer to the **IPv6 Firewall Enable** option to provide firewall support to IPv6 packet streams. This setting is enabled by default. Disabling IPv6 firewall support also disables proxy neighbor discovery.

IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the *neighbor discovery* (ND) protocol via ICMPv6 router discovery messages. These hosts require firewall packet protection unique to IPv6 traffic, as IPv6 addresses are composed uniquely of eight groups of four hexadecimal digits separated by colons.

12 Select **IPv6 Rewrite Flow Label** to provide flow label rewrites for each IPv6 packet. A flow is a sequence of packets from a particular source to a particular (unicast or multicast) destination. The flow label helps keep packet streams from looking like one massive flow. Flow label rewrites are disabled by default and must be manually enabled.

Flow label re-writes enable the re-classification of packets belonging to a specific flow. The flow label does nothing to eliminate the need for packet filtering. This setting is disabled by default.

13 Select **Enable Proxy ND** to generate neighbor discovery responses on behalf of another controller, service platform or Access Point managed device. When enabled, any IPv6 packet received on an interface is parsed to see whether it is known to be a neighbor solicitation. This setting is enabled by default.

14 Use the **Event** table to enable individual IPv6 unique events. IPv6 events can be individually enabled or collectively enabled/disabled using the **Enable All Events** and **Disable All Events** buttons. The **Description** area displays a brief description of the selected event.

Event	The *Event* column lists the name of each IPv6 specific event subject to logging.
Enable	Checking *Enable* sets the firewall policy to filter the associated IPv6 event based on the selection in the *Action* column.
Action	If a filter is enabled, choose an action from the drop-down menu to determine how the firewall treats the associated IPv6 event. *Log and Drop* - An entry for the associated IPv6 event is added to the log and then the packets are dropped. *Log Only* - An entry for the associated IPv6 event is added to the log. No further action is taken. *Drop Only* - The packet is dropped. No further action is taken.
Log Level	To enable logging to the system log, check the box in the *Log Level* column. Then select a standard *Syslog* level from the Log Level drop-down menu.

15 Select **OK** to update the firewall policy's advanced IPv6 settings. Select **Reset** to revert to the last saved configuration.

10.1.2 Configuring MAC Firewall Rules

Wireless Firewall

Use MAC based firewalls like *Access Control Lists* (ACLs) to filter/mark packets based on the IP from which they arrive, as opposed to filtering packets on Layer 2 ports.

Optionally filter Layer 2 traffic on a physical Layer 2 interface using MAC addresses. A MAC firewall rule uses *source* and *destination* MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to packet traffic.

NOTE: Once defined, a set of MAC firewall rules must be applied to an interface to be a functional filtering tool.

To add or edit a MAC based Firewall Rule policy:

1 Select **Configuration** > **Security** > **Wireless Firewall** > **MAC Firewall Rules** to display existing IP Firewall Rule policies.

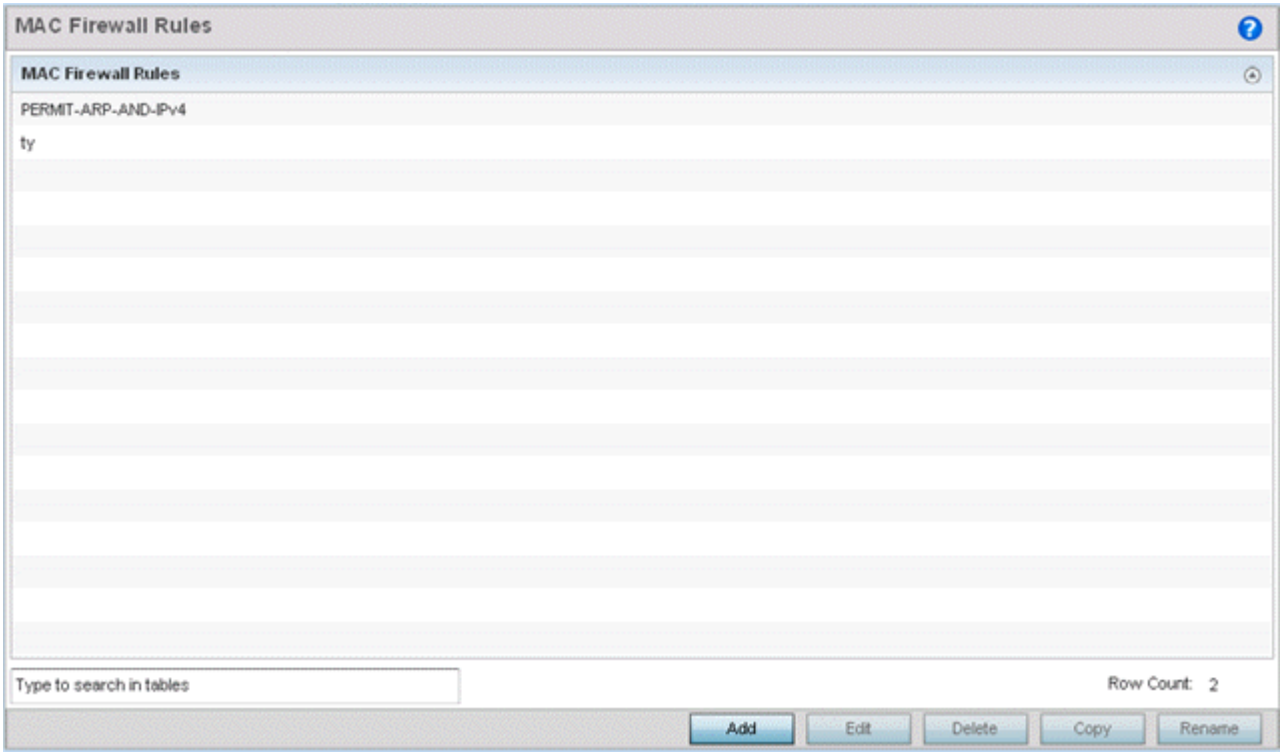


Figure 10-6 *MAC Firewall Rules screen*

2 Select **+ Add Row** to create a new MAC Firewall Rule. Select an existing policy and click **Edit** to modify the attributes of that rule's configuration.

3 Select the added row to expand it into configurable parameters for defining the MAC based firewall rule.

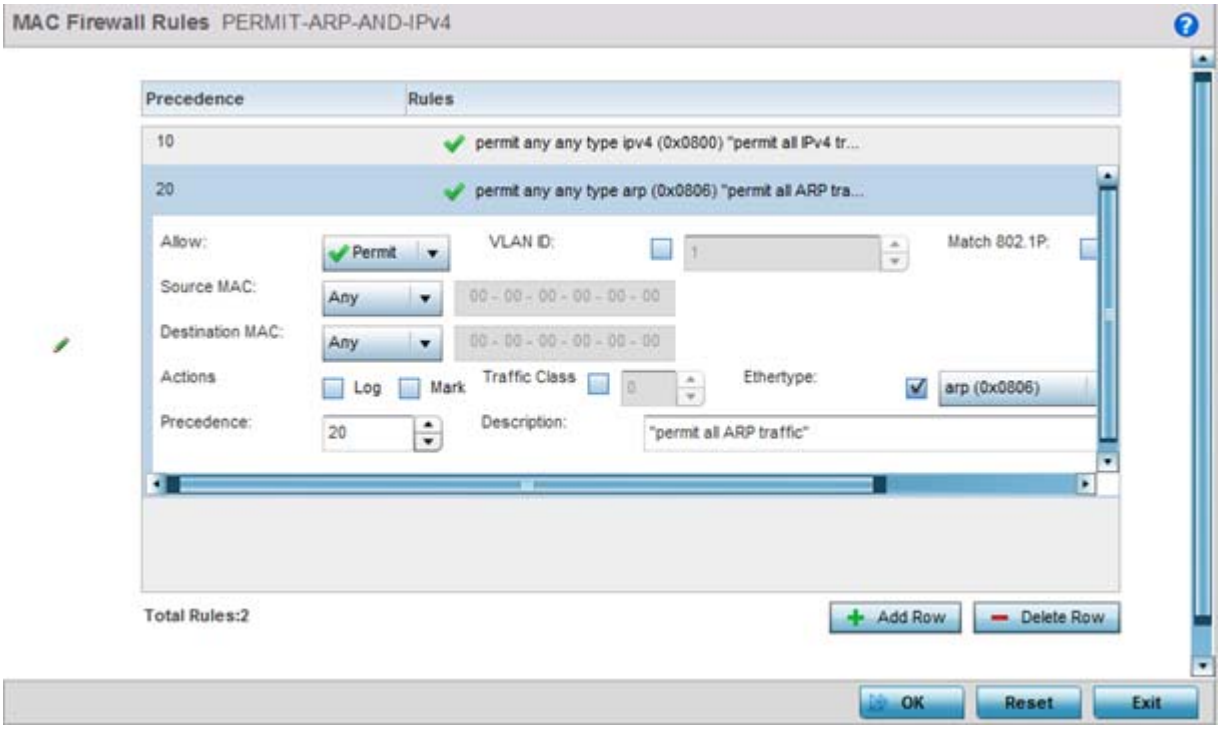


Figure 10-7 *MAC Firewall Rules Add/Edit screen*

4 If adding a new **MAC Firewall Rule,** provide a name up to 32 characters to help describe its filtering configuration.

5 Select a rule to modify it. Set the following parameters for the MAC firewall rule:

Allow	Every MAC firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported: *Deny* - Instructs the firewall to prevent a packet from proceeding to its destination when filter conditions are met. *Permit* - Instructs the firewall to allow a packet to proceed to its destination when filter conditions are met.
VLAN ID	Enter a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the local RADIUS server). The VLAN ID can be between 1 and 4094.
Match 802.1P	Configures IP DSCP to 802.1p priority mapping for untagged frames. Use the spinner control to define a setting between 0 - 7.
Source and Destination MAC	Enter both *Source* and *Destination* MAC addresses. The source IP address and destination MAC address are used as basic matching criteria. Provide a subnet mask if using a mask.

Action	The following actions are supported: *Log* - Events are logged for archive and analysis. *Mark* - Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit. - VLAN 802.1p priority. - DSCP bits in the IP header. - TOS bits in the IP header. *Mark, Log* - Conducts both mark and log functions.
Traffic Class	Select this option to enable a spinner control for traffic class prioritization. Devices that originate a packet must identify a class or priority for packets. Devices use the traffic class field in the MAC header to set this priority.
Ethertype	Use the drop-down menu to specify an Ethertype of either *ipv6*, *arp*, *wisp*, or *monitor 8021q*. An EtherType is a two-octet field within an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet frame.
Precedence	Use the spinner control to specify a precedence for this MAC firewall rule between 1 - 1500. Rules with lower precedence are always applied first to packets.
Description	Provide a description (up to 64 characters) for the rule to help differentiate the it from others with similar configurations.

6 Select **+ Add Row** as needed to add additional MAC firewall Rule configurations. Select the **- Delete Row** icon as required to remove selected MAC firewall Rules.

7 Select EX3500 **MAC ACL** tab to define MAC firewall rules specific to the EX3500 switch. Select the added row to expand it into configurable parameters for defining the MAC based firewall rule for this model switch.

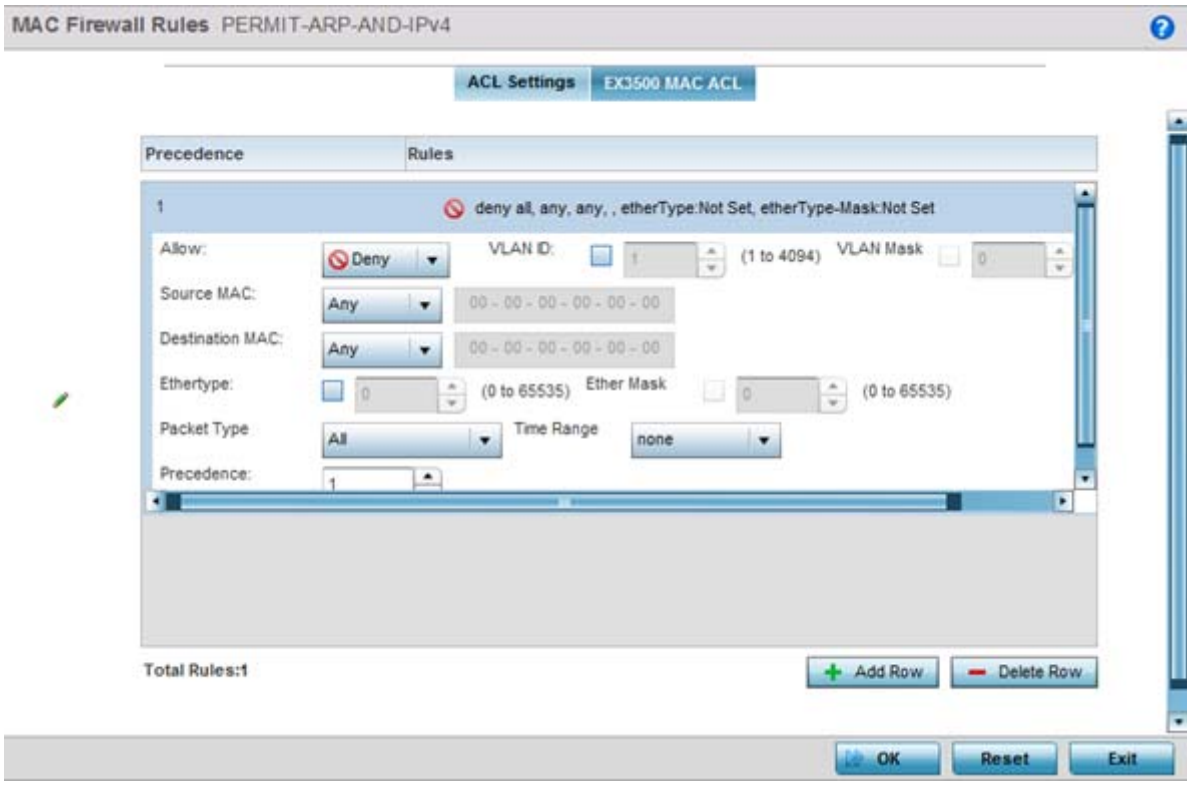


Figure 10-8 *EX3500 MAC ACL Add/Edit screen*

8 Select a rule to modify it. Define the following parameters for the MAC firewall rule:

Allow	Every EX3500 MAC ACL firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported: *Deny* - Instructs the firewall to prevent a packet from proceeding to its destination. *Permit* - Instructs the firewall to allow a packet to proceed to its destination.
VLAN ID	Enter a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the local RADIUS server). The VLAN ID can be between 1 and 4094.
VLAN Mask	Enter a VLAN ID bit mask value.
Source and Destination MAC	Enter both *Source* and *Destination* MAC addresses. The source MAC address and destination MAC address are used as basic matching criteria. Provide a subnet mask if using a mask.
Ethertype	Use the spinner control to specify an Ethertype. An EtherType is a two-octet field within an Ethernet frame. It is used to indicate which protocol is encapsulated in the payload of an Ethernet frame. Select a value in the range 0 - 65535. This field is enabled by default. The default value is 1.
Ethertype Mask	Use the spinner control to specify the Ethertype Mask. Select a value in the range 0 - 65535. This field is enabled by default. The default value is 1.
Packet Type	Use the drop-down menu to select the packet type. Packet type can be one of *all*, *tagged-eth2* or *untagged-eth2*

Time Range	Use this field to select a time range when this ACL will be enabled. For more information, see *EX3500 Time Range on page 10-64*.
Precedence	Use the spinner control to specify a precedence for this MAC firewall rule between 1 - 1500. Rules with lower precedence are always applied first to packets.

9 Select **OK** when completed to update the MAC firewall Rules. Select **Reset** to revert the screen to its last saved configuration.

10.1.3 Firewall Deployment Considerations

Configuring a Firewall Policy

Before defining a firewall configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Firewalls implement access control policies, so if you don't have an idea of what kind of access to allow or deny, a firewall is of little value.
- It's important to recognize the firewall's configuration is a mechanism for enforcing a network access policy.
- A role based firewall requires an advanced security license to apply inbound and outbound firewall policies to users and devices
- Firewalls cannot protect against tunneling over application protocols to poorly secured wireless clients.
- Firewalls should be deployed on WLANs implementing weak encryption to minimize access to trusted networks and hosts in the event the WLAN is compromised.
- Firewalls should be enabled when providing managed Hotspot guest access. Firewall policies should be applied to Hotspot enabled WLANs to prevent guest user traffic from being routed to trusted networks and hosts.

10.2 Configuring IP Firewall Rules

Wireless Firewall

IP based firewalls function like *Access Control Lists* (ACLs) to filter/mark packets, as opposed to filtering packets on layer 2 ports. IP firewalls implement uniquely defined access control policies, so if you don't have an idea of what kind of access to *allow* or *deny*, a firewall is of little value, and could provide a false sense of network security.

IP based firewall rules are specific to source and destination IP addresses and the unique *rules* and *precedence* orders assigned. Both IP and non-IP traffic on the same Layer 2 interface can be filtered by applying an IP ACL. Firewall rules are processed by a firewall supported device from first to last. When a rule matches the network traffic a controller or service platform is processing, the firewall uses that rule's action to determine whether traffic is allowed or denied.

NOTE: Once defined, a set of IP Firewall rules must be applied to an interface to be a functional filtering tool.

There are separate policy creation mechanisms for IPv4 and IPv6 traffic. With either IPv4 or IPv6, create access rules for traffic entering a controller, service platform or Access Point interface, because if you are going to deny specific types of packets, it's recommended you do it before the controller, service platform or Access Point spends time processing them, since access rules are processed before other types of firewall rules.

IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

For more information, see:

- *Setting an IPv4 or IPv6 Firewall Policy*
- *Setting an IP SNMP ACL Policy*
- *Network Group Alias*
- *Network Service Alias*
- *EX3500 ACL Standard*
- *EX3500 ACL Extended*

10.2.1 Setting an IPv4 or IPv6 Firewall Policy

Before defining a firewall configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

1 Select **Configuration** > **Security** > **IP Firewall.**

2 Expand the **IP Firewall** menu item and select either the **IPv4 ACL** or **IPv6 ACL** menu options.
Either the **IPv4 Firewall Rules** or the **IPv6 Firewall Rules** screens display the existing polices defined thus far.

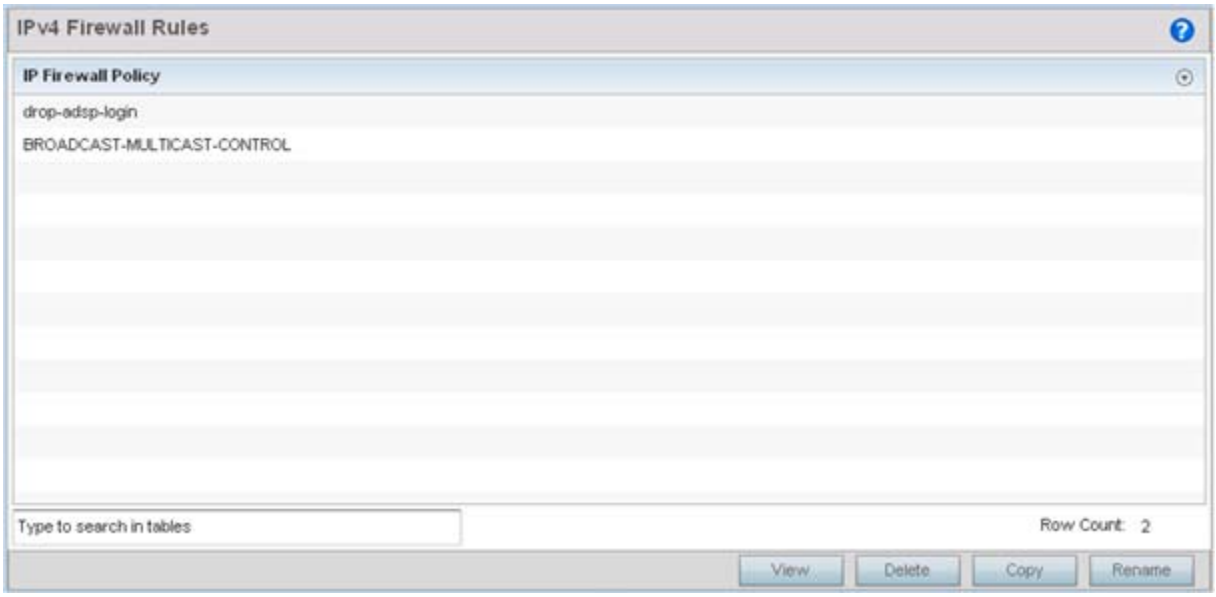


Figure 10-9 *IP Firewall Rules screen*

3 Select **Add** to create a new IPv4 or IPv6 firewall rule. Select an existing policy and click **Edit** to modify the attributes of that policy's configuration.

4 Select the added row to expand it into configurable parameters for defining the IPv4 or IPv6 based firewall policy.

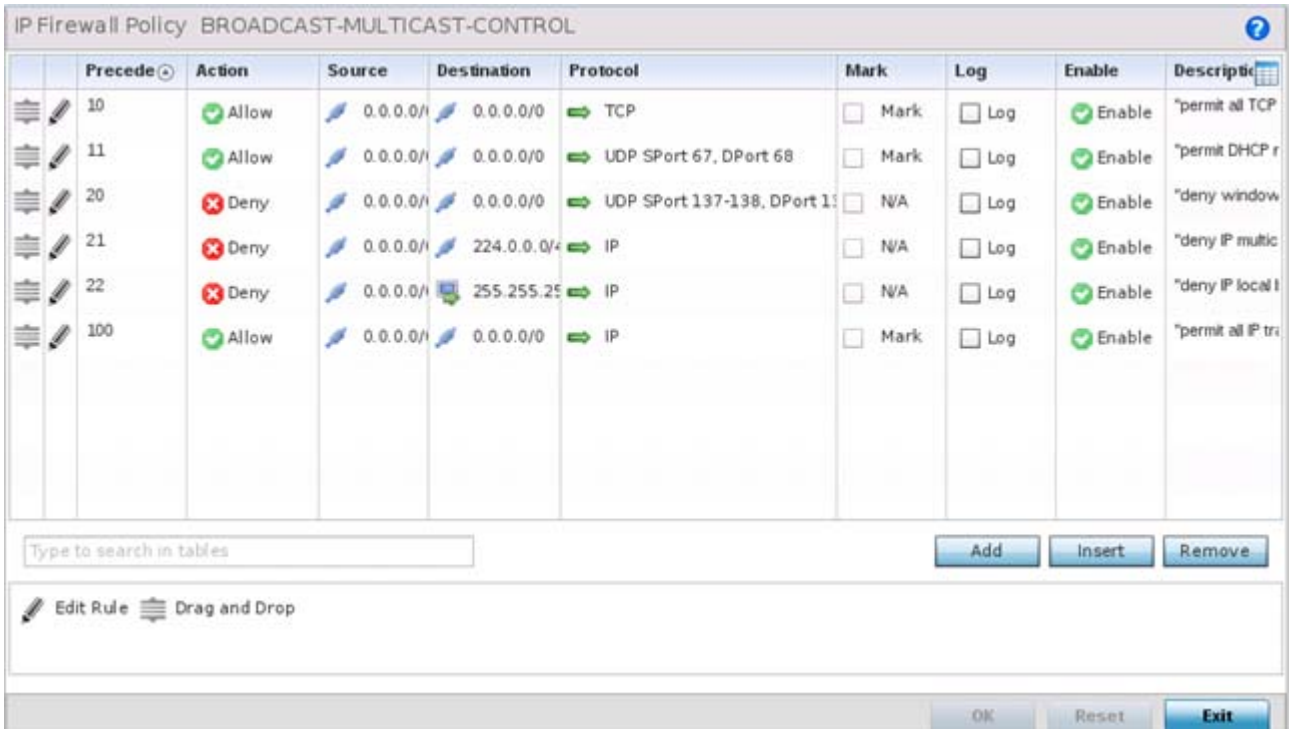


Figure 10-10 *IP v4 Firewall Rules Add screen*

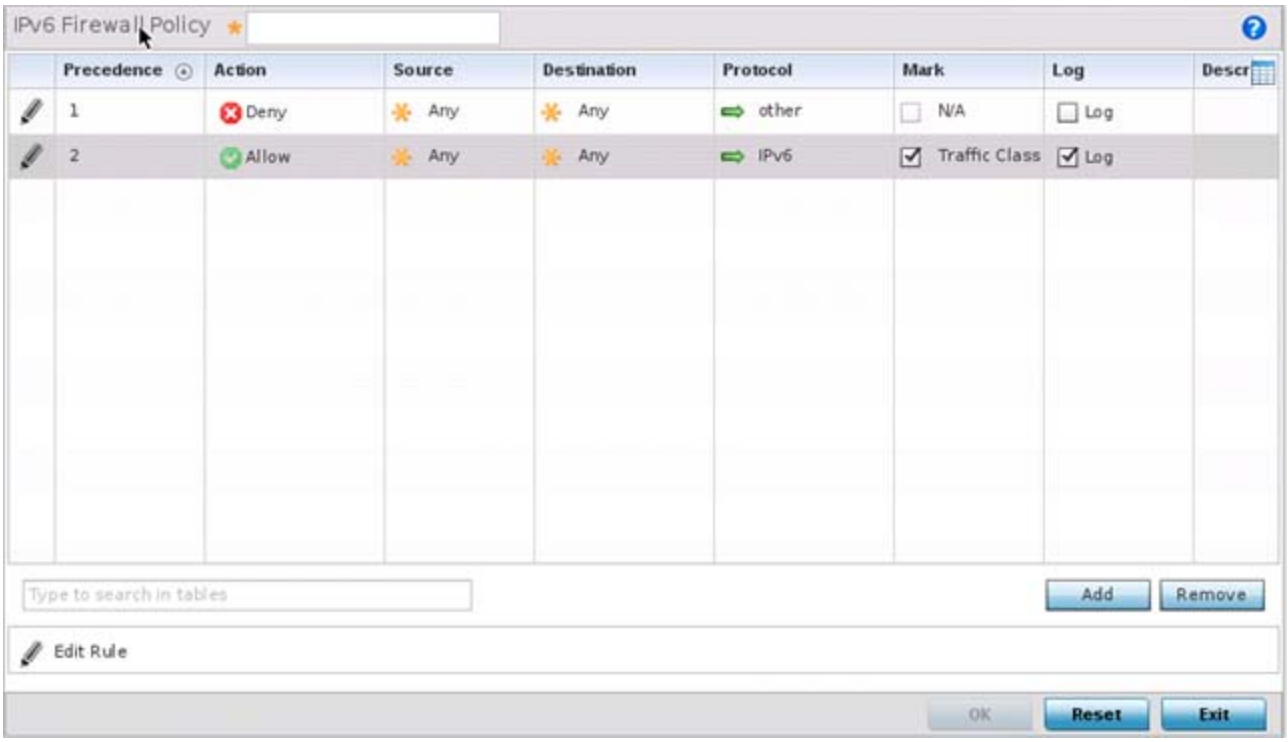


Figure 10-11 *IP v6 Firewall Rules Add screen*

IP firewall configurations can either be modified as a collective group of variables or selected and updated individually as their filtering attributes require a more refined update.

a. Select the **Edit Rule** icon to the left of a particular IP firewall rule configuration to update its parameters collectively.

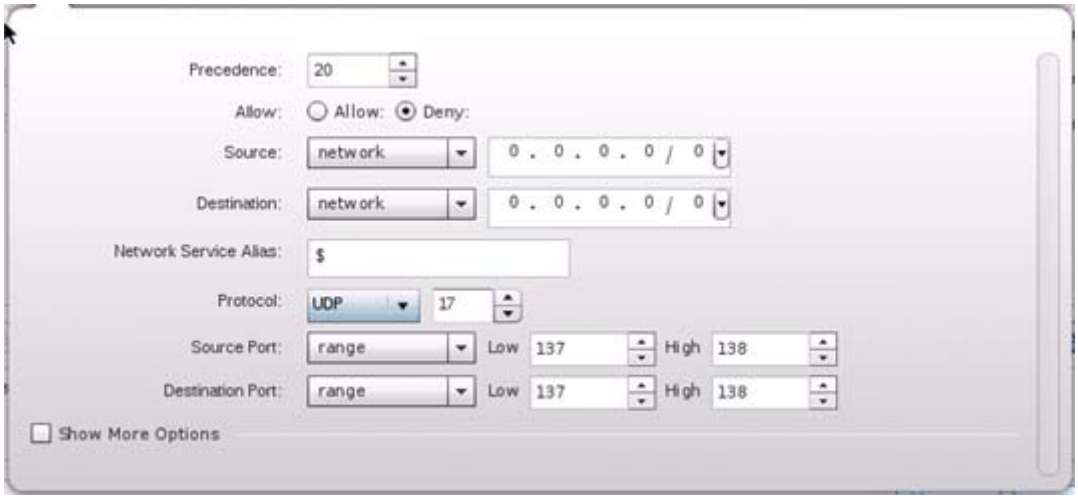


Figure 10-12 *IP Firewall Rules Add Criteria screen*

b. Click the icon within the **Description** column (top right-hand side of the screen) and select IP filter values as needed to add criteria into the configuration of the IP ACL.

Figure 10-13 *IP Firewall Rules Add Criteria screen*

NOTE: Only those selected IP ACL filter attributes display. Each value can have its current setting adjusted by selecting that IP ACL's column to display a pop-up to adjust that one value.

5 Define the following IP firewall rule settings as required:

Precedence	Specify or modify a precedence for this IP policy between 1-5000. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.
Action	Every IP Firewall rule is made up of matching criteria rules. The action defines the packet's disposition if it matches the specified criteria. The following actions are supported: *Deny* - Instructs the Firewall to restrict a packet from proceeding to its destination. *Permit* - Instructs the Firewall to allow a packet to proceed to its destination.
Source	Select the source IP address used as basic matching criteria for this IP ACL rule.

Destination	Determine whether filtered packet destinations for this IP firewall rule do not require any classification (*any*), are designated as a set of configurations consisting of protocol and port mappings (an *alias*), set as a numeric IP address (*host*) or defined as *network* IP and mask. Selecting alias requires a destination network group alias be available or created.
Protocol	Set a service alias as a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Set an alphanumeric service alias (beginning with a $) and include the protocol as relevant.
Mark	Select an IP Firewall rule's *Mark* checkbox to enable or disable event marking and set the rule's 8021p or dscp level (from 0 - 7).
Log	Select an IP Firewall rule's *Log* checkbox to enable or disable event logging for this rule's usage.
Enable	This option displays for IPv4 based firewalls only. Select an IPv4 firewall rule's *Enable* or *Disable* icon to determine this rule's inclusion with the IP firewall policy.
Description	Lists the administrator assigned description applied to the IP ACL rule. Select a description within the table to modify its character string as filtering changes warrant. Select the icon within the Description table header to launch a *Select Columns* screen used to add or remove IP ACL criteria from the table.

6 Select **Add** to add additional IP Firewall Rule configurations. Select **Remove** to remove selected IP Firewall Rules as they become obsolete for filtering network access permissions.

7 Select **OK** when completed to update the IP Firewall rules. Select **Reset** to revert the screen back to its last saved configuration.

10.2.2 Setting an IP SNMP ACL Policy

SNMP performs network management functions using a data structure called a *Management Information Base* (MIB). SNMP is widely implemented but not very secure, since it uses only text community strings for accessing controller or service platform configuration files.

Use SNMP ACLs to help reduce SNMP's vulnerabilities, as SNMP traffic can be exploited to produce a *denial of service* (DoS).

To create an IP SNMP ACL:

1 Select **Configuration** > **Security** > **IP Firewall.**

2 Expand the **IP Firewall** menu item and select **IP SNMP ACL**.

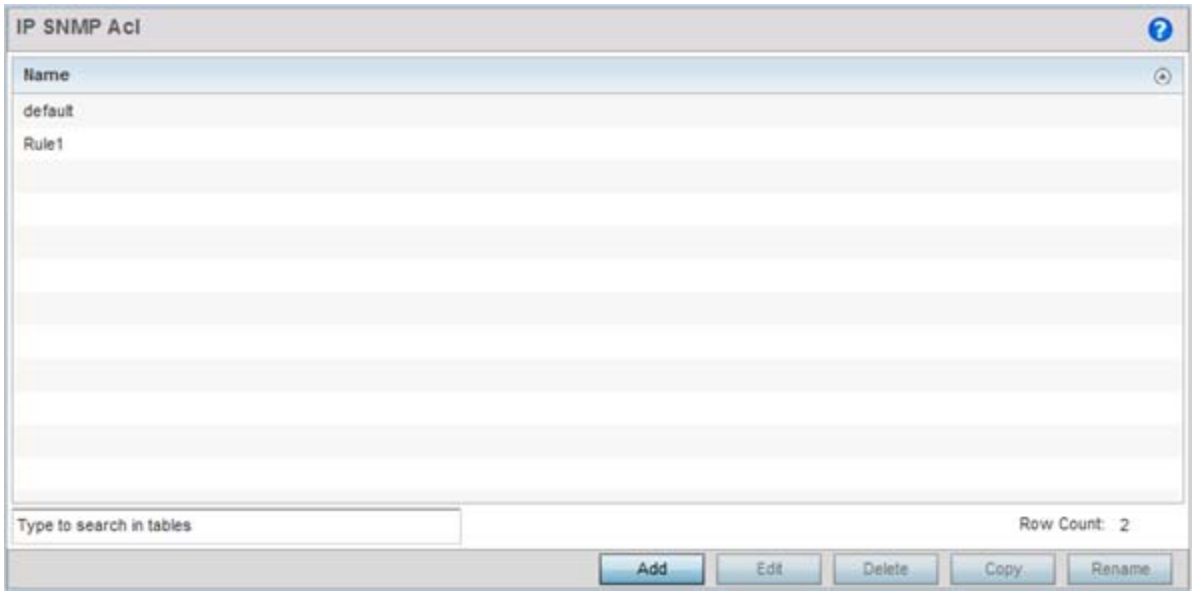


Figure 10-14 *IP Firewall Rules screen*

3 Select **Add** to create a new SNMP firewall rule. Select an existing policy and click **Edit** to modify the attributes of that policy's configuration. Existing policies can be removed by highlighting them and selecting **Delete**.

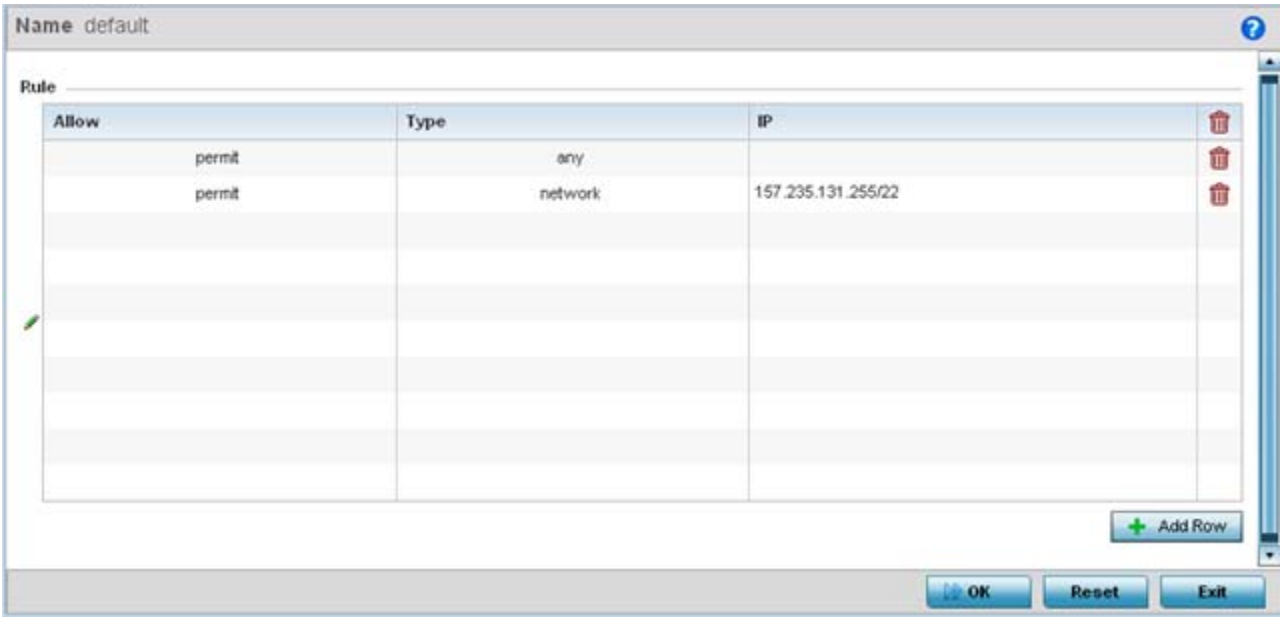


Figure 10-15 *IP SNMP ACL Add screen*

4 Provide a new IP SNMP ACL a **Name** up to 32 characters in length to help distinguish this ACL from others with similar rules.

5 Select **+ Add Row** to launch a sub screen where the ACL's permit/deny and network type rules can be applied.

Allow	Select this option to allow the SNMP MIB object traffic. The default setting is to permit SNMP traffic.
Type	Define whether the permit or deny ACL rule applied to the ACL is specific to a *Host* IP address, a *Network* address and subnet mask or is applied to *Any*. The default setting is Network.

6 Select **Add** to add additional IP Firewall Rule configurations. Select **Remove** to remove selected IP Firewall Rules as they become obsolete for filtering network access permissions.

7 Select **OK** when completed to update the IP Firewall rules. Select **Reset** to revert the screen back to its last saved configuration.

10.2.3 Network Group Alias

Configuring IP Firewall Rules

A *network group alias* is a set of configurations consisting of host and network configurations. Network configurations are complete networks in the form of 192.168.10.0/24 or an IP address range in the form of 192.168.10.10-192.168.10.20. Host configurations are in the form of a single IP address, 192.168.10.23.

A network group alias can contain multiple definitions for a host, network, and IP address range. A maximum of eight (8) Host entries, eight (8) network entries and eight (8) IP addresses range entries can be configured inside a network group alias. A maximum of 32 network group alias entries can be created.

To set a network group alias configuration for an IP Firewall:

1 Select **Configuration** > **Security > IP Firewall > Network Group Alias** from the Web UI.

2 Select the **Add** button, or highlight an existing Network Group Alias and select **Edit**.

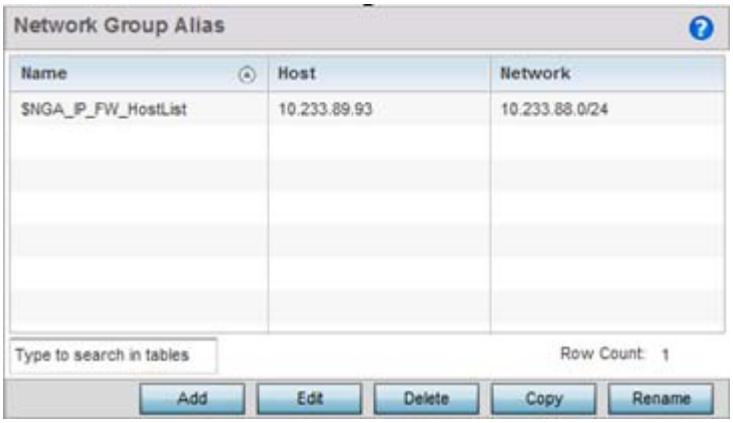


Figure 10-16 *IP Firewall Network Group Alias screen*

Name	Displays the administrator assigned name associated with the network group alias.
Host	Displays all the host aliases in the listed network group alias. Displays a blank column if no host alias is defined.
Network	Displays all network aliases in the listed network group alias. Displays a blank column if no network alias is defined.

3 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies. Use **Copy** to create a copy of the selected policy and modify it for further use. Use **Rename** to rename the selected policy.

4 Either use the **Add** button to create an new Network Group Alias or select an existing policy and click **Edit** to edit it.

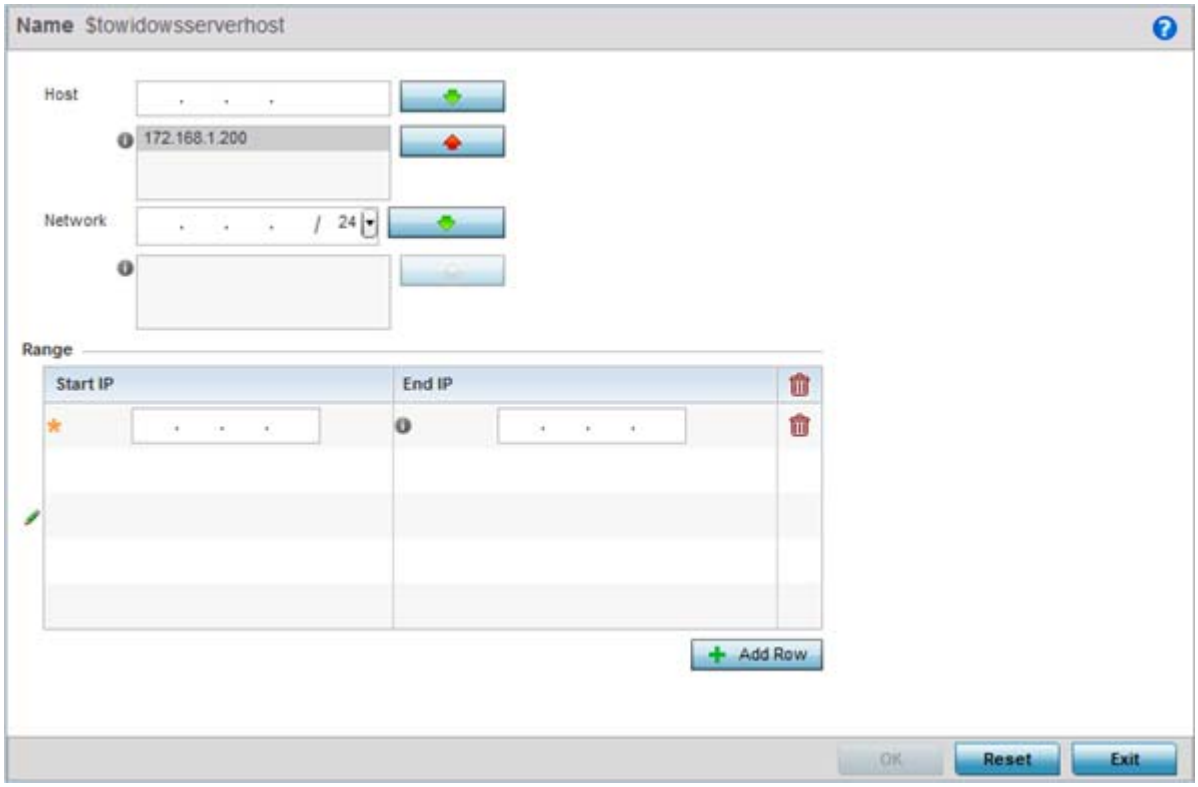


Figure 10-17 *Network Group Alias Add screen*

If adding a new **Network Alias Rule**, provide it a name up to 32 characters. The network group alias name always starts with a dollar sign ($).

5 Define the following network group alias parameters:

Host	Specify the Host IP address for up to eight IP addresses supporting network aliasing. Select the down arrow to add the IP address to the table.
Network	Specify the netmask for up to eight IP addresses supporting network aliasing. Subnets can improve network security and performance by organizing hosts into logical groups. Applying the subnet mask to an IP address separates the address into a host address and an extended network address. Select the down arrow to add the mask to the table.

6 Within the **Range** table, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the alias range or double-click on an existing an alias range entry to edit it.

7 Select **OK** when completed to update the network alias rules. Select **Reset** to revert the screen back to its last saved configuration.

10.2.4 Network Service Alias

- *Configuring IP Firewall Rules*

A *Network Service Alias* is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to 2 source port ranges and up to 2 destination port ranges can be configured. A maximum of 4 protocol entries can be configured per network service alias.

Use a service alias to associate more than one IP address to a network interface, providing multiple connections to a network from a single IP node.

To define a service alias configuration for an IP Firewall:

1 Select **Configuration** > **Security > IP Firewall > Network Service Alias** from the Web UI.
The *Network Service Alias* screen displays within the main portion of the Web UI.

2 From the *Network Service Alias* screen, either select the **Add** button or highlight an existing alias and select **Edit**.

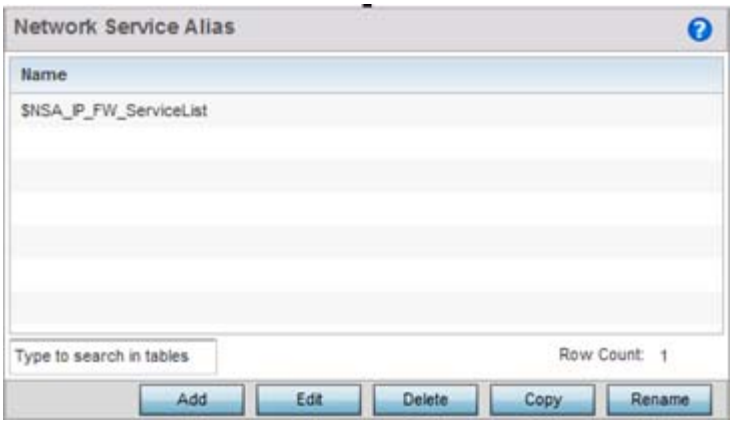


Figure 10-18 *IP Firewall Network Service Alias screen*

3 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies. Use **Copy** to create a copy of the selected policy and modify it for further use. Use **Rename** to rename the selected policy.

4 Either use the **Add** button to create an new Network Service Alias or select an existing alias and **Edit** to modify it.

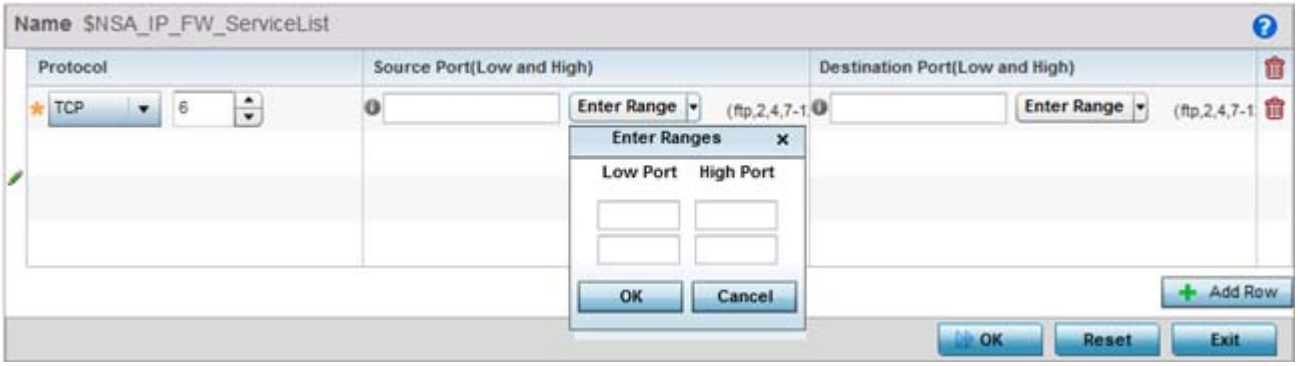


Figure 10-19 *IP Firewall Network Service Alias Add screen*

If adding a new **Network Service Alias** name, provide it a name up to 32 characters. Ensure a $ precedes the name.

5 Select **+ Add Row** and provide the following configuration parameters:

Protocol	Specify the protocol for which the alias is created. Use the drop down to select the protocol from *eigrp, gre, icmp, igmp, ip, vrrp, igp, ospf, tcp* and *udp*. Select *other* if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected.

Source Port (Low and High)	This field is only relevant if the protocol is either *tcp* or *udp*. Specify the source ports for this protocol entry. A range of ports can be specified. Select the *Enter Ranges* button next to the field to enter a lower and higher port range value. Up to eight (8) ranges can be specified.
Destination Port (Low and High)	This field is only relevant if the protocol is either *tcp* or *udp*. Specify the destination ports for this protocol entry. A range of ports can be specified. Select the *Enter Ranges* button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

6 Within the **Range** field, use the **+ Add Row** button to specify the **Start IP** address and **End IP** address for the service alias range or double-click on an existing service alias range entry to edit it.

7 Select **OK** when completed to update the service alias rules. Select **Reset** to revert the screen back to its last saved configuration.

10.2.5 EX3500 ACL Standard

Configuring IP Firewall Rules

A Standard ACL for EX3500 is a policy-based ACL that either prevents or allows specific clients from using the device.

An ACL affords a system administrator the ability to grant or restrict client access by specifying that traffic from a specific host or a specific network to either be denied or permitted.

To define a standard ACL for EX3500:

1 Select **Configuration** > **Security > IP Firewall > EX3500 ACL Standard** from the Web UI.
The EX3500 *ACL Standard* screen displays within the main portion of the Web UI.

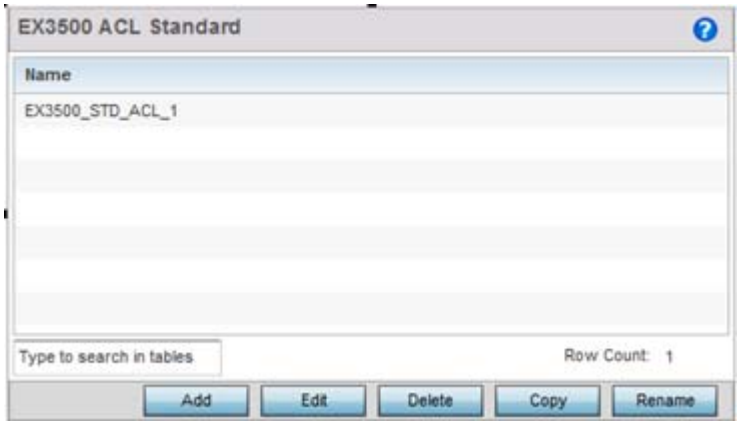


Figure 10-20 *EX3500 ACL Standard screen*

2 Select **Add** to create a new ACL, **Edit** to modify the attributes of an existing ACL or **Delete** to remove obsolete ACLs. Use **Copy** to create a copy of the selected ACL and modify it for further use. Use **Rename** to rename the selected ACL.

3 Either use the **Add** button to create an new EX3500 Standard ACL or select an existing ACL and click **Edit** to edit it. The following screen displays.

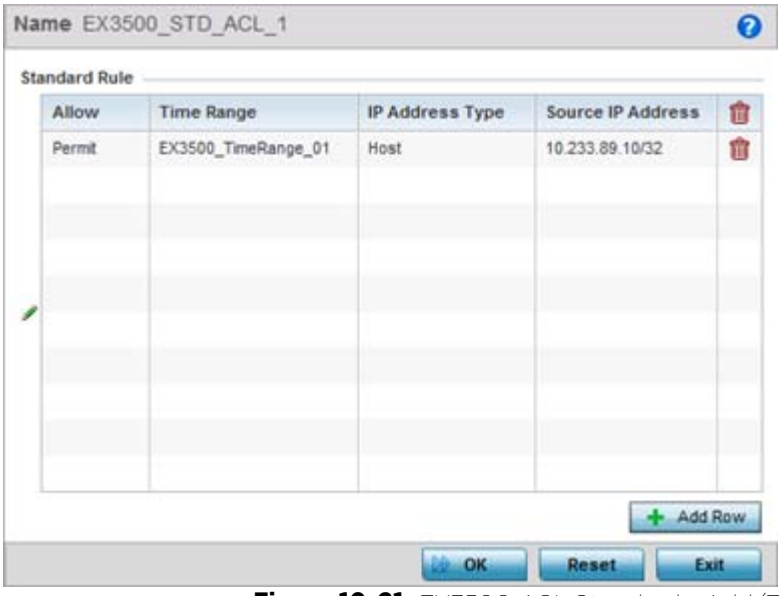


Figure 10-21 *EX3500 ACL Standard - Add/Edit screen*

4 If adding a new **EX3500 ACL Standard**, provide it a name up to 32 characters.

5 To add a new standard rule, click **Add Row**.

Figure 10-22 *EX3500 ACL Standard - Add Standard Rule screen*

6 Provide the following details:

Source IP Address	Use this drop-down menu to provide the source information. Source IP address can be one of *Any*, *Host* or *Network*. When selecting *Host* provide the IP address of the host device. When selecting *Network*, provide the IP address of the network along with the mask.
Allow	Use this drop-down menu to indicate the action to be performed. Select from *Permit* or *Deny*.
Time Range	From the drop-down menu select the pre-configured time range to use for this ACL. Select *None* to indicate no preference. For more information on time ranges, see *EX3500 Time Range on page 10-64*.

7 Select **OK** when completed to update the EX3500 Standard ACL. Select **Reset** to revert the screen back to its last saved configuration.

10.2.6 EX3500 ACL Extended

Configuring IP Firewall Rules

An extended ACL is comprised of *access control entries* (ACEs). Each ACE specifies a *source* and *destination* for matching and filtering traffic to the EX3500 switch.

An ACL affords a system administrator the ability to grant or restrict client access by specifying that traffic from a specific host or a specific network to either be denied or permitted.

IP based firewalls function like *Access Control Lists* (ACLs) to filter/mark packets, as opposed to filtering packets on layer 2 ports. IP firewalls implement uniquely defined access control policies, so if you do not have an idea of what kind of access to *allow* or *deny*, a firewall is of little value, and could provide a false sense of network security.

IP based firewall rules are specific to source and destination IP addresses and the unique *rules* and *precedence* orders assigned. Both IP and non-IP traffic on the same Layer 2 interface can be filtered by applying an IP ACL. Firewall rules are processed by a firewall supported device from first to last. When a rule matches the network traffic a controller or service platform is processing, the firewall uses that rule's action to determine whether traffic is allowed or denied.

To configure an extended ACL on EX3500:

1 Select **Configuration** > **Security > IP Firewall > EX3500 ACL Extended** from the Web UI.

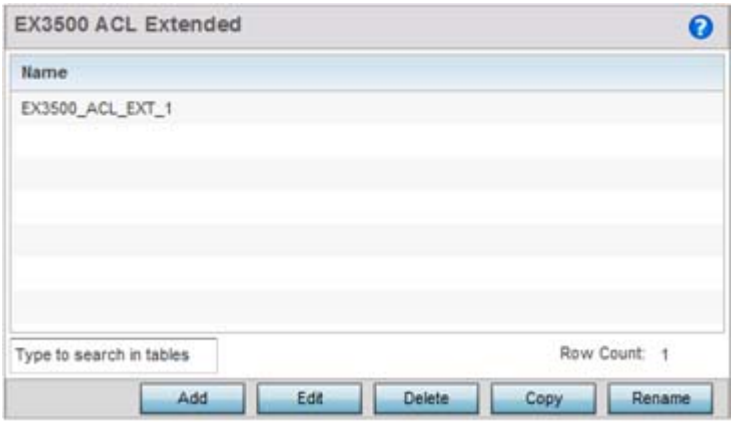


Figure 10-23 *EX3500 ACL Extended screen*

2 Select **Add** to create a new ACL, **Edit** to modify the attributes of an existing ACL or **Delete** to remove obsolete ACLs. Use **Copy** to create a copy of the selected ACL and modify it for further use. Use **Rename** to rename the selected ACL.

3 Either use the **Add** button to create an new EX3500 Extended ACL or select an existing ACL and click **Edit** to edit it. The following screen displays.

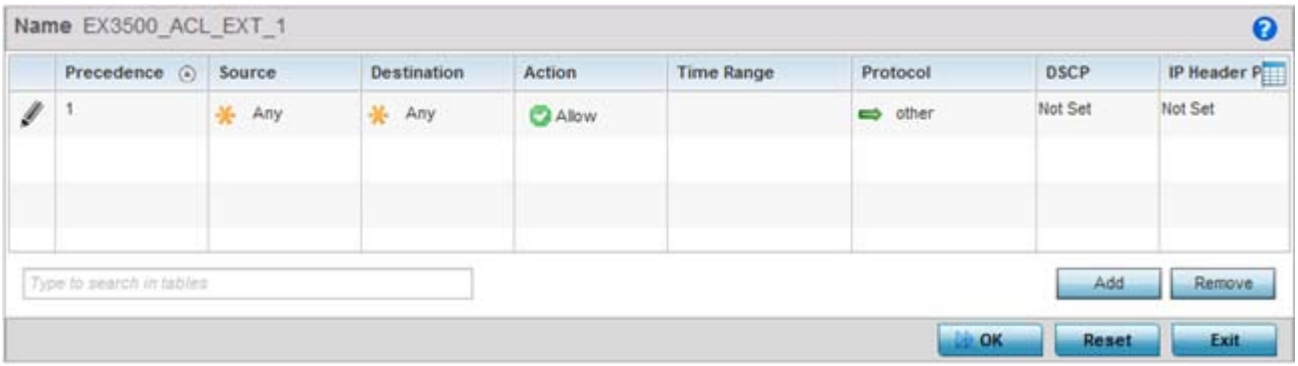


Figure 10-24 *EX3500 ACL Extended - Add/Edit screen*

EX3500 extended ACL configurations can either be modified as a collective group of variables or selected and updated individually if their filtering attributes require a more refined update.

a Select the **Edit Rule** icon to the left of a particular IP firewall rule configuration to update its parameters collectively.

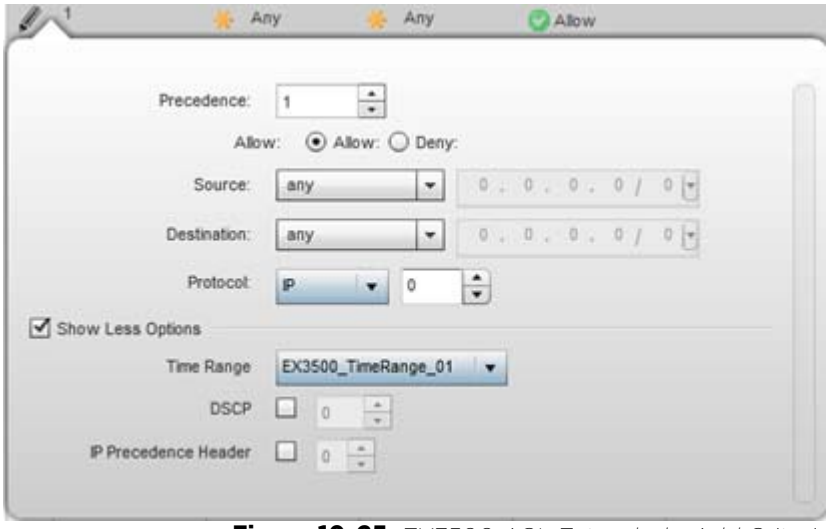


Figure 10-25 *EX3500 ACL Extended - Add Criteria screen*

b Click the icon located at the top right-hand side of the screen and select the values as needed to add/hide criteria to the configuration of the extended ACL.

Figure 10-26 *EX3500 ACL Extended - Select Fields screen*

4 Define the following Extended ACL rule settings as required:

Precedence	Specify or modify a precedence for this ACL between 1-128. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.
Action	Every ACL rule is made up of matching criteria rules. The action defines the action to be performed if it matches the specified criteria. The following actions are supported: *Deny* - Instructs the Firewall to restrict a packet from proceeding to its destination. *Permit* - Instructs the Firewall to allow a packet to proceed to its destination.
Source	Use this drop-down menu to provide the source information. Source IP address can be one of Any, Host or Network. When selecting Host provide the IP address of the host device. When selecting Network, provide the IP address of the network along with the mask.
Destination	Use this drop-down menu to provide the destination information. Destination IP address can be one of *Any*, *Host* or *Network*. When selecting *Host* provide the IP address of the host device. When selecting *Network*, provide the IP address of the network along with the mask.
Protocol	Set a service alias as a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Depending on the selected protocol, other fields might become visible and can be configured.
Time Range	Use the drop-down menu to configure a time range when this ACL is applicable. For more information on configuring Time Ranges, see *EX3500 Time Range on page 10-64*.
DSCP	*Differentiated Services Code Point* is a mechanism that specifies a simple mechanism for classifying and manage network traffic and provide a QoS mechanism. Use the spinner to select a value in the range 0-63. Use this value to classify and mark packets that match the criteria specified in this extended ACL rule. Either *DSCP* or *IP Header Precedence* can be configured. Both these fields cannot be configured together.
IP Header Precedence	Use this field to set the precedence value in the IP Header. Use the spinner to select a value in the range 0-7. Use this value to classify and mark packets that match the criteria specified in this extended ACL rule. Either *DSCP* or *IP Header Precedence* can be configured. Both these fields cannot be configured together.

5 Select **OK** when completed to update the EX3500 Extended ACL. Select **Reset** to revert the screen back to its last saved configuration.

10.3 Wireless Client Roles

Define wireless client roles to filter clients from based on matching policies. Matching policies (much like ACLs) are sequential collections of permit and deny conditions that apply to packets received from connected clients. When a packet is received from a client, the controller or service platform compares the fields in the packet against

applied matching policy rules to verify the packet has the required permissions to be forwarded, based on the criteria specified. If a packet does not meet any of the criteria specified, the packet is dropped.

Additionally, wireless client connections are also managed by granting or restricting access by specifying a range of IP or MAC addresses to include or exclude from connectivity. These MAC or IP access control mechanisms are configured as Firewall Rules to further refine client filter and matching criteria.

10.3.1 Configuring a Client's Role Policy

- *Wireless Client Roles*

To configure a wireless client's role policy and matching criteria:

1 Select **Configuration** > **Security** > **Wireless Client Roles**.The **Wireless Client Roles** screen displays the name of those client role policies created thus far.

2 Select **Add** to create a new Wireless Client Role policy, **Edit** to modify an existing policy or **Delete** to remove a policy.

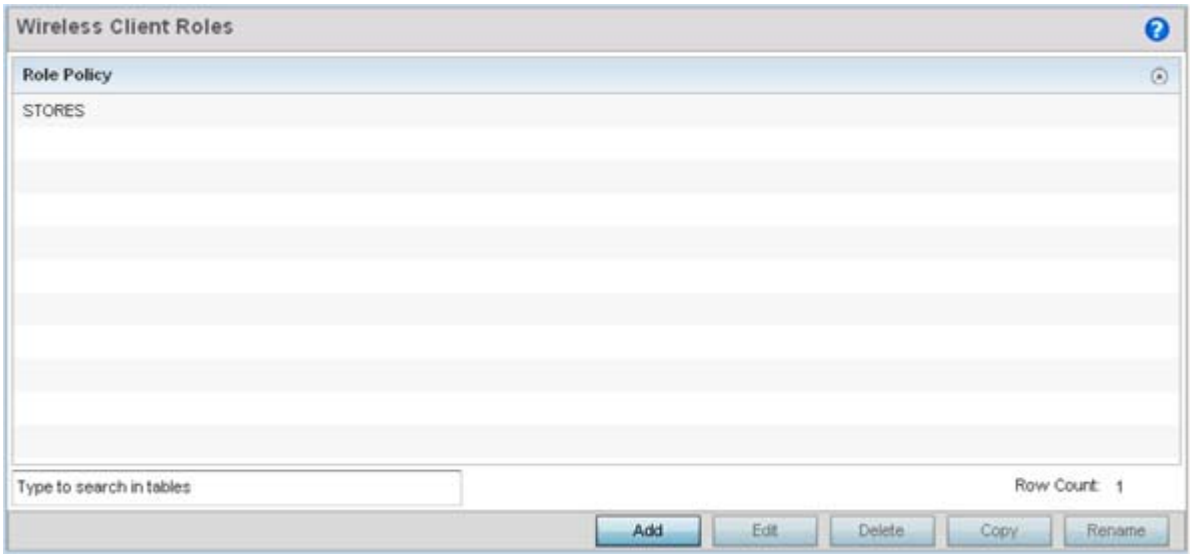


Figure 10-27 *Wireless IPS screen*

The **LDAP Settings** tab displays by default.

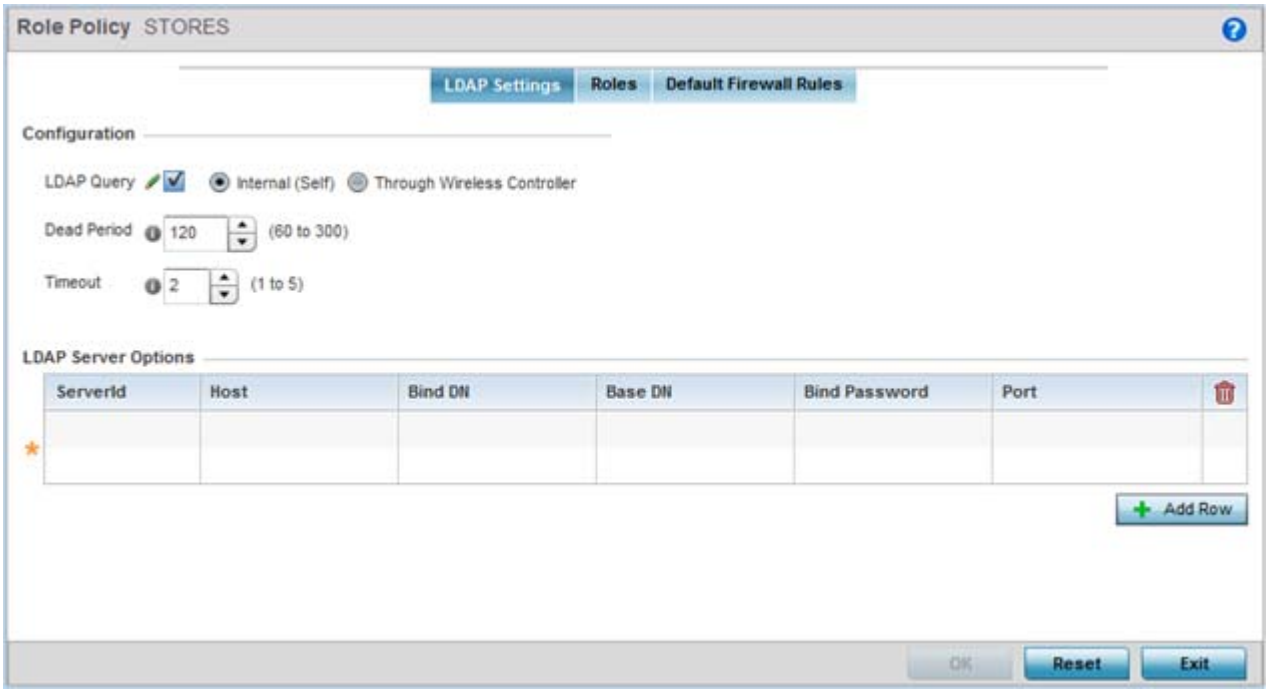


Figure 10-28 *Wireless Client LDAP Settings screen*

3 In the **Configuration** section define the following LDAP server parameters:

LDAP Query	If LDAP attributes are enabled for the selected wireless client role policy, select an LDAP query mode of either *Internal (Self)* or *Through Wireless Controller.* Select Internal (Self) to use local LDAP server resources configured in the LDAP Server Options.
Dead Period	When using an external LDAP server, select the Dead Period between 60 and 300 seconds. The Dead Period is the timeout value before the system will attempt to rebind with the LDAP server.
Timeout	When using an external LDAP server, select a Timeout value to specify how long of a delay between request and responses before LDAP bind and queries will be timed out.

4 In the **LDAP Server Options** section use the **+ Add Row** button to add an LDAP server to the list or double-click on an existing LDAP server entry to edit it. When adding or editing the LDAP server options define the following parameters:

ServerId	When adding or editing an LDAP server entry, enter the LDAP server ID as either 1 or 2.
Host	When adding or editing an LDAP server entry, enter the LDAP server's fully qualified domain name or IP address in the Host field
Bind DN	When adding or editing an LDAP server entry, enter the LDAP server's bind distinguished name in the Bind DN field.
Base DN	When adding or editing an LDAP server entry, enter the LDAP server's base distinguished name in the Base DN field.
Bind Password	When adding or editing an LDAP server entry, enter the password for bind. Click the Show button to display the password.

Port	When adding or editing an LDAP server entry, enter the LDAP server port number. To select from a list of frequently used services and their corresponding port numbers, use the drop-down menu and select a service.

5 Click on the **Roles** tab. If no policies have been created, a default wireless client role policy can be applied. The Roles screen lists existing policies. Any of these existing policies can be selected and edited or a new role can be added.

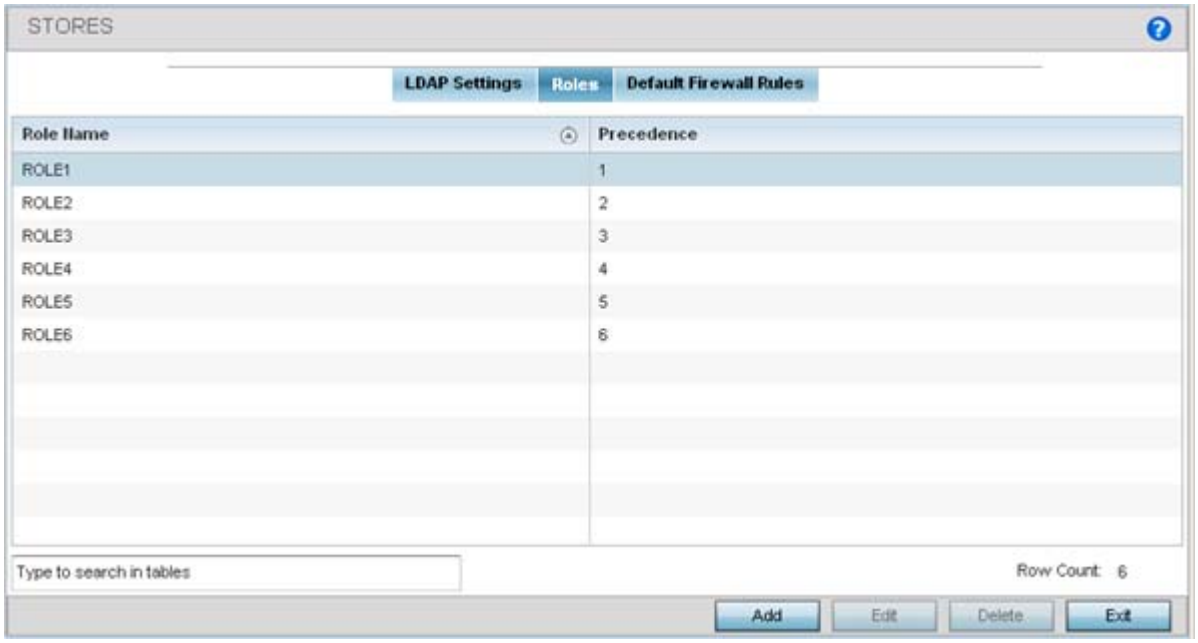


Figure 10-29 *Wireless Client Roles screen*

6 Refer to the following configuration data for existing roles:

Role Name	Displays the name assigned to the client role policy when it was initially created.
Precedence	Displays the precedence number associated with each role. Precedence numbers determine the order a role is applied. Roles with lower numbers are applied before those with higher numbers. Precedence numbers are assigned when a role is created or modified, and two or more roles can share the same precedence.

7 Select **Add** to create a new wireless client role policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available.

The Role Policy Roles screen displays with the **Settings** tab displayed by default.

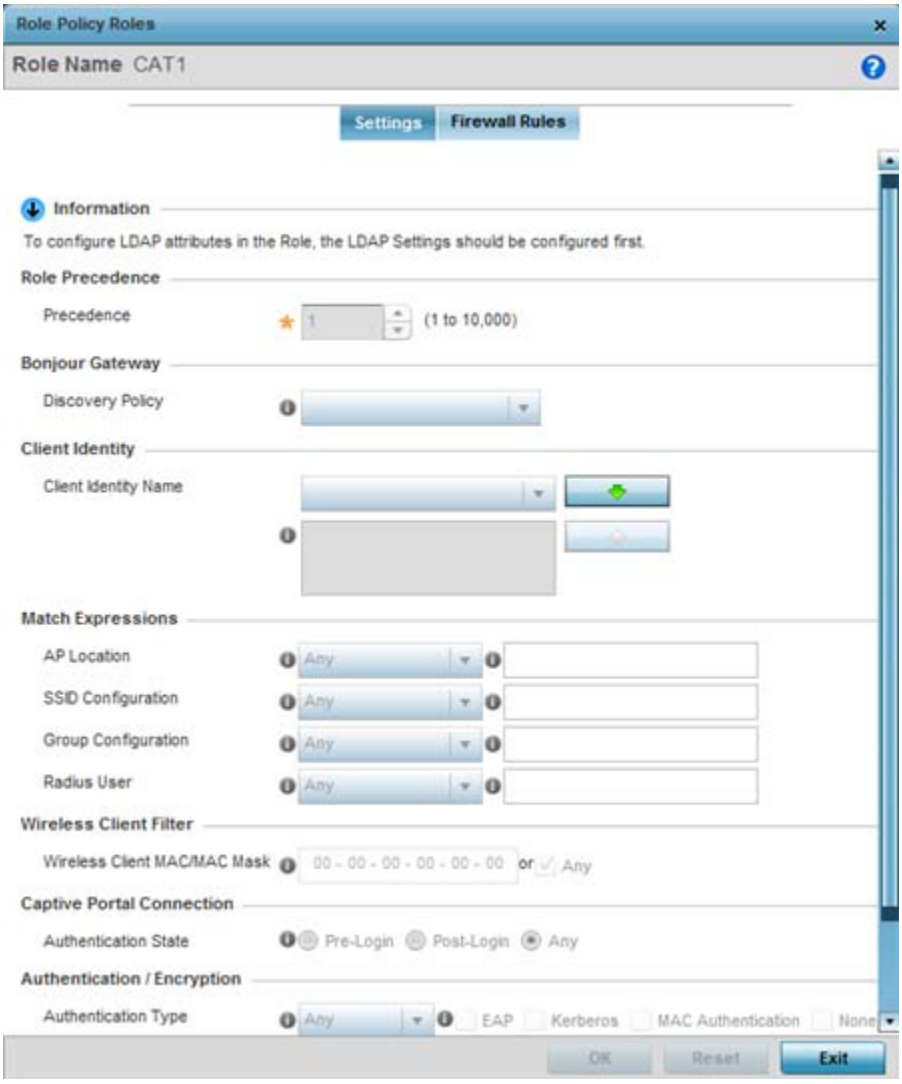


Figure 10-30 *Wireless Client Roles screen - Settings tab*

8 If creating a new role, assign it a **Role Name** to help differentiate it from others that may have a similar configuration. The role policy name cannot exceed 64 characters. The name cannot be modified as part of the edit process.

9 Within the **Role Precedence** field, use the spinner control to set a numerical precedence value between 1 - 10,000. Precedence determines the order a role is applied. Roles with lower numbers are applied before those with higher numbers. While there's no default precedence for a role, two or more roles can share the same precedence.

10 Use the **Discovery Policy** drop-down menu to specify the **Bonjour Gateway**.

Bonjour provides a method to discover services on a *local area network* (LAN). Bonjour allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.

11 Within the **Client Identity** field, define the client type (Android etc.) used as matching criteria within the client role policy. Create new client identity types or edit existing ones as required.

12 Refer to the **Match Expressions** field to create filter rules based on AP locations, SSIDs and RADIUS group memberships.

AP Location	Use the drop-down menu to specify the location of an Access Point matched in a RF Domain or the Access Point's resident configuration. Select one of the following filter options: *Exact* - The role is only applied to Access Points with the exact location string specified in the role. *Contains* - The role is only applied to Access Points whose location contains the location string specified in the role. *Does Not Contain* - The role is only applied to Access Points whose location does not contain the location string specified in the role. *Any* - The role is applied to any Access Point location. This is the default setting.
SSID Configuration	Use the drop-down menu to define a wireless client filter option based on how the SSID is specified in a WLAN. Select one of the following options: *Exact* - The role is only applied when the exact SSID string specified in the role. *Contains* - The role is only applied when the SSID contains the string specified in the role. *Does Not Contain* - The role is applied when the SSID does not contain the string specified in the role. *Any* - The role is applied to any SSID Location. This is the default setting.
Group Configuration	Use the drop-down menu to define a wireless client filter option based on how the RADIUS group name matches the provided expression. Select one of the following options: *Exact* - The role is only applied when the exact Radius Group Name string is specified in the role. *Contains* - The role is applied when the Radius Group Name contains the string specified in the role. *Does Not Contain* - The role is applied when the Radius Group Name does not contain the string specified in the role *Any* - The role is applied to any RADIUS group name. This is the default setting.
Radius User	Use the drop-down menu to define a filter option based on how the RADIUS user name (1-255 characters in length) matches the provided expression. Select one of the following options: *Exact* - The role is only applied when the exact Radius user string is specified in the role. *Starts With* - The role is applied when the Radius user starts with the string specified in the role. *Contains* - The role is applied when the Radius user contains the string specified in the role. *Does Not Contain* - The role is applied when the Radius user does not contain the string specified in the role. *Any* - The role is applied to any RADIUS user name. This is the default setting.

13 Use the **Wireless Client Filter** parameter to define a wireless client MAC address filter that is applied to each role. Select the **Any** radio button to use any MAC address. The default is **Any**.

14 Refer to the **Captive Portal Connection** parameter to define when wireless clients are authenticated when making a captive portal authentication request.

Secure guest access is referred to as *captive portal*. A captive portal is guest access policy for providing temporary and restrictive access to the wireless network. Existing captive portal policies can be applied to a WLAN to provide secure guest access.

15 Select the **Pre-Login** check box to conduct captive portal client authentication before the client is logged. Select **Post-Login** to have the client share authentication credentials after it has logged into the network. Select **Any** (the default setting) makes no distinction on whether authentication is conducted before or after the client has logged in.

16 Use the **Authentication / Encryption** field to set the authentication and encryption filters applied to this wireless client role. The options for both authentication and encryption are:

- *Equals* - The role is only applied when the authentication and encryption type matches the exact method(s) specified by the radio button selections.
- *Not Equals* - The role is only applied when the authentication and encryption type does not match the exact method(s) specified by the radio button selections.
- *Any* - The role is applied to any type. This is the default setting for both authentication and encryption.

17 Use the **+** (plus sign) to the left of the **LDAP Attributes** label to expand it. Set the following **LDAP Attributes** for the role policy:

The following filter criteria applies to each LDAP attribute:

- *Exact* - The role is only applied when the exact string is specified in the role.
- *Contains* - The role is applied when the LDAP attribute contains the string specified in the role.
- *Does Not Contain* - The role is applied when the LDAP attribute does not contain the string specified in the role.
- *Any* - The role is applied to any LDAP attribute. This is the default setting.

City	Enter a 2-31 character name of the city filtered in the role.
Company	Enter a 2-31 character name of the organizational company filtered in the role.
Country	Enter a 2-31 character name of the country (co) filtered in the role.
Department	Enter a 2-31 character name of the organizational department filtered in the role.
Email	Enter a 2-31 character description of the Email address filtered in the role.
Employee id	Enter a 2-31 character name of the employee ID filtered in the role.
State	Enter a 2-31 character name of the state filtered in the role.
Title	Enter a 2-31 character name of the job or organizational title filtered in the role.
Member Of	Provide a 64 character maximum description of the group membership in the role.

18 Select **OK** to update the Settings screen. Select **Reset** to revert to the last saved configuration.

19 Select the **Firewall Rules** tab to set default Firewall rules for *Inbound* and *Outbound* IP and MAC Firewall rules.

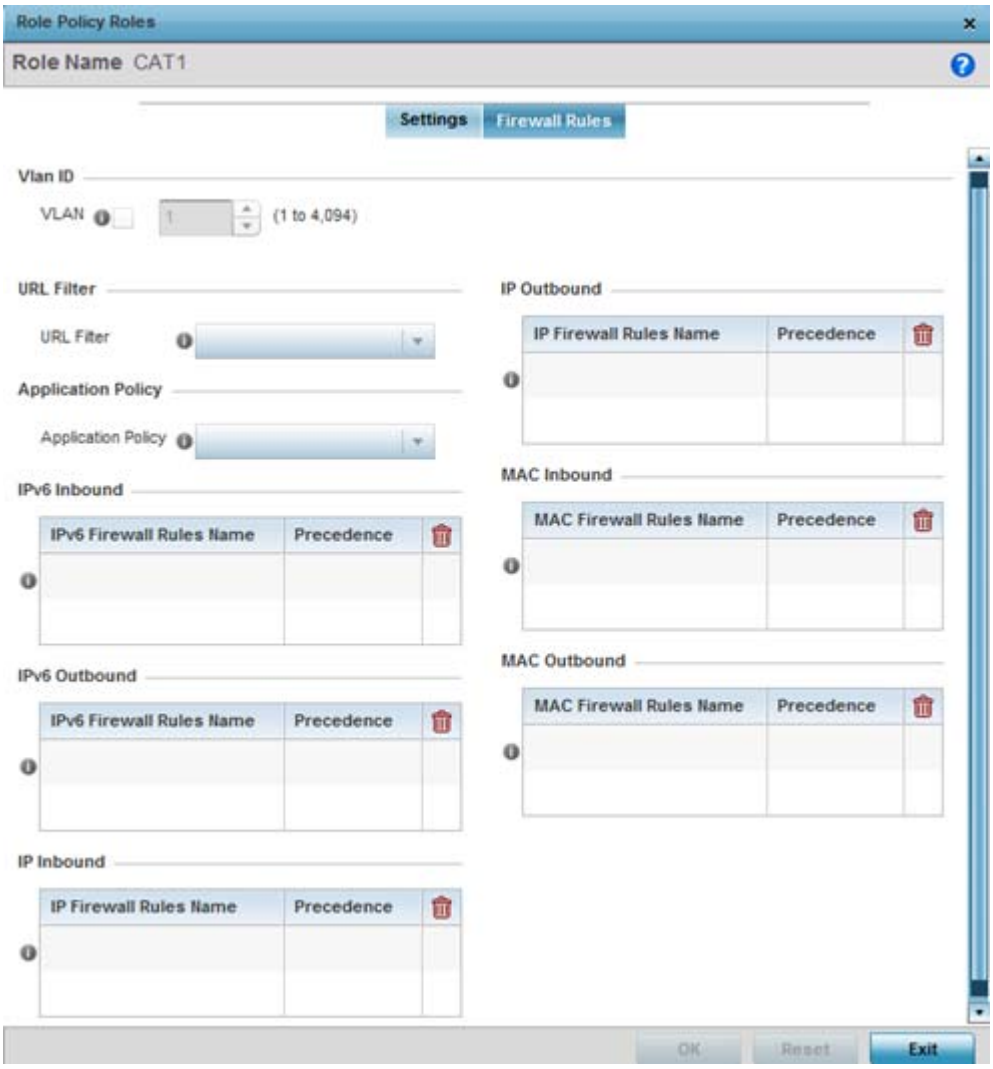


Figure 10-31 *Wireless Client Roles screen - Firewall Rules tab*

A *firewall* is a mechanism enforcing access control, and is considered a first line of defense in protecting proprietary information within the network. The means by which this is accomplished varies, but in principle, a firewall can be thought of as mechanisms both *blocking* and *permitting* data traffic based on inbound and outbound IP and MAC rules.

IP based firewall rules are specific to source and destination IP addresses and the unique rules and precedence orders assigned. Both IP and non-IP traffic on the same Layer 2 interface can be filtered by applying both an IP ACL and a MAC.

Additionally, administrators can filter Layer 2 traffic on a physical Layer 2 interface using MAC addresses. A MAC firewall rule uses source and destination MAC addresses for matching operations, where the result is a typical allow, deny or mark designation to packet traffic.

20 Set the **Vlan ID** (from 1 - 4094) for the virtual LAN used by clients matching the IP or MAC inbound and outbound rules of this policy.

21 Use the drop-down to select the appropriate **Application Policy** to use with this firewall rule. An application policy defines the rules or actions executed on recognized HTTP (Facebook), enterprise (Webex) and peer-to-peer (gaming) applications or application-categories.

22 Select the **URL Filter** used as the content filter for the Firewall Rule. If a policy requires creation, select the **Create** icon. If an existing policy requires modification, select the **Edit** icon button and update this existing policy as needed.

A URL filter is comprised of several filter rules. To construct a filter rule, either *whitelist* or *blacklist* a filter level, category type, category or a custom category. A whitelist bans all sites except the categories and lists defined in the whitelist. The blacklist allows all sites except the categories and lists defined in the blacklist.

23 Enter a 32 character maximum **Name** for the URL filter and select **Continue.**

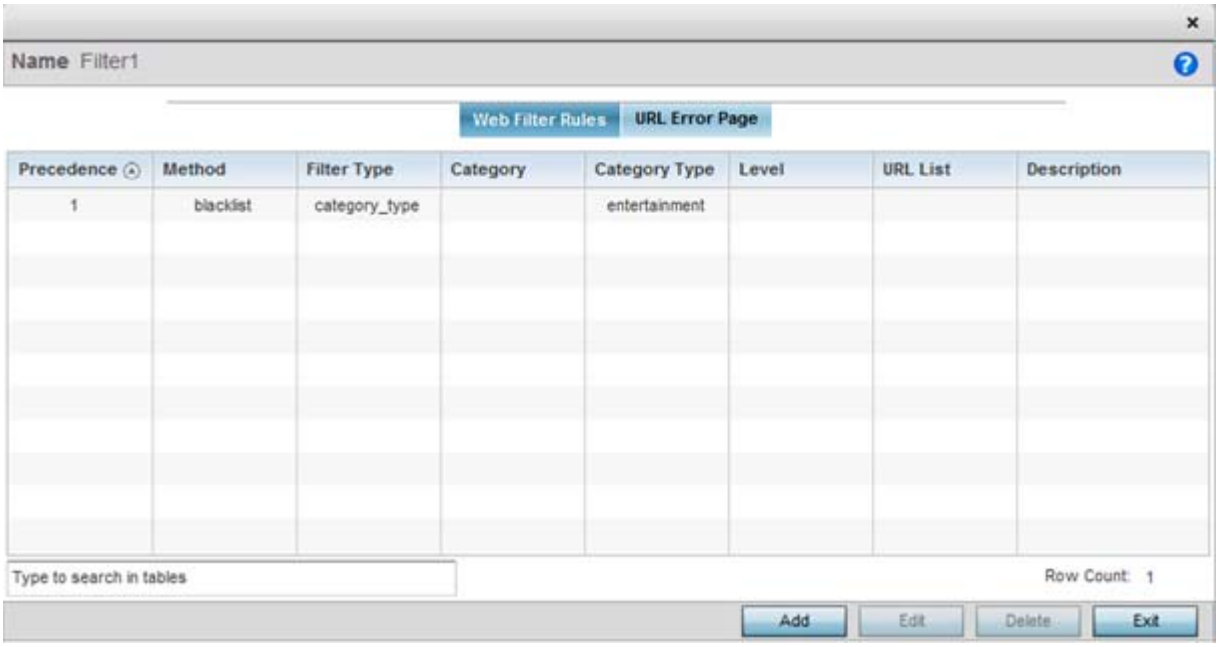


Figure 10-32 *Wireless Client Roles screen - Web Filter Rules tab*

24 Select **Add** to create a new Web filter rule configuration, or select an exiting configuration then **Edit** to modify the attributes of an existing Web filter rule.

For more information on Web filters, see *Web Filtering on page 7-67*.

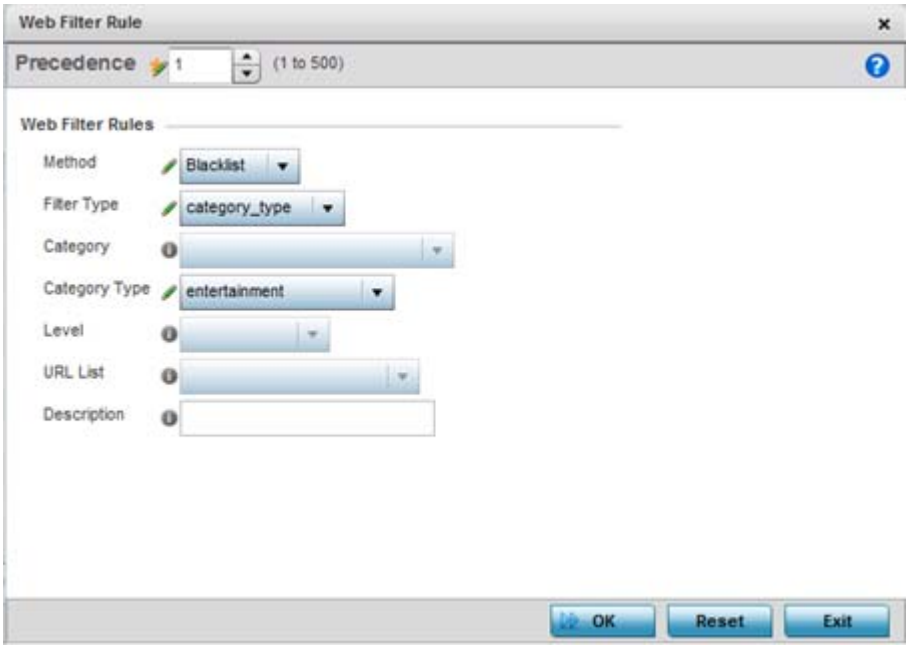


Figure 10-33 *Wireless Client Roles screen - Add/Edit Web Filter Rules*

25 Define the following filter rule settings:

Precedence	Set a precedence (priority) from 1 - 500 for the filter rule's utilization versus other filter rules. 1 is the highest priority and 500 the lowest.
Method	Select either *whitelist* or *Blacklist* to specify whether the rule is for inclusion or exclusion. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.
Filter Type	If the *Filter Type* is set to category, use the drop down menu to select from a list of predefined categories to align with the whitelist or blacklist *Method* designation and the precedence assigned.
Category	A category is a pre-defined URL list available in the WiNG software. If *category* is selected as the *Filter Type*, the *Category* drop-down menu becomes enabled for the selection of an existing URL type or whitelist or blacklist. Categories are based on an external database, and cannot be modified or removed. Custom categories can be created with the *URL List* and added to the database.
Category Type	When *category_type* is selected as the Filter Type, select an existing category type (adult-content, security-risk etc.) and either blacklist or whitelist the URLs in that category type. There are 12 category types available.
Level	*Basic, Low, Medium, medium-high* and *High* filter levels are available. Each level is pre-configured to use a set of category types. The user cannot change the categories in the category types used for these pre-configured filter-level settings, and add/modify/remove the category types mapped to the filter-level setting.
URL List	URL lists are customized categories included in the custom filter-level setting. URL lists enable an administrator to blacklist or whitelist URLs in addition to the built-in categories.

Description	Enter a 80 character maximum description for this Web filter rule to help differentiate it from others with similar category include or exclude rule configurations.

26 Select **OK** to save the changes to the Web Filter Rule. Select **Exit** to close the screen without saving the updates.

27 Select the **URL Error Page** tab to define the configuration and layout of a URL error page launched when a Web filter rule is invoked and an error page needs to be displayed to a user instead of they're expected Web page.

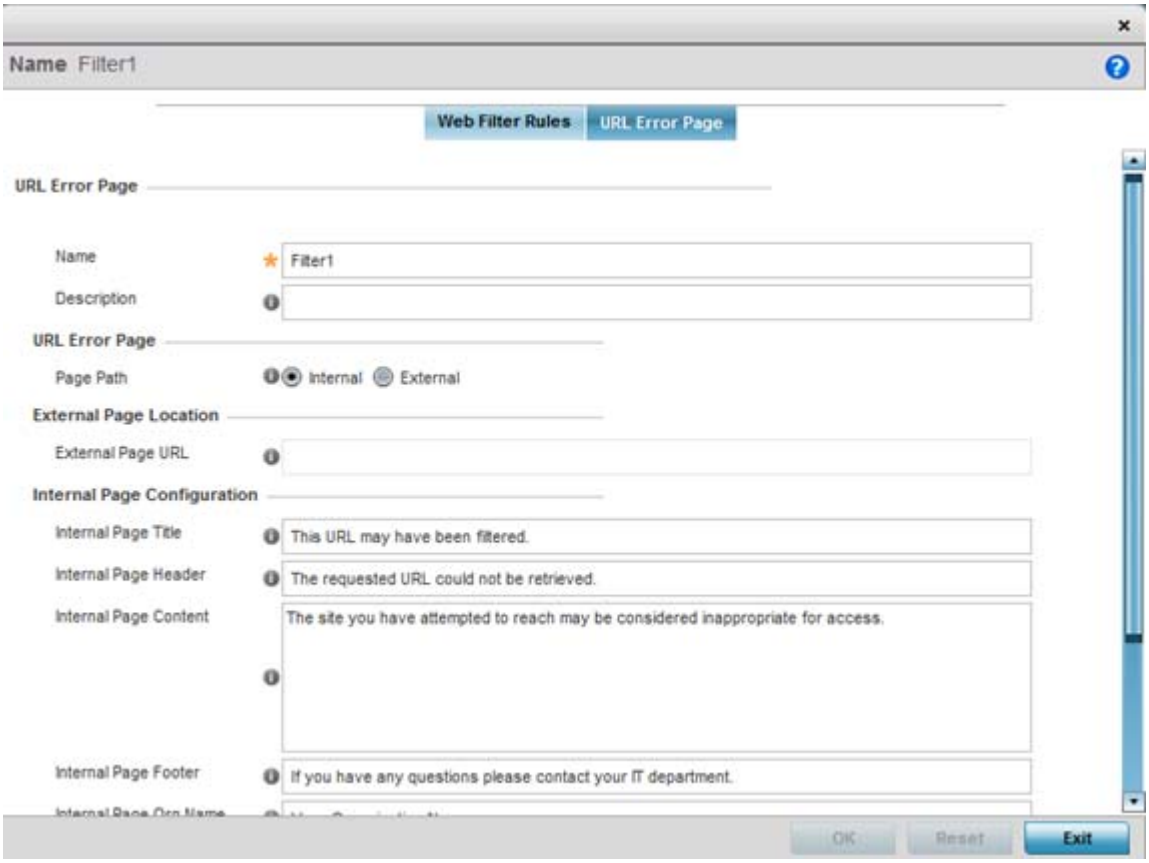


Figure 10-34 *Wireless Client Roles screen - Web Filter Rules URL Error Page*

28 Set the following **URL Error Page** display properties:

Name	Provide a 32 character maximum name for the title of the blocking page. The name should help convey that this page is launched to prevent the client's requested page from displaying.
Description	Provide a 80 character maximum description of the page to help differentiate it from other pages with similar page restriction properties.
Page Path	Set the path to the page sent back to the client browser explaining the reason for blocking the client's requested URL. It can be generated internally at the time the page is sent, or be a URL to an *External* Web server if the administrator chooses to utilize a customized page. The default setting is Internal, requiring the administrator to define the page configuration within the fields in the *Internal Page Configuration* portion of the screen.

External Page URL	If *External* is selected as the Page Path, provide a 511 character maximum External Page URL used as the Web link designation of the externally hosted blocking page.
Internal Page Title	Either enter a 255 character maximum title for the URL blocking page or use the existing default text (*This URL may have been filtered*).
Internal Page Header	Either enter a 255 character maximum header for the top of the URL blocking page or use the existing default text (*The requested URL could not be retrieved*).
Internal Page Content	Enter a 255 character maximum set of text used as the main body (middle portion) of the blocking page. Optionally use the default message (*The site you have attempted to reach may be considered inappropriate for access*).
Internal Page Footer	Either enter a 255 character maximum footer for the bottom of the URL blocking page or use the existing default text (*If you have any questions contact your IT department*).
Internal Page Org Name	Enter a 255 character maximum organizational name responsible for the URL blocking page. The default organizational name (*Your Organizational Name*) is not very practical, and is just a guideline for customization.
Internal Page Org Structure	Enter a 255 character maximum organizational signature responsible for the URL blocking page. The default organizational signature (Your Organizational Name, All Rights Reserved) is not very practical, and is just a guideline for customization.
Internal Page Logo 1	Provide the location and filename of a small graphic image displayed in the blocking page.
Internal Page Logo 2	Provide the location and filename of a main graphic image displayed in the blocking page.

29 Specify an **IP Inbound** or **IP Outbound** firewall rule by selecting a rule from the drop-down menu and use the spinner control to assign the rule Precedence. Rules with lower precedence are always applied first to packets.If no IP Inbound or Outbound rules exist meeting the required firewall filtering criteria, select the **Create** button to set the inbound or outbound rule criteria. Select the **+ Add Row** button or **Delete** icon as needed to add or remove IP firewall rules. Define the following parameters to create a new Inbound or Outbound IP firewall rule. For more information, refer to *Configuring IP Firewall Rules on page 10-20*.

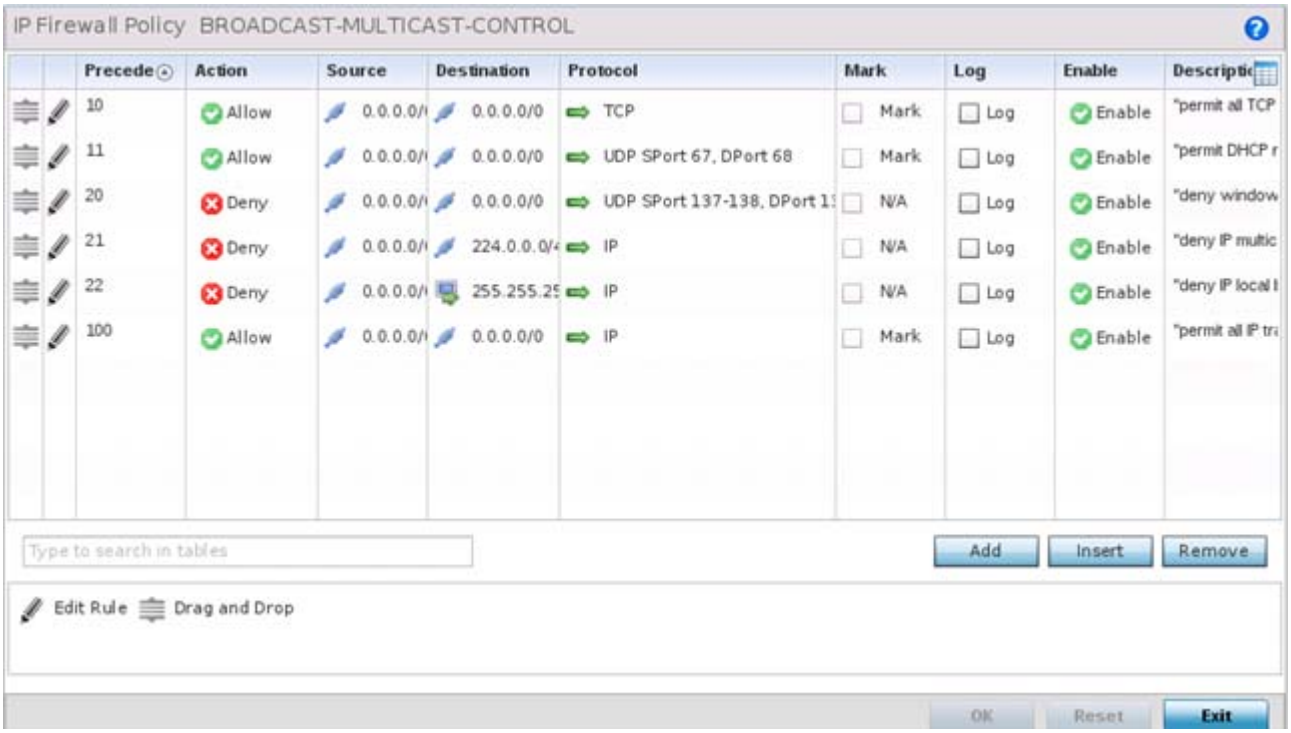


Figure 10-35 *Wireless Client Roles screen - IP Firewall Policy screen*

Precedence	Specify or modify a precedence for this IP policy between 1-5000. Rules with lower precedence are always applied to packets first. If modifying a precedence to apply a higher integer, it will move down the table to reflect its lower priority.
Action	Every IP Firewall rule is made up of matching criteria rules. The action defines the packet's disposition if it matches the specified criteria. The following actions are supported: *Deny* - Instructs the Firewall to restrict a packet from proceeding to its destination. *Permit* - Instructs the Firewall to allow a packet to proceed to its destination.
Source	Select the source IP address used as basic matching criteria for this IP ACL rule.
Destination	Determine whether filtered packet destinations for this IP firewall rule do not require any classification (*any*), are designated as a set of configurations consisting of protocol and port mappings (an *alias*), set as a numeric IP address (*host*) or defined as *network* IP and mask. Selecting alias requires a destination network group alias be available or created.
Protocol	Set a service alias as a set of configurations consisting of protocol and port mappings. Both source and destination ports are configurable. Set an alphanumeric service alias (beginning with a $) and include the protocol as relevant.
Mark	Select an IP Firewall rule's *Mark* checkbox to enable or disable event marking and set the rule's 8021p or dscp level (from 0 - 7).
Log	Select an IP Firewall rule's *Log* checkbox to enable or disable event logging for this rule's usage.

Enable	Select an IP Firewall rule's *Enable* or *Disable* icon to determine this rule's inclusion with the IP firewall policy.
Description	Lists the administrator assigned description applied to the IP ACL rule. Select a description within the table to modify its character string as filtering changes warrant. Select the icon within the Description table header to launch a *Select Columns* screen used to add or remove IP ACL criteria from the table.

30 Select **OK** to save the updates to the Inbound or Outbound IP Firewall rule. Select **Reset** to revert to the last saved configuration.

31 If required, select existing Inbound and Outbound MAC Firewall Rules using the drop-down menu. If no rules exist, select **Create** to display a screen where Inbound or Outbound Firewall rules can be created.

32 Define the following parameters required to create an **Inbound** or **Outbound MAC Firewall** rule:

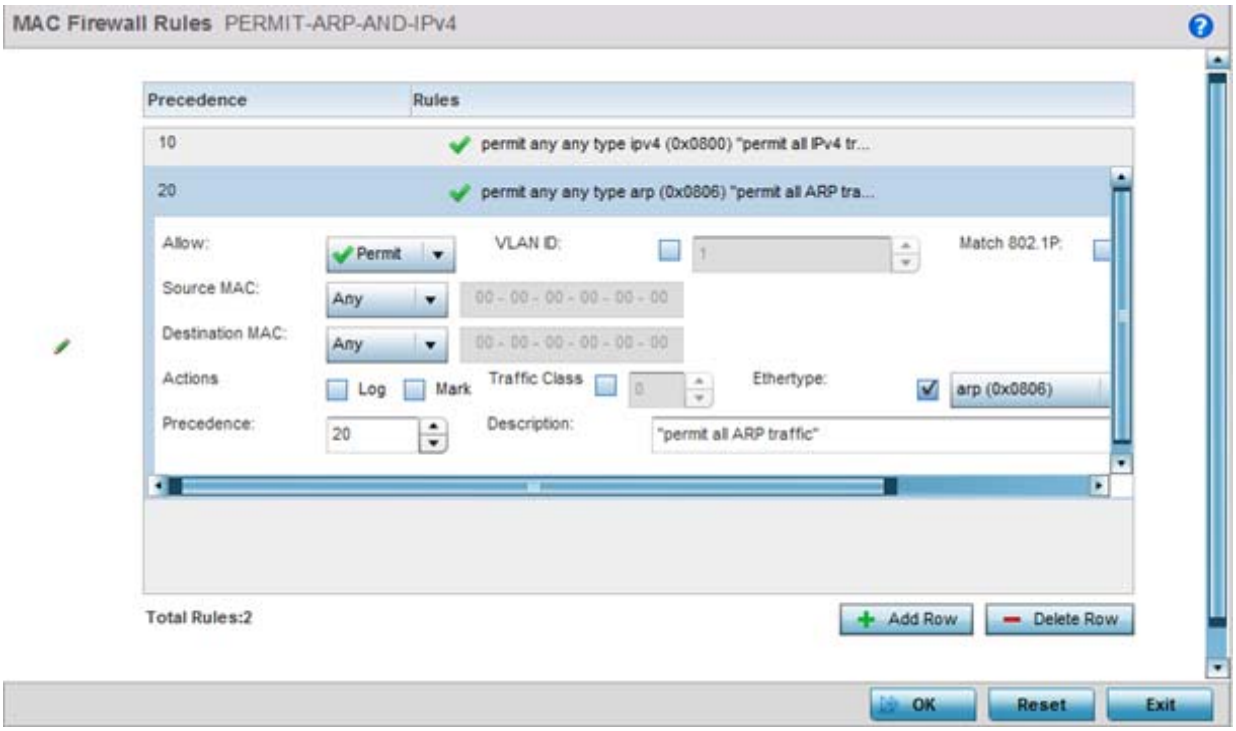


Figure 10-36 *MAC Firewall Rules - ACL Settings screen*

MAC Firewall Rules	If creating a new MAC Firewall rule, assign it a name (up to 64 characters) to help differentiate it from others that may have similar configurations.
Allow	Every MAC Firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported: *Deny* - Instructs the Firewall to prohibit a packet from proceeding to its destination when filter conditions are met. *Permit* - Instructs the Firewall to allow a packet to proceed to its destination when filter conditions are met.
VLAN ID	Enter a VLAN ID representative of the shared SSID each user employs to interoperate within the network (once authenticated by the local RADIUS server). The VLAN ID can be between1 and 4094.

Match 802.1P	Configures IP DSCP to 802.1p priority mapping for untagged frames. Use the spinner control to define a setting between 0-7.
Source / Destination MAC	Enter both *Source* and *Destination* MAC addresses as basic matching criteria.
Action	The following actions are supported: *Log* - Logs the event when this rule is applied to a wireless clients association attempt. *Mark* - Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit. - VLAN 802.1p priority. - DSCP bits in the header. - *TOS bits in the header.* *Mark, Log* — Applies both log and mark actions.
Traffic Class	Select this option to enable a spinner control for traffic class prioritization. Devices that originate a packet must identify a class or priority for packets. Devices use the traffic class field in the MAC header to set this priority.
Ethertype	Use the drop-down menu to specify an Ethertype. An EtherType is a two-octet field within an Ethernet frame. It's used to indicate which protocol is encapsulated in the payload of an Ethernet frame.
Precedence	Use the spinner control to specify a precedence for this MAC policy between 1-1500. Rules with lower precedence are always applied first to packets. More than one rule can share the same precedence value.
Description	Provide a description for the rule to differentiate the IP Firewall Rule from others with similar configurations. This should be more descriptive then simply re-applying the name of the rule.

33 Select **OK** to save the updates to the MAC Firewall rule. Select **Reset** to revert to the last saved configuration.

10.4 Device Fingerprinting

With an increase in *Bring Your Own Device* (BYOD) corporate networks, there's a parallel increase in the number of possible attack scenarios within the network. BYOD devices are inherently unsafe, as the organization's security mechanisms do not extend to these personal devices deployed in the corporate wireless network. Organizations can protect their network by limiting how and what these BYODs can access on and through the corporate network.

Device fingerprinting assists administrators by controlling how BYOD devices access a corporate wireless domain.

Device fingerprinting uses DHCP options sent by the client in request or discover packets to derive a unique signature specific to device class. For example, Apple devices have a different signature from Android devices. The signature is used to classify the devices and assign permissions and restrictions on each device class.

NOTE: Ensure DHCP is enabled on the WLAN on which device fingerprinting is to be enabled.

To define a device fingerprinting configuration on controllers, service platforms and Access Points:

1 Select **Configuration**.

2 Select **Security**

3 Select **Device Fingerprinting**. The **Client Identity** screen displays by default populated with existing client identity configurations.

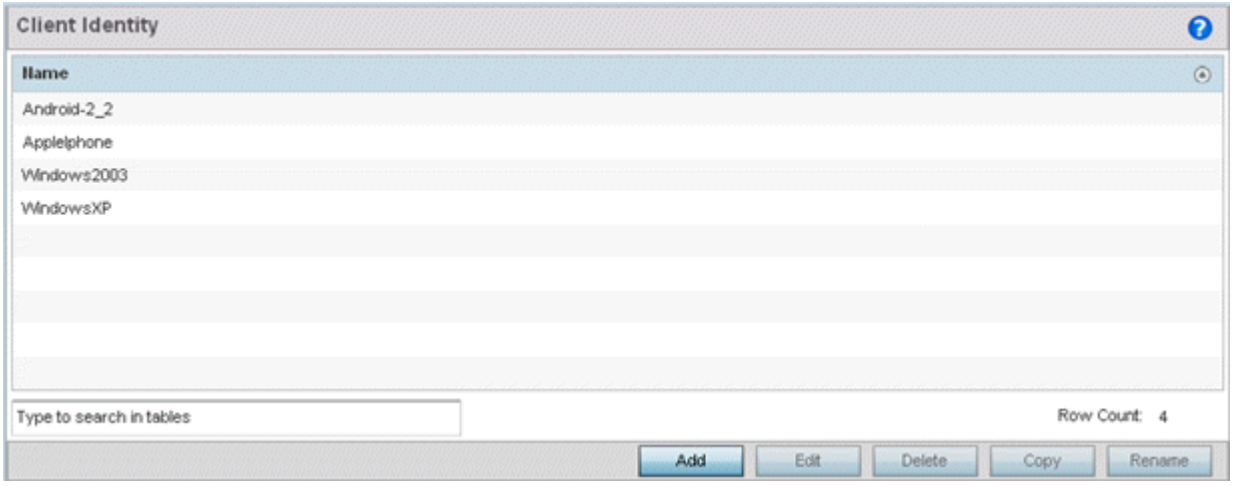


Figure 10-37 *Security - Device Fingerprinting - Client Identity screen*

4 Select **Add** to create a new client identity policy, **Edit** to modify a selected policy or **Delete** to remove obsolete policies from the list of those available. Select **Rename** to change the name of an existing client identity policy or **Copy** a policy to a different location.

Client identity policies use *signatures* to identify and group clients. Signatures are sets of attributes unique to the device model and manufacturer. Once identified, signatures classify and assign network access permissions collectively without having to administer multiple devices individually.

5 If adding a new client identity configuration, define a 32 character maximum name and select the **OK** button at the bottom of the screen to enable the remainder of the screen's editable parameters.

6 Select the **+ Add Row** button to add a new signature in the client identity.

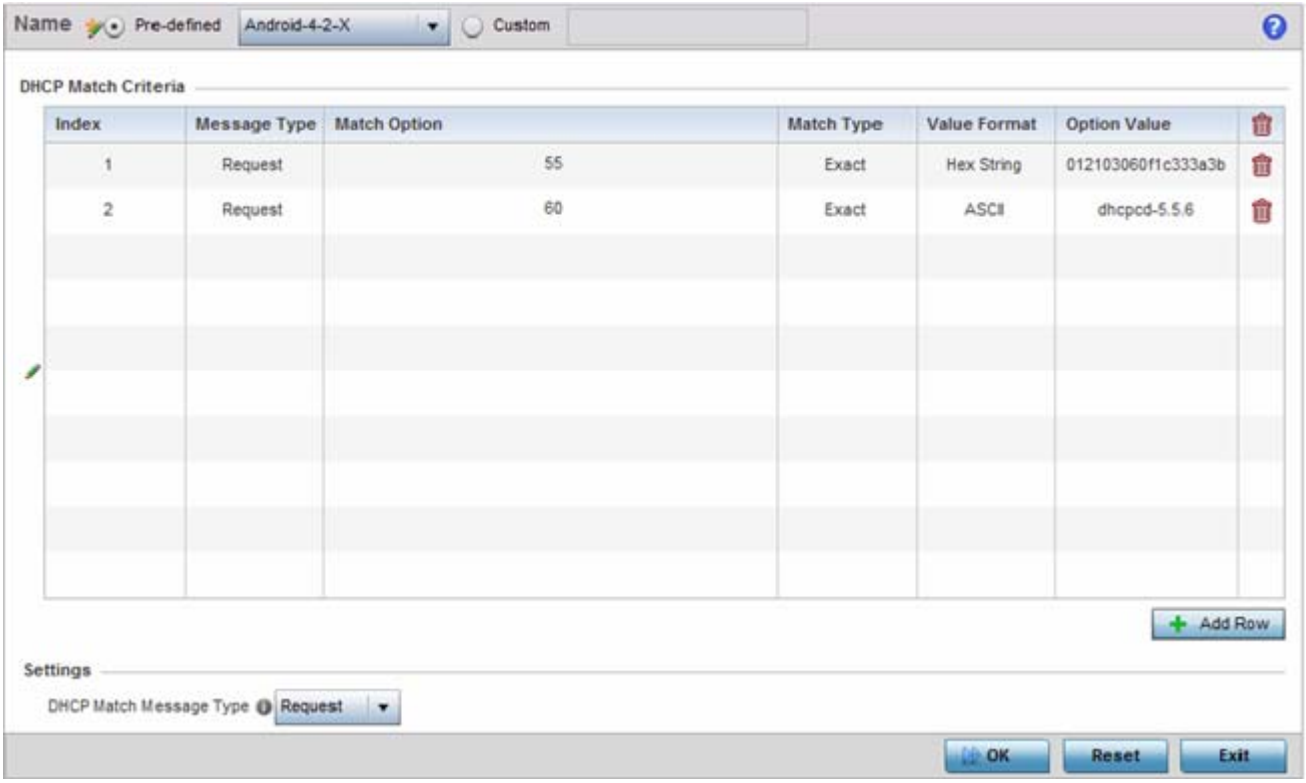


Figure 10-38 *Security - Device Fingerprining - Client Signature*

7 Optionally select **Pre-defined** and choose from a list of pre-defined client identities. Once selected, the **DHCP Match Criteria** field is populated with fingerprints for the selected client identity.

8 To create a custom identity configuration, select **Custom** and provide a name in the adjacent field. Select the **OK** button at the bottom of the screen.

9 Provide the following information for each device signature configuration:

Index	Use the spinner control to assign an index (numeric identifier) for this signature. A maximum of 16 signatures can be created.
Message Type	Use the drop-down menu to designate the DHCP message type matched for signatures. *Request* – Looks for a signature in DHCP request messages. This is the default value. *Discover* – Looks for a signature in DHCP discover messages.
Match Option	Options are passed in DHCP discover and request messages as *Option Code*, *Option Type*, and *Option Value* sets. When Option Codes is selected, the Option Code passed in the DHCP discover/request is extracted and a fingerprint is derived. The derived fingerprint is used to identify the device. *Option* – Indicates a specific DHCP Option is used to identify a device. When selected, a text box is enabled to input the DHCP Option used for fingerprinting. *Option Codes* – Indicates the Option Code passed in the DHCP request and discover message is used for matching.

Match Type	Use the drop-down menu to select how signatures are matched. Available options include: • *Exact* – The complete signature string matches the string specified in the Option Value field. • *Starts-with* – The signature is checked if it starts with the string specified in the Option Value field. • *Contains* – The signature is checked if it contains the string specified in the Option Value field.
Value Format	Use the drop-down menu to select the character format of the value being checked. The value can be either *ASCII* or *Hexadecimal*.
Option Value	Use this text box to set the 64 character maximum DHCP option value to match.

10 Use the **DHCP Match Message Type** drop-down menu (from the **Settings** field at the bottom of the screen) to specify the DHCP message type configured option values are matched against. The following options are available:

- *Discover* - Looks for a signature in DHCP discover messages.
- *Request* - Looks for a signature in DHCP request messages. This is the default value.
- *Any* - The fingerprint is checked with either the DHCP request or the DHCP discover message.
- *All* - The fingerprint is checked with both the DHCP request and the DHCP discover message.

11 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

12 Expand the **Device Fingerprinting** menu item on the left-hand side of the screen and select **Client Identity Group**.

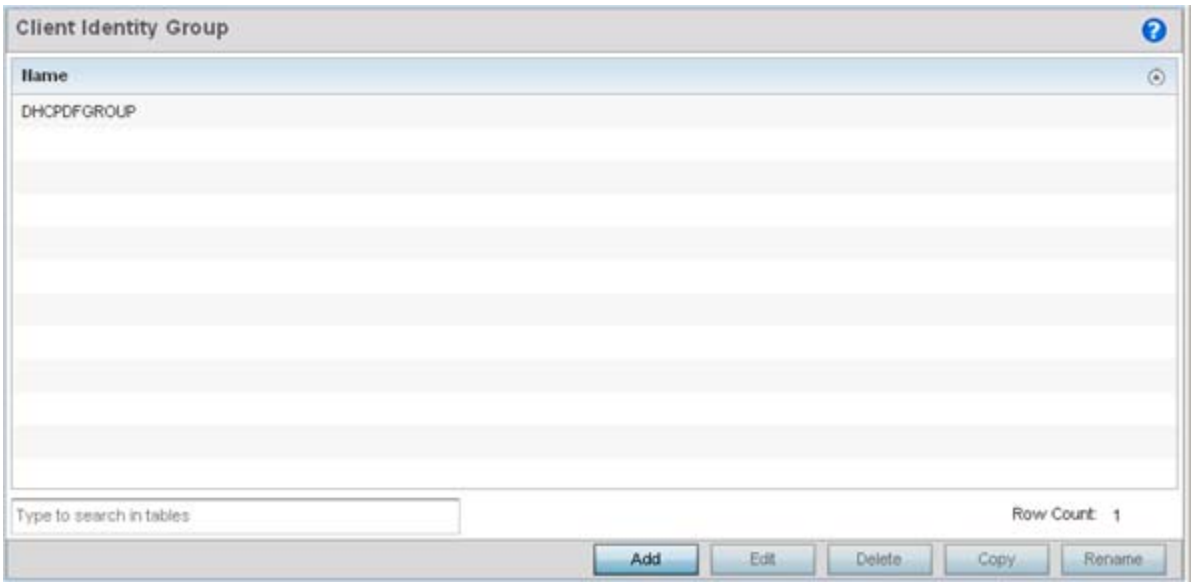


Figure 10-39 *Security - Device Fingerprining - Client Identity Group*

An *identity group* is a collection of client identity variables. Each client identity in the group is set a value indicating its priority when device fingerprinting.

Device fingerprinting relies on specific information sent by a client when acquiring an IP address and configuration information from a DHCP server. Device fingerprinting uses the DHCP options sent by the wireless client in DHCP request or discover packets to derive a signature specific to a device class. For

example, Apple devices have a different signature from Android devices. The signature is used to classify the devices and assign permissions and restrictions on each class.

13 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available. Select **Rename** to change the name of an existing policy or **Copy** a policy to a different location.

Client identity group policies configure the signatures used to identify clients and use the signatures to classify and assign network access permissions.

14 If adding a new client identity group, provide a 32 character maximum name and select the **OK** button at the bottom of the screen.

15 Select the **+ Add Row** button to populate the screen Client Identity and Precedence parameters.

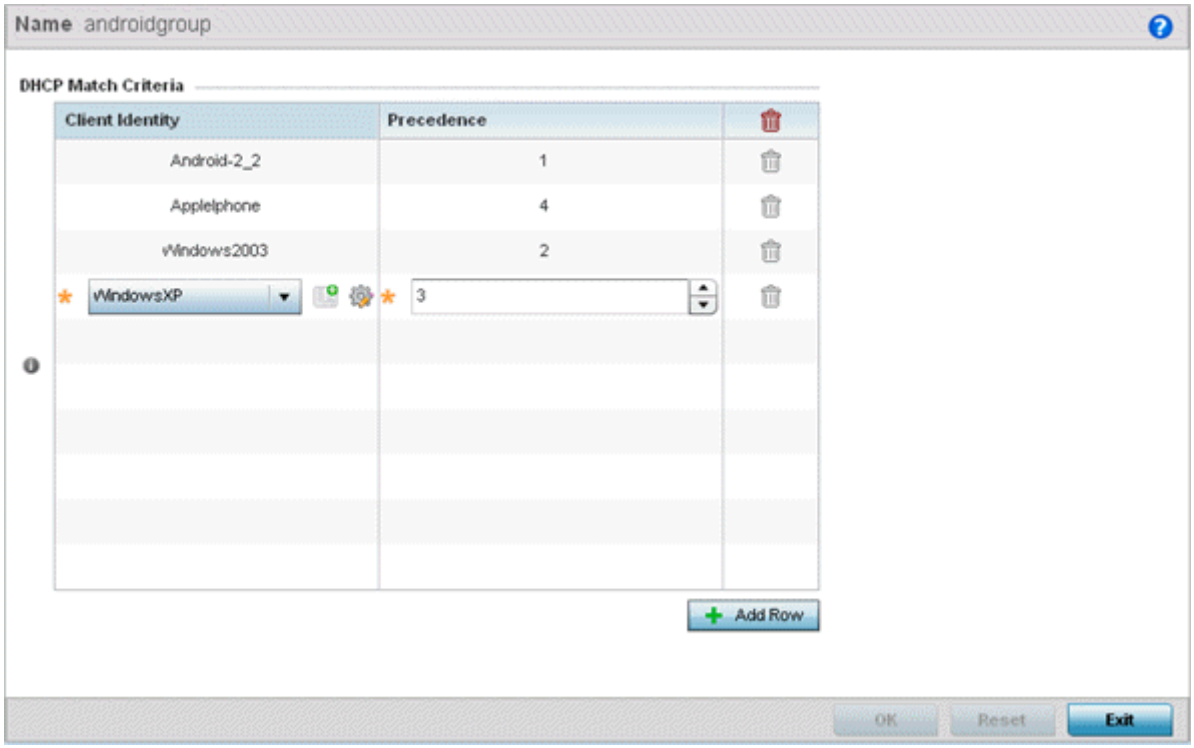


Figure 10-40 *Security - Device Fingerprining - Client Identity Group - New Client Identity Group*

16 Select the **Client Identity** policy to include in this group from the drop-down menu.

17 Use the **Precedence** spinner control to set the sequence (or priority) each listed client identity is checked or matched. Lower integers are assigned the highest priority.

18 Click **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

10.5 Intrusion Prevention

Wireless Intrusion Protection Systems (WIPS) provides continuous protection against wireless threats and acts as an additional layer of security complementing wireless VPNs and encryption and authentication policies. WIPS is supported through the use of dedicated sensor devices designed to actively detect and locate unauthorized AP devices. After detection, they use mitigation techniques to block the devices by manual termination or air lockdown.

Unauthorized APs are untrusted Access Points connected to a LAN that accept client associations. They can be deployed for illegal wireless access to a corporate network, implanted with malicious intent by an attacker, or could just be misconfigured Access Points that do not adhere to corporate policies. An attacker can install an unauthorized AP with the same ESSID as the authorized WLAN, causing a nearby client to associate to it. The unauthorized AP can then steal user credentials from the client, launch a man-in-the middle attack or take control of wireless clients to launch denial-of-service attacks.

WiNG managed wireless controllers and Access Points support unauthorized AP detection, location and containment natively. A WIPS server can alternatively be deployed (in conjunction with the wireless controller) as a dedicated solution within a separate enclosure. When used within a wireless controller managed network and its associated Access Point radios, a WIPS deployment provides the following enterprise class security management features and functionality:

- *Threat Detection* - Threat detection is central to a wireless security solution. Threat detection must be robust enough to correctly detect threats and swiftly help protect the wireless controller managed wireless network.
- *Rogue Detection and Segregation* - A WIPS supported wireless controller distinguishes itself by both identifying and categorizing nearby Access Points. WIPS identifies threatening versus non-threatening Access Points by segregating Access Points attached to the network (unauthorized APs) from those not attached to the network (neighboring Access Points). The correct classification of potential threats is critical in order for administrators to act promptly against rogues and not invest in a manual search of neighboring Access Points to isolate the few attached to the network.
- *Locationing* - Administrators can define the location of wireless clients as they move throughout a site. This allows for the removal of potential rogues though the identification and removal of their connected Access Points.
- *WEP Cloaking* - WEP Cloaking protects organizations using the *Wired Equivalent Privacy* (WEP) security standard to protect networks from common attempts used to crack encryption keys. There are several freeware WEP cracking tools available and 23 known attacks against the original 802.11 encryption standard; even 128-bit WEP keys take only minutes to crack. WEP Cloaking module enables organizations to operate WEP encrypted networks securely and to preserve their existing investment in mobile devices.

10.5.1 Configuring a WIPS Policy

Intrusion Prevention

To configure a WIPS policy:

1 Select **Configuration** > **Security** > **Intrusion Prevention**.

2 Expand the Intrusion Prevention option within the **Configuration** > **Security** menu to display the *WIPS Policy* and *Device Categorization* items available.

The Wireless IPS screen displays by default. The Wireless IPS screen lists existing WIPS policies if any are configured. Any of these existing WIPS policies can be selected and applied.

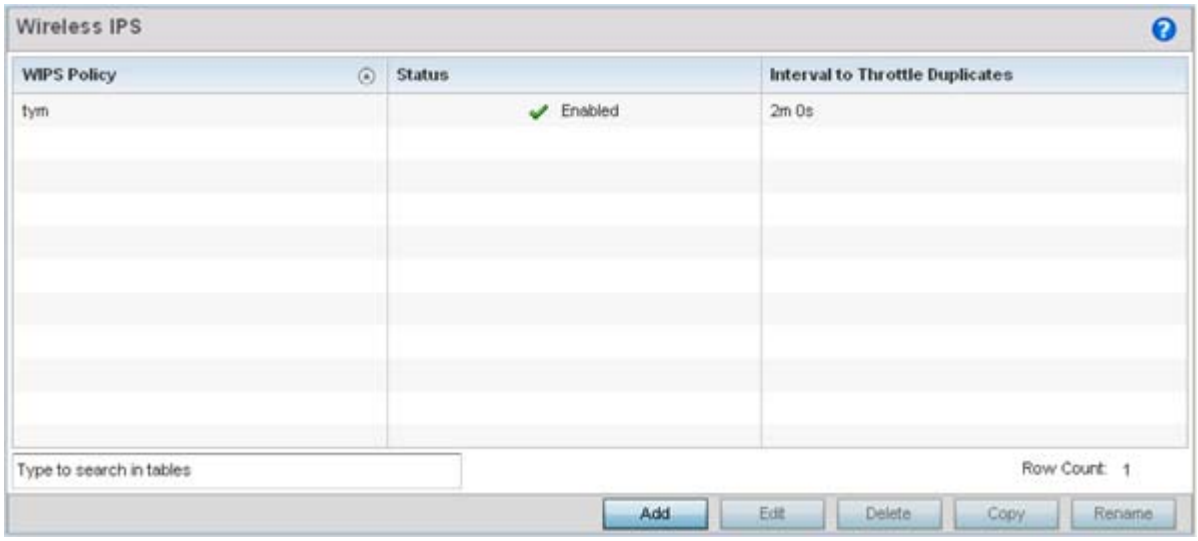


Figure 10-41 *Wireless IPS screen*

3 Refer to the following for existing WIPS policies:

WIPS Policy	Displays the name assigned to the WIPS policy when it was initially created. The name cannot be modified as part of the edit process.
Status	Displays a green checkmark if the listed WIPS policy is enabled and ready for use with a profile. A red "X" designated the listed WIPS policy as disabled.
Interval to Throttle Duplicates	Displays the duration when event duplicates (redundant events) are *not* stored in event history.

4 Select **Add** to create a new WIPS policy, **Edit** to modify the attributes of a selected policy or **Delete** to remove obsolete policies from the list of those available. Select **Rename** to change the name of an existing policy or **Copy** a policy to a different location.

If adding or editing an existing WIPS policy, the WIPS Policy screen displays with the **Settings** tab displayed by default.

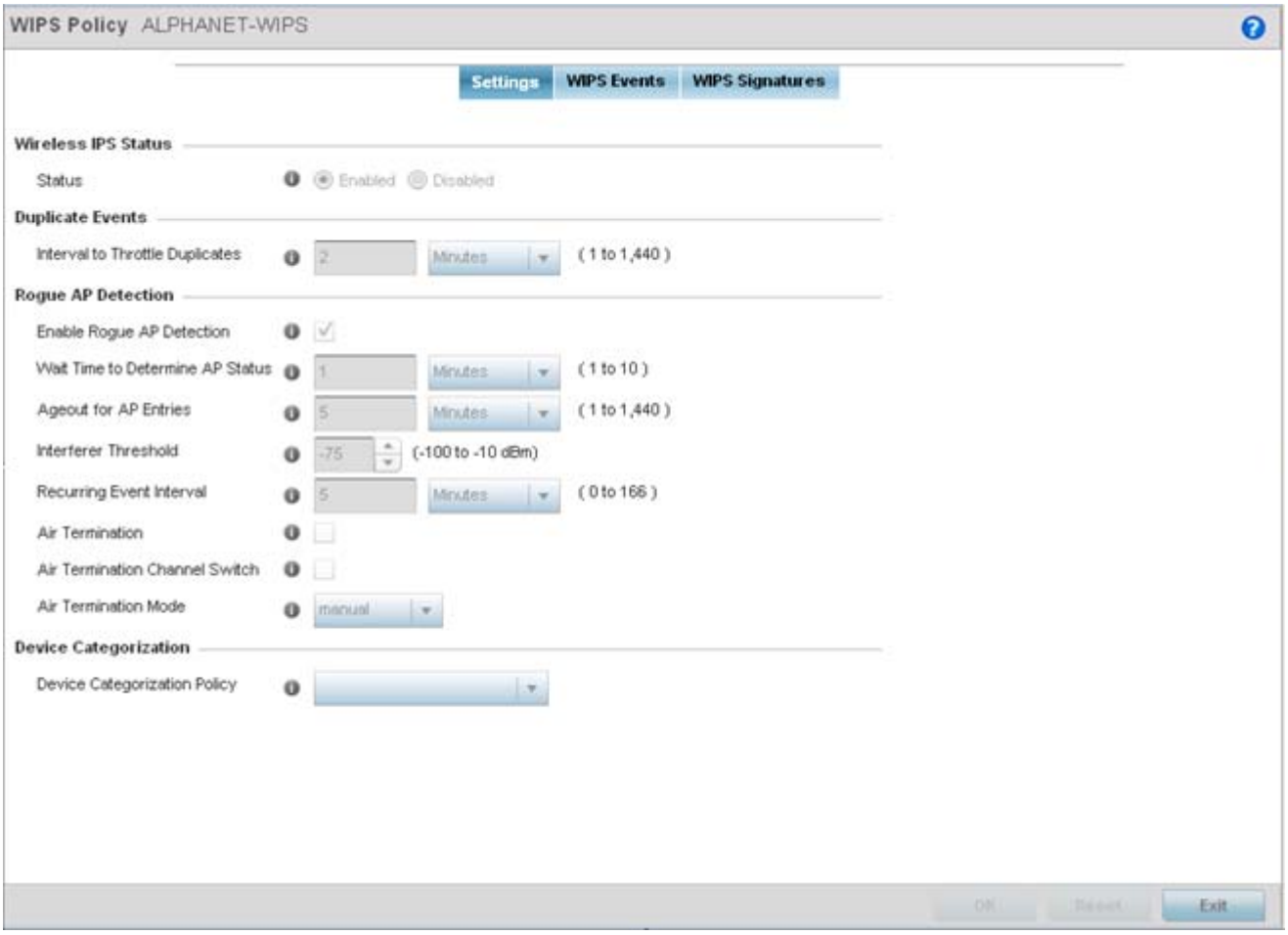


Figure 10-42 *WIPS Policy screen - Settings tab*

5 If creating a new **WIPS Policy**, assign it name to help differentiate it from others that may have a similar configuration. The policy name cannot exceed 64 characters. The name cannot be modified as part of the edit process.

6 Within the **Wireless IPS Status** field, select either the *Enabled* or *Disabled* radio button to either activate or de-activate the WIPS policy. The default setting is enabled.

7 Enter the **Interval to Throttle Packets** in either *Seconds* (1 - 86,400), *Minutes* (1 - 1,400), *Hours* (1 - 24) or *Days* (1). This interval represents the duration event duplicates are *not* stored in history. The default setting is 2 minutes.

8 Refer to the **Rogue AP Detection** field to define the following detection settings for this WIPS policy:

Enable Rogue AP Detection	Select the checkbox to enable the detection of unauthorized (unsanctioned) devices fro this WIPS policy. The default setting is disabled.
Wait Time to Determine AP Status	Define a wait time in either *Seconds* (10 - 600) or *Minutes* (1 - 10) before a detected AP is interpreted as a rogue (unsanctioned) device, and potentially removed. The default interval is 1 minute.
Ageout for AP Entries	Set the interval the WIPS policy uses to ageout rogue devices. Set the policy in either *Seconds* (30 - 86,400), *Minutes* (1- 1,440), *Hours* (1 - 24) or *Days* (1). The default setting is 5 minutes.

Interferer Threshold	Specify a RSSI threshold (from -100 to -10 dBm) after which a detected Access Point is classified as an interferer (rogue device).
Recurring Event Interval	Set an interval that, when exceeded, duplicates a rogue AP event if the rogue devices is still active (detected) in the network. The default setting is 5 minutes.
Air Termination	Select this option to enable the termination of detected rogue AP devices. Air termination lets you terminate the connection between your wireless LAN and any Access Point or client associated with it. If the device is an Access Point, all clients dis-associated with the Access Point. If the device is a client, its connection with the Access Point is terminated. This setting is disabled by default.
Air Termination Channel Switch	Select this option to allow neighboring Access Points to switch channels for rogue AP termination. This setting is disabled by default.
Air Termination Mode	If termination is enabled, use the drop-down menu to specify the termination mode used on detected rogue devices. The default setting is manual.

9 Use the **Device Categorization Policy** drop-down menu to select a policy describing whether a device is filtered as sanctioned, a client or Access Point and the MAC and SSID addresses used as filtering mechanisms.

If a policy requires creation, select the **Create** button. If an existing policy requires modification, select the **Edit** button and update the Device Categorization Policy as needed.

10 Select **OK** to update the settings. Select **Reset** to revert to the last saved configuration.

11 Select the **WIPS Events** tab to enable events, filters and threshold values for this WIPS policy. The **Excessive** tab displays by default.

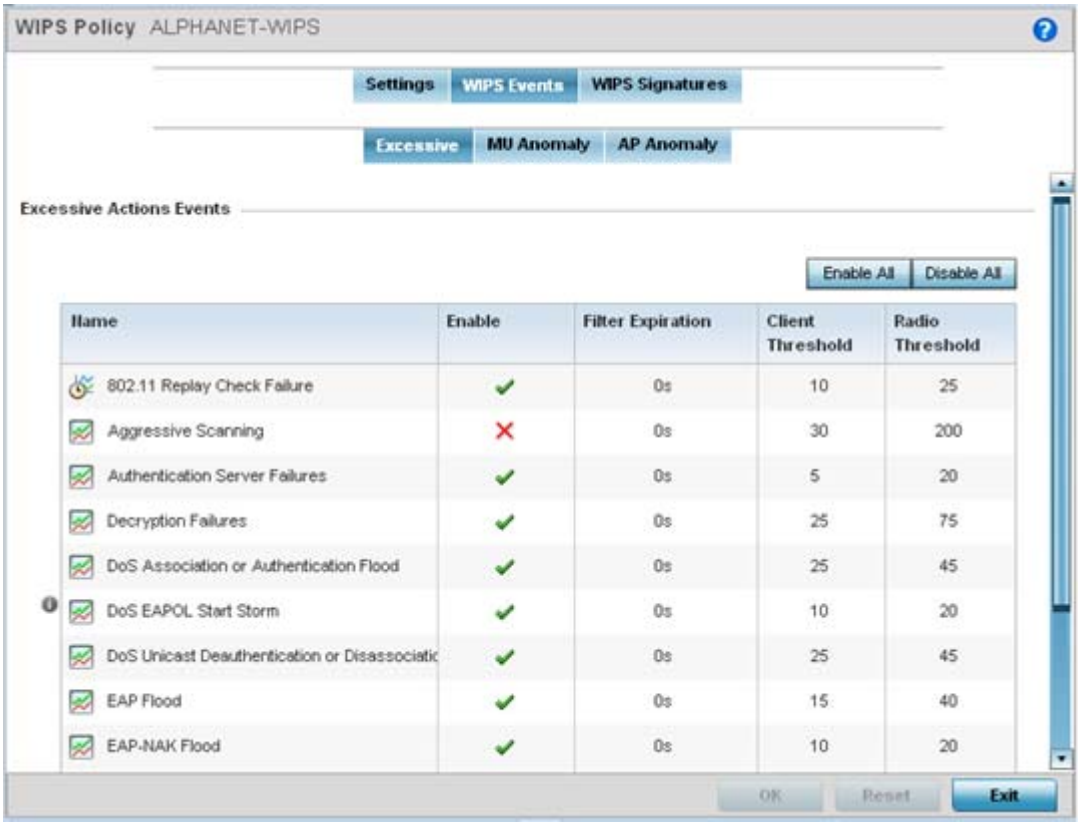


Figure 10-43 *WIPS Events screen - Excessive tab*

The Excessive tab lists a series of events that can impact the performance of the network. An administrator can enable or disable the filtering of each listed event and set the thresholds required for the generation of the event notification and filtering action.

An Excessive Action Event is an event where an action is performed repetitively and continuously. DoS attacks come under this category. Use the *Excessive Action Events* table to select and configure the action taken when events are triggered.

AP events can be globally enabled and disabled as required using the **Enable All** and **Disable All** buttons on the top-right-hand, side of the screen.

12 Set the configurations of the following **Excessive Action Events**:

Name	Displays the name of the excessive action event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted.
Enable	Displays whether tracking is enabled for each Excessive Action Event. Use the drop-down menu to enable/disable events as required. A green checkmark defines the event as enabled for tracking against its threshold values. A red “X” defines the event as disabled and not tracked by the WIPS policy. Each event is disabled by default. Events can be globally enabled and disabled as required using the *Enable All* and *Disable All* buttons on the top-right-hand, side of the screen.

Filter Expiration	Set the duration the anomaly causing client is filtered. This creates a special ACL entry and frames coming from the client are silently dropped. The default setting is 0 seconds. This value is applicable across the RF Domain. If a station is detected performing an attack and is filtered by one of the APs, the information is passed to the domain controller or service platform. The domain controller or service platform then propagates this information to all APs in the RF Domain.
Client Threshold	Set the client threshold after which the filter is triggered and an event generated.
Radio Threshold	Set the radio threshold after which an event is recorded to the events history.

13 Select **OK** to save the updates to the to excessive actions configuration used by the WIPS policy. Select **Reset** to revert to the last saved configuration.

14 Select the **MU Anomaly** tab:

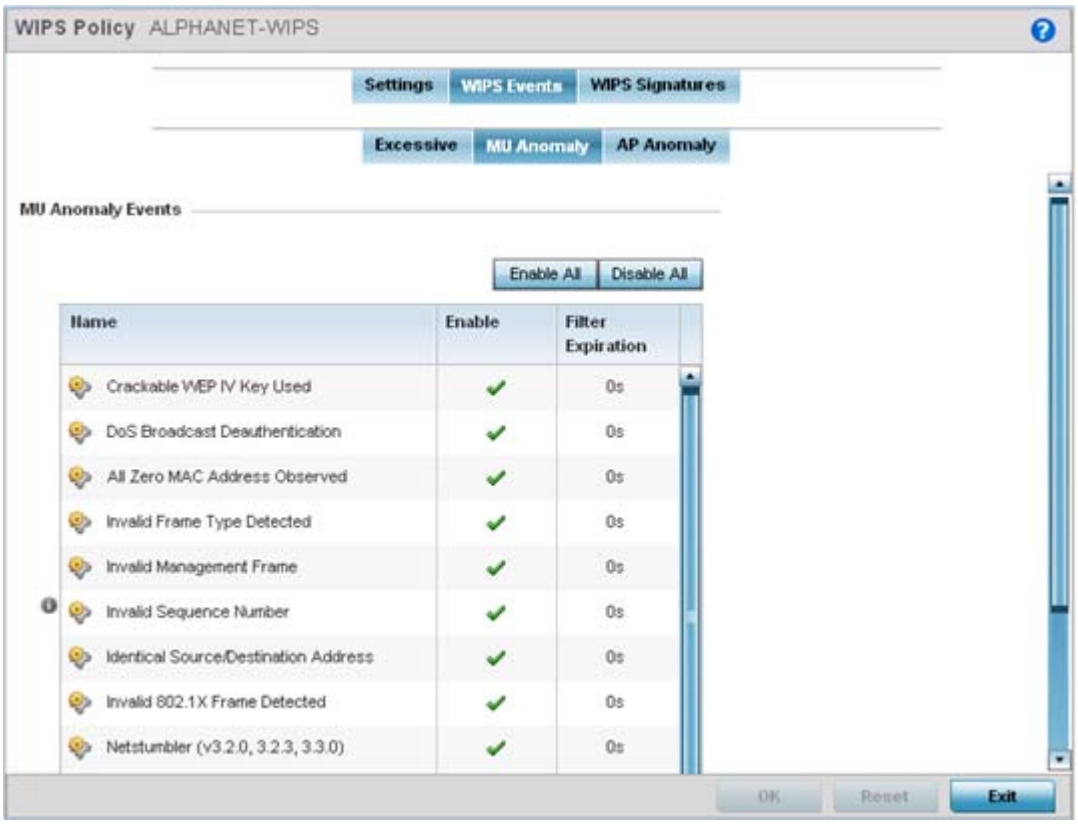


Figure 10-44 *WIPS Events screen - MU Anomaly tab*

MU anomaly events are suspicious events by wireless clients that can compromise the security and stability of the network. Use this MU anomaly screen to configure the intervals clients can be filtered upon the generation of each defined event.

MU events can be globally enabled and disabled as required using the **Enable All** and **Disable All** buttons on the top-right-hand, side of the screen.

15 Set the configurations of the following **MU Anomaly Events** configurations:

Name	Displays the name of the MU anomaly event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted.
Enable	Displays whether tracking is enabled for each event. Use the drop-down menu to enable/disable events as required. A green checkmark defines the event as enabled for tracking against its threshold values. A red "X" defines the event as disabled and not tracked by the WIPS policy. Each event is disabled by default. MU events can be globally enabled and disabled as required using the *Enable All* and *Disable All* buttons on the top-right-hand, side of the screen.
Filter Expiration	Set the duration the anomaly causing client is filtered. This creates a special ACL entry and frames coming from the client are silently dropped. The default setting is 0 seconds. For each violation, define a time to filter value in seconds which determines how long received packets are ignored from an attacking device once a violation has been triggered. Ignoring frames from an attacking device minimizes the effectiveness of the attack and the impact to the site until permanent mitigation can be performed.

16 Select **OK** to save the updates to the MU anomaly configuration used by the WIPS policy. Select **Reset** to revert to the last saved configuration.

17 Select the **AP Anomaly** tab.

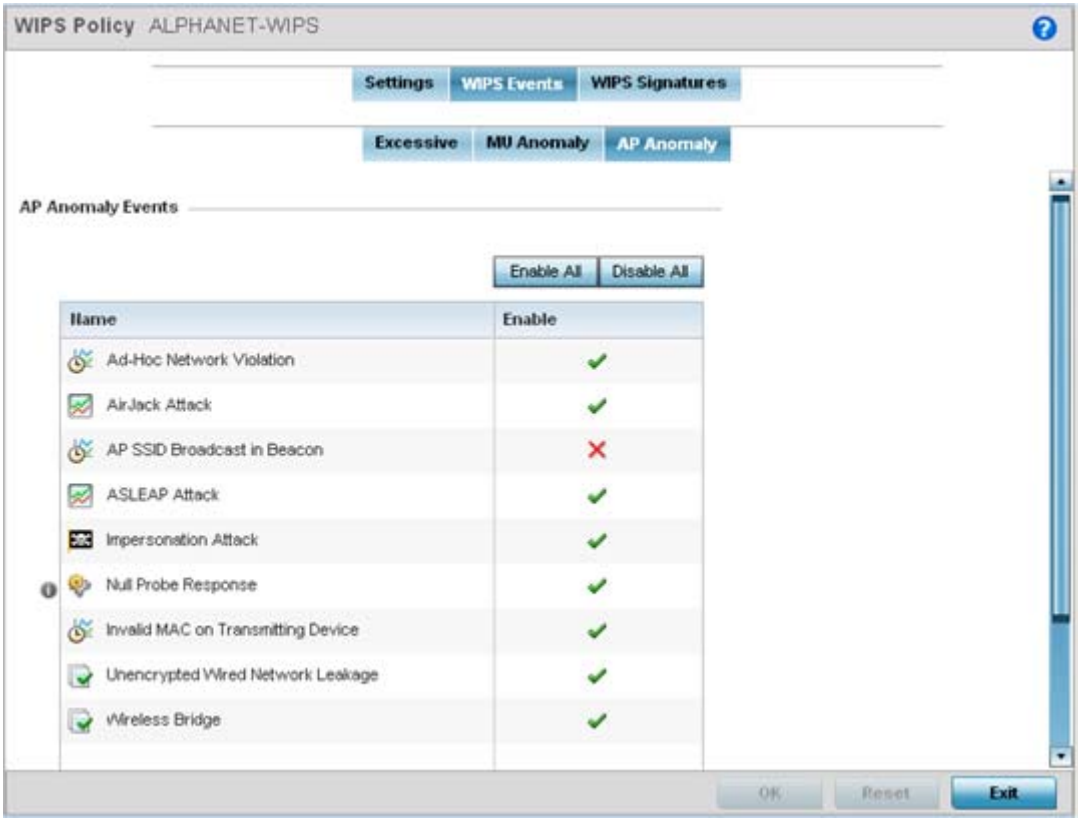


Figure 10-45 *WIPS Events screen - AP Anomaly tab*

AP anomaly events are suspicious frames sent by a neighboring APs. Use this screen to determine whether an event is enabled for tracking.

AP events can be globally enabled and disabled as required using the **Enable All** and **Disable All** buttons on the top-right-hand, side of the screen.

18 Set the following **AP Anomaly Events** parameters:

Name	Displays the name of the AP anomaly event representing a potential threat to the network. This column lists the event being tracked against the defined thresholds set for interpreting the event as excessive or permitted.
Enable	Displays whether tracking is enabled for each AP anomaly event. Use the drop-down menu to enable/disable events as required. A green checkmark defines the event as enabled for tracking against its threshold values. A red "X" defines the event as disabled and not tracked by the WIPS policy. Each event is disabled by default. AP events can be globally enabled and disabled as required using the *Enable All* and *Disable All* buttons on the top-right-hand, side of the screen.

19 Select **OK** to save the updates to the AP anomaly configuration used by the WIPS policy. Select **Reset** to revert to the last saved configuration.

20 Select the **WIPS Signatures** tab.

A WIPS signature is the set or parameters, or pattern, used by WIPS to identify and categorize particular sets of attack behaviors in order to classify them

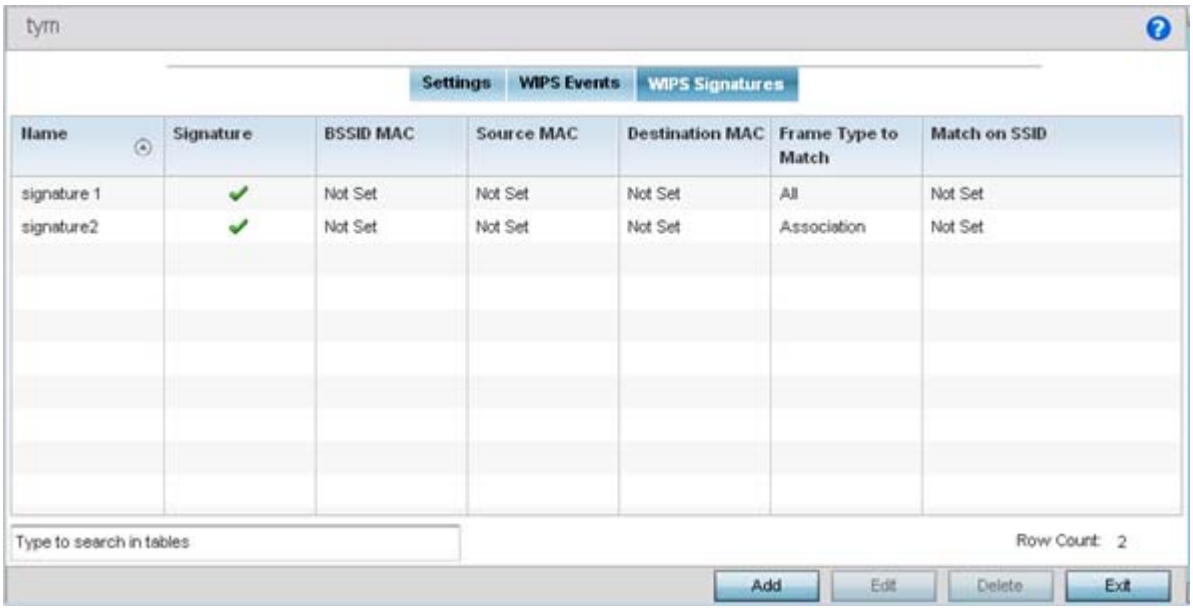


Figure 10-46 *WIPS Signatures screen*

21 The **WIPS Signatures** screen displays the following read-only data:

Name	Lists the name (in the top left-hand corner) assigned to each signature when it was created. A signature name cannot be modified as part of the edit process.
Signature	Displays whether the signature is enabled. A green checkmark defines the signature as enabled. A red "X" defines the signature as disabled. Each signature is disabled by default.
BSSID MAC	Displays each BSS ID MAC address used for matching purposes and potential device exclusion.

Source MAC	Displays each source MAC address of the packet examined for matching purposes and potential device exclusion.
Destination MAC	Displays each destination MAC address of the packet examined for matching purposes and potential device exclusion.
Frame Type to Match	Lists the frame types specified for matching with the WIPS signature.
Match on SSID	Lists each SSID used for matching purposes.

22 Select **Add** to create a new WIPS signature, **Edit** to modify the attributes of a selected WIPS signature or **Delete** to remove obsolete signatures from the list of those available.

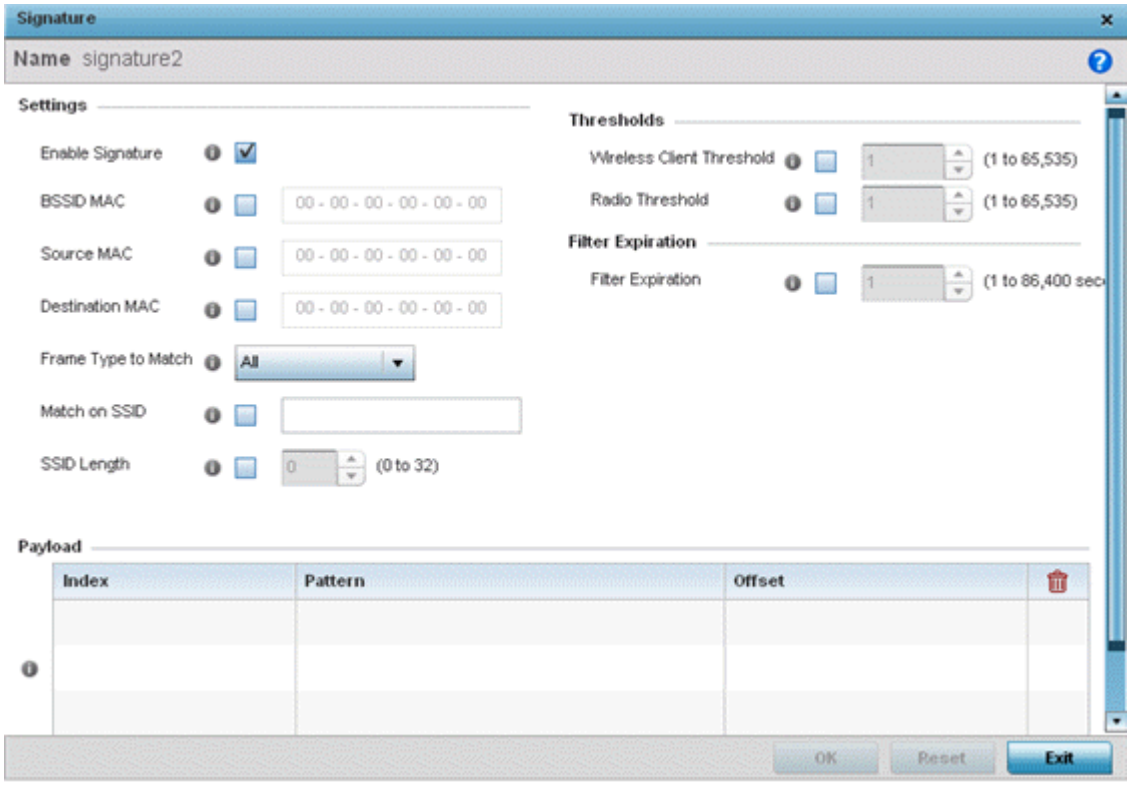


Figure 10-47 *WIPS Signatures Configuration screen*

23 If adding a new WIPS signature, define a **Name** to distinguish it from others with similar configurations. The name cannot exceed 64 characters.

24 Set the following network address information for a new or modified WIPS Signature:

Enable Signature	Select the check box to enable the WIPS signature for use with the profile. The default signature is enabled.
BSSID MAC	Define a BSS ID MAC address used for matching and filtering with the signature.
Source MAC	Define a source MAC address for packets examined for matching, filtering and potential device exclusion using the signature.
Destination MAC	Set a destination MAC address for the packet examined for matching, filtering and potential device exclusion with the signature.
Frame Type to Match	Use the drop-down menu to select a frame type for matching and filtering with the WIPS signature.

Match on SSID	Set the SSID used for matching and filtering with the signature. Ensure it's specified properly or the SSID won't be properly filtered.
SSID Length	Set the character length of the SSID used for matching and filtering with this signature. The maximum length is 32 characters.

25 Refer to **Thresholds** field to set signature threshold limitations used as filtering criteria.

Wireless Client Threshold	Specify the threshold limit per client that, when exceeded, signals the event. The configurable range is from 1 - 65,535.
Radio Threshold	Specify the threshold limit per radio that, when exceeded, signals the event. The configurable range is from 1 - 65,535.

26 Set a **Filter Expiration** (from 1 - 86,400 seconds) that specifies the duration a client is excluded from RF Domain manager radio association when responsible for triggering a WIPS event.

27 Refer to the **Payload** table to set a numerical index pattern and offset for the WIPS signature. Select **+ Add Row** and provide an **Index**, **Pattern** and **Offset** variable for the payload.

28 Select **OK** to save the updates to the WIPS Signature configuration. Select **Reset** to revert to the last saved configuration.

10.5.2 Configuring a WIPS Device Categorization Policy

Intrusion Prevention

Having devices properly classified can help suppress unnecessary unsanctioned AP alarms and allow an administrator to focus on the alarms and devices actually behaving in a suspicious manner. An intruder with a device erroneously authorized could potentially perform activities that harm your organization while appearing to be legitimate. WIPS enables devices to be categorized as Access Points, then defined as *sanctioned* or *unsanctioned* within the network.

Sanctioned Access Points are generally known to you and conform with your organization's security policies. Unsanctioned devices have been detected as interoperating within the managed network, but are not approved. These devices should be filtered to avoid jeopardizing data.

To categorize Access Points as sanctioned or unsanctioned:

1 Select **Configuration** > **Security** > **Intrusion Prevention**.

2 Expand the Intrusion Prevention option within the Configuration > Security menu and select **Device Categorization.**

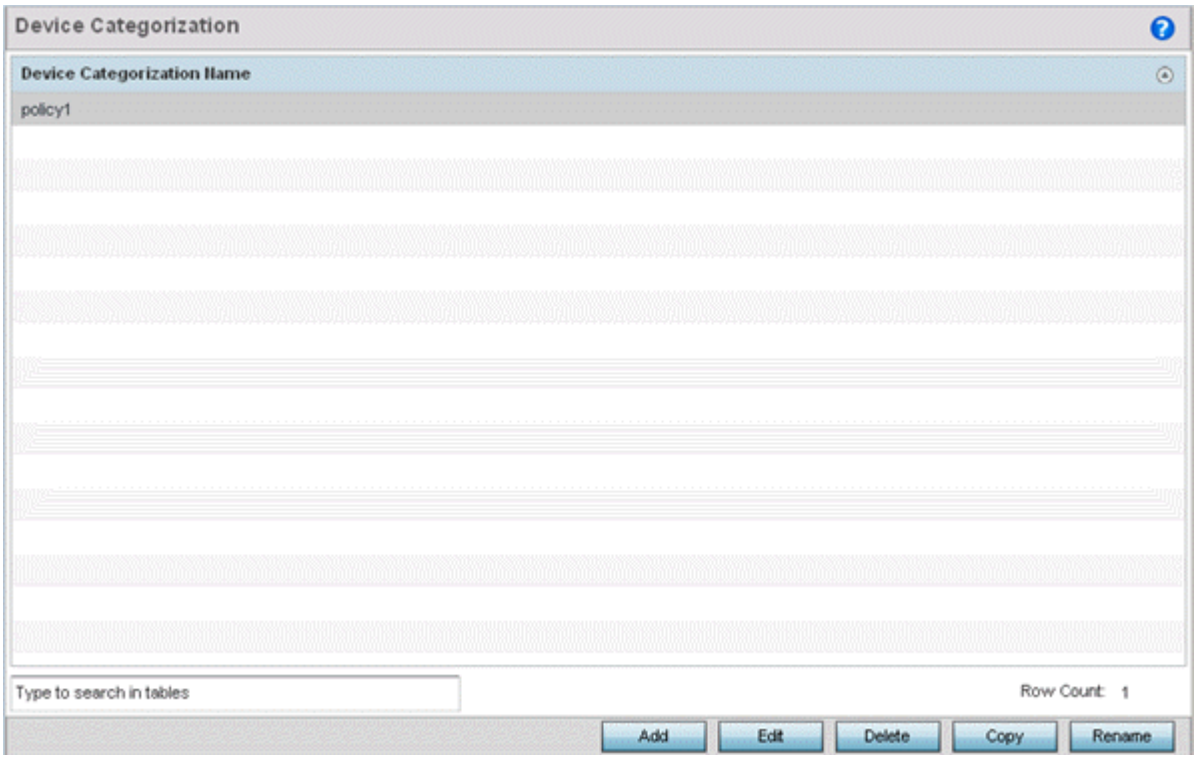


Figure 10-48 *WIPS Device Categorization screen*

The **Device Categorization** screen lists those device authorization policies defined thus far.

3 Select **Add** to create a new policy, **Edit** to modify the attributes of a selected existing policy or **Delete** to remove obsolete policies from those available. Select **Rename** to change the name of a policy or **Copy** a policy to a different location.

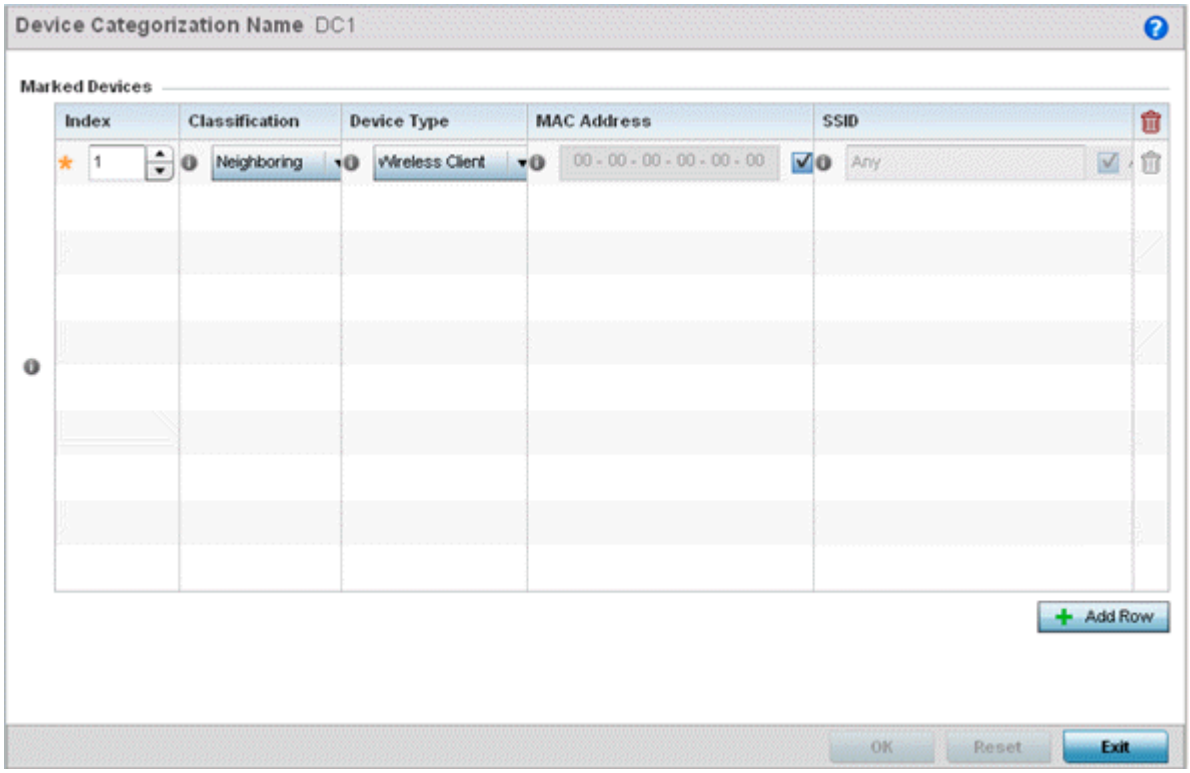


Figure 10-49 *WIPS Device Categorization Configuration screen*

4 If creating a new Device Categorization policy, provide it a **Name** (up to 64 characters) to distinguish this policy from others with similar configurations. Select **OK** to save the name and enable the remaining parameters on the screen.

5 Select **+ Add Row** to populate the **Marked Devices** field with parameters for adding an Access Point's MAC address, SSID, Access Point designation and network authorization. Select the red (-) **Delete Row** icon as needed to remove an individual table entry.

6 Define the following parameters to add a device to a list of devices categorized as sanctioned or unsanctioned for network operation:

Index	Use the spinner controls to set the numerical *Index* number for each Device Categorization Name.
Classification	Use the drop-down menu to designate the target device as either sanctioned (*True*) or unsanctioned (*False*). The default setting is False, categorizing this device as unsanctioned. Thus, each added device requires authorization. A green checkmark designates the device as sanctioned, while a red "X" defines the device as unsanctioned.
Device Type	Use the drop-down menu to designate the target device as either an Access Point (*True*) or other (*False*). The default setting is False, categorizing this device as other than an Access Point. A green checkmark designates the device as an Access Point, while a red "X" defines the categorized device as other than an Access Point.
MAC Address	Enter the factory coded MAC address of the target device. This address is hard coded by the device manufacturer and cannot be modified. The MAC address will be defined as sanctioned or unsanctioned as part of the device categorization process.

SSID	Enter the SSID of the target device requiring categorization. The SSID cannot exceed 32 characters.

7 Select **OK** to save the updates to the **Marked Devices** List. Select **Reset** to revert to the last saved configuration.

10.5.3 Intrusion Detection Deployment Considerations

Before configuring WIPS support on the wireless controller, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- WIPS is best utilized when deployed in conjunction with a corporate or enterprise wireless security policy. Since an organization's security goals vary, the security policy should document site specific concerns. The WIPS system can then be modified to support and enforce these additional security policies
- WIPS reporting tools can minimize dedicated administration time. Vulnerability and activity reports should automatically run and be distributed to the appropriate administrators. These reports should highlight areas to be to investigated and minimize the need for network monitoring.
- It's important to keep your WIPS system Firmware and Software up to date. A quarterly system audit can ensure firmware and software versions are current.
- Only a trained wireless network administrator can determine the criteria used to authorize or ignore devices. You may want to consider your organization's overall security policy and your tolerance for risk versus users' need for network access. Some questions that may be useful in deciding how to classify a device are:
  - Does the device conform to any vendor requirements you have?
  - What is the signal strength of the device? Is it likely the device is outside your physical radio coverage area?
  - Is the detected Access Point properly configured according to your organization's security policies?
- Controller or service platform visibility to all deployed VLANs is recommended. If an external L3 device has been deployed for routing services, each VLAN should be 802.1Q tagged to the controller or service platform to allow the detection any unsanctioned APs physically connected to the network.
- Trusted and known Access Points should be added to an sanctioned AP list. This will minimize the number of unsanctioned AP alarms received.

10.6 EX3500 Time Range

An **EX3500 Time Range** is a set of configurations consisting of *periodic* and *absolute* time ranges. Periodic time ranges can be configured to reoccur daily, weekly, weekends and on specific weekdays, such as Sunday. Absolute time ranges can be configured for a range of days during a particular period. Absolute time ranges do not reoccur.

The EX3500 time ranges are used when configuring EX3500 MAC ACL firewall rules. For more information, see *Configuring MAC Firewall Rules on page 10-15*.

To set an EX3500 switch periodic or absolute time ranges:

1 Select **Configuration** > **Security** > **EX3500 Time Ranges**.

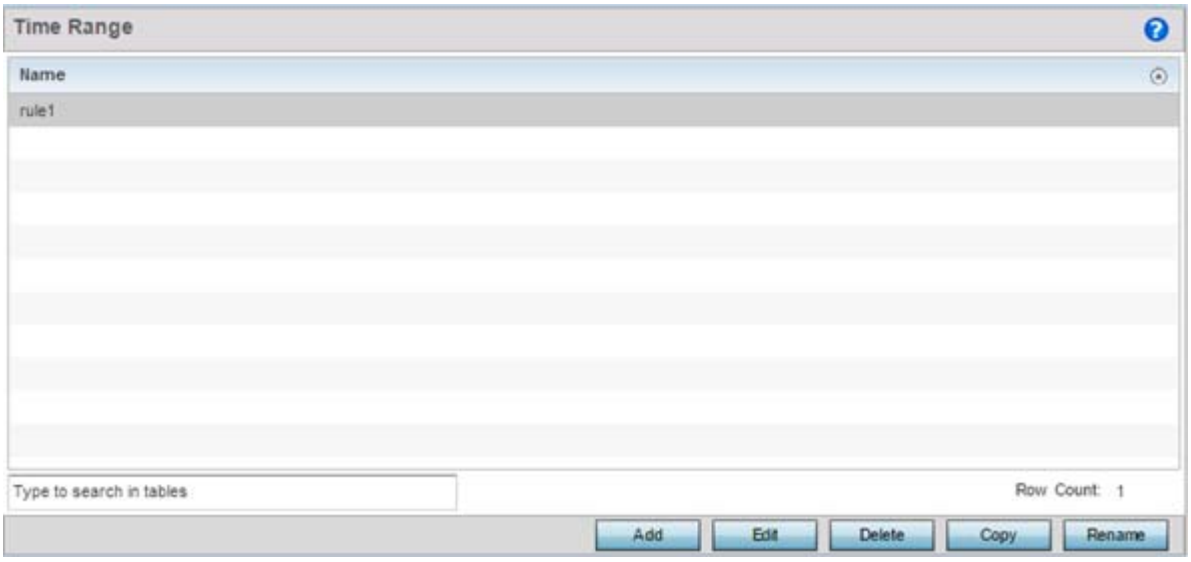


Figure 10-50 *EX3500 Time Range screen*

The Time Range screen displays within the main portion of the Web UI.

2 Select **Add** to create a new policy. **Edit** to modify the attributes of an existing time range or **Delete** to remove obsolete time ranges. Use **Copy** to create a copy of the selected time range and modify it for further use. Use **Rename** to rename the selected time range.

3 Either use the **Add** button to create an new EX3500 Time Range or select an existing range and click **Edit** to modify it.

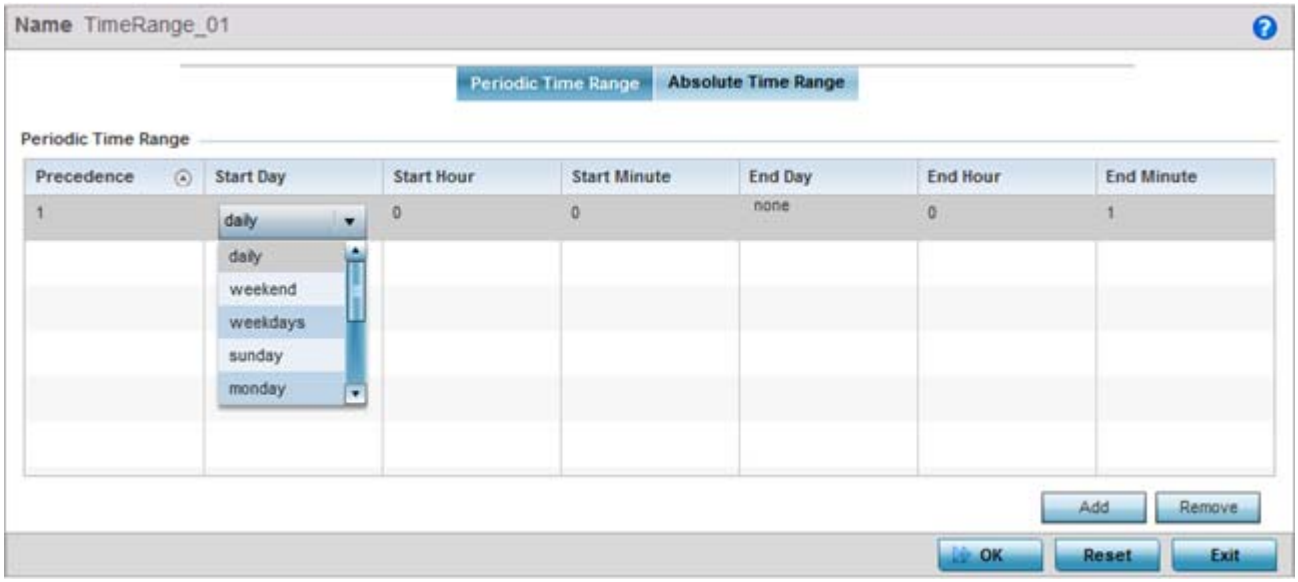


Figure 10-51 *EX3500 Time Range - Periodic Time Range screen*

The **Periodic Time Range** tab displays by default.

4 If adding a new EX3500 Time Range, provide it a name up to 32 characters.

5 Select **Add** to provide the following parameters:

Precedence	Specify or modify a precedence value for this periodic time range policy. Rules with lower precedence are always applied first. If modifying a precedence to apply a higher integer, it moves down the table to reflect its lower priority. Select a precedence value in the range 1-7.
Start Day	Specify the periodic time range's start day. Day value can be one of d*aily, weekend, weekdays, sunday, monday, tuesday, wednesday, thursday, friday* or *saturday*. Specify a start day from one of the above values.
Start Hour	Specify the periodic time range's start hour. Hours are specified in 24 hour format. Use the spinner to select the appropriate hour.
Start Minute	Specify the periodic time range's start minute. Use the spinner to select the appropriate minute.
End Day	Specify the periodic time range's end day. End day is the day when the time period ends. The options available for this field changes depending on the choice made in the *Start Day* field.
End Hour	Specify the periodic time range's end hour. Hours are specified in 24 hour format. In most cases, this value cannot be lower than the value specified in the *Start Hour* field. Use the spinner to select the correct end hour value.
End Minute	Specify the periodic time range's end minute. In most cases, this value cannot be lower than the value specified in the *Start Minute* field. Use the spinner to select the correct end.

6 Select **OK** to save the updates. Select **Reset** to revert to the last saved configuration.

7 Select the **Absolute Time Range** to configure a time range that is absolute and occurs only once.

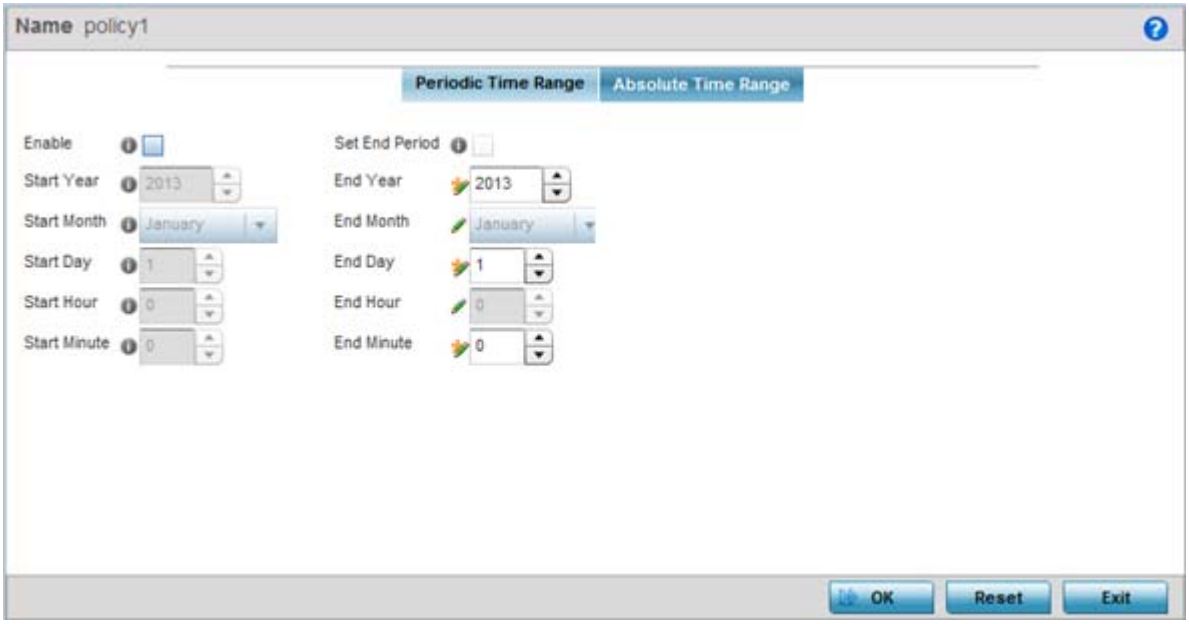


Figure 10-52 *EX3500 Time Range - Absolute Time Range screen*

8 Select **Enable** to enable this feature. Absolute time range can only be configured when Enabled.

9 Configure the following parameters:

Start Year	Specify the absolute time range's start year. Use the spinner control to select the year. Select a year in the range 2013-2037.
Start Month	Specify the absolute time range's start month. Use the drop-down menu to select the month.
Start Day	Specify the absolute time range's start day. Day value can be one of *daily, weekend, weekdays, sunday, monday, tuesday, wednesday, thursday, friday* or *saturday*. Specify a start day from one of the above values.
Start Hour	Specify the absolute time range's start hour. Hours are specified in 24 hour format. Use the spinner to select the appropriate hour.
Start Minute	Specify the absolute time range's start minute. Use the spinner to select the appropriate minute.
End Period	Select the option to set specific end periods for each of the *Year, Month, Day, Hour* and *Minute* values available for start time definitions.
End Year	Specify the absolute time range's end year. Use the spinner control to select the year. Select a year in the range 2013-2037. End year cannot be earlier than the value specified in the *Start Year* field.
End Month	Specify the absolute time range's end month. Use the drop-down menu to select the month.
End Day	Specify the absolute time range's end day. End day is the day when the time period ends. The options available for this field changes depending on the choice made in the *Start Day* field.
End Hour	Specify the absolute time range's end hour. Hours are specified in 24 hour format. In most cases, this value cannot be lower than the value specified in the *Start Hour* field. Use the spinner to select the correct end hour value.
End Minute	Specify the absolute time range's end minute. In most cases, this value cannot be lower than the value specified in the *Start Minute* field. Use the spinner to select the correct end.

10 Select **OK** when completed to update the EX3500 Time Range. Select **Reset** to revert back to its last saved configuration.

11 Services

Controllers and service platforms natively support services to provide guest user access to the network, lease DHCP IP addresses to requesting clients and provide RADIUS client authentication.

For more information, refer to the following:

- *Configuring Captive Portal Policies*
- *Setting the Guest Management Configuration*
- *Setting the DHCP Configuration*
- *Setting the Bonjour Gateway Configuration*
- *DHCPv6 Server Policy*
- *Setting the RADIUS Configuration*
- *URL Lists*

11.1 Configuring Captive Portal Policies

Services

A *captive portal* is an access policy for providing guests temporary and restrictive access to the controller or service platform managed network.

A captive portal policy provides secure authenticated controller or service platform access using a standard Web browser. Captive portals provides authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Once logged into the captive portal, additional *Terms and Agreement*, *Welcome*, *Fail* and *No Service* pages provide the administrator with a number of options on captive portal screen flow and user appearance.

Captive portal authentication is used primarily for guest or visitor access, but is increasingly used to provide authenticated access to private network resources when 802.1X EAP is not a viable option. Captive portal authentication does not provide end-user data encryption, but it can be used with static WEP, WPA-PSK or WPA2-PSK encryption.

Authentication for captive portal access requests is performed using a *username* and *password* pair, authenticated by an integrated RADIUS server. Authentication for private network access is conducted either locally on the requesting wireless client, or centrally at a datacenter.

Captive portal uses a Web provisioning tool to create guest user accounts directly on the controller or service platform. The connection medium defined for the Web connection is either *HTTP* or *HTTPS*. Both HTTP and HTTPS use a request and response procedure clients follow to disseminate information to and from requesting wireless clients.

Refer to the following sections for configuring Captive Portal Policy parameters:

- *Configuring a Captive Portal Policy*
- *Creating DNS Whitelists*
- *Captive Portal Deployment Considerations*

11.1.1 Configuring a Captive Portal Policy

Configuring Captive Portal Policies

To configure a guest access captive portal policy:

1 Select **Configuration** > **Services**.

The upper, left-hand, side of the user interface displays a **Services** menu pane where Captive Portal, DHCP and RADIUS configuration options can be selected.

2 Select **Captive Portals**.

The Captive Portal screen displays the configurations of existing policies. New policies can be created, existing policies can be modified or existing policies deleted.

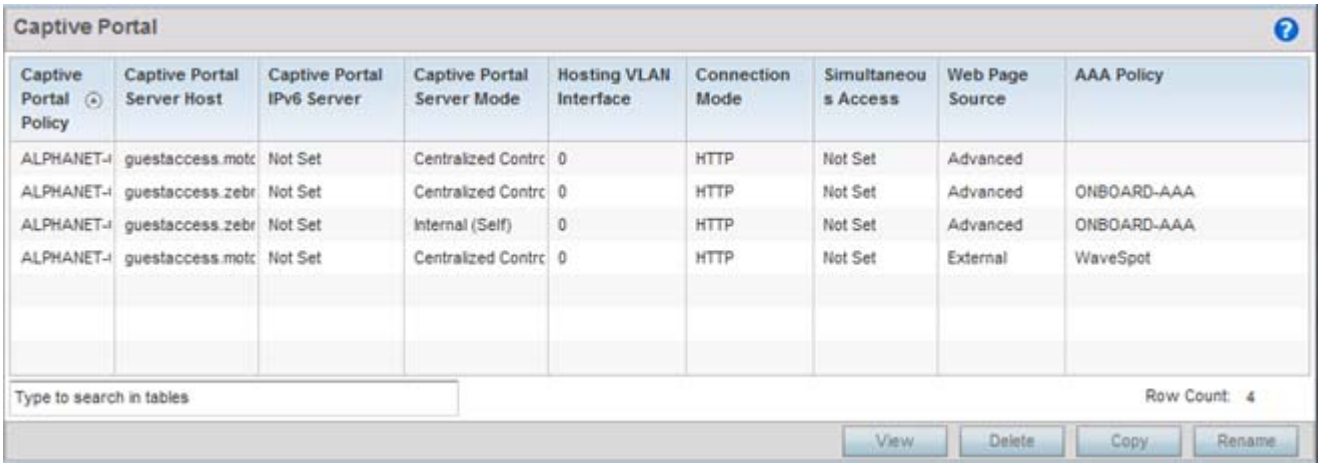


Figure 11-1 *Captive Portal Policy screen*

3 Refer to the following captive portal policy parameters to determine whether a new policy requires creation, or an existing policy requires edit or deletion:

Captive Portal Policy	Displays the name assigned to the captive portal policy when initially created. A policy name cannot be modified as part of the edit process.
Captive Portal Server Host	Lists the IP address (non DNS hostname) of the external (fixed) server validating user permissions for the listed captive portal policy. This item remains empty if the captive portal is hosted locally.
Captive Portal IPv6 Server	Lists the IPv6 formatted IP address (non DNS hostname) of the external (fixed) IPv6 server validating user permissions for the listed captive portal policy. This item remains empty if the captive portal is hosted locally. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Captive Portal Server Mode	Lists each policy's hosting mode as either *Internal (Self)* or *External (Fixed)*. If the mode is Internal (Self), the controller or service platform is maintaining the captive portal locally, while External (Fixed) means the captive portal is being hosted on an external server resource.
Hosting VLAN Interface	Lists the VLAN (from 0 - 4,096) a client utilizes for controller or service platform interoperation when the Captive Portal Server Mode is set to Centralized Controller.

Connection Mode	Lists each policy's connection mode as either *HTTP* or *HTTPS*. Both HTTP and HTTPS use the same *Uniform Resource Identifier* (URI), so requesting clients can be identified. However. the use of HTTPS is recommended, as it affords transmissions some measure of data protection HTTP cannot provide.
Simultaneous Access	Displays the number of users permitted at one time for each listed policy. A captive portal can support from 1-8192 users simultaneously.
Web Page Source	Displays whether the captive portal HTML pages are maintained *Internally*, *Externally* (on an external system you define) or are *Advanced* pages maintained and customized by the network administrator. Internal is the default setting.
AAA Policy	Lists each AAA policy used to authorize captive portal access requests. When a captive portal policy is created or modified, a AAA policy must be defined and applied to effectively authorize, authenticate and account user requests for captive portal access.

4 Select **Add** to create a new captive portal policy, **Edit** to modify an existing policy or **Delete** to remove an existing captive portal policy. Select **Rename** to change the name of an existing policy or **Copy** a policy to a different location.

A **Basic Configuration** screen displays by default. Define the policy's security, access and whitelist basic configuration before actual HTML pages can be defined for guest user access requests.

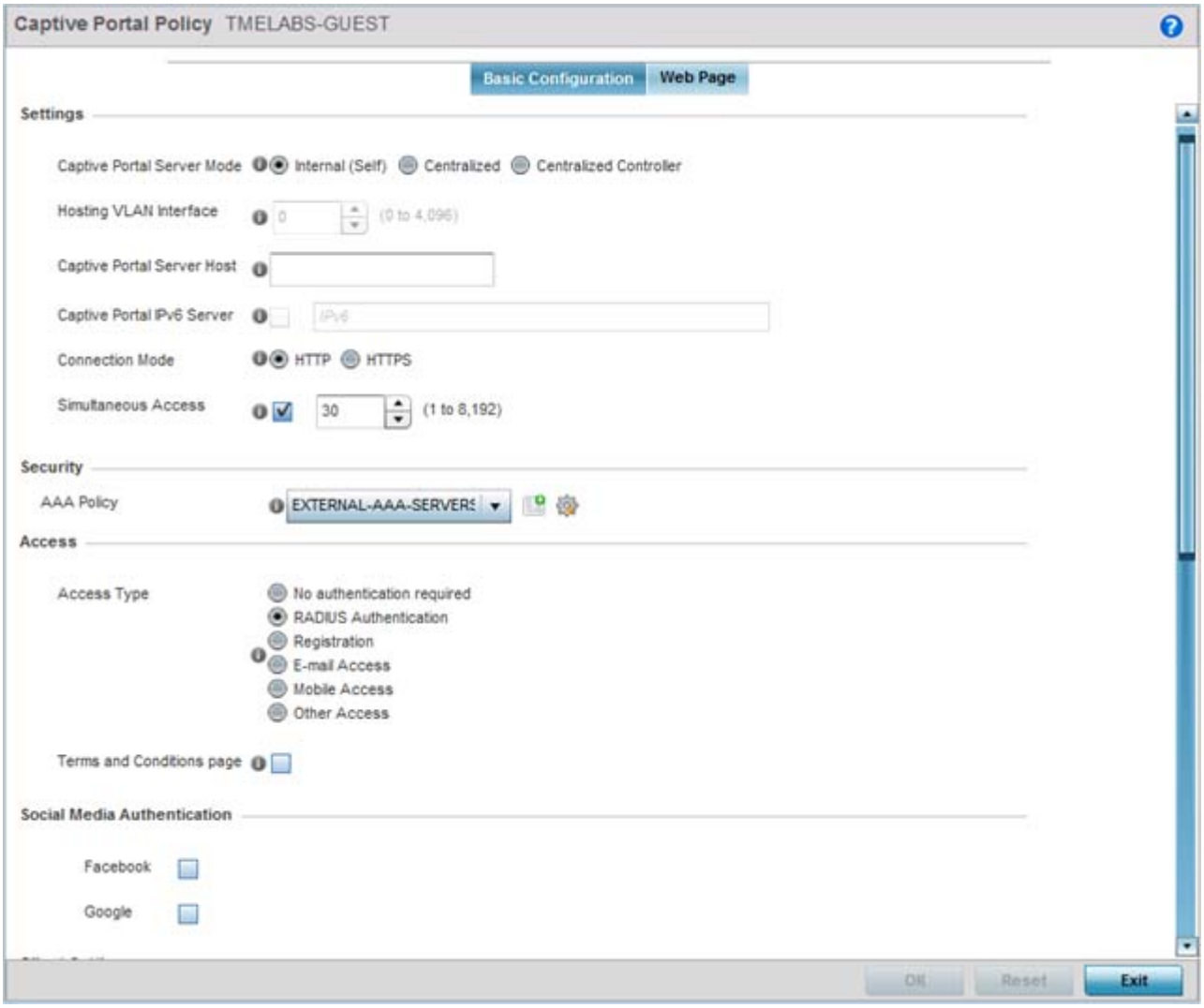


Figure 11-2 *Captive Portal Policy Basic Configuration screen*

5 Define the following **Settings** for the captive portal policy:

Captive Portal Policy	If creating a new policy, assign a name representative of its access permissions, location or intended wireless client user base. If editing an existing captive portal policy, the policy name cannot be modified. The name cannot exceed 32 characters.
Captive Portal Server Mode	Set the mode as either *Internal* (Self), *Centralized* or *Centralized Controller*. Select the *Internal* (Self) radio button to maintain the captive portal configuration (Web pages) internally. Select the *Centralized* radio button if the captive portal is supported on an external server. Select the Centralized Controller radio button if the captive portal is supported on a centralized controller or service platform. The default value is Internal (Self).
Hosting VLAN Interface	When using the Centralized Controller server mode, specify the VLAN, between 0 and 4096 for client communication. Select 0 to use the default client VLAN. 0 is the default setting.
Captive Portal Server Host	Set a numeric IP address (or DNS hostname) for the server validating guest user permissions for the captive portal policy. This option is only available if hosting the captive portal on an External (Fixed) server resource.

Captive Portal IPv6 Server	If using Centralized server mode, select this option to define an IPv6 formatted address of the controller, service platform or Access Point resource hosting the captive portal.
Connection Mode	Select either *HTTP* or *HTTPS* to define the connection medium to the Web server. The use of HTTPs is recommended, as is affords some additional data protection HTTP cannot provide. The default value however is HTTP.
Simultaneous Access	Select the checkbox and use the spinner control to set from 1-8192 users (client MAC addresses) allowed simultaneous access to the captive portal and its resources.

6 Use the **AAA Policy** drop-down menu to select the *Authentication*, *Authorization* and *Accounting* (AAA) policy used to validate user credentials and provide captive portal access to the network.

If no AAA policies exist, one must be created by selecting the **Create** icon, or an existing AAA policy can be selected and modified by selected it from the drop-down menu and selecting the **Edit** icon.

7 Set the following **Access** parameters to define access, RADIUS lookup information and whether the Login pages contain agreement terms that must be accepted before access is granted to controller or service platform resources using the captive portal:

Access Type	Select the authentication scheme applied to clients requesting captive portal guest access to the WiNG network. Within the WiNG UI there's 6 options. The WiNG CLI uses 5 options. User interface options include: *No authentication required* - Requesting clients are redirected to the captive portal Welcome page without authentication. *RADIUS Authentication* - A requesting client's user credentials require authentication before access to the captive portal is permitted. This is the default setting. *Registration* - A requesting client's user credentials require authentication through social media credential exchange. *Email Access* - Clients use E-mail username and passwords for authenticating their captive portal session. Optionally set whether E-mail access requests are RADIUS validated. *Mobile Access* - Mobile clients use their device's access permissions for authenticating their captive portal session. Optionally set whether mobile access requests are RADIUS validated. *Other Access* - Requesting guest clients use a different means of captive portal session access (aside from E-mail or mobile device permissions). Optionally set whether these other access requests are RADIUS validated.
Lookup Information	When either *E-mail Access, Mobile Access* or *Other Access* is selected as the access type, provide a 1-32 character lookup information string used as a customized authentication mechanism. Optionally select *Validate with RADIUS* to invoke a RADIUS lookup and syslog event log entry during captive portal user credential exchanges.
Terms and Conditions page	Select this option to include terms that must be adhered to for clients requesting captive portal access. These terms are included in the Terms and Conditions page when *No authentication required* is selected as the access type, otherwise the terms appear in the Login page. The default setting is disabled.

8 Set the following **Social Media Authentication** parameters to utilize a requesting client's social media profile for captive portal registration:

Facebook	If selected, the requesting client's guest user Facebook social media profile (collected from the social media server) is registered on the device. Captive portal authentication then becomes a fallback mechanism to enforce guest registration through social authentication. This option is disabled by default.
Google	If selected, the requesting client's guest user Google social media profile (collected from the social media server) is registered on the device. Captive portal authentication then becomes a fallback mechanism to enforce guest registration through social authentication.This option is disabled by default.

9 Refer to the **Bypass** field to enable or disable **Bypass Captive Portal Detection** capabilities. If enabled, captive portal detection requests are bypassed. This feature is disabled by default.

10 Set the following **Client Settings** to define client VLAN assignments, and the duration clients are allowed captive portal access and when they're timed out due to inactivity:

Radius VLAN Assignment	Select this option to enable client VLAN assignments using the RADIUS server. If, as part of the authentication process, the RADIUS server returns a client's VLAN-ID in a RADIUS access-accept packet, and this feature is enabled, all client traffic is forwarded on the post authentication VLAN. If disabled, the RADIUS server's VLAN assignment is ignored and the VLAN configuration defined within the WLAN configuration is used instead. This feature is disabled by default.
Post Authentication VLAN	When this option is selected, a specific VLAN is assigned to the client upon successful authentication. The available range is from 1 - 4,096.
Client Access Time	Use the spinner control to define the duration wireless clients are allowed access to using the captive portal policy when there is no session time value defined for the RADIUS response. Set an interval from 10 - 10,800 minutes. The default interval is 1,440 minutes.
Inactivity Timeout	Use the drop-down menu to specify an interval in either *Minutes* (1 - 1,440) or *Seconds* (60 - 86,400) that, when exceeded, times out the session. The default is 10 minutes.

11 Define the following **Loyalty App** settings to allow administrators to detect and report a captive portal client's usage of a selected (preferred) loyalty application:

Enable	Select this option to report a captive portal client's loyalty application presence and store this information in the captive portal's user database. The client's loyalty application detection occurs on the Access Point to which the client is associated and allows a retail administrator to assess whether a captive portal client is using specific retail (loyalty) applications in their captive portal. This setting is enabled by default.
App Name	Use the drop-down menu to select an existing application to track for loyalty utilization by captive portal clients. This enables an administrator to assess whether patrons are accessing an application as expected in specific retail environments. To create an application if none exists suiting the specific reporting needs of captive portal clients, see *Application on page 7-58*.

12 Use the **DNS Whitelist** parameter to create a set of allowed destination IP addresses. These allowed DNS destination IP addresses are called a *Whitelist.*

To effectively host captive portal pages on an external Web server, the IP address of the destination Web server(s) should be in the Whitelist.

13 Refer to the drop-down menu of existing DNS White List entries to select a policy to be applied to this captive portal policy. If no DNS Whitelist entries exist, select the **Create** or **Edit** icons and follow the sub-steps below:

a. If creating a new Whitelist, assign it a name up to 32 characters. Use the + Add Row button to populate the Whitelist with Host and IP Index values.

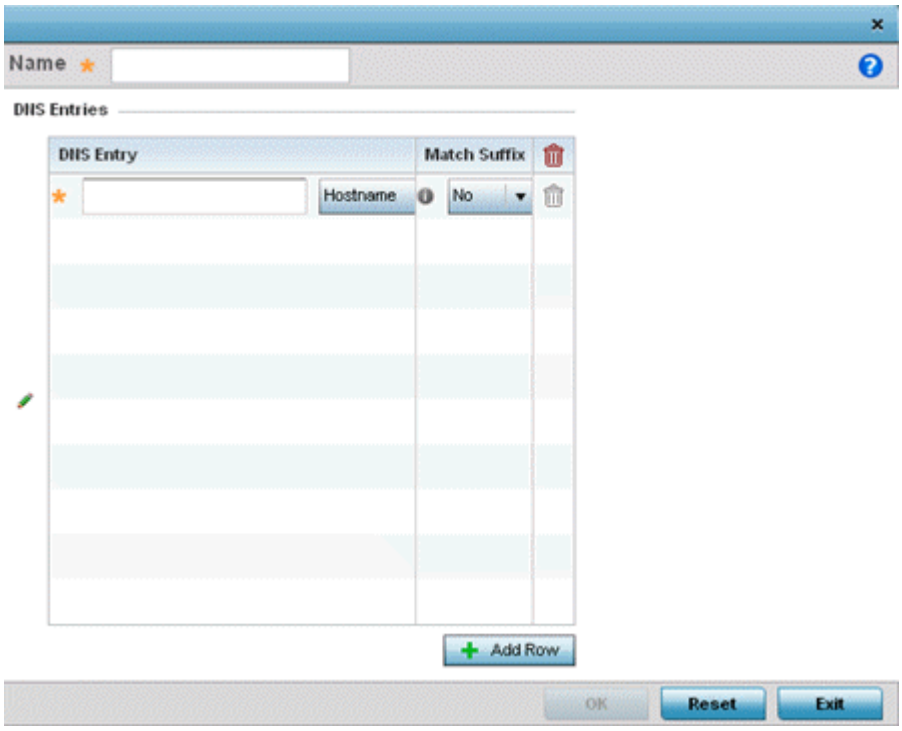


Figure 11-3 *Captive Portal Whitelist screen*

b. Provide a numerical *IP address* or *Hostname* within the **DNS Entry** parameter for each destination IP address or host included in the Whitelist. Hostnames cannot contain an underscore.

c. Use the **Match Suffix** parameter to match any hostname or domain name as a suffix. The default setting is disabled.

d. If necessary, select the radio button of an existing Whitelist entry and select the **- Delete** icon to remove the entry from the Whitelist.

14 Set the following **Accounting** parameters to define how accounting is conducted for clients entering and exiting the captive portal. Accounting is the method of collecting and sending security server information for billing, auditing and reporting user data; such as captive portal start and stop times, executed commands (such as PPP), number of packets and number of bytes. Accounting enables wireless network administrators to track captive portal services users are consuming.

Enable RADIUS Accounting	Select this option to use an external RADIUS resource for AAA accounting. When selected, a AAA Policy field displays. This setting is disabled by default.

Enable Syslog Accounting	Select this option to log information about the use of remote access services by users using an external syslog resource. This information is of great assistance in partitioning local versus remote users. Remote user information can be archived to an external location for periodic network and user administration. This feature is disabled by default.
Syslog Host	When syslog accounting is enabled, use the drop-down menu to determine whether an *IP address* or *Hostname* is used as a syslog host. The IP address or hostname of an external server resource is required to route captive portal syslog events to that destination external resource destination. A hostname cannot contain an underscore.
Syslog Port	When syslog accounting is enabled, define the numerical syslog port the used to route traffic with the external syslog server. The default port is 514.

15 Set the following **Data Limit** parameters values to define a data limit for clients accessing the network using the restrictions of a captive portal:

Limit	Select this option to enable data limits for captive portal clients. Specify the maximum amount of data, in MegaBytes, allowed for each captive portal client. When a user reaches this threshold, from 1 and 102,400 MegaBytes, it triggers the specified action.
Action	When a captive portal client reaches its data usage limit, a specified log action is executed. Available actions are *Log Only* and *log-and-disconnec*t. When Log Only is selected, an entry is added to the log file any time a captive portal client exceeds the data limit. When log-and-disconnect is selected, an entry is added to the log file when the data limit is exceeded and the client is disconnected from the captive portal.

16 Set the **Logout FQDN** as the FQDN address to logout of the captive portal session from the client (for example, *logout.guest.com).*

17 Set the following **Localization** settings to add a URL to trigger a one-time redirect on demand. The defined URL is triggered from a mobile application to derive location information from the wireless network so an application can be localized to a particular store or region.

FQDN	Provide the FQDN address (for example, *local.guestaccess.com*) used to obtain localization parameters for a client.
Response	Enter a 512 character maximum response message directed back to the client for localization HTTP requests.

18 Refer to the **Destination Ports for Redirection** parameter (within the **Redirection Ports** field), and enter destination ports (separated by commas, or using a dash for a range) for consideration when re-directing client connections. Standard ports 80 and 443 are always considered for client connections regardless of what's entered by the administrator.

19 Select the **Web Page** tab to create locally or externally hosted HTML pages.

The **Login** page displays by default.

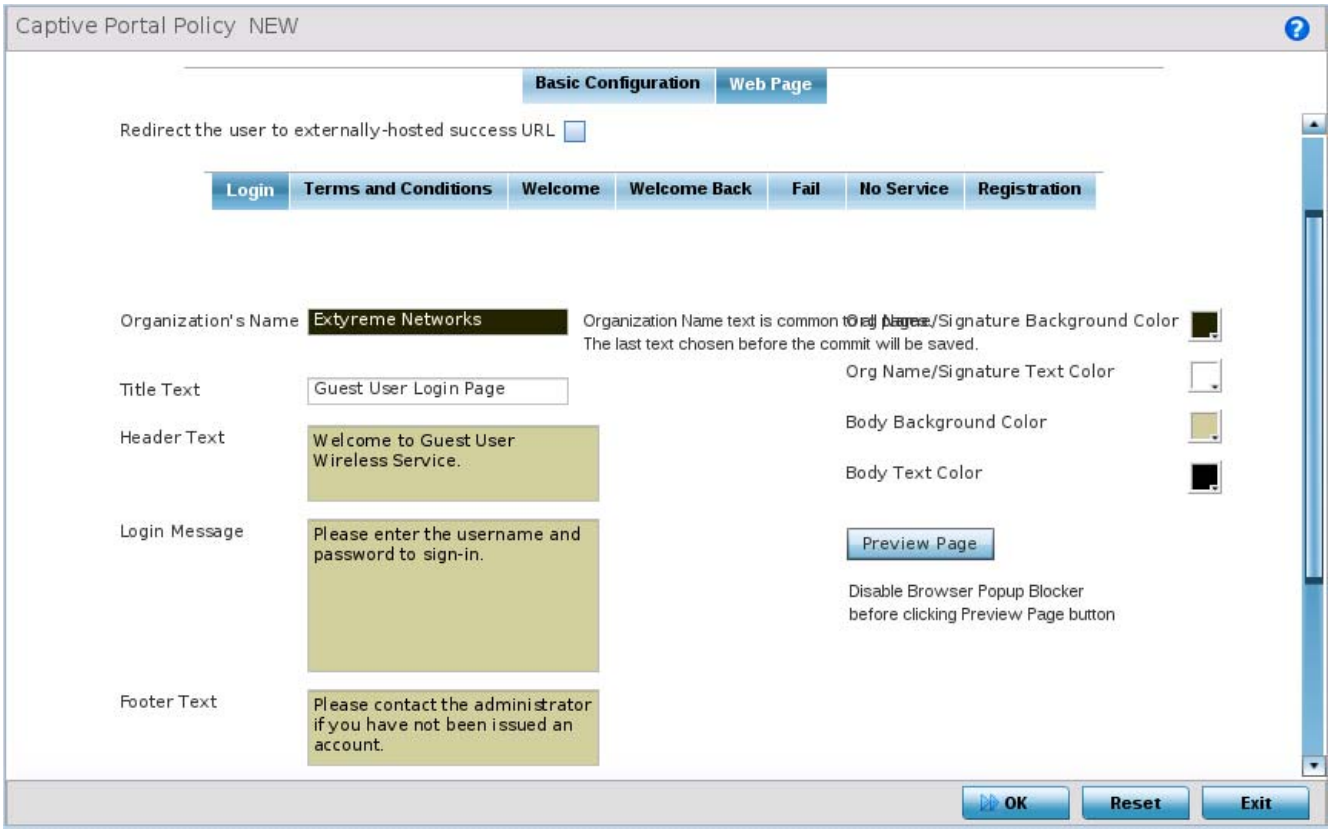


Figure 11-4 *Captive Portal Policy Internal Web Page screen*

The *Login* screen prompts the user for a username and password to access the captive portal and proceed to either the *Terms and Conditions* page (if used) or the *Welcome* page. The Terms and Conditions page provides conditions that must be agreed to before captive portal access is permitted. The *Welcome* page asserts a user has logged in successfully and can access the captive portal. The *Welcome Back* oage greets returning users. The *Fail* page asserts authentication attempt has failed, the user is not allowed to access the Internet (using this captive portal) and must provide the correct login information again to access the Internet. The *No Service* page asserts the captive portal service is temporarily unavailable due to technical reasons. Once the services become available, the captive portal user is automatically connected back to the services available through the captive portal.

20 Select the location where the captive portal *Login*, *Terms and Conditions*, *Welcome*, *Fail*, *No Service* and *Registration* Web pages are hosted. Available sources include *Internal*, *External* and *Advanced*. If Internal is selected, provide the information for each of the screens. If Advanced is selected, follow the on-screen instructions to upload custom Web pages. If Externally hosted is selected, provide the URLs for each of the necessary pages in the fields below.

21 Provide the following information for the **Login**, **Terms and Conditions**, **Welcome**, **Welcome Back, Fail, No Service** and **Registration** tabs:

Organization Name	Set any organizational specific name or identifier which clients see during login. The Organization Name setting is only available for the Login page.
Title Text	Set the title text displayed on the pages when wireless clients access captive portal pages. The text should be in the form of a page title describing the respective function of each page and should be unique to each function.

Header Text	Provide header text unique to the function of each page.
Login Message	Specify a message containing unique instructions or information for the users who access the Login, Terms and Condition, Welcome, Fail, No Service or Registration pages. In the case of the Terms and Agreement page, the message can be the conditions requiring agreement before captive portal access is permitted.
Footer Text	Provide a footer message displayed on the bottom of each page. The footer text should be any concluding message unique to each page before accessing the next page in the succession of hotspot Web pages.
Main Logo URL	The Main Logo URL is the URL for the main logo image displayed on the screens. Use the *Browse* button to navigate to the location of the target file. Optionally select the *Use as banner* option to designate the selected main logo as the page's banner as well. The banner option is disabled by default.
Small Logo URL	The Small Logo URL is the URL for a small logo image displayed on the screens. Use the *Browse* button to navigate to the location of the target file.
Signature	Provide the copyright and legal signature associated with the usage of the captive portal and the usage of the organization name provided. The Signature setting is only available for the Login page.

22 Refer to the right-hand side of each screen to define how the **Org Name Signature Background Color**, **Org Name. Signature Text Color**, **Body Background Color** and **Body Text Color** display for current screen.

Select the box to the right of each of these four items to launch a color palette where screen colors can be selected uniquely. Select **Preview Page** to review your color selections before committing the updates to captive portal screens. Each of the *Login*, *Terms and Conditions*, *Welcome*, *Fail*, *No Service* and *Registration* screens can have their background and signature colors set uniquely.

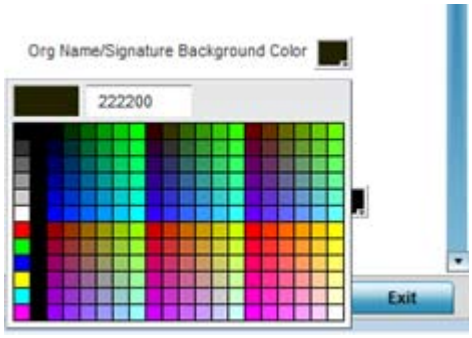


Figure 11-5 *Captive Portal Page Color Palette screen*

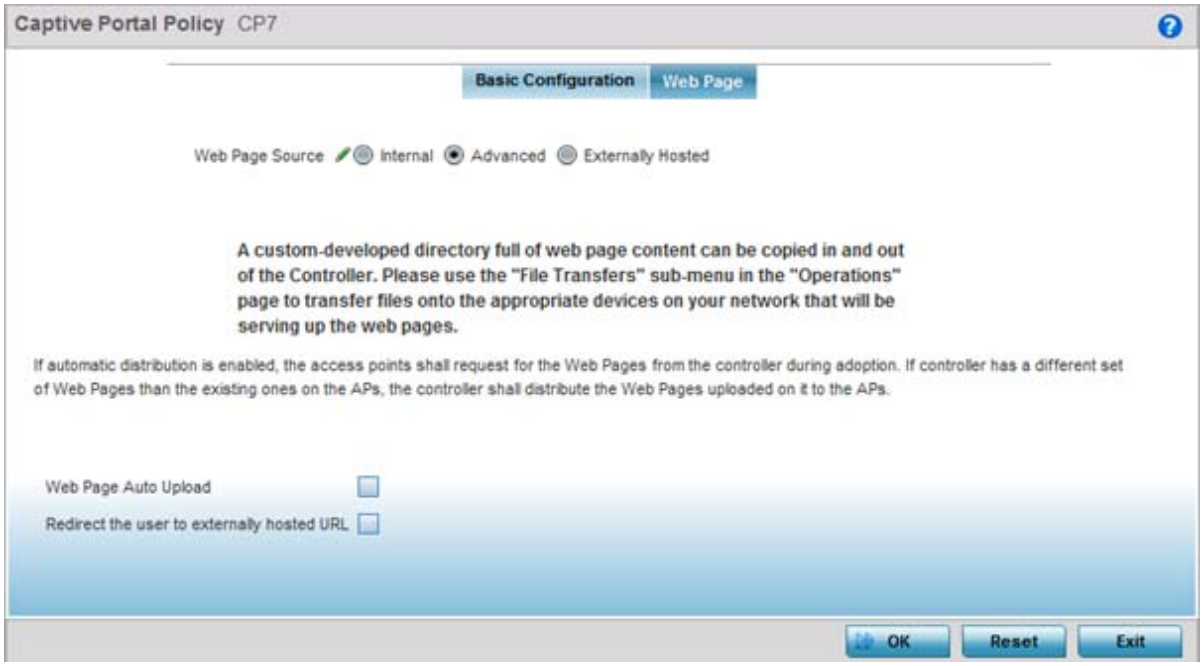
23 When setting the properties of the **Registration** screen, refer to the bottom portion of the screen to define email, country, gender, mobile, zip, street and name filters used as additional authentication criteria. Guest users are redirected to the registration portal on association to the captive portal SSID. Users are displayed an internal (or) externally hosted registration page where the guest user must complete the registration process if not previously registered.

These fields are customizable to meet the needs of retailers providing guest access. The captive portal sends a message to the user (on the phone number or Email address provided at registration) containing an access code. The user inputs the access code and the captive portal verifies the code before returning the Welcome page and providing access. This allows a retailer to verify the phone number or Email address is correct and can be traced back to a specific individual.

Figure 11-6 *Registration screen customizable filters*

24 Select **OK** to save the changes made within any of the Internal Page screens. Selecting **Reset** reverts the settings back to the last saved configuration.

25 Select **Advanced** to use a custom-developed directory full of Web page content can be copied in and out of the controller or service platform. Please use the *File Transfers* sub-menu in the *Operations* page to transfer files to the appropriate devices serving up the Web pages.



26 Select the **Externally Hosted** radio button if hosting the captive portal on an external server resource.

Select **Web Page Auto Upload** to automatically launch the advanced pages for requesting clients upon association. This setting is disabled by default.

Select **Redirect the user to externally hosted URL** to use an externally hosted server resource and its login permissions for logging into the advanced page. This setting is disabled by default.

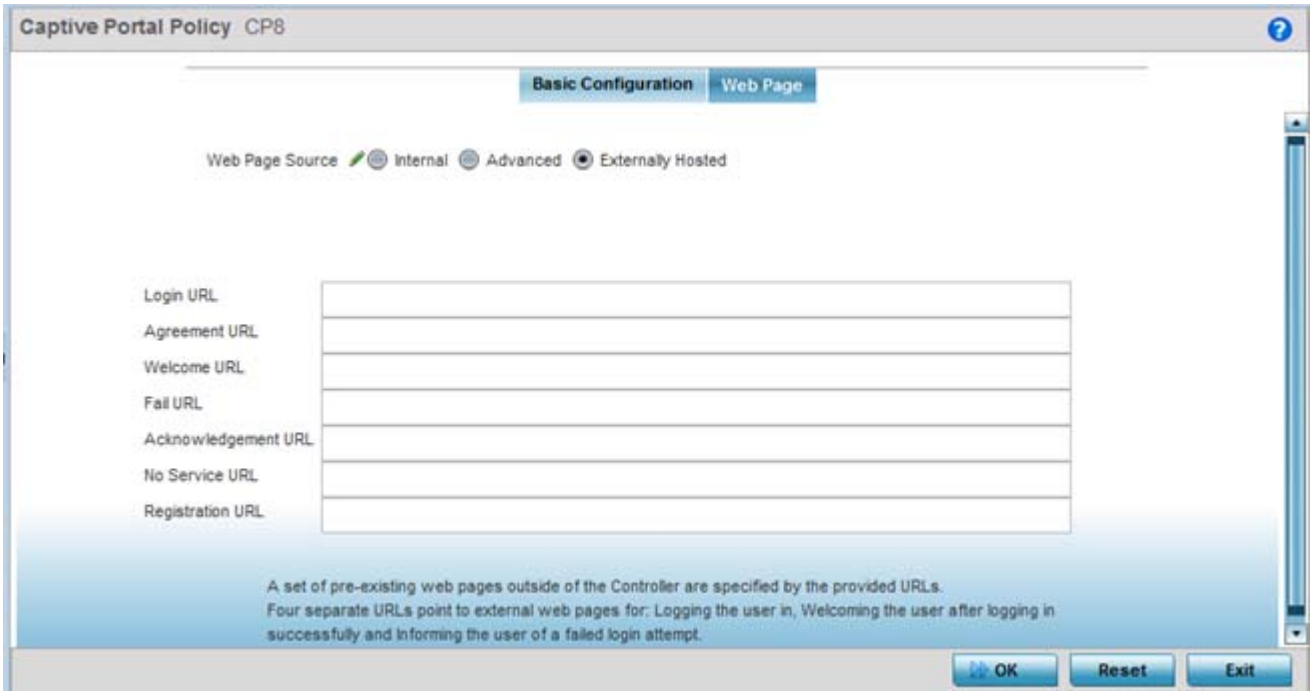


Figure 11-7 *Captive Portal Policy Externally Hosted Web Page screen*

Login URL	Define the complete URL for the location of the Login screen. The Login screen prompts the user for a *username* and *password* to access either the Terms and Conditions or Welcome page.
Agreement URL	Define the complete URL for the location of the Terms and Conditions page. The Terms and Conditions page provides conditions that must be agreed to before wireless client access is provided.
Welcome URL	Define the complete URL for the location of the Welcome page. The Welcome page asserts the user has logged in successfully and can access network resources via the captive portal.
Fail URL	Define the complete URL for the location of the Fail page. The Fail page asserts authentication attempt has failed, and the client cannot access the captive portal.The client needs to provide correct login information to regain access.
Acknowledgement URL	Define the complete URL to the location of the Acknowledgement page. The Acknowledgement URL is needed by returning users whose MAC addresses has been validated previously, but must accept the conditions of the captive portal again.
No Service URL	Define the complete URL to the location of the No URL page. The No Service URL is needed by users encountering difficulties connecting to the external resource used to host the captive portal pages.
Registration URL	Define the complete URL to the location of the Registration page. The Registration URL is supported by NX9500, NX9600 and NX75XX service platform models as an adopting controller verifying (registering) user information before client access is provided to captive portal managed Internet resources.

27 Select **OK** when completed to update the captive portal's advanced configuration. Select **Reset** to revert the screen back to its last saved configuration.

11.1.2 Creating DNS Whitelists

Configuring Captive Portal Policies

A DNS whitelist is used in conjunction with a captive portal to provide access services to wireless clients. Use the whitelist to create a set of allowed destination IP addresses within the captive portal. To effectively host hotspot pages on an external Web server, the IP address of the destination Web server(s) should be in the whitelist.

To define the whitelist:

1 Select **Configuration** > **Services**.

The upper, left-hand, side of the user interface displays a **Services** menu pane where Captive Portal, DHCP and RADIUS configuration options can be selected.

2 Select **Captive Portals**.

The Captive Portal screen displays the configurations of existing policies. New policies can be created, existing policies can be modified or existing policies deleted.

3 Select **DNS Whitelist**

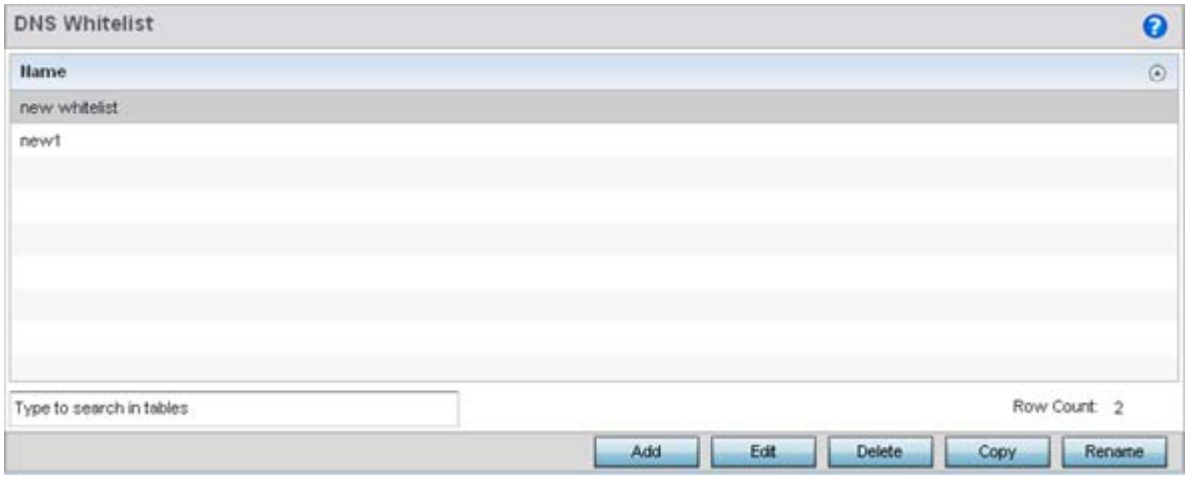


Figure 11-8 *Captive Portal DNS Whitelist screen*

4 Review the names of existing whitelists and click **Add** to create a new whitelist entry or select an existing whitelist and click **Edit** to modify it.

5 Use the **DNS Whitelist** parameter to create a set of allowed destination IP addresses.

To effectively host pages on an external Web server, the IP address of the destination Web server(s) should be in the whitelist.

6 Refer to the drop-down menu of existing whitelist entries to select a policy to be applied to this captive portal policy. If no entries exist, select the **Create** or **Edit** icons and follow the sub-steps below:

a. If creating a new Whitelist, assign it a name up to 32 characters. Select the **+ Add Row** button to populate the Whitelist with Host and IP Index values.

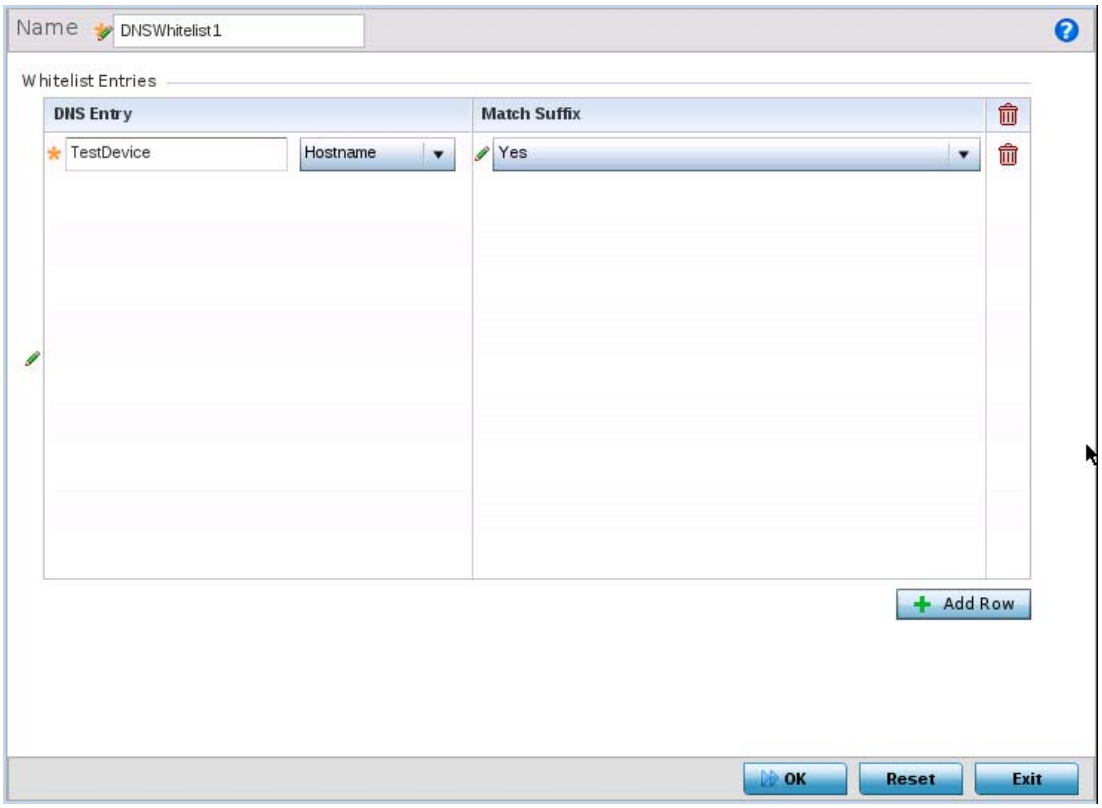


Figure 11-9 *Captive Portal Whitelist screen*

b. Provide a *Hostname* or numeric *IPv4 Address* or *IPv6 Address* within the **DNS Entry** parameter for each destination IP address or host included in the Whitelist. IPv6 formatted addresses are composed of eight groups of four hexadecimal digits separated by colons.

c. Use the **Match Suffix** parameter to match any hostname or domain name as a suffix. The default setting is disabled.

d. If necessary, select the radio button of an existing Whitelist entry and select the **- Delete** icon to remove the entry from the Whitelist.

11.1.3 Captive Portal Deployment Considerations

Configuring Captive Portal Policies

Before defining a captive portal configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- The architecture should consider the number of wireless clients allowed and the services provided. Each topology has benefits and disadvantages which should taken into consideration to meet each deployment's requirements.
- Captive portal authentication uses secure HTTPS to protect user credentials, but doesn't typically provide encryption for user data once they have been authenticated. For private access applications, WPA2 (with a strong passphrase) should be enabled to provide strong encryption.
- Guest user traffic should be assigned a dedicated VLAN, separate from other internal networks.
- Guest access configurations should include firewall policies to ensure logical separation is provided between guest and internal networks so internal networks and hosts are not reachable from guest devices.

- Guest access services should be defined in a manner whereby end-user traffic doesn't cause network congestion.
- A valid certificate should be issued and installed on all devices providing captive portal access to the WLAN and wireless network. The certificate should be issued from a public certificate authority ensuring guests can access the captive portal without browser errors.

11.2 Setting the Guest Management Configuration

Services

Establish a guest management configuration to redirect guest users to a registration portal upon association to the captive portal SSID, The guest users are redirected to an internally (or) externally hosted registration page (registration.html) where the guest user can complete the registration process if not previously registered. The internal captive portal adds a new *registration* page that's customizable based on business requirement.

A guest management policy is for configuration of E-mail host and SMS gateway related commands along with the credentials required for sending passcode to guest via email and SMS. Configure up to 32 different guest management policies. Each guest management policy allows an administrator to configure the SMS gateway, SMS message body, E-mail SMTP server, E-mail subject contents and E-mail message body. At any point of time, there can be only one guest management policy active per device.

Guest registration is supported on NX90000 series service platforms as an adopting controller with up to 2 million user identity entries. Guest registration is supported on NX75000 series service platforms as an adopting controller with up to 1 million user identity entries. Guest management and registration is not supported on all other WiNG supported platforms.

NOTE: An option to backup the guest registration configuration is not available in the user interface. To backup the guest user database, a `guest-database-backup` command must be invoked using the CLI. For more information, refer to the *WiNG CLI Reference Guide* available from www.extremenetworks.com/support.

Refer to the following sections for configuring Guest Management parameters:

- *Email*
- *SMS*
- *SMS SMTP*
- *DB Export*

To set the guest management configuration:

1 Select **Configuration** > **Services** > **Guest Management**.

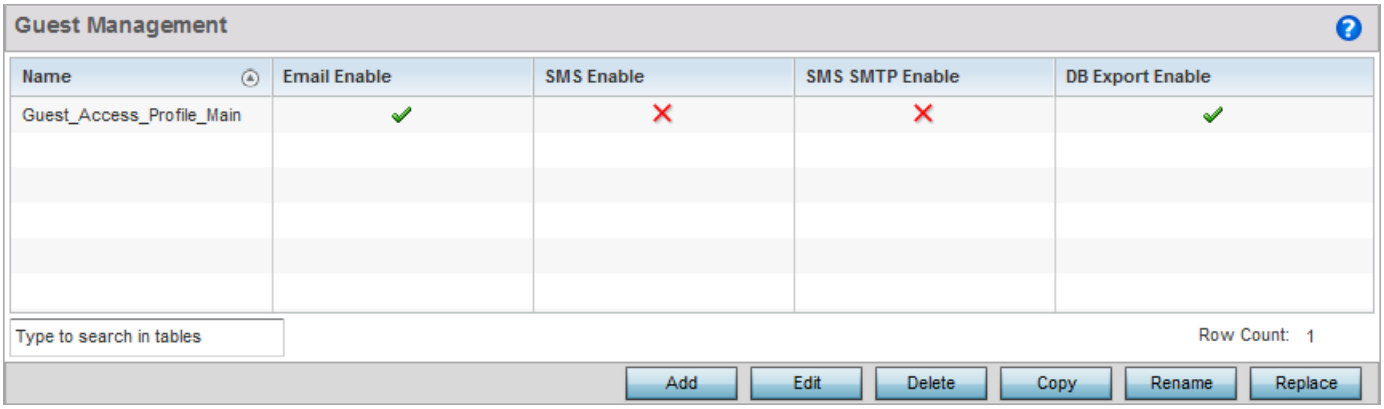


Figure 11-10 *Guest Management screen*

2 Review the following (at a high level) to determine if a new guest management requires creation, an existing guest management configuration requires modification or requires deletion:

Name	Lists the name(s) of up to 32 guest user policies created on the service platform for registering guest user credentials.
Email Enable	A green check mark defines Email as enabled for guest management, a red X defines Email as disabled. Guest users can register themselves with their E-mail credentials as a primary key for authentication; captive portal system provides the pass code for their registration and the guest users needs to use the registered email/mobile/member id and the received pass code for further login to the captive portal.
SMS Enable	A green check mark defines SMS as enabled for guest management, a red X defines SMS as disabled.SMS enables guest users to registers themselves with their E-mail or mobile device ID as the primary key for authentication. The captive portal provides the passcode for registration, and the guest users utilizes use their registered E-mail or mobile device ID and received passcode for login to the captive portal.
SMS SMTP Enable	A green check mark defines SMS SMTP as enabled for guest management, a red X defines SMS SMTP as disabled. Optionally configure an E-mail host server (for example: *smtp.gmail.com*) along with sender related credentials and the recipient gateway E-mail address to which the message is E-mailed. The gateway server converts the E-mail into SMS and sends the message to guest users's mobile device.
DB Export Enable	A green check mark indicates that exporting the guest user database is enabled for this device. When enabled, the list of guest users on the captive portal can be periodically exported to an external server.

3 Select **Add** to create a new guest management configuration, choose an existing configuration and select the **Edit** button to modify its properties or choose an existing guest management and select **Delete** to remove it from those available. Select **Rename** to change the name of an existing guest management configuration or **Copy** a configuration to a different location. Select **Replace** to replace an existing **Guest Management** policy with a new policy.

11.2.1 Email

Setting the Guest Management Configuration

Guest users can register themselves with their E-mail credentials as a primary key for authentication; captive portal system provides the pass code for their registration and the guest users needs to use the registered email/mobile/member id and the received pass code for further login to the captive portal.

To define a guest management configuration using E-mail as the primary key for authentication:

1 Select **Configuration** > **Services** > **Guest Management**.

Review existing guest management configurations to determine whether new E-mail configuration requires creation or an existing guest user configuration requires modification or deletion.

2 Select the **Email** tab.

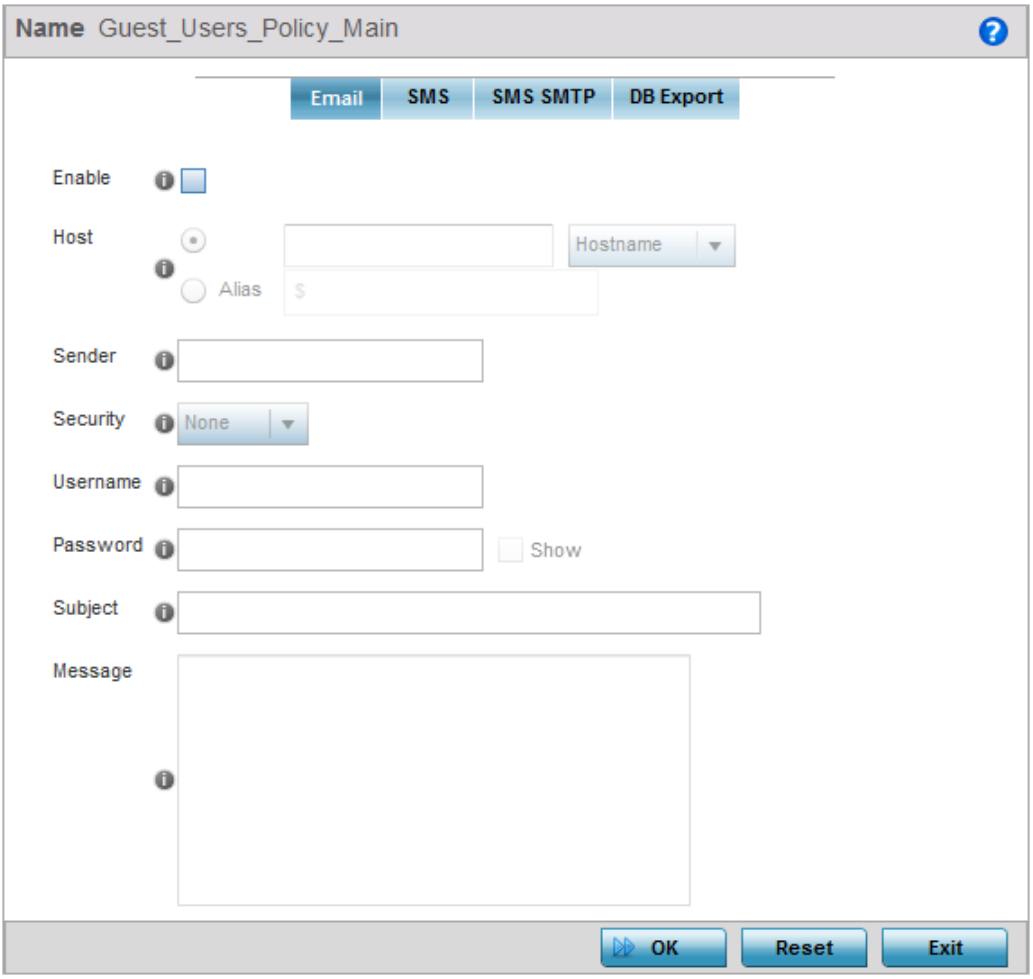


Figure 11-11 *Guest Management screen - Email tab*

3 Set the following E-mail guest user network address and message content information required for notifying a guest with a passcode using E-mail:

Enable	Enable this option so guest users can register themselves with their E-mail credentials as a primary key for authentication; captive portal system provides the pass code for their registration and the guest users needs to use the registered E-mail/mobile/member id and the received pass code for further login to the captive portal. This setting is disabled by default and must be enabled to define the required settings.
Host	Define a hostname or IPv4 formatted IP address of the SMTP server resource used for guest management E-mail traffic, guest user credential validation and passcode reception. Optionally create an alias to define the host once and use the alias across different configuration items.
Sender	Provide a 100 character maximum sender name for the guest user receiving the passcode required for registering their guest E-mail credentials.
Security	Use the drop-down menu to select *ssl* or *starttls* as the E-mail host server user authentication validation scheme for this particular username and password combination. Optionally select *None* to apply to no additional user authentication beyond the required username and password combination.
Username	Provide a unique 100 character maximum username unique to this guest management configuration. This username will require its own password and must be correctly provided to receive the required passcode for registering guest E-mail credentials.
Password	Define a 63 character maximum password that must be correctly provided with the unique username to receive the required passcode for registering guest E-mail credentials.
Subject	Enter the 100 character maximum E-mail subject for the E-mail message sent to the guest user along with the required passcode. You can use the tag 'GM_NAME' in the subject which is replaced by the guest user's name.
Message	Create the 1024 character maximum message content for the E-mail sent to the guest user along with the passcode. You can use the following tags in the message body. • GM_NAME – indicates the guest user's name in the message. This tag is replaced by the guest user's name when the E-mail is created. • GM_PASSCODE - indicates the password assigned to the user. The tag is replaced by the actual password when the E-mail is created. • CR-NL - indicates a line break. When used, the word next to this tag starts on a new line when the E-mail is created.

4 Select **OK** to save the updates to the guest management E-Mail configuration. Select **Reset** to revert the screen back to its last saved configuration.

11.2.2 SMS

SMS enables guest users to registers themselves with their E-mail or mobile device ID as the primary key for authentication. The captive portal provides the passcode for registration, and the guest users utilizes use their registered E-mail or mobile device ID and received passcode for login to the captive portal.

NOTE: When utilizing SMS, the WLAN's authentication type should be *None* and the registration type should be enabled as user registration. Captive portal authentication must always enforce guest registration.

SMS is similar to MAC address based self registration, but in addition a captive portal sends a SMS message to the user on the mobile phone number provided at registration containing an access code. The user then inputs the access code on the user screen. The captive portal verifies the code, returns the *Welcome* page and provides access. This allows the administrator to verify the phone number provided and can be traced back to a specific individual should the need arise.

The default gateway used with SMS is *Clickatell.* A passcode can be sent with SMS to the guest user directly using Clickatell, or the passcode can be sent via E-mail to the SMS Clickatell gateway server, and Clickatell sends the passcode SMS to the guest user.

To define a guest management configuration using SMS:

1 Select **Configuration** > **Services** > **Guest Management**.

Review existing guest management configurations to determine whether new configuration requires creation or an existing guest user configuration requires modification or deletion.

2 Select the **SMS** tab.

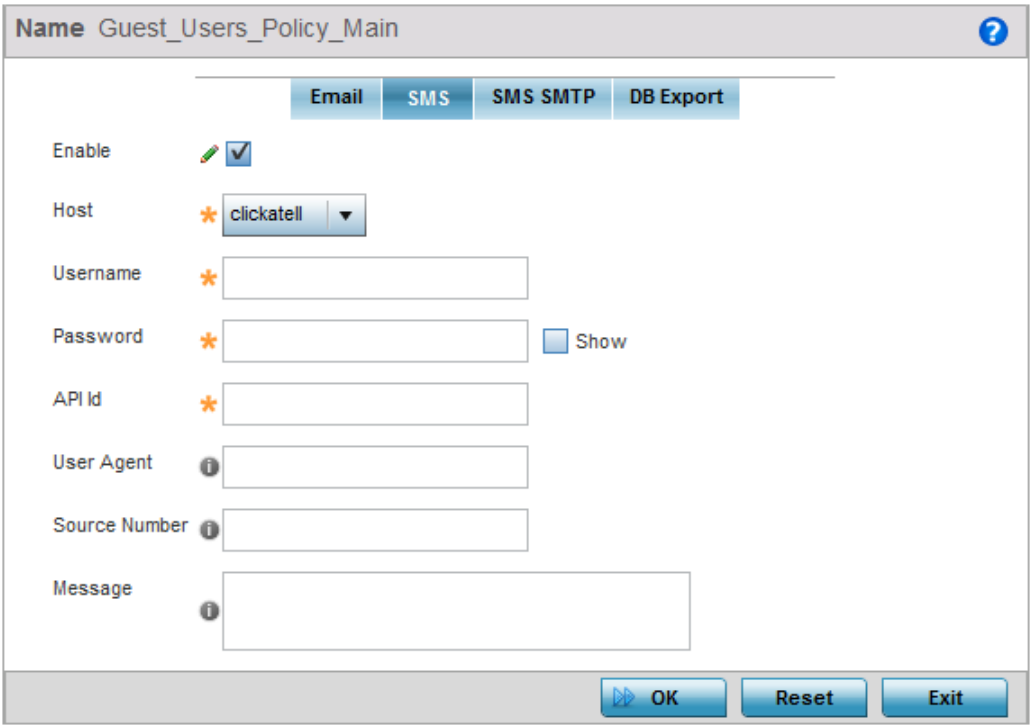


Figure 11-12 *Guest Management screen - SMS tab*

3 Set the following **SMS** guest user network and message content information required for notifying a guest with a passcode:

Enable	Select this option to enable guest users to registers themselves with their E-mail or mobile device ID as the primary key for authentication. This setting is disabled by default and must be enabled to define the required settings.
Host	By default, *clickatell* is the only host SMS gateway server resource. Upon receiving the passcode E-mail, the SMS gateway sends the actual notification passcode SMS to the guest user.

Username	Provide a unique 32 character maximum username unique to this SMS guest management configuration. This username will require its own password and must be correctly provided to receive the required passcode for registering guest user credentials with SMS.
Password	Define a 63 character maximum password that must be correctly provided with the unique username to receive the required passcode for registering guest user credentials with SMS.
API Id	Set a 32 character maximum API Id for the configuration of the clickatell api_id (http/smtp api_id).
User Agent	Select the user agent for configuring the clickatell SMS gateway server and its related credentials for sending the passcode to guests.
Source Number	Set a 32 character maximum source-address from the number associated with clickatell. It can be a large integer or short code. The source number is only applicable to certain countries (like the United States).
Message	Create the 1024 character maximum message content for the SMS based request sent to the guest user along with the passcode.

4 Select **OK** to save the updates to the guest management SMS configuration. Select **Reset** to revert the screen back to its last saved configuration.

11.2.3 SMS SMTP

Optionally configure an E-mail host server (for example: *smtp.gmail.com*) along with sender related credentials and the recipient gateway E-mail address to which the message is E-mailed. The gateway server converts the E-mail into SMS and sends the message to guest users's mobile device.

When sending an E-mail, the E-mail client interacts with a SMTP server to handle the content transmission. The SMTP server on the host may have conversations with other SMTP servers to deliver the Email.

To define a guest management configuration using SMS SMTP:

1 Select **Configuration** > **Services** > **Guest Management**.

Review existing guest management configurations to determine whether new configuration requires creation or an existing guest user configuration requires modification or deletion.

2 Select the **SMS SMTP** tab.

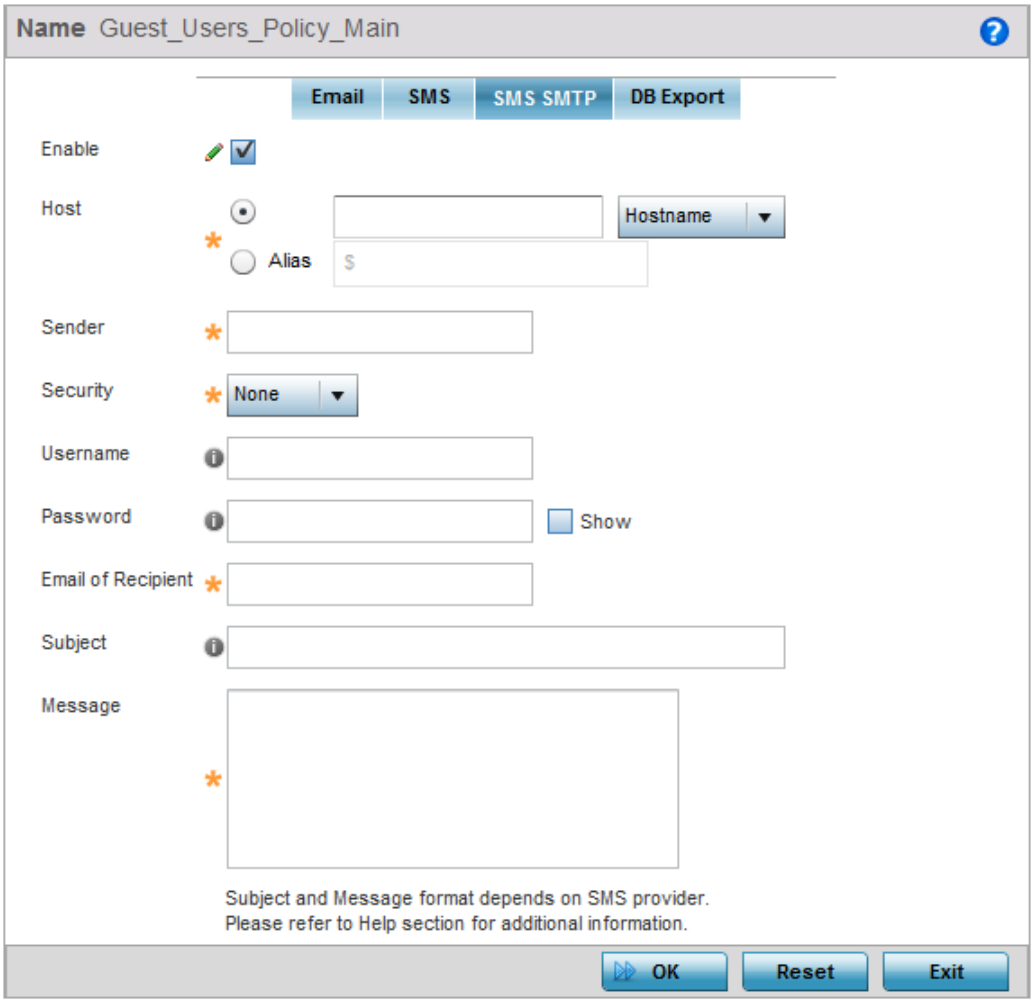


Figure 11-13 *Guest Management screen - SMS SMTP tab*

3 Set the following **SMS SMTP** guest user network and message content information required for notifying a guest with a passcode:

Enable	Enable this setting to configure an E-mail host server (for example: smtp.gmail.com) along with sender related credentials and the recipient gateway E-mail address to which the message is E-mailed. This setting is disabled by default and must be enabled to define the required settings.
Host	Define a hostname or IPv4 formatted IP address of the SMS gateway server resource used for guest management E-mail traffic, guest user credential validation and passcode reception. Consider providing the host as an alias. An alias enables an administrator to define a configuration item, such as a hostname, as an alias once and use the alias across different configuration items.
Sender	Provide a 100 character maximum sender name for the guest user receiving the passcode required for registering their guest E-mail credentials using SMTP.
Security	Use the drop-down menu to select *ssl* or *starttls* as the SMTP server user authentication validation scheme for this particular username and password combination. Optionally select *None* to apply to no additional user authentication beyond the required username and password combination. The default value is *ssl*.

Username	Provide a unique 64 character maximum username unique to this SMTP guest management configuration. This username requires its own password and must be correctly provided to receive the required passcode for registering guest user credentials.
Password	Define a 64 character maximum password that must be correctly provided with the unique username to receive the required passcode for registering guest user credentials with SMTP.
Email of Recipient	Enter a 64 character maximum E-mail address for the recipient of guest management E-mail traffic.
Subject	Enter a 100 character maximum E-mail subject for the E-mail message sent to the guest user along with the required passcode.
Message	Enter a 1024 character maximum E-mail message per the message format required by the gateway server. The *sms-over-smtp* message format is the required format from *clickatell* while sending E-mail to the SMS gateway server.

Select **OK** to save the updates to the guest management SMS SMTP configuration. Select **Reset** to revert the screen back to its last saved configuration.

11.2.4 DB Export

Setting the Guest Management Configuration

Optionally configure the guest user database export parameters. The guest user database can be periodically exported to an external server for backup and analysis.

To define the database export parameters:

1 Select **Configuration** > **Services** > **Guest Management**.

Review existing guest management configurations to determine whether new configuration requires creation or an existing guest user configuration requires modification or deletion.

2 Select the **DB Export** tab.

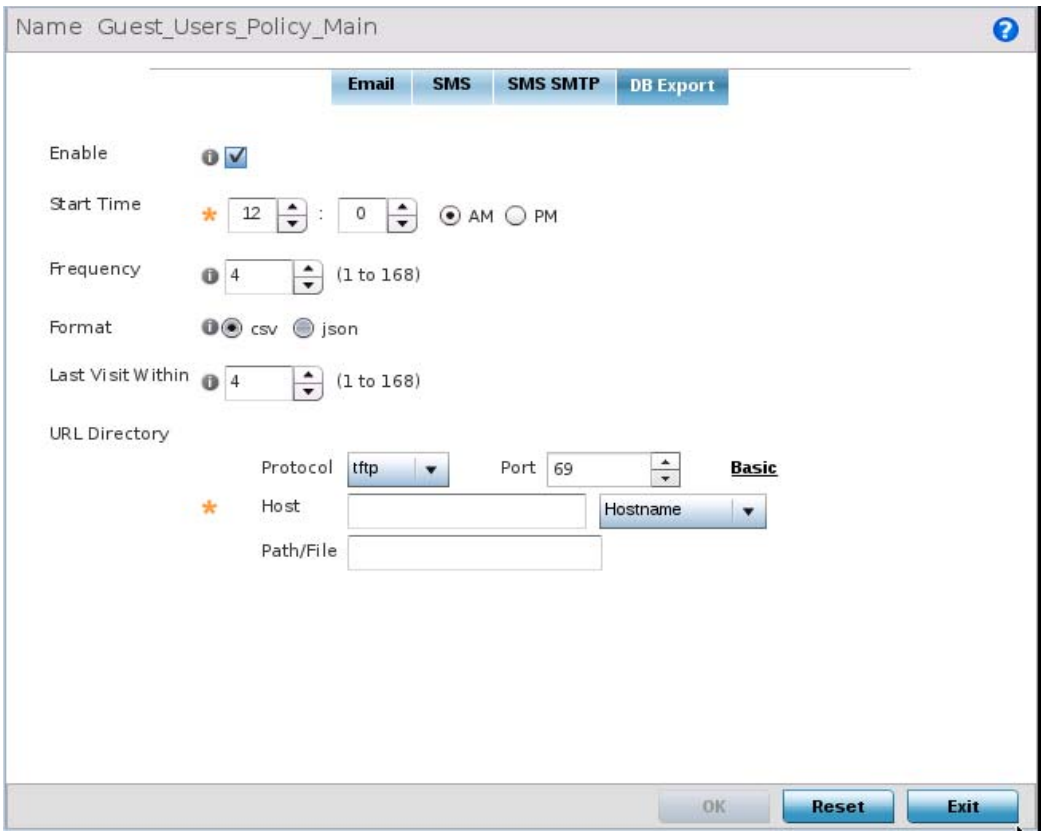


Figure 11-14 *Guest Management screen - DB Export tab*

3 Set the following **DB Export** parameters:

Enable	Enable this setting to configure the guest user database to an external server for backup and analysis. This setting is disabled by default and must be enabled to define the required settings.
Start Time	Define the start time when the first database backup occurs. The first run of the guest user database backup is always the current day. Use the spinner controls to set the start hour and minute. Use the AM/PM options to configure the exact hour. The default value is 12:00 AM.
Frequency	Define the backup frequency. This is the time interval between two consecutive backups. Use the spinner control to set the value between 1 hour and 168 hours. The default frequency is 4 hours.
Format	Guest user database can be exported in the following formats: • CSV • JSON Select the appropriate export format. The default export format is *CSV.*
Last Visit Time	Use this field to filter or restrict the amount of data that is exported. Use the spinner to set a value in the range 1 - 168 hours. When set, any data that is older than the set period - from when the database is being backed up - is not exported. The default value is 4 hours.
URL Directory	Use the field to provide the URL to which the guest user database is exported. Select the *Advanced* link to expose fields for setting the remote server's URL.

Protocol	Select the protocol used for exporting the guest user database. Available options include: • *tftp* • *ftp* • *sftp* • *http* • *cf* • *usb1-4*
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1-4*.
Host	Provide the hostname string or numeric IP address of the server to export the guest user database to. Hostnames cannot include an underscore character. This option is not valid for *cf* and *usb1-4*. Select *IPv4 Address* to use an IPv4 formatted address as the host. Select IPv6 Address to use an IPv6 formatted address as the host. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Path/File	Specify the path on the remote server where the guest user database file is copied to. Enter the complete relative path to the file on the remote server.

4 Select **OK** to save the updates to the guest management DB Export configuration. Select **Reset** to revert the screen back to its last saved configuration.

11.3 Setting the DHCP Configuration

Services

Dynamic Host Configuration Protocol (DHCP) allows hosts on an IP network to request and be assigned IP addresses and discover information about the network where they reside. Each subnet can be configured with its own address pool. Whenever a DHCP client requests an IP address, the DHCP server assigns an IP address from that subnet's address pool. When the onboard DHCP server allocates an address for a DHCP client, the client is assigned a lease, which expires after an pre-determined interval. Before a lease expires, wireless clients (to which leases are assigned) are expected to renew them to continue to use the addresses. Once the lease expires, the client is no longer permitted to use the leased IP address. The DHCP server ensures all IP addresses are unique, and no IP address is assigned to a second client while the first client's assignment is valid (its lease has not yet expired). Therefore, IP address management is conducted by the internal DHCP server, not by an administrator.

The internal DHCP server groups wireless clients based on defined user-class options. Clients with a defined set of user class values are segregated by class. A DHCP server can associate multiple classes to each pool. Each class in a pool is assigned an exclusive range of IP addresses. DHCP clients are compared against classes. If the client matches one of the classes assigned to the pool, it receives an IP address from the range assigned to the class. If the client doesn't match any of the classes in the pool, it receives an IP address from a default pool range (if defined). Multiple IP addresses for a single VLAN allow the configuration of multiple IP addresses, each belonging to different subnet. Class configuration allows a DHCP client to obtain an address from the first pool to which the class is assigned.

Numerous DHCP network address credentials can have an *alias* applied. An alias enables an administrator to define a configuration item (such as a IP address or domain name) once, and then use this single alias across different configurable values. For example, if a central network DNS server is set a static IP address, and a remote location's

local DNS server is defined, this host can be overridden at the remote location. At the remote location, the network is functional with a local DNS server, but uses the name set at the central network. A new host need not be created at the remote location. This simplifies creating and managing hosts and allows an administrator to better manage specific local requirements. An alias name always starts with a dollar sign ($) and should not exceed 32 characters. An alias that's applied to a DHCP configuration can be either a *Global*, *Profile*, *RF Domain* or *Device* alias. For more information on aliases and their application, see *Setting a Profile's Alias Configuration on page 8-155*.

NOTE: DHCP server updates are only implemented when the controller or service platform is restarted.

Refer to the following sections for more information on configuring DHCP parameters:

- *Defining DHCP Pools*
- *Defining DHCP Server Global Settings*
- *DHCP Class Policy Configuration*
- *DHCP Deployment Considerations*

To access and review the local DHCP server configuration:

1 Select **Configuration** > **Services** > **DHCP Server Policy**.

The **DHCP Server** screen displays. Clients with a defined set of user class values are segregated by class. A DHCP server can associate multiple classes to each pool. Each class in a pool is assigned an exclusive range of IP addresses. DHCP clients are then compared against classes.

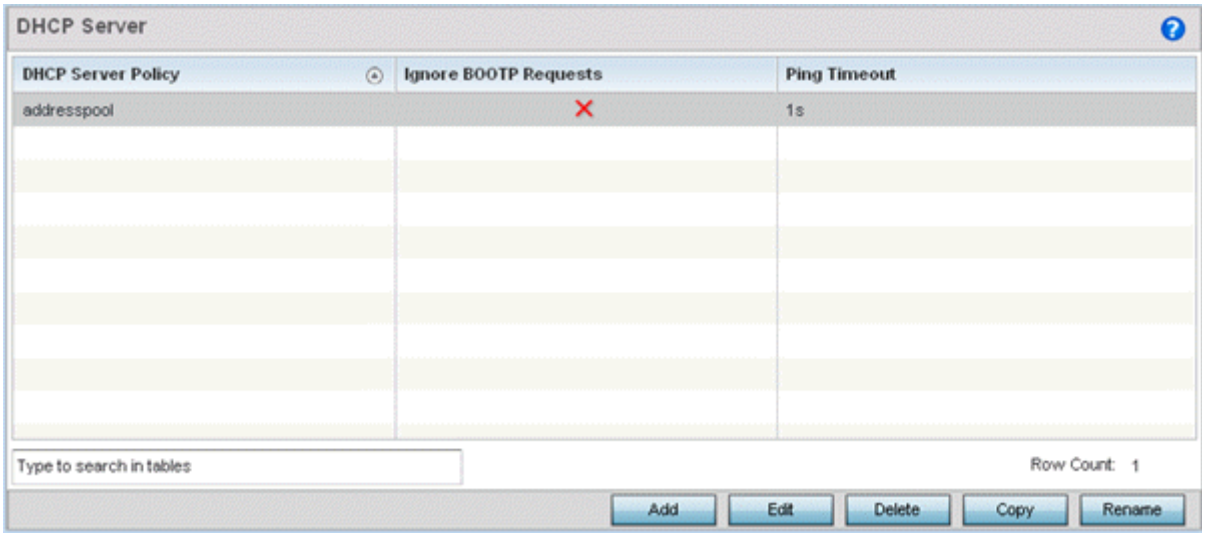


Figure 11-15 *DHCP Server Policy screen*

2 Review the following DHCP server configurations (at a high level) to determine whether a new server policy requires creation, an existing policy requires modification or an existing policy requires deletion:

DHCP Server Policy	Lists the name assigned to each DHCP server policy when it was initially created. The name assigned to a DHCP server policy cannot be modified as part of the policy edit process. However, obsolete policies can be deleted as needed.

Ignore BOOTP Requests	A green checkmark within this column means this policy has been set to ignore BOOTP requests. A red "X" defines the policy as accepting BOOTP requests. BOOTP (boot protocol) requests boot remote systems within the controller or service platform managed network. BOOTP messages are encapsulated inside UDP messages and are forwarded by the controller or service platform. This parameter can be changed within the DHCP server *Global Settings* screen.
Ping Timeout	Lists the interval (from 1 -10 seconds) for a DHCP server ping timeout. The timeout is used to intermittently ping and discover whether a client requested IP address is already in use. This parameter can be changed within the DHCP Server *Global Settings* screen.

3 Select **Add** to create a new DHCP server policy, choose an existing policy and select the **Edit** button to modify the policy's properties or choose an existing policy and select **Delete** to remove the policy from those available. Adding or Editing a DHCP server policy displays the **DHCP Server Policy** screen by default. Select **Rename** to change the name of an existing policy or **Copy** a policy to a different location.

11.3.1 Defining DHCP Pools

- *Setting the DHCP Configuration*

DHCP services are available for specific IP interfaces. A pool (or range) of IP network addresses and DHCP options can be created for each IP interface defined. This range of addresses can be made available to DHCP enabled wireless devices on either a permanent or leased basis. DHCP options are provided to each DHCP client with a DHCP response and provide DHCP clients information required to access network resources (default gateway, domain name, DNS server and WINS server configuration). An option exists to identify the vendor and functionality of a DHCP client. The information is a variable-length string of characters (or octets) with a meaning specified by the vendor of the DHCP client.

To define the parameters of a DHCP pool:

1 Select **Configuration** > **Services** > **DHCP Server Policy**. The DHCP Server screen displays the DHCP Pool tab by default.

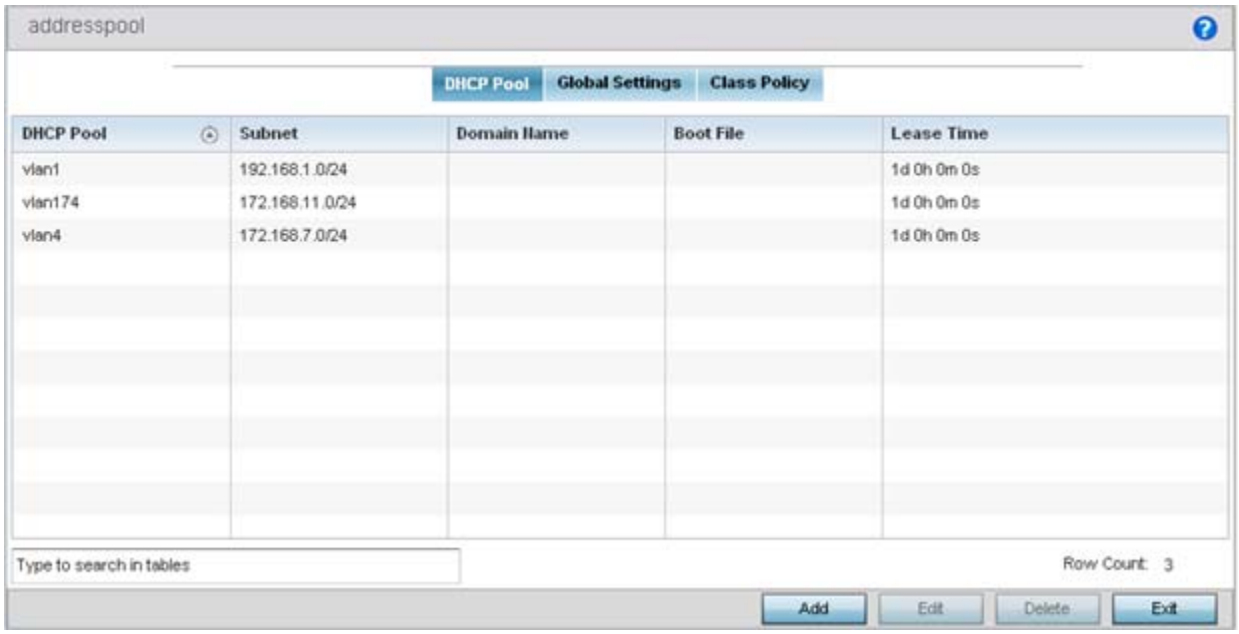


Figure 11-16 *DHCP Server Policy screen - DHCP Pool tab*

2 Review the following DHCP pool configurations to determine if an existing pool can be used as is, a new one requires creation or edit, or a pool requires deletion:

DHCP Pool	Displays the name assigned to the network pool when created. The DHCP pool name represents the group of IP addresses used to assign to DHCP clients upon request. The name assigned cannot be modified as part of the edit process. However, if the network pool configuration is obsolete it can be deleted.
Subnet	Displays the network address or alias used by clients requesting DHCP resources.
Domain Name	Displays the domain name or alias used with this network pool. *Domain Name Services* (DNS) convert human readable host names into IP addresses. Host names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. A *fully qualified domain name* (FQDN) consists of a host name plus a domain name. For example, *computername.domain.com.*
Boot File	Boot files (*Boot Protocol*) are used to boot remote systems over the network. BOOTP messages are encapsulated inside UDP messages, so requests and replies can be forwarded. Each DHCP network pool can use a different file as needed.
Lease Time	If a lease time has been defined for a listed network pool, it displays in an interval from 1 - 31,622,399 seconds. DHCP leases provide addresses for defined times to various clients. If a client does not use the leased address for the defined time, that IP address can be re-assigned to another DHCP client.

3 Select **Add** to create a new DHCP pool, **Edit** to modify an existing pool's properties or **Delete** to remove a pool from amongst those available.

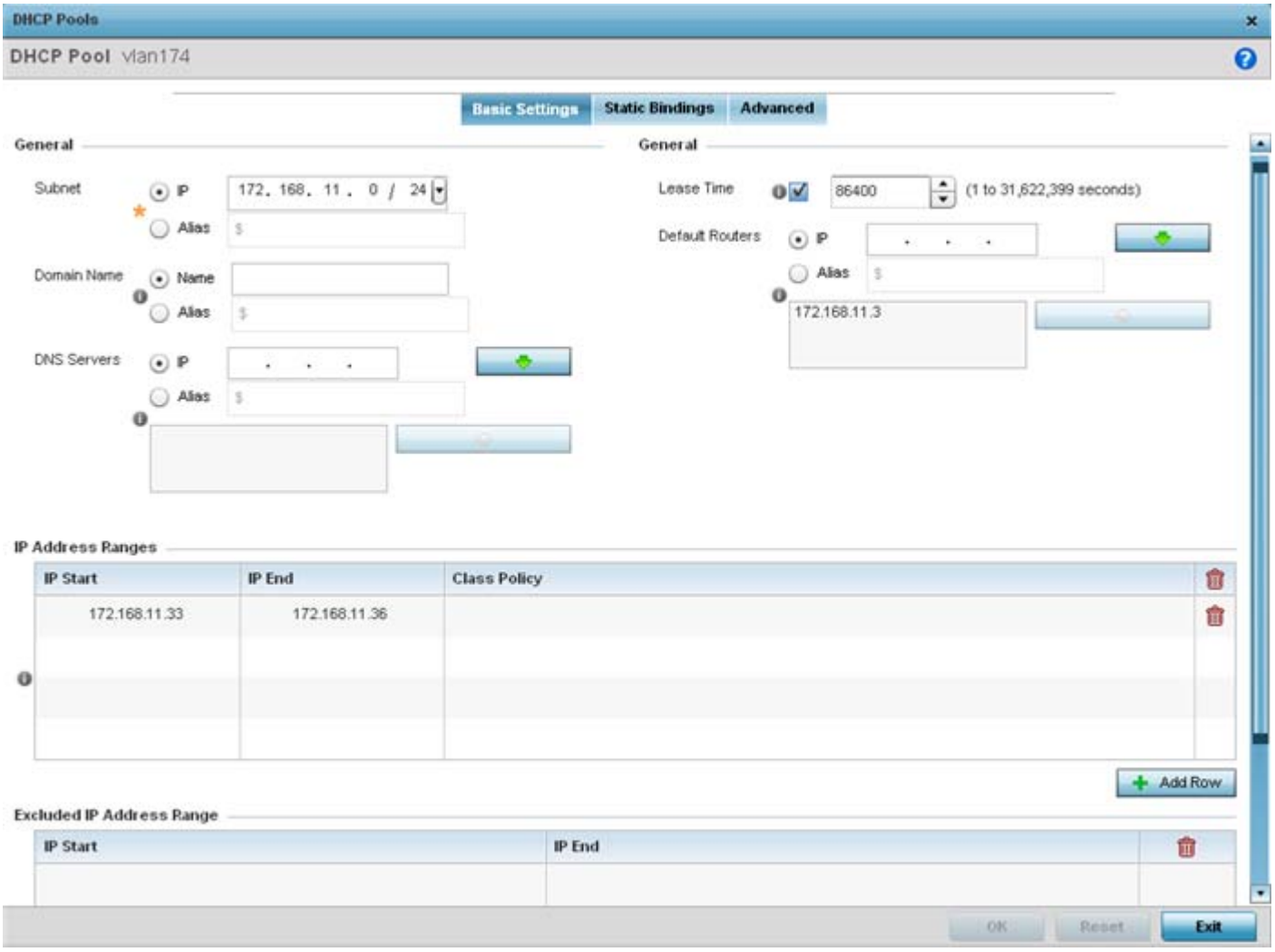


Figure 11-17 *DHCP Pools screen - Basic Settings tab*

If adding or editing a DHCP pool, the DHCP Pool screen displays the **Basic Settings** tab by default. Define the required parameters for the *Basic Settings*, *Static Bindings* and *Advanced* tabs to complete the creation of the DHCP pool.

4 Set the following **General** parameters, or aliases, from within the **Basic Settings** tab. An alias enables an administrator to define a configuration item (such as a IP address or domain name) once, and then use this single alias across different configurable values.

DHCP Pool	If adding a new pool, a name is required. The pool is the range of IP addresses defined for DHCP assignment or lease. The name assigned cannot be modified as part of the edit process. However, if the network pool configuration is obsolete it can be deleted. The name cannot exceed 32 characters.

Subnet	Define the *IP address/Subnet Mask* or IP alias used for DHCP discovery and requests between the local DHCP server and clients. The IP address and subnet mask (or its alias) is required to match the addresses of the layer 3 interface for the addresses to be supported through that interface. If setting a subnet IP alias, ensure it begins with a dollar sign ($) and does not exceed 32 characters. A numeric IP address is the default setting, not an alias.
Domain Name	Provide the domain name or domain alias used with this pool. Domain names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. A *fully qualified domain name* (FQDN) consists of a host name plus a domain name. For example, *computername.domain.com*. If setting a domain name alias, ensure it begins with a dollar sign ($) and does not exceed 32 characters. An actual domain name is the default setting, not an alias.
DNS Servers	Define one (or a group) of *Domain Name Servers* (DNS) to translate domain names to IP addresses. An alias can alternatively be applied for a DNS server IP address. Up to 8 IP addresses can be supported.If setting a DNS IP alias, ensure it begins with a dollar sign ($) and does not exceed 32 characters. An actual DNS IP address is the default setting, not an alias.
Lease Time	DHCP leases provide addresses for defined times to various clients. If a client does not use the leased address within the defined time, that IP address can be re-assigned to another DHCP supported client. Select this option to assign a lease in either *Seconds* (1 - 31,622,399), *Minutes* (1 - 527,040), *Hours* (1 - 8,784) or *Days* (1 - 366). The default setting is enabled, with a lease time of 1 day.
Default Routers	After a DHCP client has booted, the client begins sending packets to its default router. Set the IP address or IP alias for one or more routers used to map host names into IP addresses for clients. Up to 8 default router IP addresses are supported. If setting a default router IP alias, ensure it begins with a dollar sign ($) and does not exceed 32 characters. An actual router IP address is the default setting, not an alias.

5 Use the **IP Address Ranges** field define the range of included (starting and ending IP addresses) addresses for this particular pool.

a. Select the **+ Add Row** button at the bottom of the IP addresses field to add a new range. Select the radio button of an existing IP address range and select the **Delete** icon to remove it from the list of those available.

b. Enter a viable range of IP addresses in the **IP Start** and **IP End** columns. This is the range of addresses available for assignment to requesting clients.

c. Select the **Create** icon or **Edit** icon within the **Class Policy** column to display the **DHCP Server Policy** screen if a class policy is not available from the drop-down menu.

6 Refer to the **Excluded IP Address Range** field and select the **+Add Row** button. Add ranges of IP address to exclude from lease to requesting clients. Having ranges of unavailable addresses is a good practice to ensure IP address resources are in reserve. Select the **Delete** icon as needed to remove an excluded address range.

7 Select **OK** to save the updates to the DHCP Pool Basic Settings tab. Select **Reset** to revert to the last saved configuration.

8 Select the **Static Bindings** tab from within the DHCP Pools screen.

A binding is a collection of configuration parameters, including an IP address, associated with, or *bound to*, a DHCP client. Bindings are managed by DHCP servers. DHCP bindings automatically map a device MAC address to an IP address using a pool of DHCP supplied addresses. Static bindings assign IP addresses without creating

numerous host pools with manual bindings. Static host bindings use a text file the DHCP server reads. It eliminates the need for a lengthy configuration file and reduces the space required to maintain address pools.

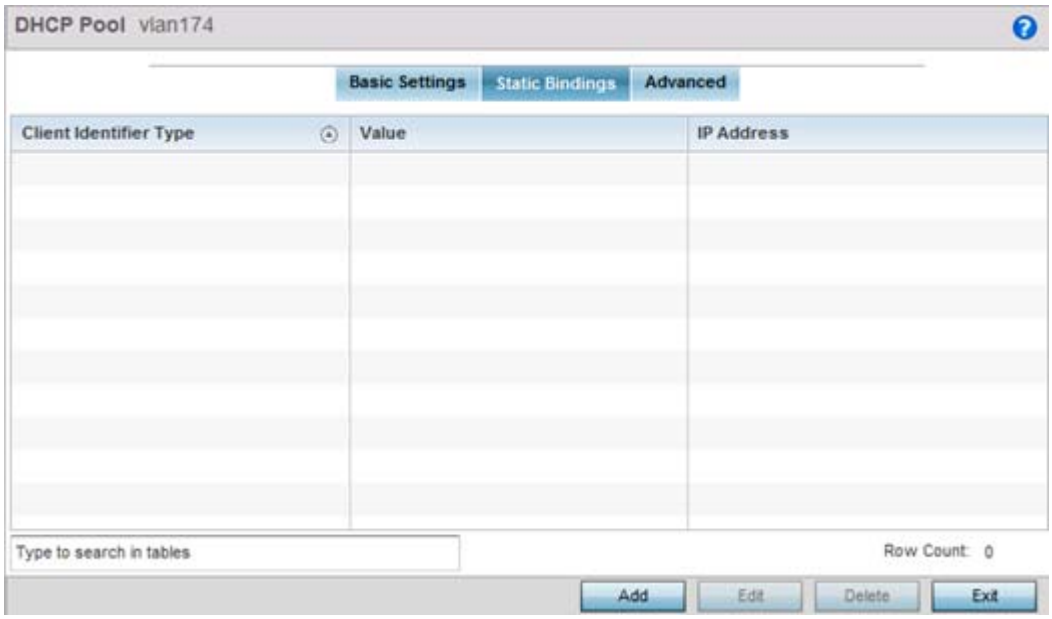


Figure 11-18 *DHCP Pools screen - Static Bindings tab*

9 Review the following to determine if a static binding can be used as is, a new binding requires creation or edit, or if a binding requires deletion:

Client Identifier Type	Lists whether the reporting client is using a *hardware address* or *client identifier* as its identifier type within requests to the DHCP server.
Value	Lists the hardware address or client identifier assigned to the client when added or last modified.
IP Address	Displays the IP address of the client on this interface that's currently using the pool name listed.

10 Select **Add** to create a new static binding configuration, **Edit** to modify an existing static binding configuration or **Delete** to remove a static binding from amongst those available.

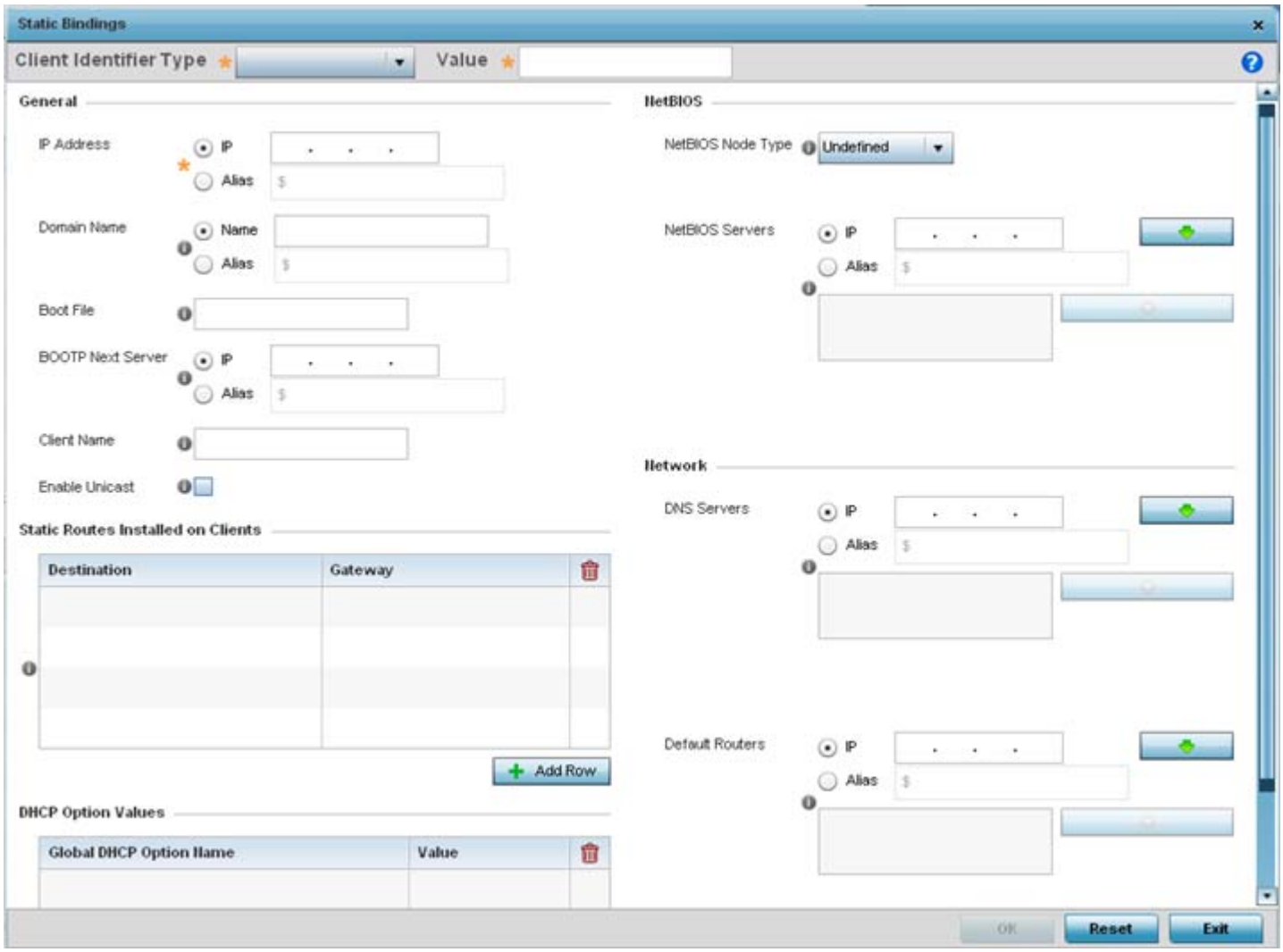


Figure 11-19 *Static Bindings Add screen*

11 Set the following **General** parameters or aliases to complete the creation of the static binding configuration. An alias enables an administrator to define a configuration item (such as a IP address or domain name) once, and then use this single alias across different configurable values.

IP Address	Set an IP address of the client using this host pool for DHCP resources. The IP option is selected by default. Optionally select *Alias* to provide an IP alias beginning with a dollar sign ($) and not exceeding 32 characters.
Domain Name	Provide a domain name of the current interface. Domain names aren't case sensitive and can contain alphabetic or numeric letters or a hyphen. A *fully qualified domain name* (FQDN) consists of a host name plus a domain name. For example, *computername.domain.com.* The Name option is selected by default. Optionally select *Alias* to provide a domain name alias beginning with a dollar sign ($) and not exceeding 32 characters.

Boot File	Enter the name of the boot file used with this pool. Boot files (Boot Protocol) can be used to boot remote systems over the network. BOOTP messages are encapsulated inside UDP messages so requests and replies can be forwarded. Each DHCP network pool can use a different file as needed. The IP option is selected by default. Optionally select *Alias* to provide a boot file IP alias beginning with a dollar sign ($) and not exceeding 32 characters.
BOOTP Next Server	Provide the numerical IP address or alias of the server providing BOOTP resources. BOOTP (boot protocol) requests boot remote systems within the controller or service platform managed network. BOOTP messages are encapsulated inside UDP messages and are forwarded by the controller or service platform. The IP option is selected by default. Optionally select *Alias* to provide a next BOOTP server IP alias beginning with a dollar sign ($) and not exceeding 32 characters.
Client Name	Provide the name of the client requesting DHCP Server support.
Enable Unicast	Unicast packets are sent from one location to another location (there's just one sender, and one receiver). Select this option to forward unicast messages to just a single device within this network pool. This settings is disabled by default.

12 Define the following **NetBIOS** parameters to complete the creation of the static binding configuration:

NetBIOS Node Type	Set the NetBios Node Type used with this particular pool. The following options are available: *Broadcast* - Uses broadcasting to query nodes on the network for the owner of a NetBIOS name. *Peer-to-Peer* - Uses directed calls to communicate with a known NetBIOS name server (such as a WINS server), for the IP address of a NetBIOS machine. *Mixed* - A mixed node using broadcasted queries to find a node, and failing that, queries a known p-node name server for the address. *Hybrid* - A combination of two or more nodes. *Undefined* - No node type is applied.
NetBIOS Servers	Specify a numerical IP address of a single or group of NetBIOS WINS servers available to requesting clients. A maximum of 8 server IP addresses can be assigned. The IP option is selected by default. Optionally select *Alias* to provide a NetBIOS server IP alias beginning with a dollar sign ($) and not exceeding 32 characters.

13 Refer to the **Static Routes Installed on Clients** field to set **Destination IP** and **Gateway** addresses enabling the assignment of static IP addresses without creating numerous host pools with manual bindings. This eliminates the need for a long configuration file and reduces the space required in NVRAM to maintain address pools. Select the **+ Add Row** button to add individual destinations. Select the **Delete** icon to remove it from the list of those available.

14 Refer to the **DHCP Option Values** table to set Global DHCP options. A set of global DHCP options applies to all clients, whereas a set of subnet options applies only to the clients on a specified subnet. If you configure the same option in more than one set of options, the precedence of the option type decides which the DHCP server supports a client.

a. Select the **+ Add Row** button to add individual options. Assign each a **Global DHCP Option Name** to help differentiate it from others with similar configurations. Select the radio button of an existing option and select the **- Delete** button to remove it from the list of those available.

b. Assign a **Value** to each option with codes from 1 - 254. A vendor-specific option definition only applies to the vendor class for which it is defined.

15 Within the **Network** field, define one or group of **DNS Servers** and **Default Routers** to translate domain names to IP addresses. Up to 8 IP addresses can be provided. The IP option is selected by default for both DNS Servers and Default Routers. Optionally select *Alias* to provide an IP alias beginning with a dollar sign ($) and not exceeding 32 characters.

16 Select **OK** when completed to update the static bindings configuration. Select **Reset** to revert the screen back to its last saved configuration.

17 Select the **Advanced** tab to define additional NetBIOS and Dynamic DNS parameters.

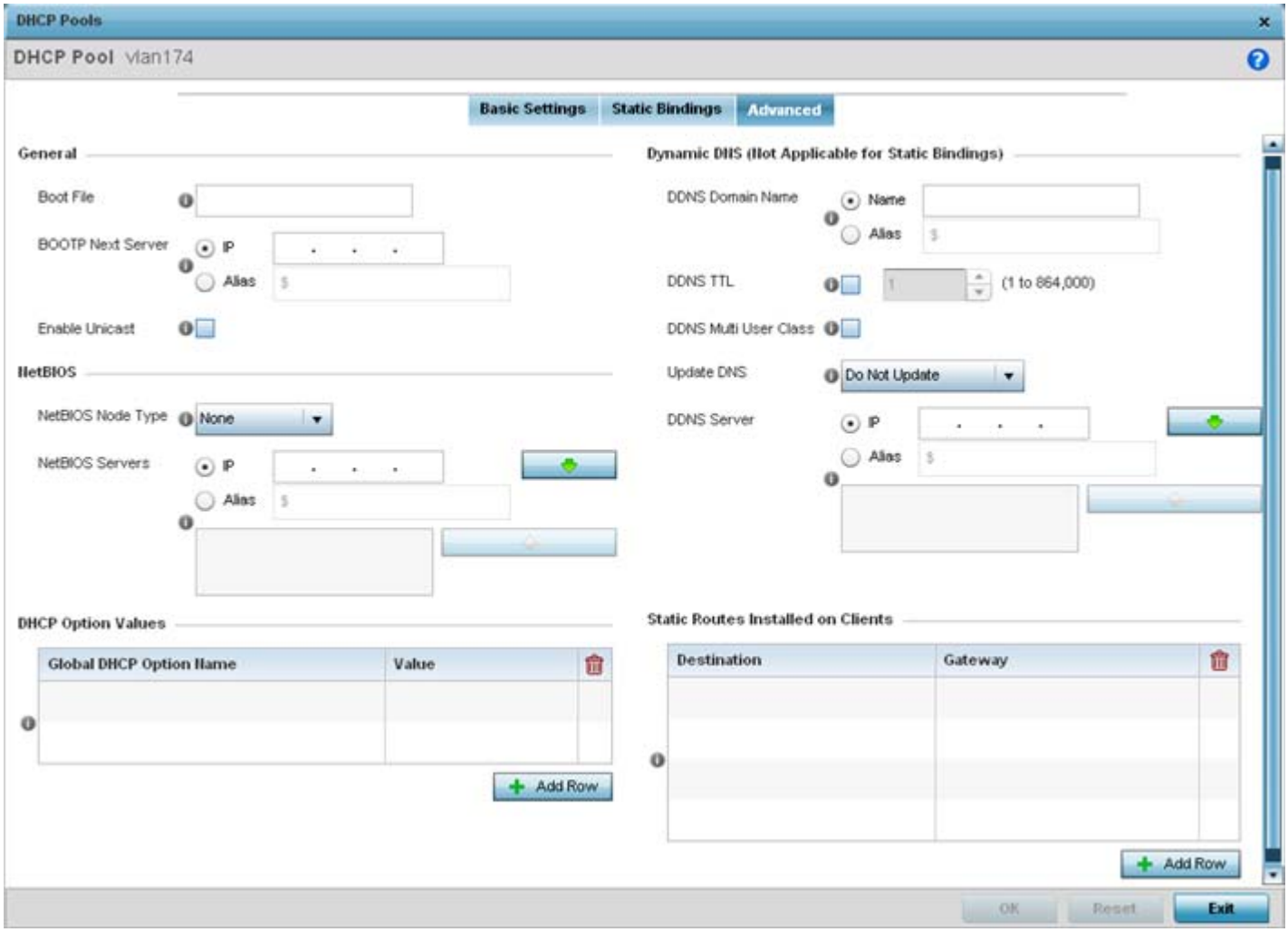


Figure 11-20 *DHCP Pools screen - Advanced tab*

18 The addition or edit of the DHCP pool's advanced settings requires the following **General** parameters be set:

Boot File	Enter the name of the boot file used with this pool. Boot files (Boot Protocol) can be used to boot remote systems over the network. BOOTP messages are encapsulated inside UDP messages so requests and replies can be forwarded. Each pool can use a different file as needed.

BOOTP Next Server	Provide the numerical IP address or alias of the server providing BOOTP resources. BOOTP (boot protocol) requests boot remote systems within the controller or service platform managed network. BOOTP messages are encapsulated inside UDP messages and are forwarded by the controller or service platform. The IP option is selected by default. Optionally select *Alias* to provide a next BOOTP server IP alias beginning with a dollar sign ($) and not exceeding 32 characters.
Enable Unicast	Unicast packets are sent from one location to another location (there's just one sender, and one receiver). Select this option to forward unicast messages to just a single device within the network pool. This setting is disabled by default.

19 Set the following **NetBIOS** parameters for the network pool:

NetBIOS Node Type	Set the NetBIOS Node Type used with this pool. The following types are available: *Broadcast* - Uses broadcasting to query nodes on the network for the owner of a NetBIOS name. *Peer-to-Peer* - Uses directed calls to communicate with a known NetBIOS name server, such as a WINS server, for the IP address of a NetBIOS machine. *Mixed* - Mixed uses broadcasted queries to find a node, and failing that, queries a known p-node name server for the address. *Hybrid* - Is a combination of two or more nodes. *Undefined* - No NetBIOS Node Type is used.
NetBIOS Servers	Specify a numerical IP address of a single or group of NetBIOS WINS servers. A maximum of 8 server IP addresses can be assigned. The IP option is selected by default. Optionally select *Alias* to provide a NetBIOS server IP alias beginning with a dollar sign ($) and not exceeding 32 characters.

20 Refer to the **DHCP Option Values** table to set global DHCP options applicable to all clients, whereas a set of subnet options applies to just the clients on a specified subnet.

a Select the **+ Add Row** button to add individual options. Assign each a **Global DHCP Option Name** to help differentiate it from others with similar configurations. Select the radio button of an existing option and select **Delete** to remove it from the list.

b Assign a **Value** to each option from 1 - 254. A vendor-specific option definition only applies to the vendor class for which it's defined.

21 Define the following set of **Dynamic DNS (Not Applicable for Static Bindings)** parameters used with the network pool configuration. Using DDNS controllers and service platforms can instruct a DNS server to change, in real time (ad-hoc) the active DNS configuration of its configured hostnames, addresses or other information stored in DNS.

DDNS Domain Name	Enter a domain name for DDNS updates representing the forward zone in the DNS server. For example, *test.net*. The *Name* option is selected by default. Optionally select *Alias* to provide a DDNS domain name alias beginning with a dollar sign ($) and not exceeding 32 characters.
DDNS TTL	Select this option to set a TTL (Time to Live) to specify the validity of DDNS records. The maximum value configurable is 864000 seconds.
DDNS Multi User Class	Select the check box to associate the user class option names with a multiple user class. This allows the user class to transmit multiple option values to DHCP servers supporting multiple user class options.

Update DNS	Set if DNS is updated from a client or a server. Select either *Do Not Update*, *Update from Server* or *Update from Client*. The default setting is Do Not Update, implying that no DNS updates occur at all.
DDNS Server	Specify a numerical IP address of one or two DDNS servers. *Dynamic DNS* (DDNS) prompts a computer or network to obtain a new IP address lease and dynamically associate a hostname with that address, without having to manually enter the change every time. Since there are situations where an IP address can change, it helps to have a way of automatically updating hostnames that point to the new address every time. The IP option is selected by default. Optionally select *Alias* to provide a DDNS server IP alias beginning with a dollar sign ($) and not exceeding 32 characters.

22 Click the **+ Add Row** button and enter a **Destination** and **Gateway** IP Address to add **Static Routes Installed on Clients**.

23 Select **OK** to save the updates to the DHCP pool's Advanced settings. Select **Reset** to revert the screen back to its last saved configuration.

11.3.2 Defining DHCP Server Global Settings

Setting the DHCP Configuration

Set a DHCP server global configuration by defining whether BOOTP requests are ignored and DHCP global server options.

To define DHCP server global settings:

1 Select **DHCP Server Policy** from within Services menu pane. **Add** or **Edit** an existing policy.

2 Select the **Global Settings** tab.

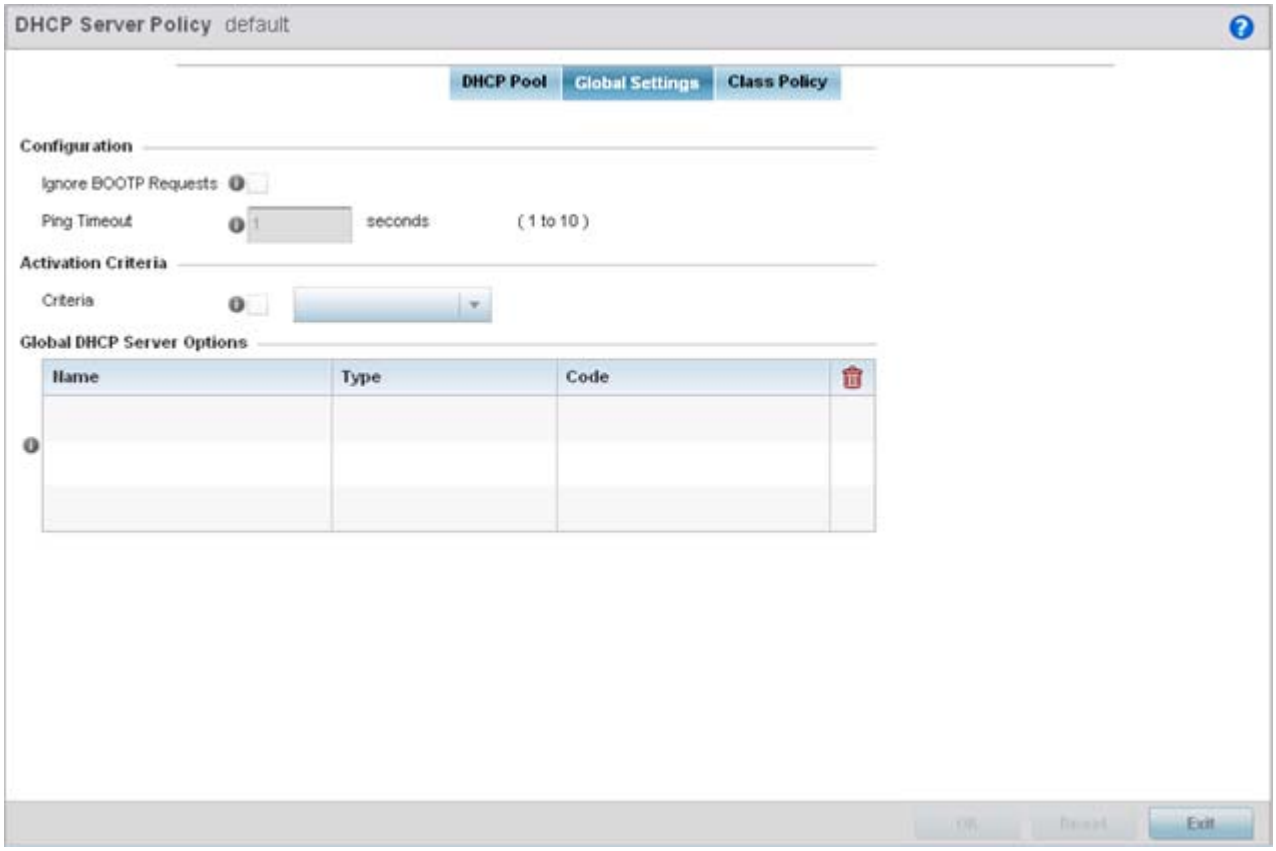


Figure 11-21 *DHCP Server Policy screen - Global Settings tab*

3 Set the following parameters within the **Configuration** field:

Ignore BOOTP Requests	Select the checkbox to ignore BOOTP requests. BOOTP (boot protocol) requests boot remote systems within the network. BOOTP messages are encapsulated inside UDP messages and forwarded. This feature is disabled by default, so unless selected, BOOTP requests are forwarded.
Ping Timeout	Set an interval (from 1 -10 seconds) for the DHCP server ping timeout. The timeout is the intermittent ping and discover interval to discern whether a client requested IP address is already used.

4 Set the following **Activation Criteria** for the DHCP server policy:

Criteria	Select the *Criteria* option to invoke a drop-down menu to determine when the DHCP daemon is invoked. Options include *vrrp-master, cluster-master*, and *rf-domain-manager*. A VRRP master responds to ARP requests, forwards packets with a destination link MAC layer address equal to the virtual router MAC layer address, rejects packets addressed to the IP associated with the virtual router and accepts packets addressed to the IP associated with the virtual router. The solitary cluster master is the cluster member elected, using a priority assignment scheme, to provide management configuration and Smart RF data to other cluster members. Cluster requests go through the elected master before dissemination to other cluster members. The RF Domain manager is the elected member of the RF Domain capable of storing and provisioning configuration and firmware images for other members of the RF Domain.

5 Refer to the **Global DHCP Server Options** field.

a. Use the **+ Add Row** button at the bottom of the field to add a new global DHCP server option. Select the radio button of an existing global DHCP server option and select the **Delete** icon to remove it from the list of those available.

b. Use the **Type** drop-down menu to specify whether the DHCP option is being defined as a numerical IP address or ASCII or Hex string. Highlight an entry from within the Global Options screen and click the **Remove** button to delete the name and value.

6 Select **OK** to save the updates to the DHCP server global settings. Select **Reset** to revert the screen back to its last saved configuration.

11.3.3 DHCP Class Policy Configuration

Setting the DHCP Configuration

The local DHCP server assigns IP addresses to DHCP enabled wireless clients based on user class option names. Clients with a defined set of user class option names are identified by their user class name. The DHCP server can assign IP addresses from as many IP address ranges as defined by the administrator. The DHCP user class associates a particular range of IP addresses to a device in such a way that all devices of that type are assigned IP addresses from the defined range.

Refer to the **DHCP Class Policy** screen to review existing DHCP class names and their current multiple user class designations. Multiple user class options enable a user class to transmit option values to DHCP servers supporting multiple user class options. Either add a new class policy, edit the configuration of an existing policy or permanently delete a policy as required.

To review DHCP class policies:

1 Select **DHCP Server Policy** from within Services menu pane. **Add** or **Edit** an existing policy.

2 Select the **Class Policy** tab.

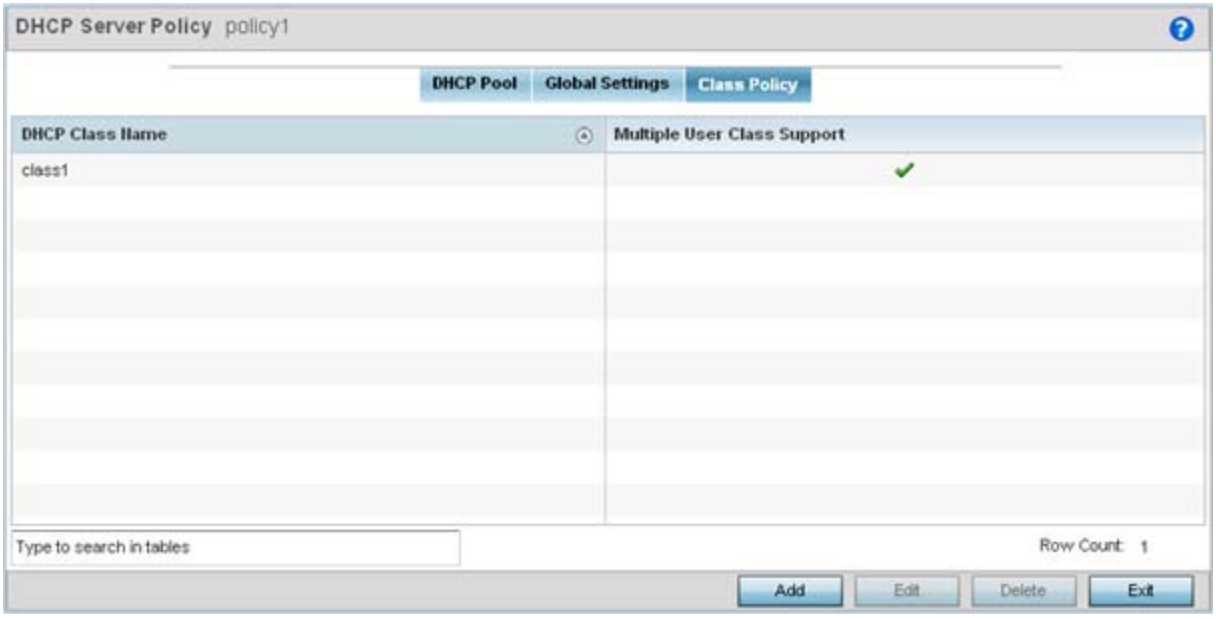


Figure 11-22 *DHCP Server Policy screen - Class Policy tab*

3 Refer to the following to determine whether a new class policy requires creation, an existing class policy requires edit or an existing policy requires deletion:

DHCP Class Name	Displays client names grouped by the class name assigned when the class policy was created.
Multiple User Class Support	A green check mark in this column defines multiple user class support as enabled from the listed DHCP class name. A red "X" defines multiple user class support as disabled. Multiple user class support can be *enabled/disabled* for existing class names by editing the class name's configuration.

4 Select **Add** to create a new DHCP class policy, **Edit** to update an existing policy or **Delete** to remove an existing policy.

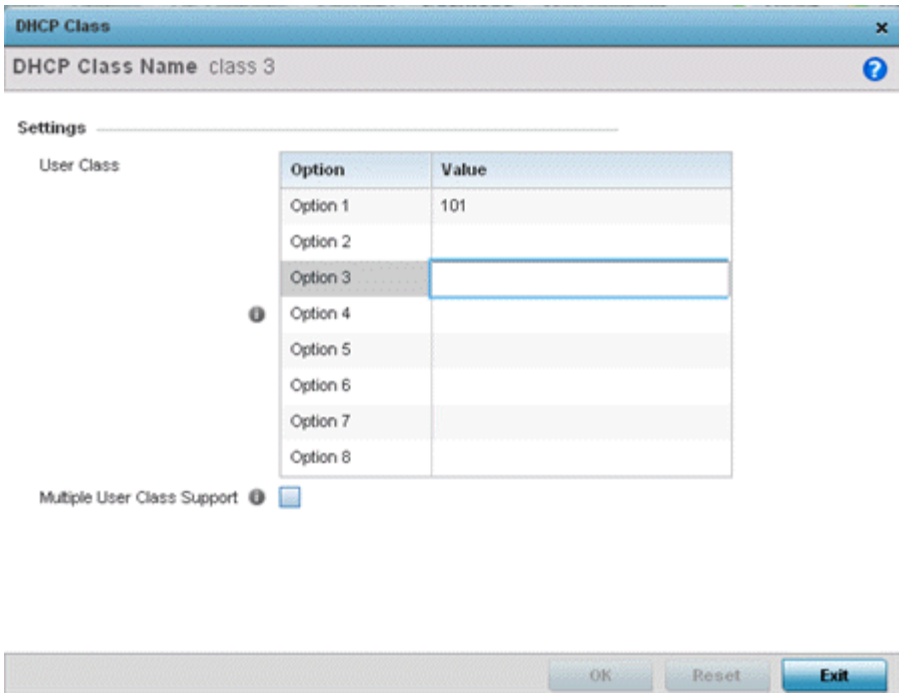


Figure 11-23 *DHCP Class Name Add screen*

5 If adding a new **DHCP Class Name**, assign a name representative of the device class supported. The DHCP user class name should not exceed 32 characters.

6 Select a row within the **Value** column to enter a 32 character maximum value string.

7 Select the **Multiple User Class** check box to enable multiple option values for the user class. This allows the user class to transmit multiple option values to DHCP servers supporting multiple user class options.

8 Select **OK** to save the updates to this DHCP class policy. Select **Reset** to revert the screen back to its last saved configuration.

11.3.4 DHCP Deployment Considerations

Setting the DHCP Configuration

Before defining an internal DHCP server configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- DHCP option 189 is required when AP650 Access Points are deployed over a layer 3 network and require layer 3 adoption. DHCP services are not required for AP650 Access Points connected to a VLAN that's local to the controller or service platform.
- DHCP's lack of an authentication mechanism means a DHCP server cannot check if a client or user is authorized to use a given user class. This introduces a vulnerability when using user class options. For example, if a user class is used to assign a special parameter (for example, a database server), there is no way to authenticate a client and it's impossible to check if a client is authorized to use this parameter.
- Ensure traffic can pass on UDP ports 67 and 68 for clients receiving DHCP information.

11.4 Setting the Bonjour Gateway Configuration

Services

Bonjour is Apple's zero-configuration networking (Zeroconf) implementation. Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates the devices (printers, computers etc.) and services these computers provide over a local network.

Bonjour provides a method to discover services on a *local area network (*LAN). Bonjour allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.

NOTE: Up to eight (8) Bonjour discovery policies can be configured.

The following options can be configured:

- *Configuring a Bonjour Discovery Policy*
- *Configuring a Bonjour Forwarding Policy*

11.4.1 Configuring a Bonjour Discovery Policy

Setting the Bonjour Gateway Configuration

The Bonjour discovery policy configures how Bonjour services are located. It configures the VLANs on which these services can be found.

To display Bonjour discovery policy information:

1 Select **Configuration**.

2 Select **Services**.

3 Select **Bonjour Gateway** to expand its submenu.

4 Select **Discovery Policy**.

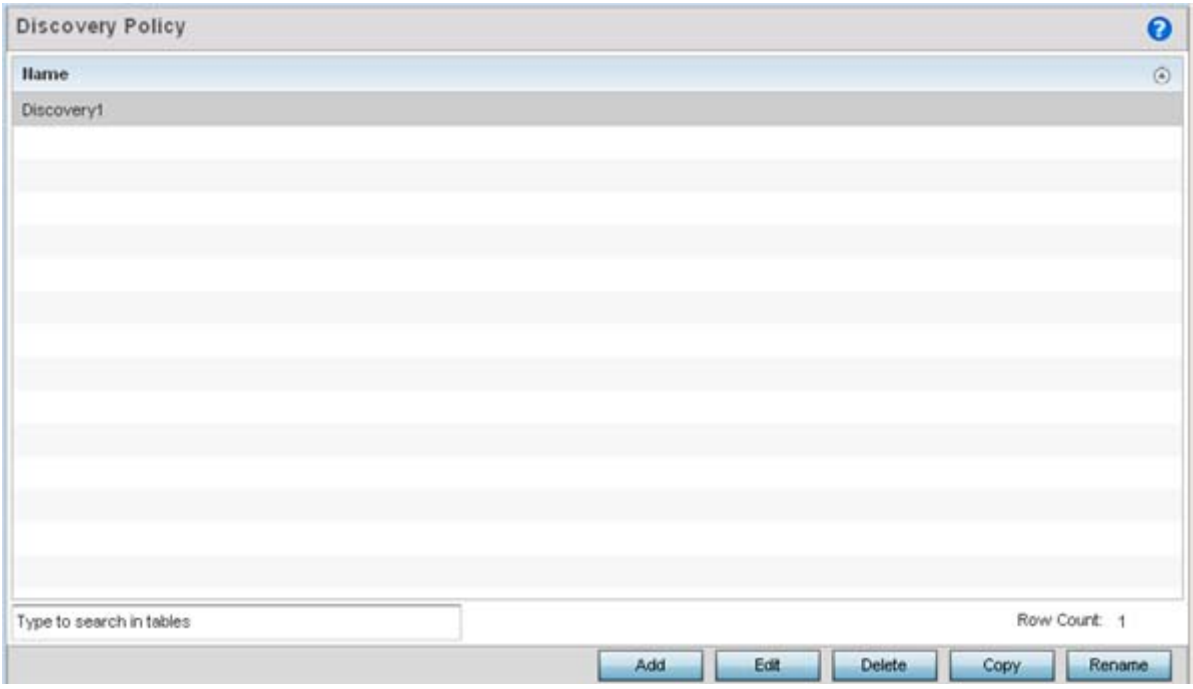


Figure 11-24 *Bonjour - Discovery Policy screen*

The **Discovery Policy** screen displays the name of the configured Bonjour discovery policies.

5 Select an existing policy and select **Edit** to modify its configuration or select **Add** to create a new configuration. Optionally **Rename** a policy or **Copy** a policy to a different location.

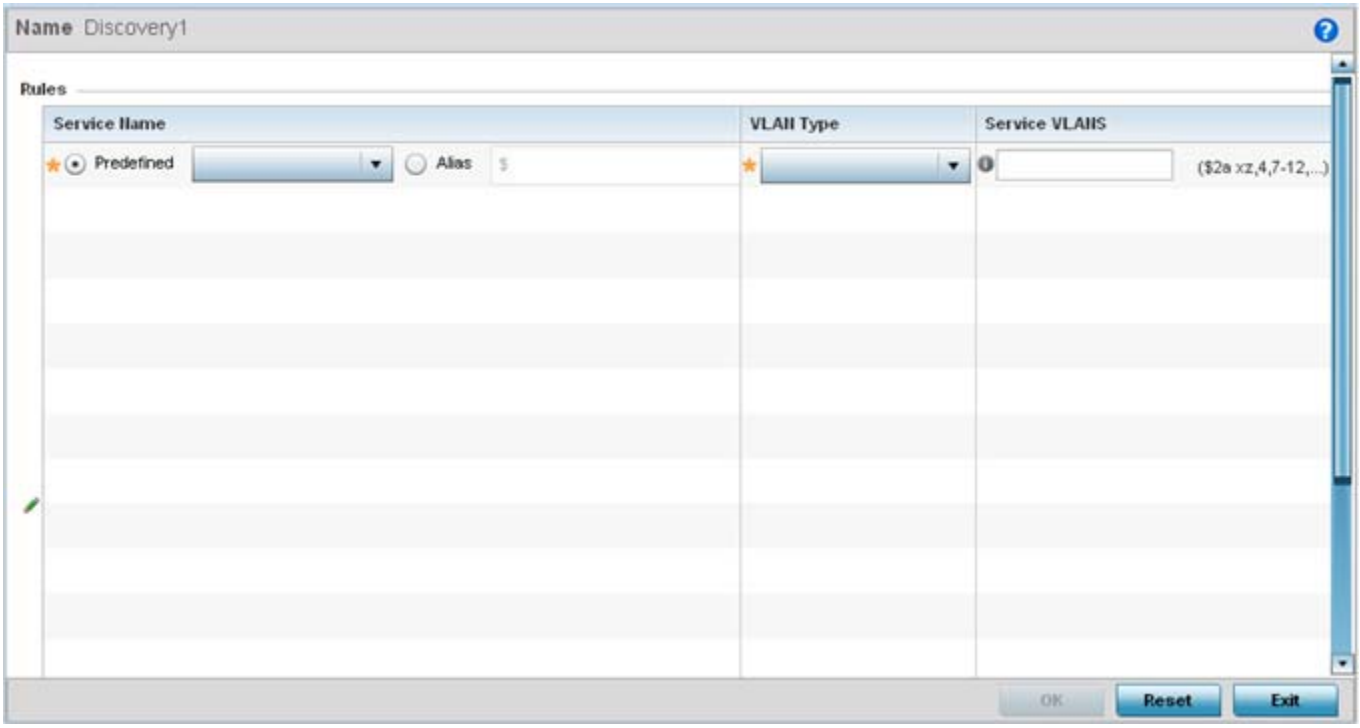


Figure 11-25 *Bonjour - Discovery Policy - Add/Edit Policy screen*

6 Select the **+ Add Row** button to add a rule configuration. These are the services discoverable by the Bonjour gateway.

7 Set the following discovery attributes for the discovery policy configuration:

Service Name	Define the service that can be discovered by the Bonjour gateway. *Predefined* – Use the drop-down menu to select from a list of predefined Apple services (*Scanner, Printer, HomeSharing* etc.). *Alias* – Use an existing alias to define a service not available in the predefined list.
VLAN Type	Use the drop-down menu to select the VLAN type. *Local* – Indicates the VLAN(s) defined in *Service VLAN* field uses a local bridging mode. *tunneled* – Indicates the VLAN(s) defined in Service VLAN field are shared tunnel VLANs.
Service VLANs	Provide a VLAN or a list of VLANs on which the selected service is discoverable.

8 Select **OK** to save the updates to this Bonjour Discovery Policy. Select **Reset** to revert to the last saved configuration.

11.4.2 Configuring a Bonjour Forwarding Policy

- *Setting the Bonjour Gateway Configuration*

A Bonjour forwarding policy enables the discovery of services on VLANs not visible to the device running the Bonjour Gateway. Bonjour forwarding enables the forwarding of Bonjour advertisements across VLANs to enable the Bonjour gateway to build a list of services and VLANs where services are available.

NOTE: Only one (1) Bonjour forwarding policy is configurable.

NOTE: There must be Layer 2 connectivity between devices for forwarding to work.

To display Bonjour forwarding policy information:

1 Select **Configuration**.

2 Select **Services**.

3 Select **Bonjour Gateway** to expand its submenu.

4 Select **Forwarding Policy**.

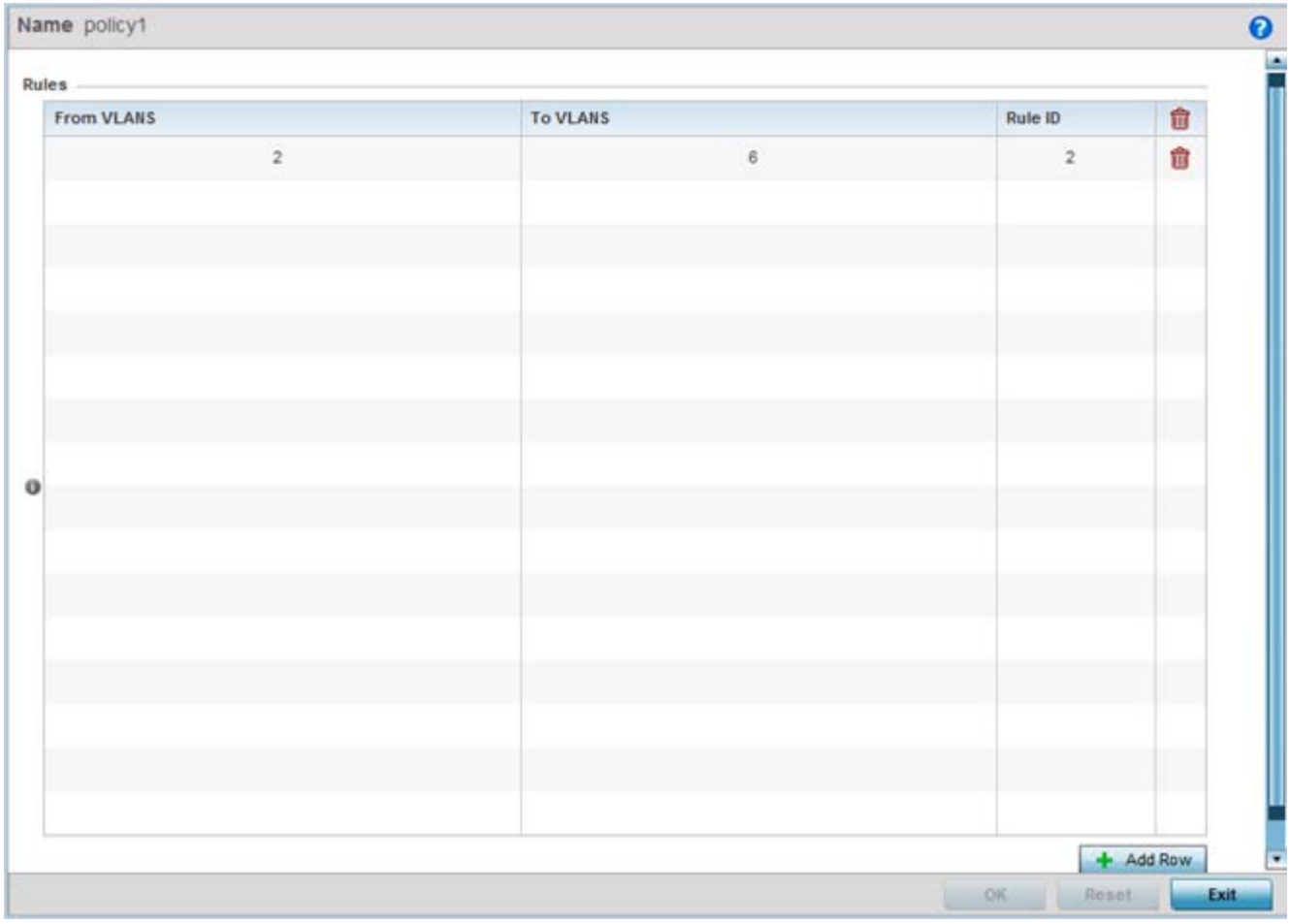


Figure 11-26 *Bonjour Gateway - Forwarding Policy screen*

The screen displays the name of existing Bonjour forwarding policies.

5 Select an existing policy and select **Edit** to modify its configuration or select **Add** to create a new configuration.

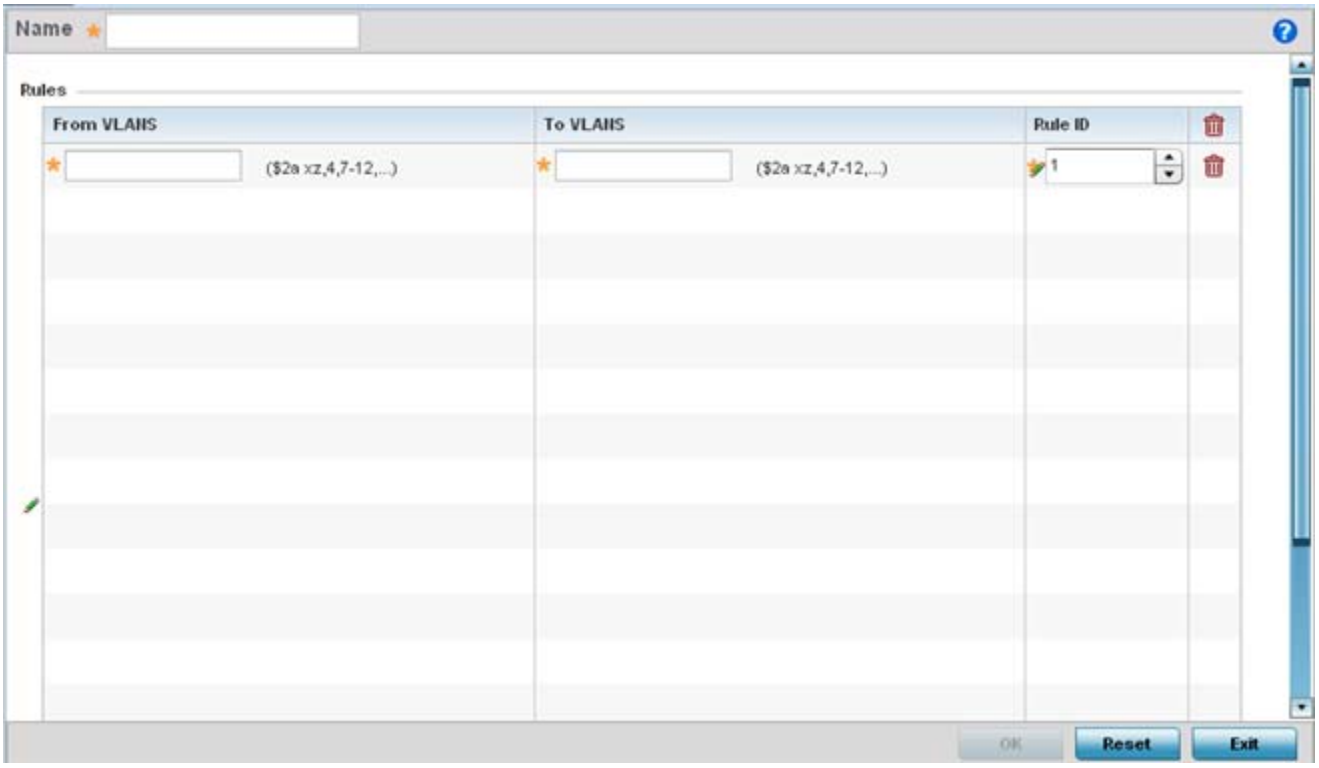


Figure 11-27 *Bonjour Gateway - Forwarding Policy - Add screen*

6 Select the **+ Add Row** button to add a forwarding rule to the Bonjour Forwarding Policy. Advertisements from VLANs that contain services are forwarded to VLANs containing clients.

From VLANs	*From VLANs* are virtual interfaces where the Apple services are available. Enter a VLAN ID or a range of VLANs. Aliases can also be used.
To VLANs	*To VLANs* are virtual interfaces where clients for the services are available. Enter a VLAN ID or a range of VLANs. Aliases can also be used.
Rule ID	Use the spinner to set a unique rule ID (from 1 - 16) for this rule. This acts as numerical differentiator from other indexes.

7 Select **OK** to save the updates to this Bonjour Gateway Forwarding policy. Select **Reset** to revert to the last saved configuration.

11.5 DHCPv6 Server Policy

Services

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network.

DHCPv6 servers pass IPv6 network addresses to IPv6 clients. The DHCPv6 address assignment feature manages non-duplicate addresses in the correct prefix based on the network where the host is connected. Assigned addresses can be from one or multiple pools. Additional options, such as the default domain and DNS name-server

address, can be passed back to the client. Address pools can be assigned for use on a specific interface or on multiple interfaces, or the server can automatically find the appropriate pool.

NOTE: DHCPv6 server updates are only implemented when the controller, service platform or service platform is restarted.

Refer to the following for more information on configuring the DHCPv6 Server Policy parameters:

- *Defining DHCPv6 Options*
- *DHCPv6 Pool Configuration*

To access and review the local DHCPv6 server configuration:

1 Select **Configuration** > **Services** > **DHCPv6 Server Policy**.
The **DHCPv6 Server Policy** screen displays.

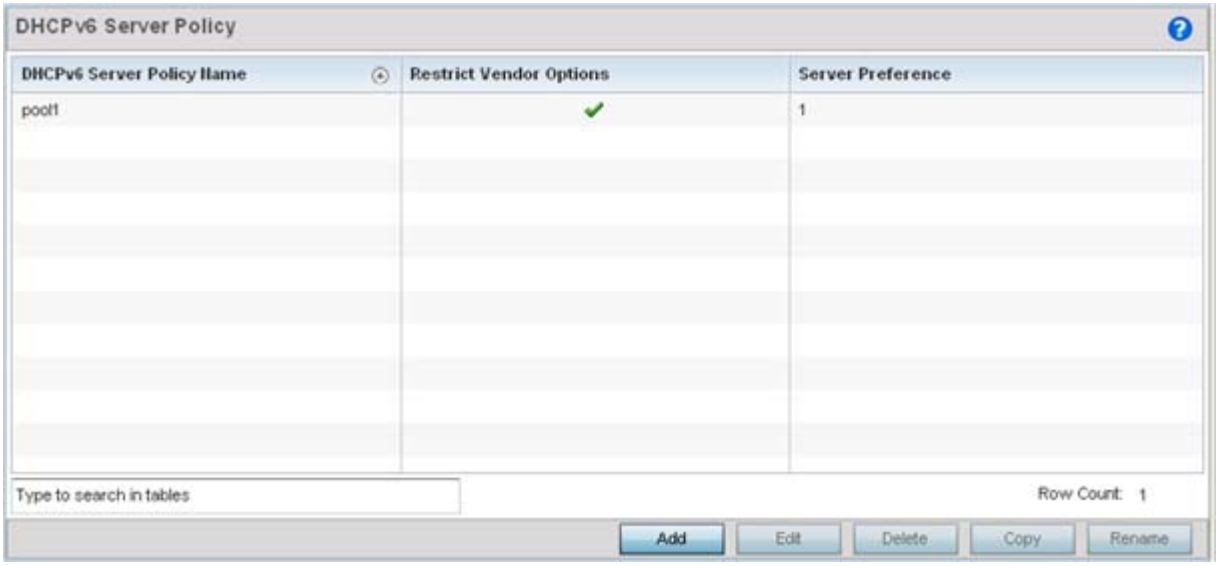


Figure 11-28 *DHCPv6 Server Policy screen*

2 Review the following DHCPv6 server configurations (at a high level) to determine whether a new server policy requires creation, an existing policy requires modification or an existing policy requires deletion:

DHCPv6 Server Policy Name	Lists the name assigned to each DHCPv6 server policy when it was initially created. The name assigned to a DHCPv6 server policy cannot be modified as part of the policy edit process. However, obsolete policies can be deleted, copied (archived) or renamed as needed.
Restrict Vendor Options	A green checkmark within this column means this policy has been set to restrict vendor DHCP options. A red "X" defines the policy as accepting all DHCP vendor options. Vendor specific DHCPv6 options are only applicable to the vendor class defined.
Server Preference	Lists the server preference (from 0 - 255) specified for each DHCPv6 server policy. The default value is 0.

3 Select **Add** to create a new DHCPv6 server policy, choose an existing policy and select the **Edit** button to modify the policy's properties or choose an existing policy and select **Delete** to remove the policy from those available. Adding or Editing a DHCP server policy displays the **DHCPv6 Server Policy Name** screen by default. Optionally **Rename** or **Copy** a policy to a different location.

11.5.1 Defining DHCPv6 Options

DHCPv6 Server Policy

DHCPv6 services are available for specific IP interfaces. A pool (or range) of IPv6 network addresses and DHCPv6 options can be created for each IPv6 interface defined. This range of addresses can be made available to DHCPv6 enabled devices on either a permanent or leased basis. DHCPv6 options are provided to each client with a DHCPv6 response and provide DHCPv6 clients information required to access network resources (default gateway, domain name, DNS server and WINS server configuration). An option exists to identify the vendor and functionality of a DHCPv6 client. The information is a variable-length string of characters (or octets) with a meaning specified by the vendor of the DHCPv6 client.

To set DHCPv6 options:

1 Select **Configuration** > **Services** > **DHCPv6 Server Policy**.

2 Select **Add** to create a new policy or **Edit** to modify the policy's properties of a selected DHCPv6 server policy. Select **+ Add Row** to populate the screen with editable rows for DHCPv6 option configuration.

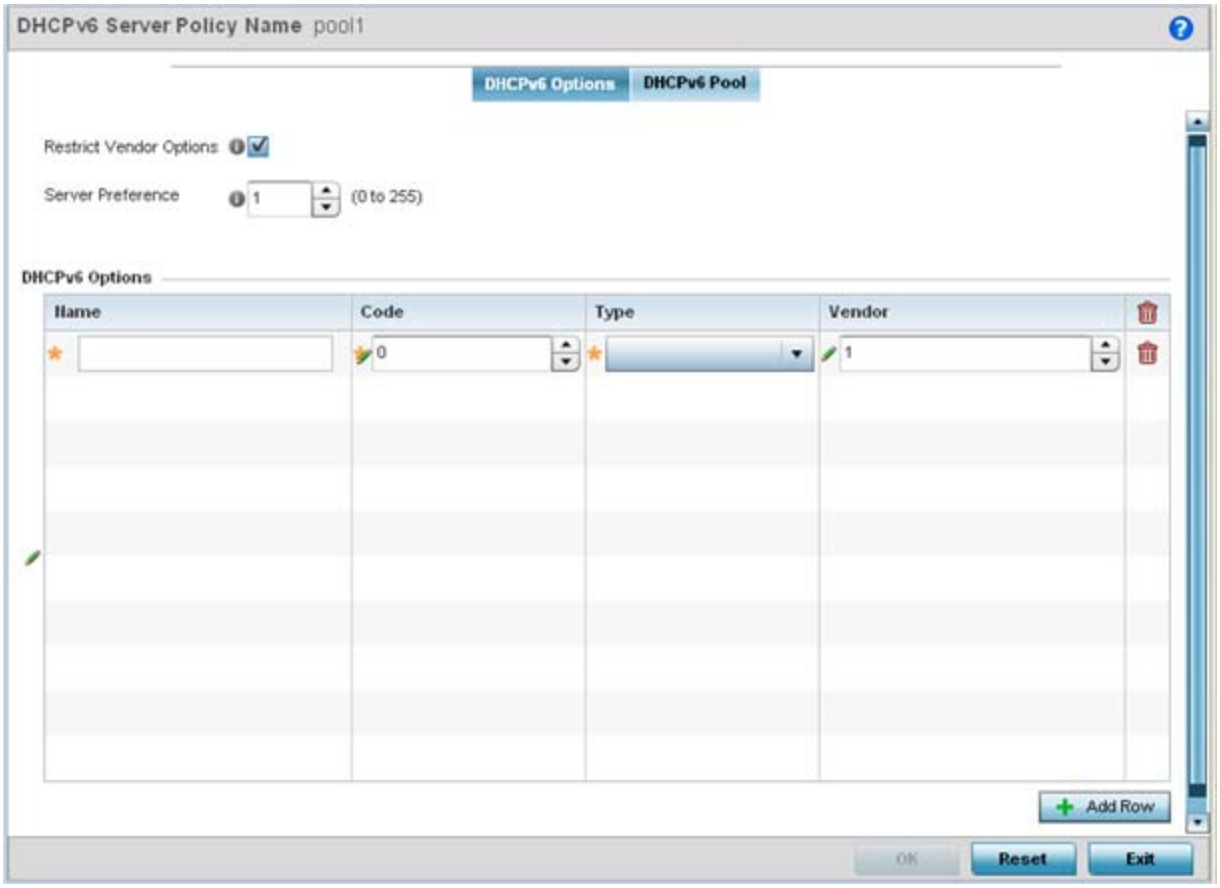


Figure 11-29 *DHCP v6Server Policy - DHCPv6 Options tab*

3 Select **Restrict Vendor Options** to restrict the use of vendor specific DHCPv6 options. This limits the use of vendor specific DHCP options in this specific DHCPv6 policy.

4 Use the spinner control to select a DHCPv6 **Server Preference** from 0 - 255. The default value is 0.

5 Set the following **DHCPv6 Option** configuration parameters:

Name	Enter a name to associate with the new DHCP option. This name should describe the new option's function.
Code	Use the spinner control to specify a DHCP option code (from 0 - 254) for the option. Only one code for each DHCPv6 option of the same value can be used in each DHCPv6 server policy.
Type	Use the drop-down menu to select the DHCP option type for the new option. The option can be either *ASCII,* which sends an ASCII compliant string to the client, *ipv6* which sends an IPv6 compatible address to the client or *Hex String* which sends a hexadecimal string to the client.
Vendor	Use the spinner control to specify the numeric Vendor ID for the new option. Each vendor should have a unique vendor ID used by the DHCPv6 server to issue vendor specific DHCP options.

6 Select **OK** to save the updates to the DHCPv6 options. Select **Reset** to revert the screen back to its last saved configuration.

11.5.2 DHCPv6 Pool Configuration

DHCPv6 Server Policy

A DHCPv6 pool includes information about available configuration parameters and policies controlling the assignment of the parameters to requesting clients from the pool.

To create a DHCPv6 pool configuration:

1 Select **Configuration** > **Services** > **DHCPv6 Server Policy**. The **DHCPv6 Options** tab displays by default.

2 Select **Add** to create a new policy or **Edit** to modify the policy's properties of a selected DHCPv6 server policy. Select **+ Add Row** to populate the screen with editable rows for DHCPv6 option configuration.

3 Select the **DHCPv6 Pool** tab.

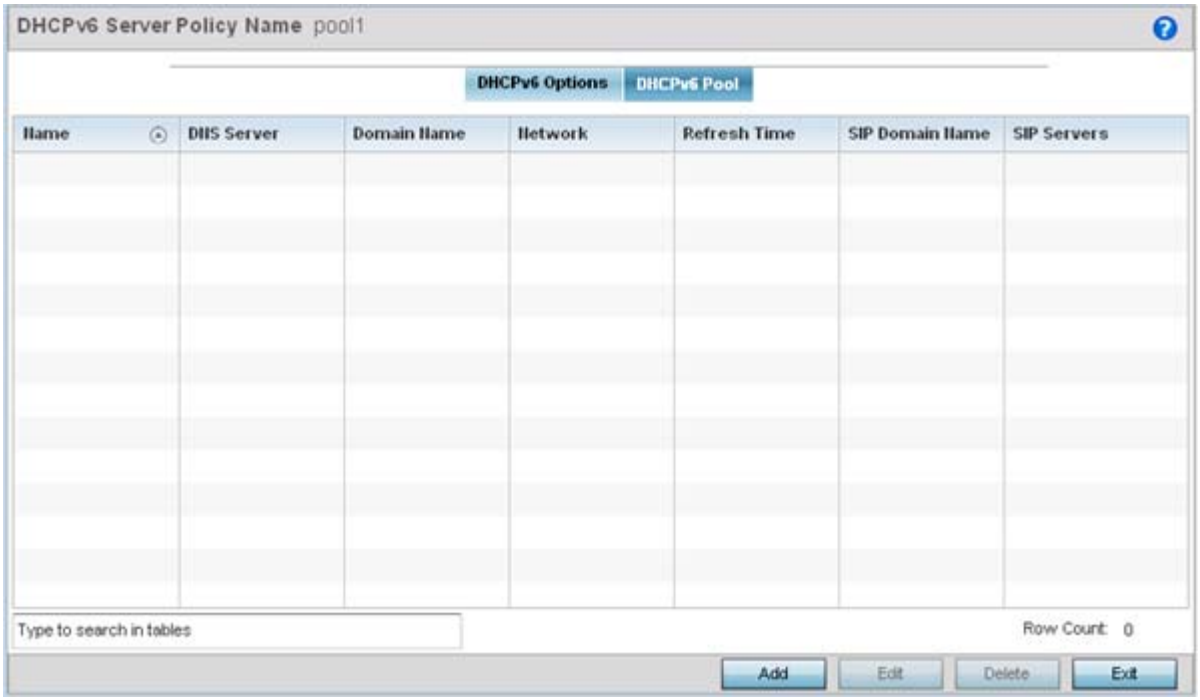


Figure 11-30 *DHCP Server Policy - DHCPv6 Pool tab*

4 Set the following parameters within the **Configuration** field:

Name	Lists the administrator assigned name of the IPv6 pool resource from which IPv6 formatted addresses can be issued to DHCPv6 client requests. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
DNS Server	Displays the address of the DNS server resource utilized with the DHCPv6 pool.
Domain Name	Displays the hostname of the domain associated with the DHCPv6 pool.
Network	Displays the IPv6 formatted address and mask utilized with the DHCPv6 address pool. The address can be configured in the add or edit screen.
Refresh Time	Displays the time, in seconds, between refreshes of the DHCPv6 address pool.
SIP Domain Name	Displays the domain name associated with the *Session Initiation Protocol* (SIP) server which is used to prioritize voice and video traffic on a network. SIP is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. A SIP system has several components (user agents, proxy servers, redirect servers, and registrars). User agents can contain SIP clients; proxy servers always contain SIP clients.
SIP Servers	Displays the IPv6 formatted address of the SIP server associated with the DHCP pool.

5 Select **Add** to create a new DHCPv6 pool configuration or **Edit** to modify the policy's properties of a selected DHCPv6 pool. **Delete** obsolete policies as warranted.

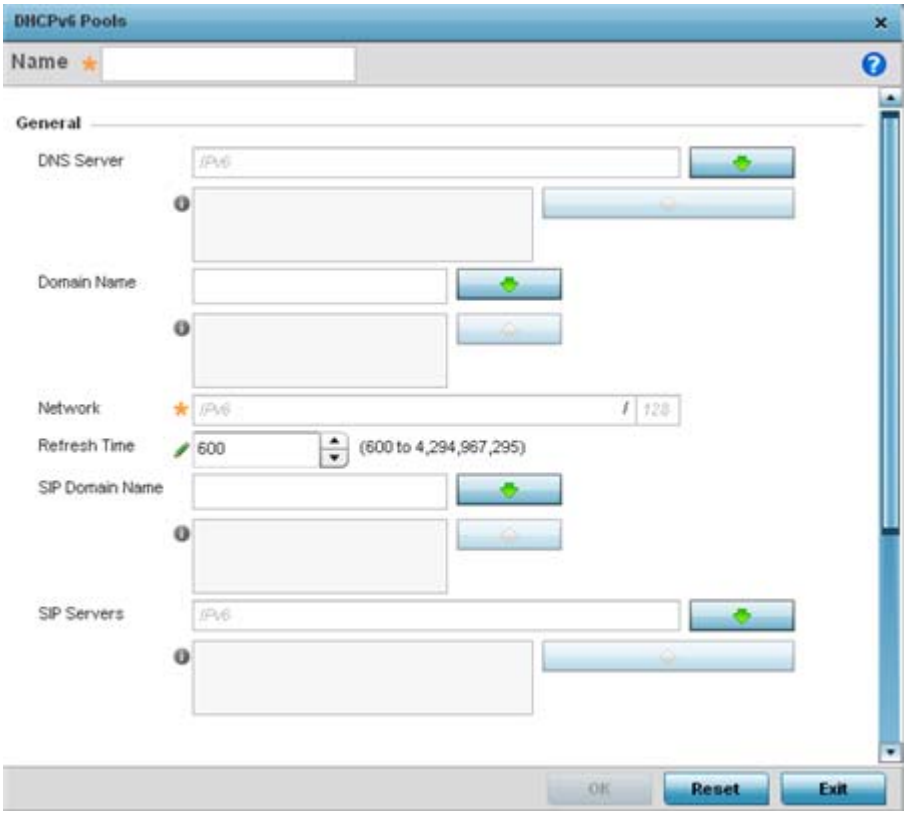


Figure 11-31 *DHCP Server Policy - DHCPv6 Pool - Add/Edit screen*

6 Set the following **General** DHCPv6 pool parameters:

Name	Provide as administrator assigned name for the IPv6 pool resource from which IPv6 formatted addresses can be issued to DHCPv6 client requests. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
DNS Server	Enter the IPv6 formatted address of the DNS server utilized by the DHCP pool.
Domain Name	Enter the hostname or hostnames of the domain(s) utilized with the DHCP pool. A hostname cannot contain an underscore.
Network	Enter the IPv6 formatted address and mask associated with the DHCPv6 pool.
Refresh Time	Use the spinner control to set the time, in seconds, between refreshes of the DHCPv6 address pool. The refresh time can be set from 600 - 4,294,967,295 seconds.
SIP Domain Name	Configure the domain name or domain names associated with the *Session Initiation Protocol* (SIP) servers used to prioritize voice and video traffic on a network. SIP is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. A SIP system has several components (user agents, proxy servers, redirect servers, and registrars). User agents can contain SIP clients; proxy servers always contain SIP clients.
SIP Servers	Configure the IPv6 formatted address or addresses of the SIP servers associated with the DHCP pool.

7 If using DHCPv6 options in the pool, set the following within the **DHCPv6 Options Value** table

Name	Use the drop-down menu to select an existing DHCP option name from the existing options configured in DHCPv6 Options. If no suitable option is available click the create button to define a new option.
Value	Enter or modify the numeric ID setting for the selected DHCP option.

8 Click **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

11.6 Setting the RADIUS Configuration

Services

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software enabling remote access servers to authenticate users and authorize their access. RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients send authentication requests to the local RADIUS server containing user authentication and network service access information.

RADIUS enables centralized management of authentication data (usernames and passwords). When a client attempts to associate to the RADIUS supported controller or service platform, authentication requests are sent to the RADIUS server. Authentication and encryption takes place through the use of a shared secret password (not transmitted over the network).

The local RADIUS server stores the user database locally, and can optionally use a remote user database. It ensures higher accounting performance. It allows the configuration of multiple users, and assign policies for the group authorization.

The local enforcement of user-based policies is configurable. User policies include dynamic VLAN assignment and access restrictions based on time of day. A certificate is required for EAP TTLS,PEAP and TLS RADIUS authentication (configured with the RADIUS service).

Dynamic VLAN assignment is achieved based on the RADIUS server response. A user who associates to WLAN1 (mapped to VLAN1) can be assigned a different VLAN after authentication with the RADIUS server. This dynamic VLAN assignment overrides the WLAN's VLAN ID to which the user associates.

To view RADIUS configurations:

1 Select **Configuration** tab from the main menu.

2 Select the **Services** tab from the **Configuration** menu.

The upper, left-hand side pane of the User interface displays the **RADIUS** option. The **RADIUS Group** screen displays (by default).

For information on creating the groups, user pools and server policies needed to validate user credentials against a server policy configuration, refer to the following:

- *Creating RADIUS Groups*
- *Defining User Pools*
- *Configuring RADIUS Server Policies*
- *RADIUS Deployment Considerations*

11.6.1 Creating RADIUS Groups

Setting the RADIUS Configuration

The RADIUS server allows the configuration of user groups with common user policies. User group names and associated users are stored in a local database. The user ID in the received access request is mapped to the specified group for authentication. RADIUS groups allows the enforcement of the following policies managing user access.

- Assign a VLAN to the user upon successful authentication
- Define a start and end of time in (HH:MM) when the user is allowed to authenticate
- Define the list of SSIDs to which a user belonging to this group is allowed to associate
- Define the days of the week the user is allowed to login
- Rate limit traffic

To access RADIUS Groups menu:

1 Select the **Configuration** tab from the main menu.

2 Select the **Services** tab from the **Configuration** menu.

3 Select **RADIUS > Groups** from the **Configuration > Services** menu.
The browser displays a list of the existing groups.

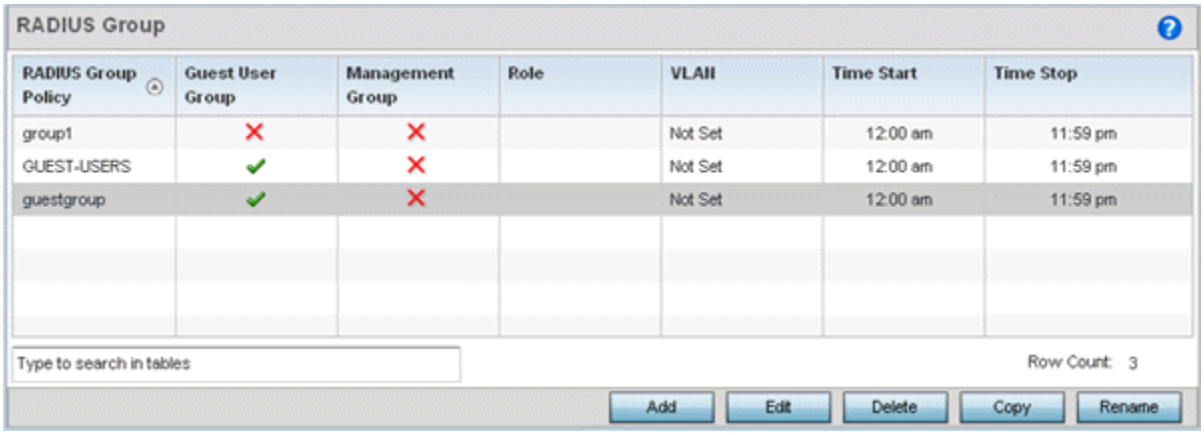


Figure 11-32 *RADIUS Group screen*

4 Select a group from the **Group Browser** to view the following read-only information for existing groups:

RADIUS Group Policy	Displays the group name or identifier assigned to each listed group when it was created. The name cannot exceed 32 characters or be modified as part of the group edit process.
Guest User Group	Specifies whether a user group only has guest access and temporary permissions to the local RADIUS server. The terms of the guest access can be set uniquely for each group. A red “X” designates the group as having permanent access to the local RADIUS server. Guest user groups cannot be made management groups with unique access and role permissions.
Management Group	A green checkmark designates this RADIUS user group as a management group. Management groups can be assigned unique access and role permissions.

Role	If a group is listed as a management group, it may also have a unique role assigned. Available roles include: *monitor* - Read-only access. *helpdesk* - Helpdesk/support access *network-admin* - Wired and wireless access *security-admin* - Grants full read/write access *system-admin* - System administrator access
VLAN	Displays the groups's VLAN ID. The VLAN ID is representative of the shared SSID each group member (user) employs to interoperate within the network (once authenticated by the local RADIUS server).
Time Start	Specifies the time users within each listed group can access local RADIUS resources.
Time Stop	Specifies the time users within each listed group lose access to local RADIUS resources.

5 To modify the settings of an existing group, select the group and click the **Edit** button.To delete an obsolete group, select the group and click the **Delete** button. Optionally **Rename** or **Copy** group configurations as needed.

11.6.1.1 Creating RADIUS Groups

To create a RADIUS group:

1 Select the **Configuration** tab from the main menu.

2 Select the **Services** tab from the **Configuration** menu.

3 Select **RADIUS > Groups** from the **Configuration > Services** menu.

4 Click the **Add** to create a new RADIUS group, **Edit** to modify the configuration of an existing group or **Delete** to permanently remove a selected group.

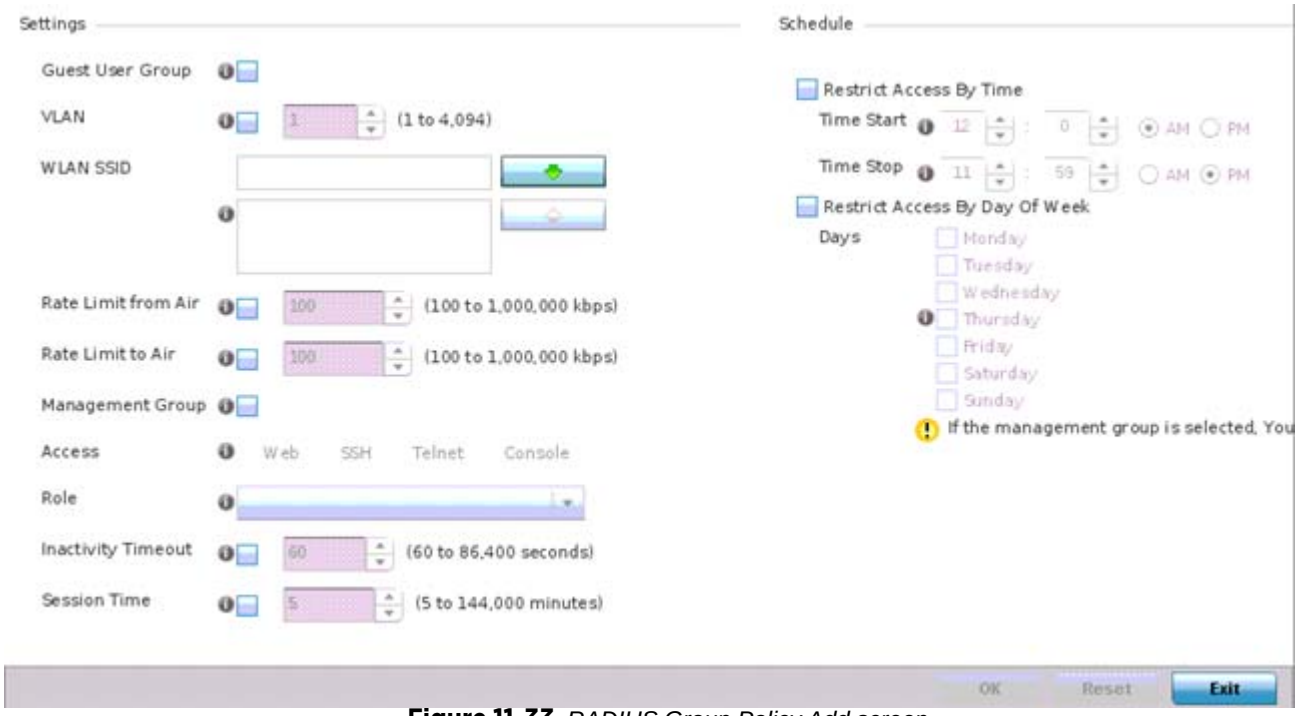


Figure 11-33 *RADIUS Group Policy Add screen*

5 Define the following **Settings** to define the user group configuration:

RADIUS Group Policy	If creating a new RADIUS group, assign it a name to help differentiate it from others with similar configurations. The name cannot exceed 32 characters or be modified as part of a RADIUS group edit process.
Guest User Group	Select this option to assign only guest access and temporary permissions to the local RADIUS server. Guest user groups cannot be made management groups with unique access and role permissions.
VLAN	Select this option to assign a specific VLAN to this RADIUS user group. Ensure Dynamic VLAN assignment (single VLAN) is enabled for the WLAN in order for the VLAN assignment to work properly.
WLAN SSID	Assign a list of SSIDs users within this RADIUS group are allowed to associate with. An SSID cannot exceed 32 characters. Assign WLAN SSIDs representative of the configurations a guest user will need to access. The parameter is not available if this RADIUS group is a management group.
Rate Limit from Air	Select the checkbox to set the rate limit for clients within the RADIUS group. Use the spinner to set value from 100-1,000,000 kbps. Setting a value of 0 disables rate limiting.
Rate Limit to Air	Select the checkbox to set the rate limit from clients within the RADIUS group. Use the spinner to set value from 100-1,000,000 kbps. Setting a value of 0 disables rate limiting.
Management Group	Select this option to designate this RADIUS group as a management group. This feature is disabled by default. If set as management group, assign member roles (System-Admin, Help Desk etc.) using the *Role* drop-down menu.
Access	Select those interfaces (*Web*, *SSH*, *Telnet* or *Console*) to apply to the RADIUS Group Policy. The conditions defined within the policy are applied to authentication requests on these interfaces only.
Role	If a group is listed as a management group, it may also have a unique role assigned. Available roles include: *monitor* - Read-only access. *helpdesk* - Helpdesk/support access. *network-admin* - Wired and wireless access. *security-admin* - Grants full read/write access. *system-admin* - System administrator access.
Inactivity Timeout	Enable this option to set an inactivity timeout from 60 - 86,400 seconds. If a frame is not received from a client within the set time, the current session is terminated.
Session Time	Enable this option to set a client session time from 5 - 144,000 minutes. This is the session time a client is granted upon successful authentication. Upon experation, the RADIUS session is terminated.

6 Set the **Schedule** to configure access times and dates.

Time Start	To schedule an access time, select the *Restrict Access by Time* option. Use the spinner control to set the time (in HH:MM format) RADIUS group members are allowed access the RADIUS server resources. Select either the *AM* or *PM* radio button to set the time as morning or evening.
Time Stop	Use the spinner control to set the time (in HH:MM format) RADIUS group members are denied access to RADIUS server resources. Select either the *AM* or *PM* radio button to set the time as morning or evening. If already logged in, the RADIUS group user is deauthenticated from the WLAN.

Days	Optionally select the *Restrict Access by Day Of Week* option, and select the *Days* RADIUS group members can access RADIUS resources. This is an additional means of refining the access permissions of RADIUS group members.

7 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

11.6.2 Defining User Pools

Setting the RADIUS Configuration

A user pool defines policies for individual user access to local RADIUS resources. User or pools provide a convenient means of providing RADIUS resources based on the pool's unique permissions (either temporary or permanent). A pool can contain a single user or group of users.

To configure a RADIUS user pool and unique user IDs:

1 Select **Configuration** from the main menu.

2 Select **Services** tab from the Configuration screen.

3 Select **RADIUS > User Pools** from the **Configuration > Services** menu.

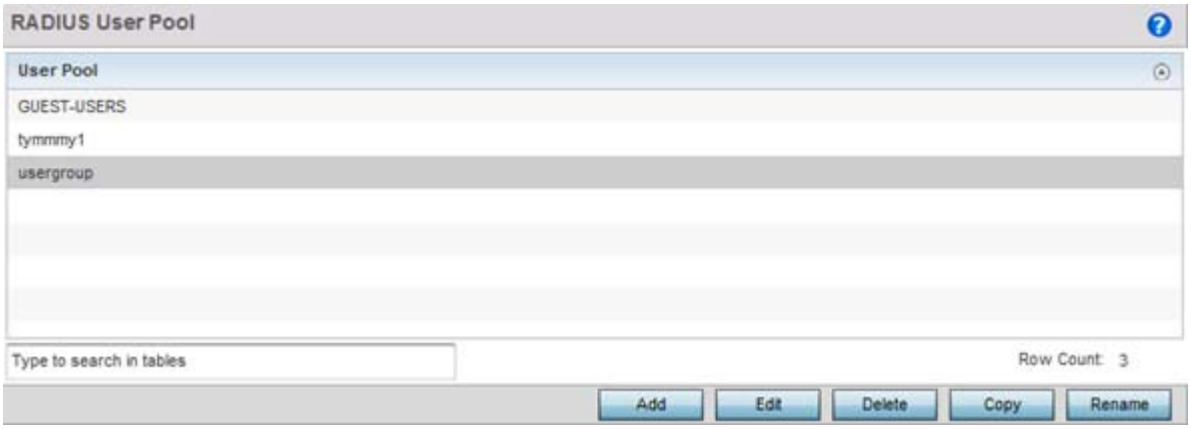


Figure 11-34 *RADIUS User Pool screen*

The **RADIUS User Pool** screen lists the default pool along with any other admin created user pool.

4 Select **Add** to create a new user pool, **Edit** to modify the configuration of an existing pool or **Delete** to remove a selected pool.

5 If creating a new pool, assign it a name up to 32 characters and select **Continue**. The name should be representative of the users comprising the pool and/or the temporary or permanent access privileges assigned.

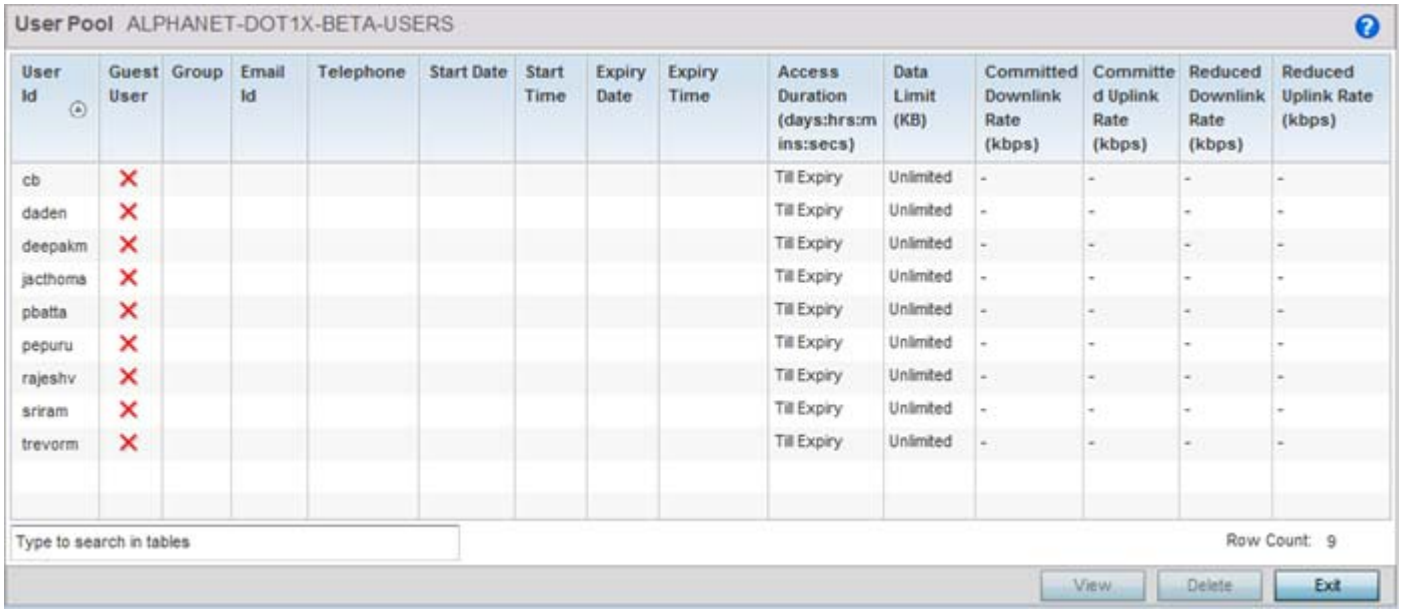


Figure 11-35 *RADIUS User Pool Add screen*

6 Refer to the following **User Pool** configurations to discern when specific user IDs have access to RADIUS resources:

User Id	Displays the unique string identifying this user. This is the ID assigned to the user when created and cannot be modified with the rest of the configuration.
Guest User	Specifies (with a green check) the user has guest access and temporary permissions to the local RADIUS server. The terms of the guest access can be set uniquely for each user. A red "X" designates the user as having permanent access to the local RADIUS server.
Group	Displays the group name each configured user ID is a member.
Email ID	Displays the Email address (in 64 characters or less) of the client user (user ID) requesting authentication validation to the controller or service platform using this user pool.
Telephone	Lists the 12 character maximum telephone number of the client user (user ID) requesting authentication validation to the controller or service platform using this user pool.
Start Date	Lists the month, day and year the listed user ID can access local RADIUS server resources.
Start Time	Lists the time the listed user ID can access local RADIUS server resources. The time is only relevant to the range defined by the start and expiry date.
Expiry Date	Lists the month, day and year the listed user Id can no longer access (expires) local RADIUS server resources.
Expiry Time	Displays the time the listed user loses access to RADIUS server resources. The time is only relevant to the range defined by the start and expiry date.
Access Duration (days:hrs:mins:secs)	Displays the amount of time a user is allowed access when time based access privilege are applied. The duration cannot exceed 365 days.

Data Limit (KB)	Lists the total amount of bandwidth (in KiloBytes) consumable by each guest user.
Committed Downlink Rate (kbps)	Displays the download speed (in KiloBytes) allocated to the guest user. When bandwidth is available, the user can download data at the specified rate. If a guest user has a bandwidth based policy and exceeds the specified Data Limit, their speed is throttled to the Reduced Downlink Rate.
Committed Uplink Rate (kbps)	Displays the upload speed (in KiloBytes) allocated to the guest user. When bandwidth is available, the user can download data at the specified rate. If a guest user has a bandwidth based policy and exceeds the specified Data Limit, their speed is throttled to the Reduced Uplink Rate.
Reduced Downlink Rate (kbps)	Displays the reduced speed the guest utilizes (in KiloBytes) when exceeding their specified data limit, if applicable. If a guest user has a bandwidth based policy and exceeds the specified Data Limit, their speed is throttled to the Reduced Downlink Rate.
Reduced Uplink Rate (kbps)	Displays the reduced speed the guest utilizes (in KiloBytes) when exceeding their specified data limit, if applicable. If a guest user has a bandwidth based policy and exceeds the specified Data Limit, their speed is throttled to the Reduced Uplink Rate.

7 Select the **Add** button to add a new RADIUS user, **Edit** to modify the configuration of an existing user or **Delete** to remove an existing user Id.

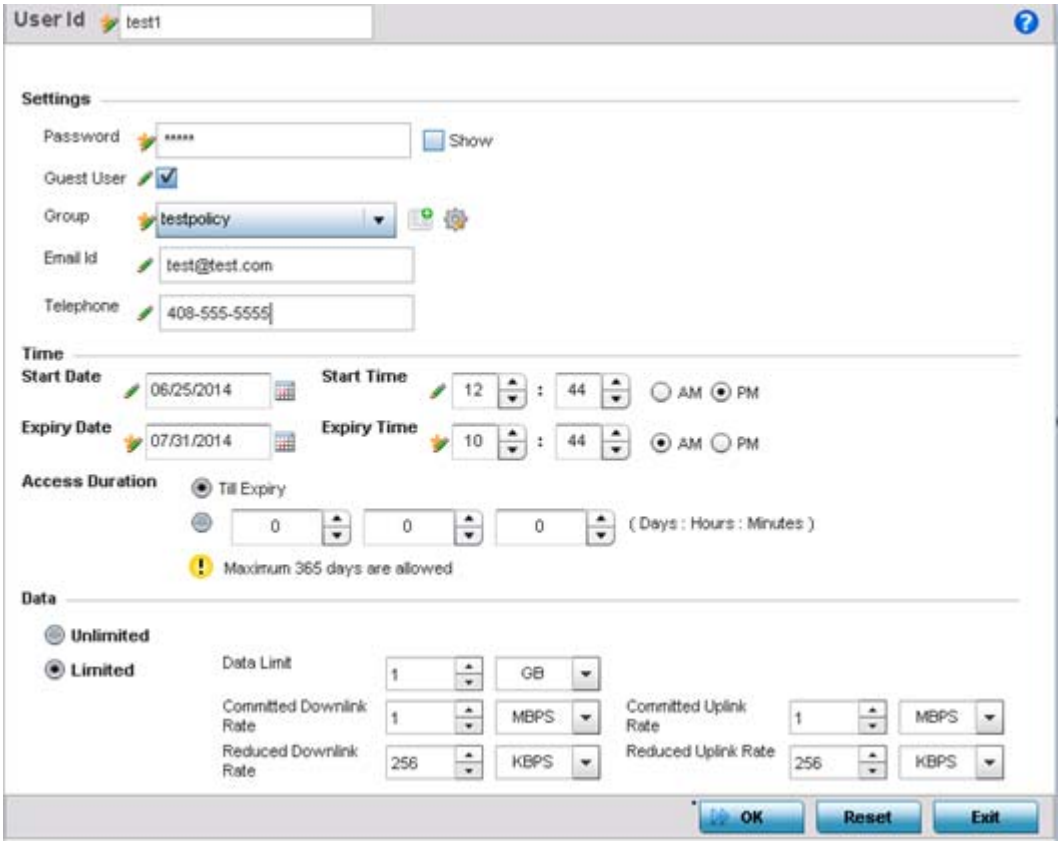


Figure 11-36 *RADIUS User screen*

8 Refer the following **Settings** to create a new user Id with unique access privileges:

User Id	Assign a unique character string identifying this user. The Id cannot exceed 64 characters.
Password	Provide a password unique to this user ID. The password cannot exceed 32 characters. Select the *Show* checkbox to expose the password's actual character string, leaving the option unselected displays the password as a string of asterisks (*).
Guest User	Select the checkbox to designate this user as a guest with temporary access. The guest user must be assigned unique access times to restrict their access.
Group	If the user Id has been defined as a guest, use the *Group* to assign the user a group with temporary access privileges. If the user is defined as a permanent user, select a group from the group list. If there's no groups listed relevant to the user's intended access, select the *Create* link (or icon for guests) and create a new group configuration suitable for the user Id's membership.
Email ID	Enter the Email address (in 64 characters or less) of the client user (user ID) requesting authentication validation to the controller or service platform using this user pool.
Telephone	Provide the 12 character maximum telephone number of the client user (user ID) requesting authentication validation to the controller or service platform using this user pool.

9 Refer the following **Time** settings to define time based guest user access privileges:

Start Date	Enter a start date, or use the calendar icon to select a starting date for the user's credentials to start working.
Start Time	Enter a start time, or use the spinner controls to select a starting time for the user's credentials to start working. Use the *AM* and *PM* buttons to apply a morning or afternoon/evening designation.
Expiry Date	Enter an end date, or use the calendar icon to define an expiration date for the user's credentials. Selecting this option enables the *Til Expiry* radio button.
Expiry Time	If using the *Til Expiry* option, enter an end time, or use the spinner controls to select an ending time for the user's credentials to expire. Use the *AM* and *PM* buttons to apply a morning or afternoon/evening designation.
Access Duration	Specify the time a user can access the system when time based access privilege are applied. Select *Til Expiry* to allow user access until their configured expiry date and time are met. To limit the time a user can access the captive portal during their configured time period, specify the *Days, Minutes* and *Seconds* the user is allowed access. The Access Duration cannot exceed 365 days.

10 To allow the guest user unlimited data usage select **Unlimited**. To limit bandwidth, select **Limited** and refer to the **Data** field to create bandwidth based access privileges:

Data Limit	Use the spinner control to specify the maximum bandwidth consumable by the guest user. Once a value is configured, select the measurement as either *GB* (Gigabytes) or *MB* (Megabytes).

Committed Downlink Rate	Use the spinner control to specify the download speed dedicated to the guest user. When bandwidth is available, the user can download data at the specified rate. Once a value is configured, select the measurement as either *MBPS* (Megabytes per second) or *KBPS* (Kilobytes per second). If a guest user has a bandwidth based policy and exceeds the specified Data Limit, their speed is throttled to the defined *Reduced Downlink Rate*.
Reduced Downlink Rate	Use the spinner control to specify a reduced speed for guest operation when they've exceeded their specified data limit, if applicable. If a guest user has a bandwidth based policy and exceeds the specified Data Limit, their speed is throttled to the *Reduced Downlink Rate*. Once a value is configured, select the measurement as either *MBPS* (Megabytes per second) or *KBPS* (Kilobytes per second).
Committed Uplink Rate	Use the spinner control to specify the upload speed dedicated to the guest user. When bandwidth is available, the user is able to upload data at the specified rate. Once a value is configured, select the measurement as either *MBPS* (Megabytes per second) or *KBPS* (Kilobytes per second). If a guest user has a bandwidth based policy and exceeds the specified Data Limit, their speed is throttled to the *Reduced Uplink Rate.*
Reduced Uplink Rate	Use the spinner control to specify a reduced speed for guest operation when they've exceed their specified data limit, if applicable. If a guest user has a bandwidth based policy and exceeds the specified Data Limit, their speed is throttled to the *Reduced Uplink Rate*. Once a value is configured, select the measurement as either *MBPS* (Megabytes per second) or *KBPS* (Kilobytes per second).

11 Select **OK** to save the user Id's group membership configuration. Select **Reset** to revert to the last saved configuration.

11.6.3 Configuring RADIUS Server Policies

- *Setting the RADIUS Configuration*

A RADIUS server policy is a unique authentication and authorization configuration for receiving user connection requests, authenticating users and returning the configuration information necessary to deliver service to the requesting client and user. The client is the entity with authentication information requiring validation. The local RADIUS server has access to a database of authentication information used to validate the client's authentication request.

The RADIUS server ensures the information is correct using an authentication scheme like *PAP, CHAP* or *EAP*. The user's proof of identification is verified, along with, optionally, other information. A RADIUS server policy can also use an external LDAP resource to verify user credentials.

To review RADIUS existing server policies, manage the creation of new policies of manage the modification of existing policies:

1 Select **Configuration** from the main menu.

2 Select **Services** tab from the Configuration screen.

3 Select **RADIUS > Server Policy** from the **Configuration > Services** menu.

The **Server Policy Browser** lists existing server policies by group or randomly. A policy can be selected and modified from the browser.

4 Refer to the RADIUS Server screen to review high-level server policy configuration data.

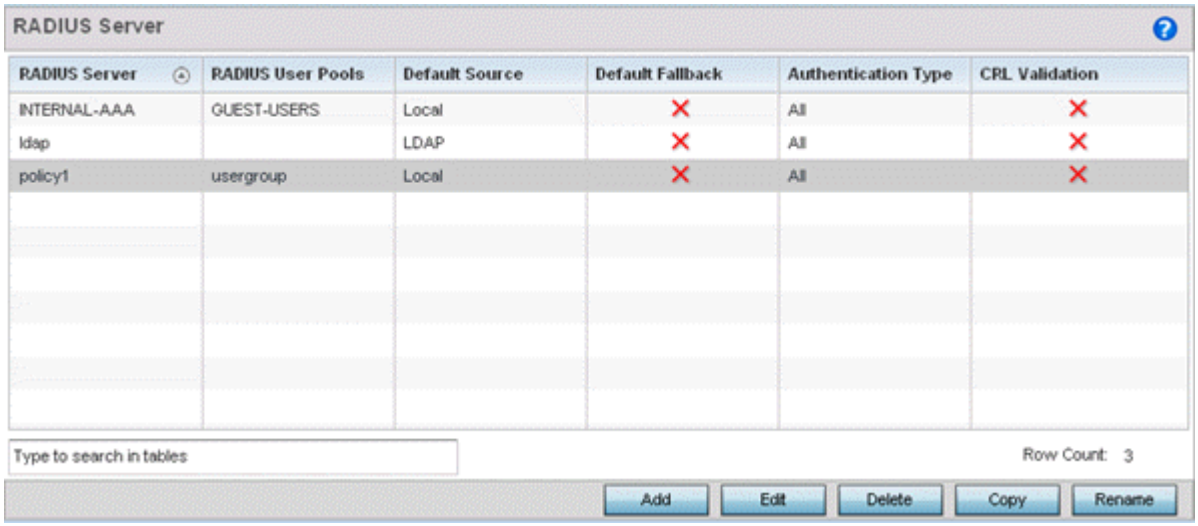


Figure 11-37 *RADIUS Server Policy screen*

5 Select a server policy from the **Server Policy Browser**. The user has the option of adding a new policy, modifying an existing one, or deleting a policy.

RADIUS Server Policy	Lists the administrator assigned policy name defined upon creation of the server policy.
RADIUS User Pools	Lists the user pools assigned to this server policy. These are the client users who an administrator has assigned to each listed group and who must adhere to its network access requirements before granted access to controller or service platform resources.
Default Source	Displays the RADIUS resource designated for user authentication requests. Options include *Local* (resident controller or service platform RADIUS server resources) or *LDAP* (designated remote LDAP resource).
Default Fallback	States whether a fallback is enabled providing a revert back to local RADIUS resources if the designated external LDAP resource were to fail or become unavailable. A green checkmark indicates Default Fallback is enabled. A red “X” indicates it’s disabled. Default Fallback is disabled by default.

Authentication Type	Lists the local EAP authentication scheme used with this policy. The following EAP authentication types are supported by the local RADIUS and remote LDAP servers: *All* – Enables both TTLS and PEAP. *TLS* - Uses TLS as the EAP type. *TTLS and MD5* - The EAP type is TTLS with default authentication using MD5. *TTLS and PAP* - The EAP type is TTLS with default authentication using PAP. *TTLS and MSCHAPv2* - The EAP type is TTLS with default authentication using MSCHAPv2. *PEAP and GTC* - The EAP type is PEAP with default authentication using GTC. *PEAP and MSCHAPv2* - The EAP type is PEAP with default authentication using MSCHAPv2. However, when user credentials are stored on an LDAP server, the RADIUS server cannot conduct PEAP-MSCHAPv2 authentication on its own, as it is not aware of the password. Use LDAP agent settings to locally authenticate the user. Additionally, an authentication utility (such as Samba) must be used to authenticate the user. Samba is an open source software used to share services between Windows and Linux machine.
CRL Validation	Specifies whether a *Certificate Revocation List* (CRL) check is made. A green checkmark indicates CRL validation is enabled. A red "X" indicates it's disabled. A CRL is a list of revoked certificates issued and subsequently revoked by a *Certification Authority* (CA). Certificates can be revoked for a number of reasons including failure or compromise of a device using a certificate, a compromise of a certificate key pair or errors within an issued certificate. The mechanism used for certificate revocation depends on the CA.

6 Select the **Copy** button to copy the settings of a selected (existing) RADIUS server configuration to a new or existing policy.

When selected, a small dialogue displays prompting the administrator to enter the name of policy to copy the existing policy settings to. Enter the name of the RADIUS server policy receiving the existing server policy settings within the **Copy To** field and select the **Copy** button to initiate the configuration copy operation. This feature streamlines the creation of RADIUS server policies using the attributes of existing server policies.

7 An existing RADIUS server policy can be renamed at any time by selecting it from amongst the listed policies and selecting the **Rename** button.

This allows an administrator to simply rename a server policy without having to create (or edit) a new policy with all the same settings.

8 Select either **Add** to create a new RADIUS server policy, **Edit** to modify an existing policy or **Delete** to permanently remove a policy.

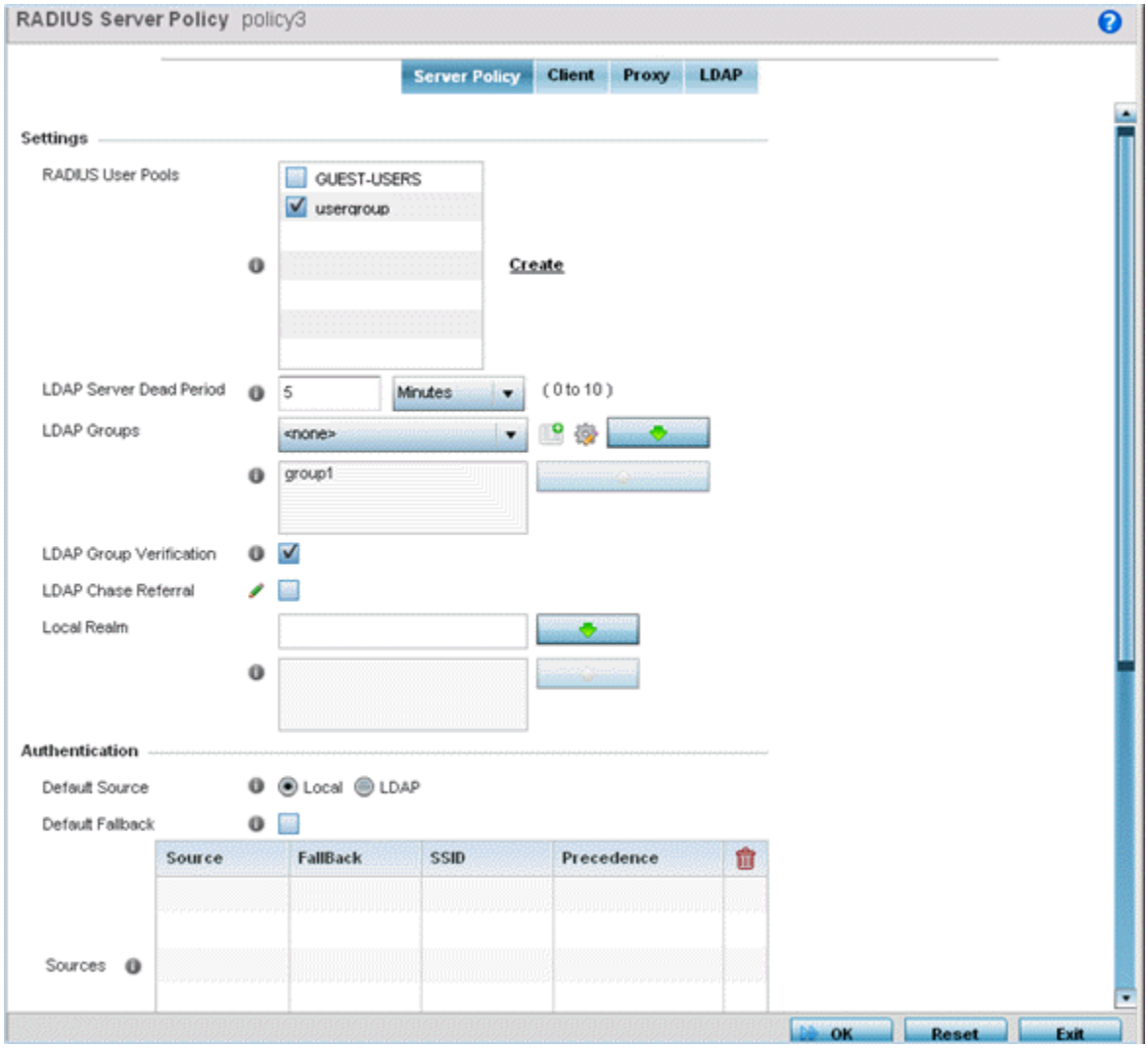


Figure 11-38 *RADIUS Server Policy screen - Server Policy tab*

The **Server Policy** tab displays by default.

9 If creating a new policy, assign it a **RADIUS Server Policy** name up to 32 characters.

10 Configure the following **Settings** required in the creation or modification of the server policy:

RADIUS User Pools	Select the user pools (groups of existing client users) to apply to this server policy. If there is not an existing user pool configuration suitable for the deployment, select the Create link and define a new configuration.
LDAP Server Dead Period	Set an interval in either *Seconds* (0 - 600) or *Minutes* (0 - 10) for planned LDAP server inactivity. A *dead period* is only implemented when additional LDAP servers are configured and available for LDAP failover. The default setting is 5 minutes.
LDAP Groups	Use the drop-down menu to select LDAP groups to apply the server policy configuration. Select the *Create* or *Edit* icons to either create a new group or modify an existing group. Use the arrow icons to add and remove groups as required.
LDAP Group Verification	Select the checkbox to set the LDAP group search configuration.

LDAP Chase Referral	Select this option to enable the chasing of referrals from an external LDAP server resource. An LDAP referral is a controller or service platform's way of indicating to a client it does not hold the section of the directory tree where a requested content object resides. The *referral* is the controller or service platform's direction to the client a different location is more likely to hold the object, which the client uses as the basis for a DNS search for a domain controller. Ideally, referrals always reference a domain controller that indeed holds the object. However, it is possible for the domain controller to generate another referral, although it usually does not take long to discover the object does not exist and inform the client. This feature is disabled by default.
Local Realm	Define the LDAP performing authentication using information from an LDAP server. User information includes user name, password, and groups to which the user belongs.

11 Set the following **Authentication** parameters to define server policy authorization settings.

Default Source	Select the RADIUS resource for user authentication with this server policy. Options include *Local* for the local user database or *LDAP* for a remote LDAP resource. The default setting is Local.
Default Fallback	Define whether a fallback is enabled providing a revert back to local RADIUS resources if the designated external LDAP resource were to fail or become unavailable. The default fallback feature is disabled by default.
Authentication Type	Use the drop-down menu to select the EAP authentication scheme used with this policy. The following EAP authentication types are supported by the local RADIUS and remote LDAP servers: *All* – Enables all authentication schemes. *TLS* - Uses TLS as the EAP type *TTLS and MD5* - The EAP type is TTLS with default authentication using MD5. *TTLS and PAP* - The EAP type is TTLS with default authentication using PAP. *TTLS and MSCHAPv2* - The EAP type is TTLS with default authentication using MSCHAPv2. *PEAP and GTC* - The EAP type is PEAP with default authentication using GTC. *PEAP and MSCHAPv2* - The EAP type is PEAP with default authentication using MSCHAPv2. However, when user credentials are stored on an LDAP server, the RADIUS server cannot conduct PEAP-MSCHAPv2 authentication on its own, as it is not aware of the password. Use LDAP agent settings to locally authenticate the user. Additionally, an authentication utility (such as Samba) must be used to authenticate the user. Samba is an open source software used to share services between Windows and Linux machine.
Do Not Verify Username	Select this option to use certificate expiration as matching criteria, as opposed to the hostname. This setting is disabled by default.

Enable EAP Termination	Select this option to enable EAP termination with this RADIUS server policy. This setting is disabled by default.
Enable CRL Validation	Select this option to enable a *Certificate Revocation List* (CRL) check. Certificates can be checked and revoked for a number of reasons including failure or compromise of a device using a certificate, a compromise of a certificate key pair or errors within an issued certificate. This option is disabled by default.
Bypass CRL Check	Select the option to bypass a *certificate revocation list* (CRL) check when a CRL is not detected. This setting is enabled by default. A CRL is a list of certificates that have been revoked or are no longer valid.
Allow Expired URL	Select this option to allow the use of an expired CRL. This option is enabled by default.

12 Select **+ Add Row** within the Authentication field to define the following **Authentication Data Source** rules for the RADIUS server policy:

Precedence	Use the spinner control to set the numeric precedence (priority) for this authentication data source rule. Rules with the lowest precedence receive the highest priority. Set the value between 1 - 5000. This value is mandatory.
SSID	Enter or modify the SSID associated with the authentication data source rule. The maximum number of characters is 32. Do not use any of these characters (< > | " & \ ? ,).
Source	Use the drop-down menu to define the RADIUS data source for this authentication data source rule as Local or LDAP.
Fallback	Select this option to fallback to the Local resource for RADIUS data authentication from LDAP for this authentication data source rule.

13 If using LDAP as the default authentication source, select **+ Add Row** to set **LDAP Agent** settings.

When a user's credentials are stored on an external LDAP server, the controller or service platform's local RADIUS server cannot successfully conduct PEAP-MSCHAPv2 authentication, since it is not aware of the user's credentials maintained on the external LDAP server resource. Therefore, up to two LDAP agents can be provided locally so remote LDAP authentication can be successfully accomplished on the remote LDAP resource (using credentials maintained locally).

Username	Enter a 63 character maximum username for the LDAP server's domain administrator. This is the username defined on the LDAP server for RADIUS authentication requests.
Password	Enter and confirm the 32 character maximum password (for the username provided above). The successful verification of the password maintained on the controller or service platform enables PEAP-MSCHAPv2 authentication using the remote LDAP server resource.
Retry Timeout	Set the number of *Seconds* (60 - 300) or *Minutes* (1 - 5) to wait between LDAP server access requests when attempting to join the remote LDAP server's domain. The default settings is one minute.
Redundancy	Define the *Primary* or *Secondary* LDAP agent configuration used to connect to the LDAP server domain.
Domain Name	Enter the name of the domain (from 1 - 127 characters) to which the remote LDAP server resource belongs.

14 Set the following **Session Resumption/Fast Reauthentication** settings to define how server policy sessions are re-established once terminated and require cached data to resume:

Enable Session Resumption	Select the checkbox to control volume and the duration cached data is maintained by the server policy upon the termination of a server policy session. The availability and quick retrieval of the cached data speeds up session resumption. This setting is disabled by default.
Cached Entry Lifetime	If enabling session resumption, use the spinner control to set the lifetime (1 - 24 hours) cached data is maintained by the RADIUS server policy. The default setting is 1 hour.
Maximum Cache Entries	If enabling session resumption, use the spinner control to define the maximum number of entries maintained in cache for this RADIUS server policy. The default setting is 128.

15 Select **OK** to save the settings to the server policy configuration. Select **Reset** to revert to the last saved configuration.

Refer to the following to add RADIUS clients, proxy server configurations, LDAP server configurations and review deployment considerations impacting the effectiveness of the RADIUS supported deployment:

- *Configuring RADIUS Clients*
- *Configuring a RADIUS Proxy*
- *Configuring an LDAP Server Configuration*

11.6.3.1 Configuring RADIUS Clients

Configuring RADIUS Server Policies

A RADIUS client is a mechanism to communicate with a central server to authenticate users and authorize access to the network.

The client and server share a *secret* (a password). That shared secret, followed by the request authenticator, is put through a MD5 hash to create a 16 octet value which is XORed with the password entered by the user. If the user password is greater than 16 octets, additional MD5 calculations are performed, using the previous ciphertext instead of the request authenticator. The server receives a RADIUS *access request* packet and verifies the server possesses a shared secret for the client. If the server does not possess a shared secret for the client, the request is dropped. If the client received a verified *access accept* packet, the username and password are considered correct, and the user is authenticated. If the client receives a verified *access reject* message, the username and password are considered to be incorrect, and the user is not authenticated.

To define a RADIUS client configuration:

1 Select the **Client** tab from the RADIUS Server Policy screen.

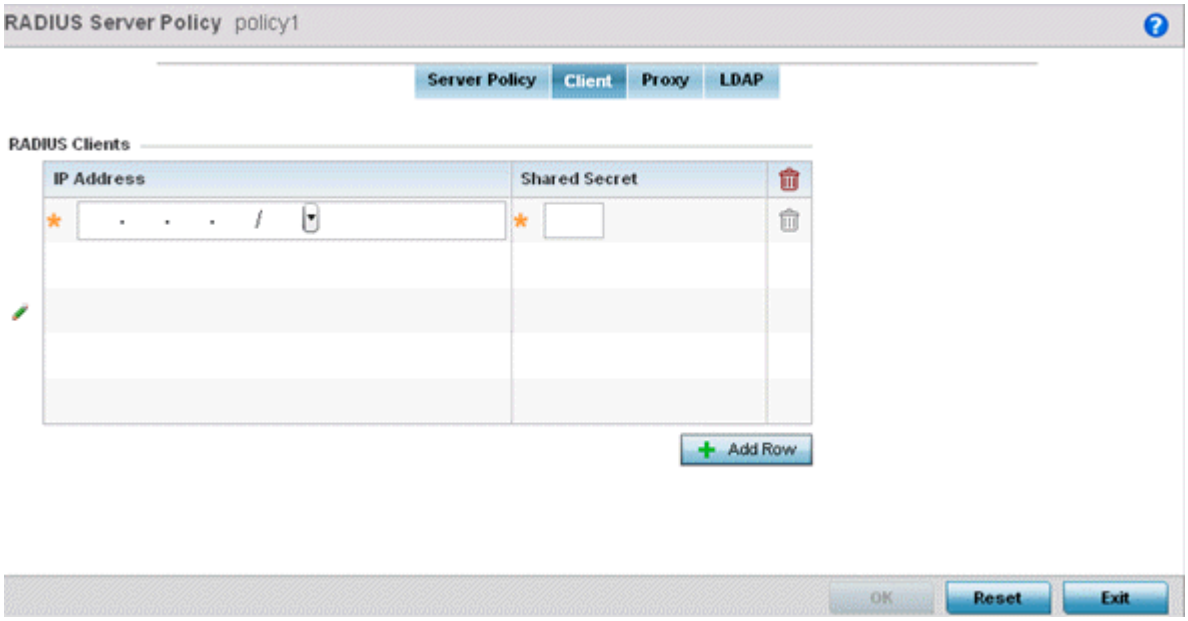


Figure 11-39 *RADIUS Server Policy screen - Client tab*

2 Select the **+ Add Row** button to add a table entry for a new client's IP address, mask and shared secret. To delete a client entry, select the **Delete** icon on the right-hand side of the table entry.

3 Specify the **IP Address** and mask of the RADIUS client authenticating with the RADIUS server.

4 Specify a **Shared Secret** for authenticating the RADIUS client.

Shared secrets verify RADIUS messages with RADIUS enabled device configured with the same shared secret. Select the **Show** checkbox to expose the shared secret's actual character string, leaving the option unselected displays the shared secret as a string of asterisks (*).

5 Click **OK** button to save the server policy's client configuration. Click the **Reset** button to revert to the last saved configuration.

11.6.3.2 Configuring a RADIUS Proxy

Configuring RADIUS Server Policies

A user's access request is sent to a proxy server if it cannot be authenticated by local RADIUS resources. The proxy server checks the information in the user access request and either accepts or rejects the request. If the proxy server accepts the request, it returns configuration information specifying the type of connection service required to authenticate the user.

The RADIUS proxy appears to act as a RADIUS server to the NAS, whereas the proxy appears to act as a RADIUS client to the RADIUS server.

When the RADIUS server receives a request for a user name containing a realm, the server references a table of configured realms. If the realm is known, the server proxies the request to the RADIUS server. The behavior of the proxying server is configuration-dependent on most servers. In addition, the proxying server can be configured to add, remove or rewrite requests when they are proxied.

To define a proxy configuration:

1 Select the **Proxy** tab from the RADIUS Server Policy screen.

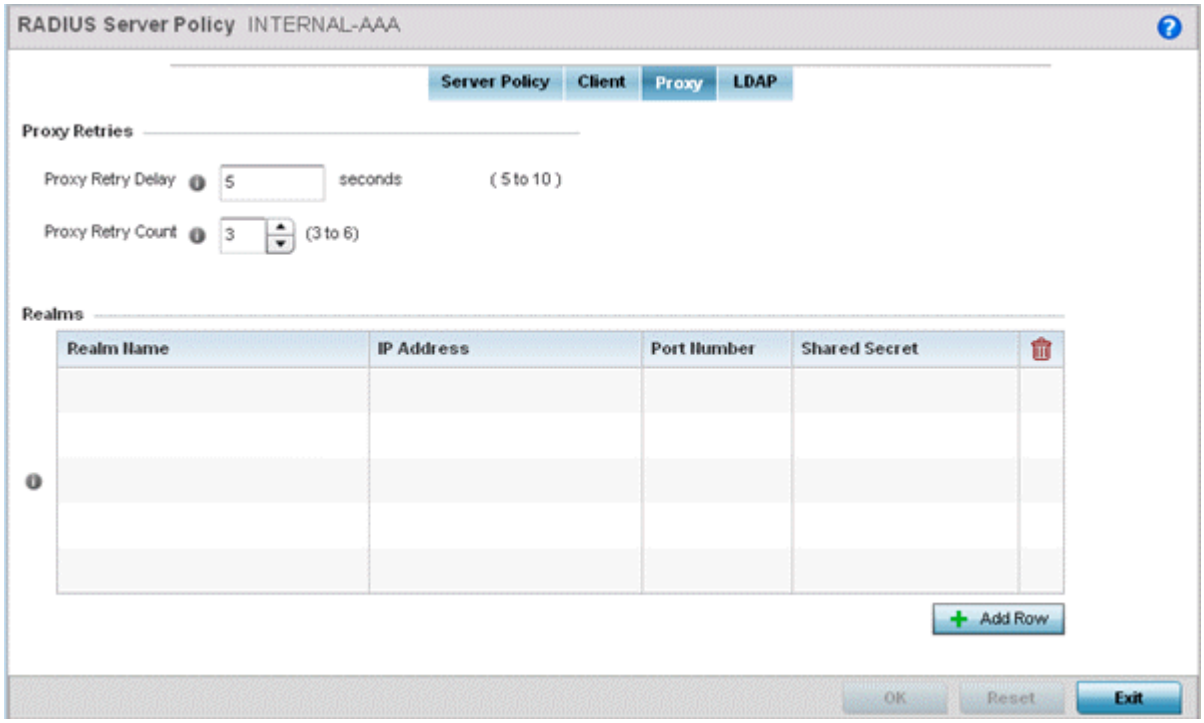


Figure 11-40 *RADIUS Server Policy screen - Proxy tab*

2 Enter the Proxy server retry delay time in the **Proxy Retry Delay** field. Enter a value from 5 -10 seconds. This is the interval the RADIUS server waits before making an additional connection attempt. The default delay interval is 5 seconds.

3 Enter the Proxy server retry count value in the **Proxy Retry Count** field. Set from 3 - 6 to define the number of retries sent to the proxy server before giving up the request. The default retry count is 3 attempts.

4 Select the **+ Add Row** button to add a RADIUS server proxy realm name and network address. To delete a proxy server entry, select the **Delete** icon on the right-hand side of the table entry.

5 Enter the realm name in the **Realm Name** field. The realm name cannot exceed 50 characters. When the RADIUS server receives a request for a user name with a realm, the server references a table of realms. If the realm is known, the server proxies the request to the RADIUS server.

6 Enter the Proxy server IP address in the **IP Address** field. This is the address of server checking the information in the user access request and either accepting or rejecting the request on behalf of the local RADIUS server.

7 Enter the TCP/IP port number for the server that acts as a data source for the proxy server in the **Port Number** field. Use the spinner to select a value between 1024 - 65535. The default port is 1812.

8 Enter the RADIUS client shared secret password in the **Shared Secret** field. This password is for authenticating the RADIUS proxy.

Select the **Show** checkbox to expose the shared secret's actual character string, leaving the option unselected displays the shared secret as a string of asterisks (*).

9 Click the **OK** button to save the changes. Click the **Reset** button to revert to the last saved configuration.

11.6.3.3 Configuring an LDAP Server Configuration

Configuring RADIUS Server Policies

Administrators have the option of using RADIUS server resources to authenticate users against an external LDAP server resource. Using an external LDAP user database allows the centralization of user information and reduces administrative user management overhead making the RADIUS authorization process more secure and efficient.

RADIUS is not just a database. It's a protocol for asking intelligent questions to a user database (like LDAP). LDAP however is just a database of user credentials that can be used optionally with the RADIUS server to free up resources and manage user credentials from a secure remote location. Local RADIUS resources provide the tools to perform user authentication and authorize users based on complex checks and logic. There's no way to perform such complex authorization checks from a LDAP user database alone.

To configure an LDAP server configuration for use with the RADIUS server:

1 Select the **LDAP** tab from the RADIUS Server screen.

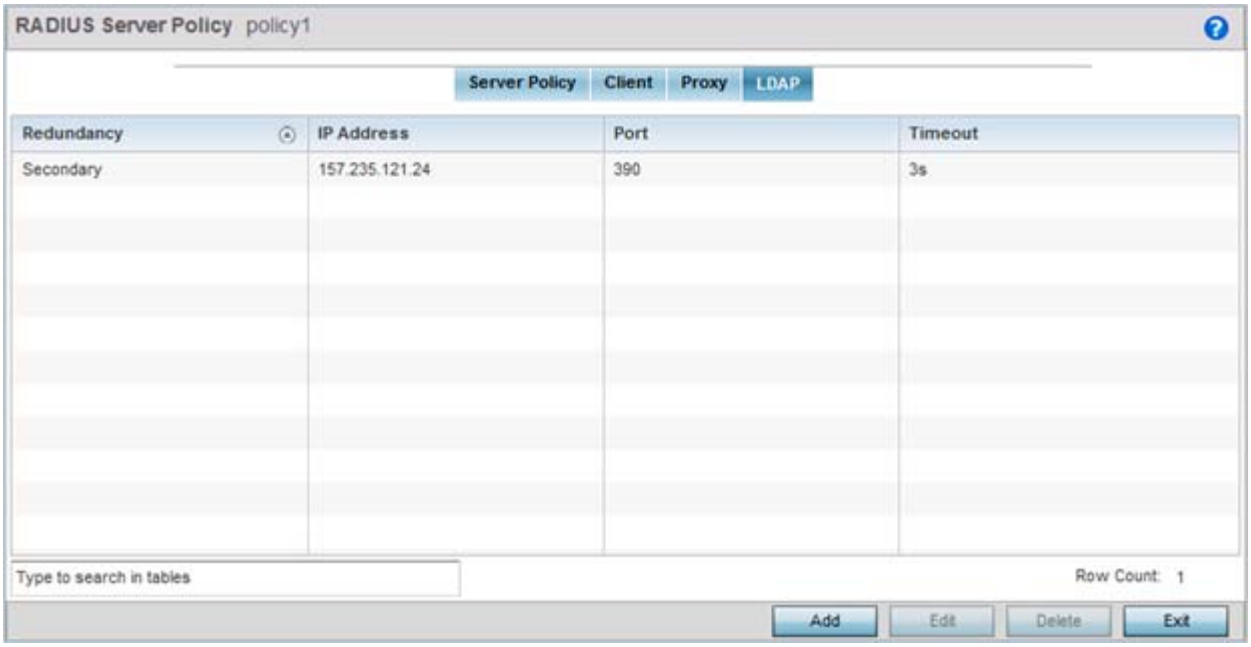


Figure 11-41 *RADIUS Server Policy screen - LDAP tab*

NOTE: If using LDAP for external authentication, PEAP-MSCHAPv2 can only be used if the LDAP server returns the password as plain text. PEAP-MSCHAPv2 is not supported if the LDAP server returns encrypted passwords. This restriction does not apply for Microsoft's Active Directory Server.

2 Refer to the following to determine whether an LDAP server can be used as is, a server configuration requires creation or modification or a configuration requires deletion and permanent removal.

Redundancy	Displays whether the listed LDAP server IP address has been defined as a *primary* or *secondary* server resource. Designating at least one secondary server is a good practice to ensure RADIUS resources are available if a primary server were to become unavailable.
IP Address	Displays the IP address of the external LDAP server acting as the data source for the RADIUS server.

Port	Lists the physical port number used by the RADIUS server to secure a connection with the remote LDAP server resource.
Timeout	Lists the number of seconds (1- 10) this server session waits for a connection before aborting the connection attempt with the listed RADIUS server resource.

3 Click the **Add** button to add a new LDAP server configuration, **Edit** to modify an existing LDAP server configuration or **Delete** to remove a LDAP server from the list of those available.

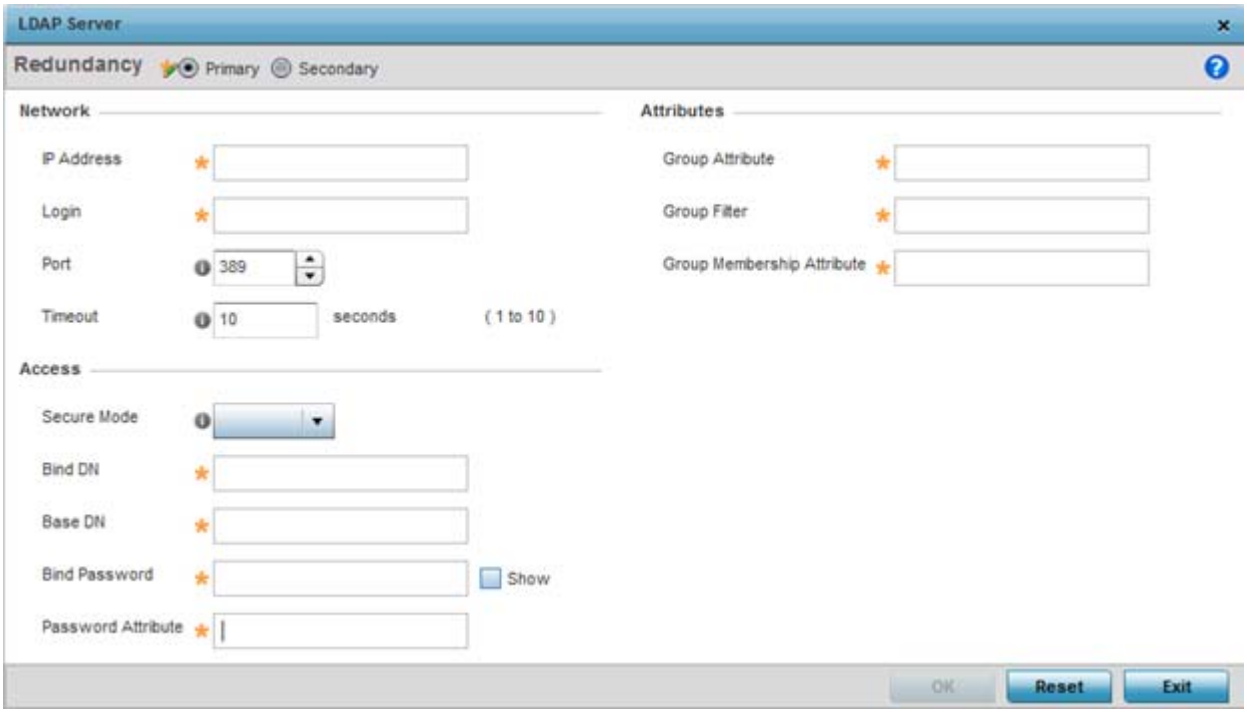


Figure 11-42 *LDAP Server Add screen*

4 Set the following **Network** address information required for the connection to an external LDAP server resource:

Redundancy	Define whether this LDAP server is a *primary* or *secondary* server resource. Primary servers are always queried for connection first. However, designating at least one secondary server is a good practice to ensure RADIUS user information is available if a primary server were to become unavailable.
IP Address	Set the 128 character maximum IP address or FQDN of the external LDAP server acting as the data source for the RADIUS server.
Login	Define a unique login name used for accessing the remote LDAP server resource. Consider using a unique login name for each LDAP server provided to increase the security of the connection to the remote LDAP server.
Port	Use the spinner control to set the physical port number used by the RADIUS server to secure a connection with the remote LDAP server.
Timeout	Set an interval from 1 - 10 seconds the local RADIUS server uses as a wait period for a response from the primary or secondary LDAP server. The default setting is 10 seconds.

5 Set the following **Access** address information required for the connection to the external LDAP server resource:

Secure Mode	Specify the security mode when connecting to an external LDAP server. Use start-tls or tls-mode to connect. The start-tls mode provides a way to upgrade a plain text connection to an encrypted connection using TLS. Default port value for start-tls is 389. Default port value for stls-mode is 636.
Bind DN	Specify the distinguished name to bind with the LDAP server. The DN is the name that uniquely identifies an entry in the LDAP directory. A DN is made up of attribute value pairs, separated by commas.
Base DN	Specify a *distinguished name* (DN) that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching. LDAP DNs begin with the most specific attribute (usually some sort of name), and continue with progressively broader attributes, often ending with a country attribute. The first component of the DN is referred to as the *Relative Distinguished Name* (RDN). It identifies an entry distinctly from any other entries that have the same parent.
Bind Password	Enter a valid password for the LDAP server. Select the *Show* checkbox to expose the password's actual character string, leaving the option unselected displays the password as a string of asterisks (*). The password cannot 32 characters.
Password Attribute	Enter the LDAP server password attribute. The password cannot exceed 64 characters.

6 Set the following **Attributes** for LDAP groups to optimally refine group queries:

Group Attribute	LDAP systems have the facility to poll dynamic groups. In an LDAP dynamic group, an administrator can specify search criteria. All users matching the search criteria are considered a member of this dynamic group. Specify a group attribute used by the LDAP server. An attribute could be a group name, group ID, password or group membership name.
Group Filter	Specify the group filters used by the LDAP server. This filter is typically used for security role-to-group assignments and specifies the property to look up groups in the directory service.
Group Membership Attribute	Specify the group member attribute sent to the LDAP server when authenticating users.

7 Click the **OK** button to save the changes to the LDAP server configuration. Select **Reset** to revert to the last saved configuration.

11.6.4 RADIUS Deployment Considerations

Setting the RADIUS Configuration

Before defining the RADIUS server configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Each RADIUS client should use a different shared secret. If a shared secret is compromised, only the one client poses a risk, as opposed all the additional clients that potentially share the secret password.
- Consider using an LDAP server as a database of user credentials that can be used optionally with the RADIUS server to free up resources and manage user credentials from a secure remote location.

11.7 URL Lists

Services

URL Lists are used to select highly utilized URLs for smart caching. The selected URLs are monitored and routed according to existing cache content policies.

To configure a URL Lists policy:

1 Select **Configuration** tab from the main menu.

2 Select the **Services** tab from the **Configuration** menu.
The upper, left-hand, side of the user interface displays a **Services** menu pane where Captive Portal, DHCP Server Policy, RADIUS and Smart Caching configuration options can be selected.

3 Select **URL Lists**.
The URL Lists screen displays existing policies. New policies can be created, existing policies can be modified, deleted or copied.

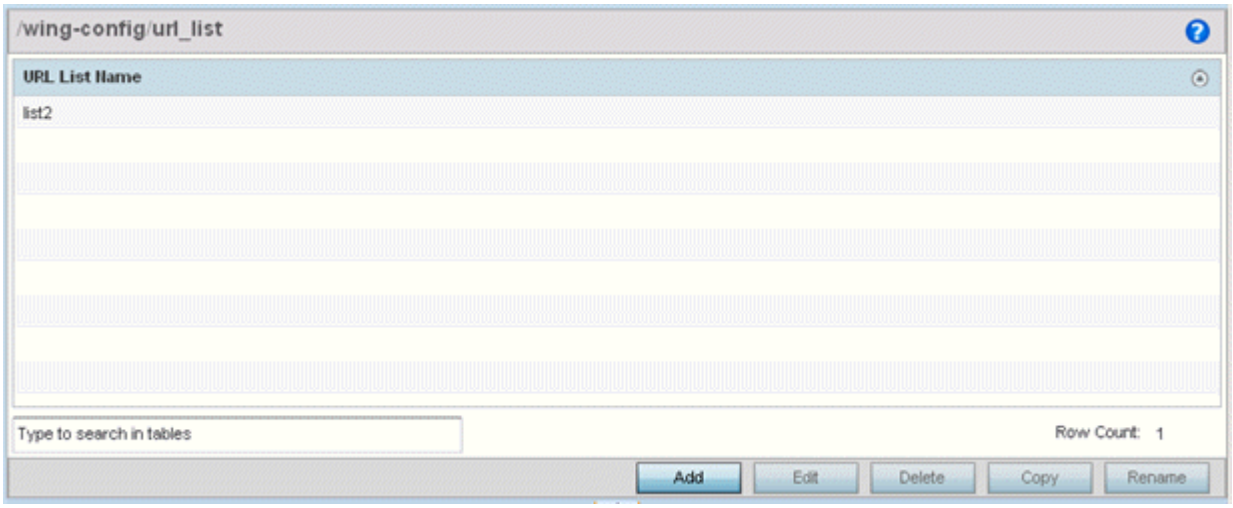


Figure 11-43 *Smart Caching - URL List Name screen*

4 Refer to the **URL List Name** table to review the administrator assigned name applied to the URL list policy upon creation.

5 Select **Add** to create a URL lists policy. Select an existing policy and click **Edit** to modify, **Delete** to remove or **Copy** to copy the settings of a selected (existing) URL lists policy.

11.7.1 Adding or Editing URL Lists

URL Lists

Use the URL Entries screen to define URLs for smart caching. These URLs are monitored and routed according to existing cache content policies.

To add URLs to those available for smart caching:

1 From the URL List screen, select **Add** to create a URL lists policy or **Edit** to modify an existing policy.

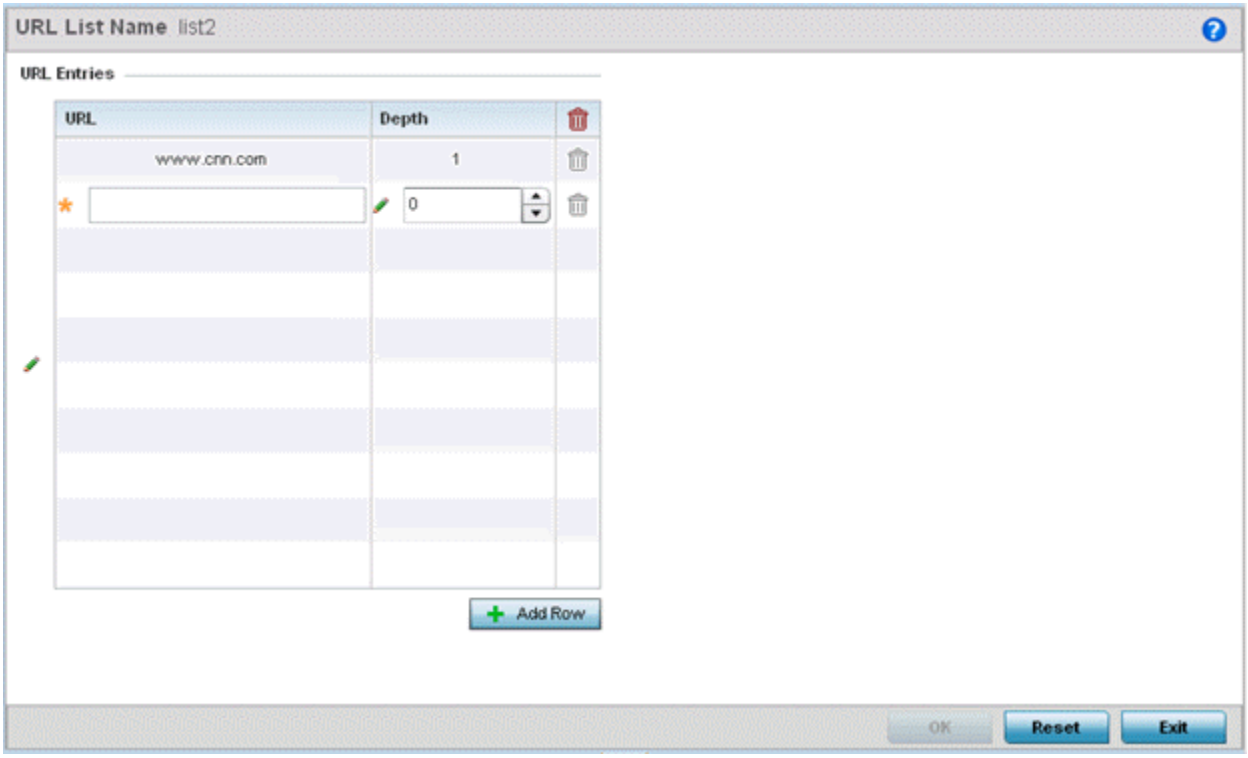


Figure 11-44 *URL List Name - Add/Edit screen*

2 Select **+ Add Row** to display configurable parameters for defining a URL and its depth.

3 If creating a new URL lists policy, assign it a **Name**. If editing an existing URL Lists policy, the policy name cannot be modified. The name cannot exceed 32 characters.

4 Set the following **URL Lists** parameters:

URL	Set the requested URL monitored and routed according to existing cache content policies.This value is mandatory.
Depth	Select the number of levels to be cached. Since Web sites have different parameters to uniquely identify specific content, the same content may be stored on multiple origin servers. Smart caching uses subsets of these parameters to recognize that the content is the same and serves it from cache. The available range is from 1 - 10. This value is mandatory.

5 Select **OK** to save the URL Entries list configuration. Select **Reset** to revert to the last saved configuration.

12 Management Access

Controllers and service platforms have mechanisms to allow/deny device access for separate interfaces and protocols (*HTTP, HTTPS*, *Telnet*, *SSH* or *SNMP*). Management access can be enabled/disabled as required for unique policies. The Management Access functionality is not meSNMPv1ant to function as an ACL (in routers or other firewalls), where administrators specify and customize specific IPs to access specific interfaces.

Controllers and service platforms can be managed using multiple interfaces (SNMP, CLI and Web UI). By default, management access is unrestricted, allowing management access to any enabled IP interface from any host using any enabled management service.

To enhance security, administrators can apply various restrictions as needed to:

- Restrict SNMP, CLI and Web UI access to specific hosts or subnets
- Disable un-used and insecure interfaces as required within managed access profiles. Disabling un-used management services can dramatically reduce an attack footprint and free resources on managed devices
- Provide authentication for management users
- Apply access restrictions and permissions to management users

Management restrictions can be applied to meet specific policies or industry requirements requiring only certain devices or users be granted access to critical infrastructure devices. Management restrictions can also be applied to reduce the attack footprint of the device when guest services are deployed.

12.1 Viewing Management Access Policies

Management Access policies display in the lower left-hand side of the screen. Existing policies can be updated as management permissions change, or new policies can be added as needed.

To view existing Management Access policies:

1 Select **Configuration** > **Management** > **Management Policy** to display the main Management Policy screen and Management Browser.

2 Select a policy from the Management Browser or refer to the Management screen (displayed by default) to review existing Management Access policy configurations at a higher level.

Figure 12-1 *Management Browser screen*

The **Management Policy** screen displays existing management policies and their unique protocol support configurations.

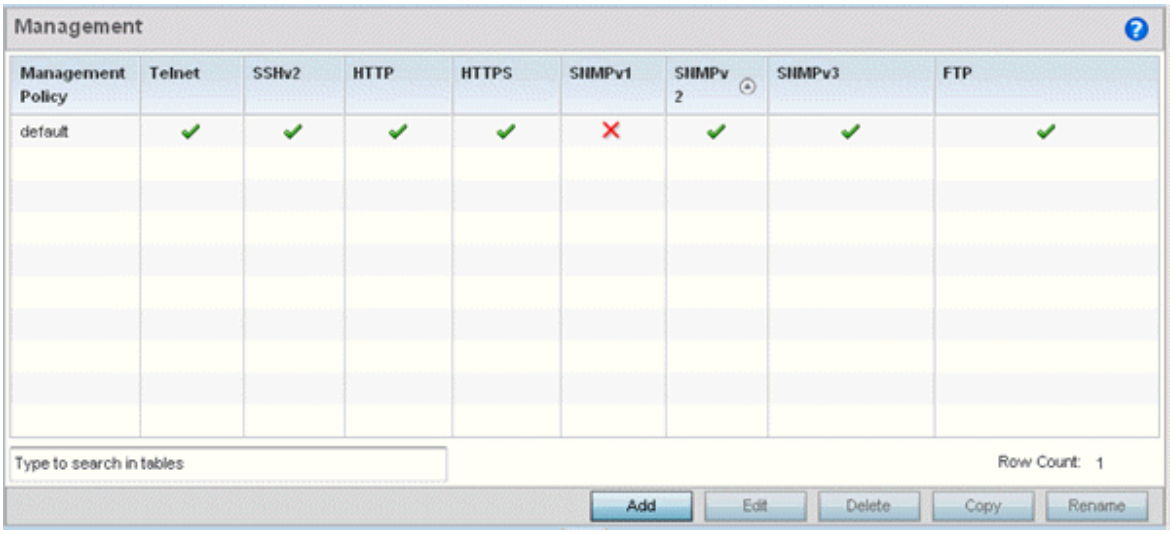


Figure 12-2 *Management Policy screen*

3 Refer to the following **Management** access policy configurations to discern whether these existing policies can be used as is, require modification or a new policy requires creation:

A green check mark indicates controller or service platform device access is allowed using the listed protocol. A red X indicates device access is denied using the listed protocol.

Management Policy	Displays the name of the Management Access policy assigned when initially created. The name cannot be updated when modifying a policy.
Telnet	Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but it does provide a measure of authentication.
SSHv2	SSH (*Secure Shell*) version 2, like Telnet, provides a command line interface to a remote host. However, all SSH transmissions are encrypted, increasing their security.

HTTP	HTTP (*Hypertext Transfer Protocol*) provides access to the device's GUI using a Web browser. This protocol is not very secure.
HTTPS	HTTPS (*Hypertext Transfer Protocol Secure*) provides fairly secure access to the device's GUI using a Web browser. Unlike HTTP, HTTPS uses encryption for transmission, and is therefore more secure.
SNMPv1	SNMP (*Simple Network Management Protocol*) exposes a device's management data so it can be managed remotely. Device data is exposed as variables that can be accessed and modified. SNMP is generally used to monitor a system's performance and other parameters. SNMP v1 is easy to set up, and only requires a plain text. It does not support 64 bit counters, only 32 bit counters, and that provides little security.
SNMPv2	SNMP v2 is identical to version 1, but it adds support for 64 bit counters. Most devices support SNMP v2c automatically. However, there are some devices that require you to explicitly enable v2, and that poses no risk.
SNMPv3	SNMP v3 adds security to the 64 bit counters provided with SNMP v2. SNMP v3 adds both encryption and authentication, which can be used together or separately. Its setup is more complex than just defining a community string. But if you require security, SNMP v3 is recommended.
FTP	FTP (*File Transfer Protocol*) is a standard protocol for files transfers over a TCP/IP network.

4 If it's determined a Management Access policy requires creation or modification, refer to *Adding or Editing a Management Access Policy on page 12-3*. If necessary, select an existing Management Access policy and select **Delete** to permanently remove it from the list of those available. Optionally **Rename** or **Copy** a policy as needed.

12.1.1 Adding or Editing a Management Access Policy

Viewing Management Access Policies

To add a new Management Access policy, or edit an existing configuration:

1 Select **Configuration** > **Management** > **Management Policy** to display the main Management Policy screen and Management Browser.

Existing policies can be modified by either selecting a policy from the **Management Browser** and selecting the **Edit** button.

New policies can be created by selecting the **Add** button from the bottom right-hand side of the Management screen.

2 A name must be supplied to the new policy before the **Administrators**, **Access Control**, **Authentication**, **SNMP** and **SNMP Traps** tabs become enabled and the policy's configuration defined. The name cannot exceed 32 characters.

3 Select **OK** to commit the new policy name.

Once the new name is defined, the screen's four tabs become enabled, with the contents of the **Administrators** tab displayed by default. Refer to the following to define the configuration of the new Management Access policy:

- *Creating an Administrator Configuration* - Use the *Administrators* tab to create specific users, assign them permissions to specific protocols and set specific administrative roles for the network.

- *Setting an Allowed Location Configuration* - Use the *Allowed Locations* tab to administrate user roles supported in both WiNG and NSight, as a user logging into the NSight UI should also have an access control restriction based on the role they're assigned in that application.
- *Setting the Access Control Configuration* - Use the *Access Control* tab to enable/disable specific protocols and interfaces. Again, this kind of access control is not meant to function as an ACL, but rather as a means to enable/disable specific protocols (HTTP, HTTPS, Telnet etc.) for each Management Access policy.
- *Setting the Authentication Configuration* - Refer to the *Authentication* tab to set the authentication scheme used to validate user credentials with this policy.
- *Setting the SNMP Configuration* - Refer to the *SNMP* tab to enable SNMPv2, SNMPv3 or both and define specific community strings for this policy.
- *SNMP Trap Configuration* - Use the *SNMP Traps* tab to enable trap generation for the policy and define trap receiver configurations.
- *T5 PowerBroadband SNMP* - Use the *T5 PowerBroadband* tab set a unique SNMP configuration for T5 controller models.

For deployment considerations and recommendations impacting a controller or service platform's Management Access policy configuration, refer to *Management Access Deployment Considerations on page 12-36*.

12.1.1.1 Creating an Administrator Configuration

Adding or Editing a Management Access Policy

Management services (Telnet, SSHv2, HTTP, HTTPs and FTP) require administrators enter a valid username and password which is authenticated locally or centrally on a RADIUS server. SNMPv3 also requires a valid username and password which is authenticated by the SNMPv3 module. For CLI and Web UI users, the controller or service platform also requires user role information to know what permissions to assign.

- If local authentication is used, associated role information is defined on the controller or service platform when the user account is created.
- If RADIUS is used, role information is supplied using RADIUS vendor specific return attributes. If no role information is supplied by RADIUS, the controller or service platform applies default read-only permissions.

Administrators can limit users to specific management interfaces. During authentication, the controller or service platform looks at the user's access assignment to determine if the user has permissions to access an interface:

- If local authentication is used, role information is defined on the controller or service platform when the user account is created.
- If RADIUS is used, role information is supplied by RADIUS using vendor specific return attributes.

The controller or service platform also supports multiple RADIUS server definitions as well as fallback to provide authentication in the event of failure. If the primary RADIUS server is unavailable, the controller or service platform authenticates with the next RADIUS sever, as defined in the AAA policy. If a RADIUS server is not reachable, the controller or service platform can fall back to the local database for authentication. If both RADIUS and local authentication services are unavailable, read-only access can be optionally provided.

The controller or service platform authenticates users using the integrated local database. When user credentials are presented the controller or service platform validates the username and password against the local database and assigns permissions based on the associated roles assigned. The controller or service platform can also deny the authentication request if the user is attempting to access a management interface not specified in the account's access mode list.

Use the **Administrators** tab to review existing administrators, their access medium and their administrative role within the network. New administrators can be added, existing administrative configurations modified or deleted as required.

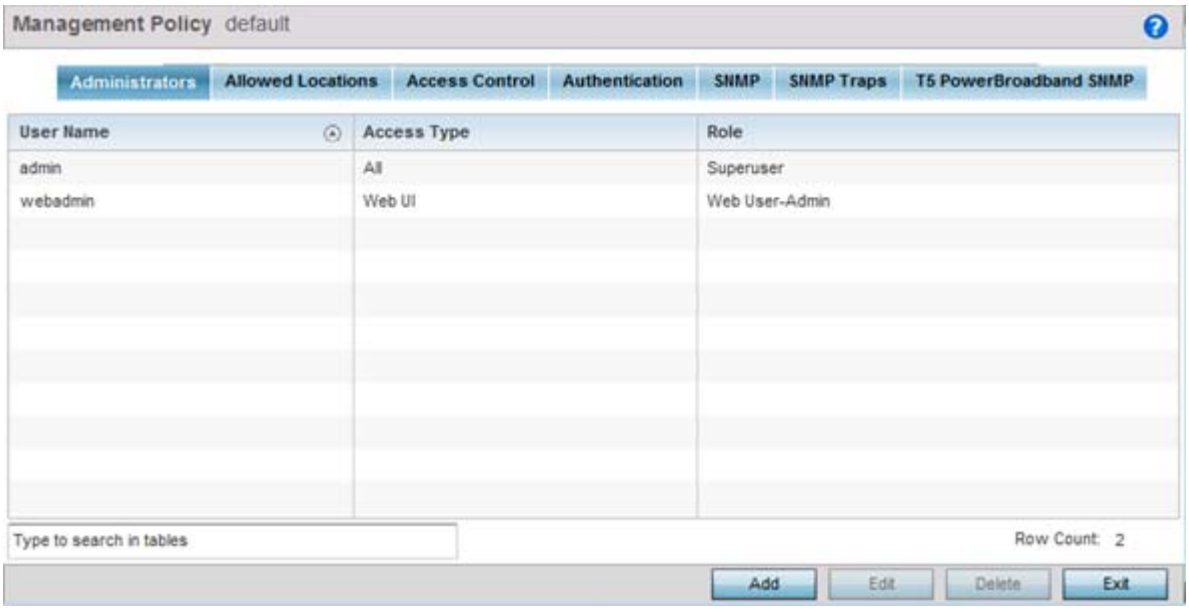


Figure 12-3 *Management Policy screen - Administrators tab*

1 Refer to the following to review the high-level configurations of existing administrators.

User Name	Displays the name assigned to the administrator upon creation of their account. The name cannot be modified as part of the administrator configuration edit process.
Access Type	Lists the *Web UI*, *Telnet*, *SSH* or *Console* access type assigned to each listed administrator. A single administrator can have any one (or all) of these roles assigned at the same time.
Role	Lists the *Superuser*, *System*, *Network, Security*, *Monitor*, *Help Desk, Web User, Device Provisioning* or *Vendor Admin* role assigned to each listed administrator. An administrator can only be assigned one role at a time.

2 Select **Add** to create a new administrator configuration, **Edit** to modify an existing configuration or **Delete** to permanently remove an Administrator from the list of those available.

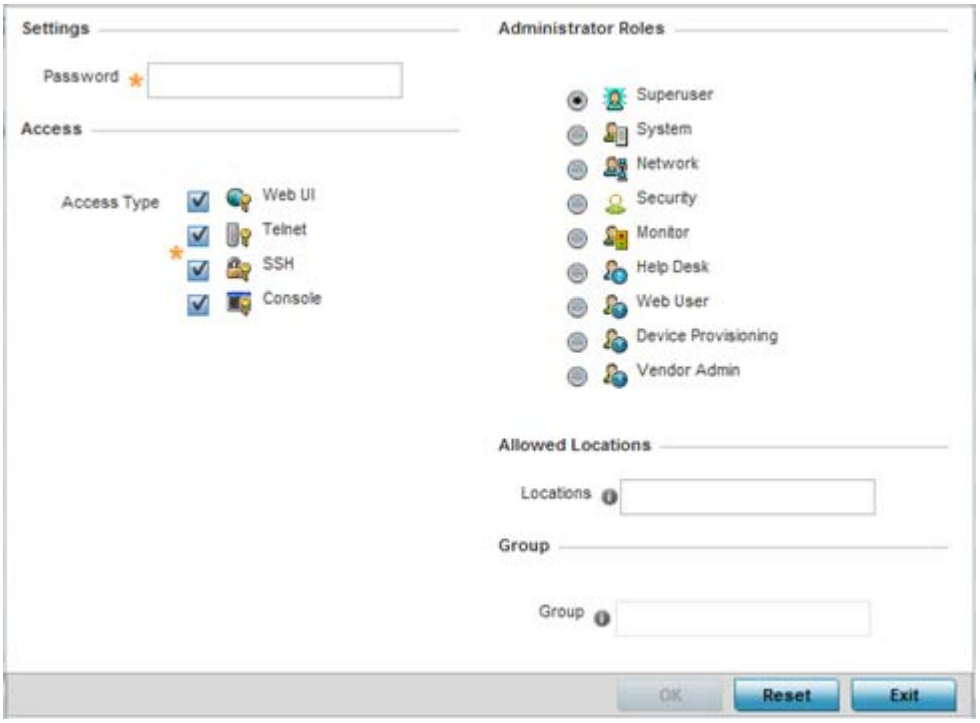


Figure 12-4 *Administrators screen*

3 If creating a new administrator, enter a user name in the **User Name** field. This is a mandatory field for new administrators and cannot exceed 32 characters. Optimally assign a name representative of the user and role.

4 Provide a strong password for the administrator within the **Password** field, once provided, **Reconfirm** the password to ensure its accurately entered. This is a mandatory field.

5 Select **Access** options to define the permitted access for the user. Access modes can be assigned to management user accounts to restrict which management interfaces the user can access. A management user can be assigned one or more access roles allowing access to multiple management interfaces. If required, all four options can be selected and invoked simultaneously.

Web UI	Select this option to enable access to the device's Web User Interface.
Telnet	Select this option to enable access to the device using TELNET.
SSH	Select this option to enable access to the device using SSH.
Console	Select this option to enable access to the device's console.

6 Select the **Administrator Role** for the administrator using this profile. Only one role can be assigned.

Superuser	Select this option to assign complete administrative rights to the user. This entails all the roles listed for all the other administrative roles.
System	The *System* role provides permissions to configure general settings like NTP, boot parameters, licenses, perform image upgrades, auto install, manager redundancy/clustering and control access.
Network	The *Network* role provides privileges to configure all wired and wireless parameters like IP configuration, VLANs, L2/L3 security, WLANs, radios, and captive portal.
Security	Select Security to set the administrative rights for a security administrator allowing configuration of all security parameters.

Monitor	Select Monitor to assign permissions without any administrative rights. The Monitor option provides read-only permissions.
Help Desk	Assign this role to someone who typically troubleshoots and debugs problems reported by the customer. The Help Desk manager typically runs troubleshooting utilities (like a sniffer), executes service commands, views/retrieves logs and reboots the controller or service platform. However, Help Desk personnel are *not* allowed to conduct controller or service platform reloads.
Web User	Select Web User to assign the administrator privileges needed to add users for authentication.
Device Provisioning	Select Device Provisioning to assign an administrator privileges to update (provision) device configuration files or firmware. Such updates run the risk of overwriting and losing a device's existing configuration unless the configuration is properly archived.
Vendor Admin	Select this option to create a vendor-admin user role group so this particular user type can access offline device-registration portal data. Vendors are assigned username/password credentials for securely on-boarding devices. Devices are moved to a vendor allowed VLAN immediately after this on-boarding process, so vendors do require unique administration roles. When the Vendor-Admin role is selected, provide the vendor's *Group* name for RADIUS authentication. The vendor's RADIUS group takes precedence over the statically configured group for device registration.

7 Select the **OK** button to save the administrator's configuration. Select **Reset** to revert to the last saved configuration.

12.1.1.2 Setting an Allowed Location Configuration

- *Adding or Editing a Management Access Policy*

Extreme Networks' WiNG and NSight applications may have the same users with different permissions defined in each application. Various user roles are supported in WiNG (superuser, system-admin, network-admin, security-admin, device-provisioning-admin, helpdesk and monitor). With NSight, a user logging into the NSight UI should also have an access control restriction based on the role they're assigned. For example, a WiNG user with helpdesk privileges should have access to only the site (RF Domain) in which the helpdesk is situated, and the location tree should contain only one RF Domain. Similarly, when a user responsible for a set of sites logs in NSight, their location tree needs to contain the RF Domains for which they're responsible.

To set an allowed location configuration:

1 Select the **Allowed Locations** tab from the Management Policy screen.

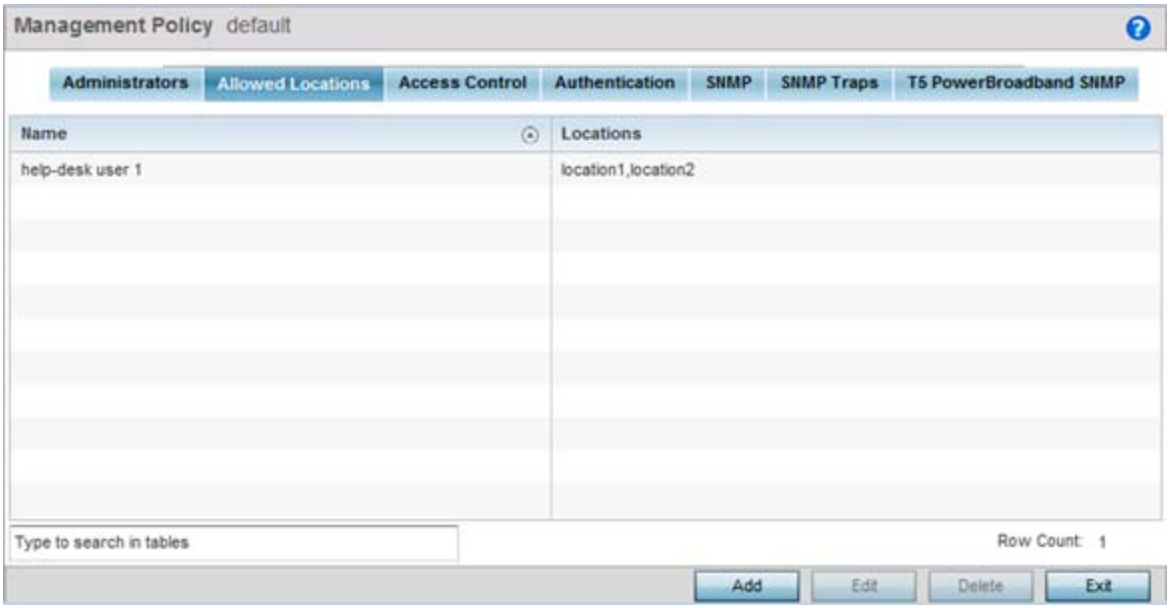


Figure 12-5 *Management Policy screen - Allowed Locations tab*

The Allowed Locations screen lists existing users and their permitted locations.

2 Select **Add** to create a new allowed location, **Edit** to modify an existing location or **Delete** to permanently remove a user name and location from the list of those available.

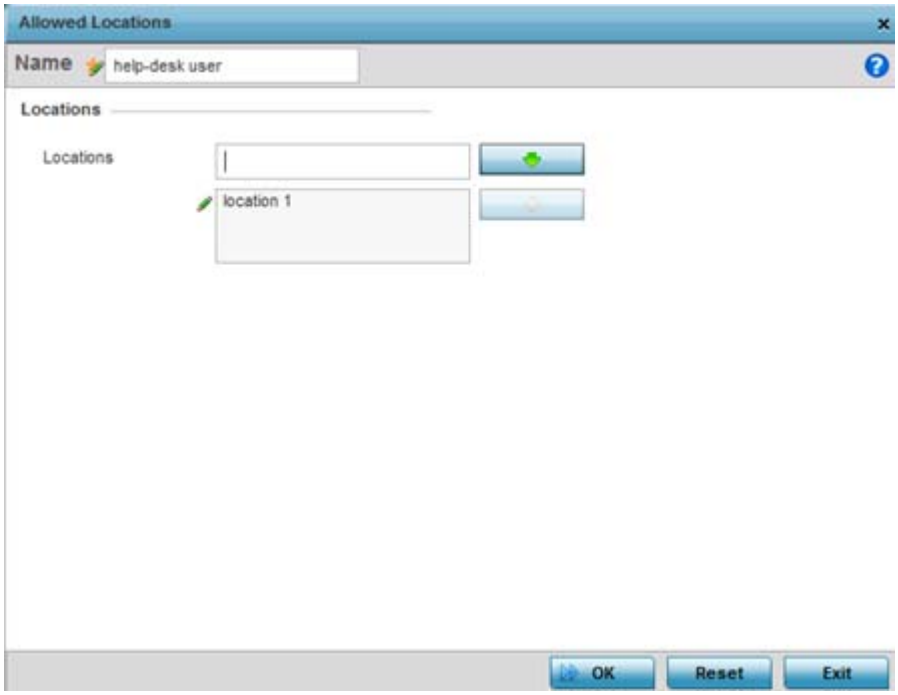


Figure 12-6 *Adding Allowed Locations screen*

3 Set the following allowed location parameters:

Name	Define a 32 character maximum user name whose access is a mapped to a specific site (RF Domain).

Locations	Create locations and use the navigation arrows to move them into the list of those enabled once saved.

4 Select **OK** to update the allowed location configuration. Select **Reset** to the last saved configuration.

12.1.1.3 Setting the Access Control Configuration

Adding or Editing a Management Access Policy

Restricting remote access to a controller or service platform ensures only trusted hosts can communicate with enabled management services. This ensures only trusted hosts can perform management tasks and provide protection from brute force attacks from hosts attempting to break into the controller or service platform managed network.

Administrators can permit management connections to be established on any IP interface on the controller or service platform (including IP interfaces used to provide captive portal guest access). Administrators can restrict management access by limiting access to a specific host (IP address), subnet, or ACL on the controller or service platform.

Refer to the Access Control tab to allow/deny management access to the network using strategically selected protocols (HTTP, HTTPS, Telnet, SSH or SNMP). Access options can be either enabled or disabled as required. Disabling unused interfaces is recommended to close unnecessary security holes. The Access Control tab is not meant to function as an ACL (in routers or other firewalls), where you can specify and customize specific IPs to access specific interfaces.

- *Source hosts* - Management access can be restricted to one or more hosts by specifying their IP addresses
- *Source subnets* - Management access can be restricted to one or more subnets
- *IP ACL* - Management access can be based on the policies defined in an IP based ACL

In the following example, a controller has two IP interfaces defined with VLAN10 hosting management and network services and VLAN70 providing guest services. For security the guest network is separated from all trusted VLANs by a firewall.

Interface	Description	IP Address	Management
VLAN10	Services	Yes	Yes
VLAN70	Guest	Yes	No

By default, management services are accessible on both VLAN10 and VLAN70, and that's not desirable to an administrator. By restricting access to VLAN10, the controller only accepts management sessions on VLAN10. Management access on VLAN70 is longer available.

Administrators can secure access to a controller or service platform by disabling less secure interfaces. By default, the CLI, SNMP and FTP disable interfaces that do not support encryption or authentication. However, Web management using HTTP is enabled. Insecure management interfaces such as Telnet, HTTP and SNMP should be disabled, and only secure management interfaces, like SSH and HTTPS should be used to access the controller or service platform managed network.

The following table demonstrates some interfaces provide better security than others:

Access Type	Encrypted	Authenticated	Default State
Telnet	No	Yes	Disabled
SNMPv2	No	No	Enabled

SNMPv3	Yes	Yes	Enabled
HTTP	No	Yes	Disabled
HTTPS	Yes	Yes	Disabled
FTP	No	Yes	Disabled
SSHv2	Yes	Yes	Disabled

To set an access control configuration for the Management Access policy:

1 Select the **Access Control** tab from the Management Policy screen.

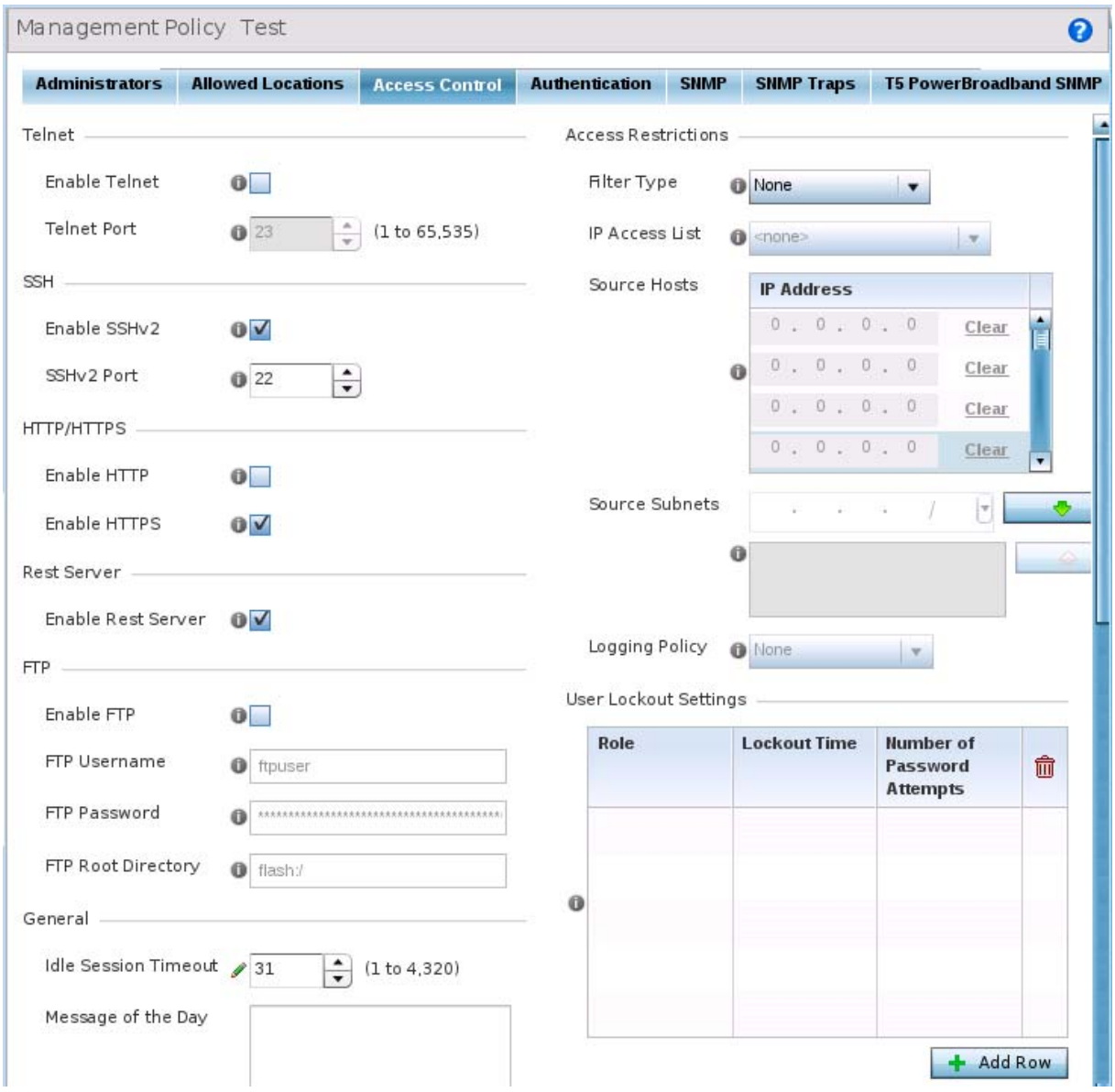


Figure 12-7 *Management Policy screen - Access Control tab*

2 Set the following parameters required for **Telnet** access:

Enable Telnet	Select the checkbox to enable Telnet device access. Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but it does provide a measure of authentication. Telnet access is disabled by default.
Telnet Port	Set the port on which Telnet connections are made (1 - 65,535). The default port is 23. Change this value using the spinner control next to this field or by entering the port number in the field.

3 Set the following parameters required for **SSH** access:

Enable SSHv2	Select the checkbox to enable SSH device access. SSH (*Secure Shell*) version 2, like Telnet, provides a command line interface to a remote host. SSH transmissions are encrypted and authenticated, increasing the security of transmission. SSH access is disabled by default.
SSHv2 Port	Set the port on which SSH connections are made. The default port is 22. Change this value using the spinner control next to this field or by entering the port number in the field.

4 Set the following **HTTP/HTTPS** parameters:

Enable HTTP	Select the checkbox to enable HTTP device access. HTTP provides limited authentication and no encryption.
Enable HTTPS	Select the checkbox to enable HTTPS device access. HTTPS (*Hypertext Transfer Protocol Secure*) is more secure plain HTTP. HTTPS provides both authentication and data encryption as opposed to just authentication (as is the case with HTTP).

NOTE: If the a RADIUS server is not reachable, HTTPS or SSH management access to the controller or service platform may be denied.

5 Select the **Enable Rest Server** option, within the **Rest Server** field, to facilitate device on-boarding. When selected, the REST server allows vendor-specific users access to the online device registration portal. All requests and responses to and from the on-boarding portal are handled by the REST server through restful *Application Programming Interface* (API) transactions. The REST server serves the Web pages used to associate a device's MAC address with a specific vendor group. This option is enabled by default.

6 Set the following parameters required for **FTP** access:

Enable FTP	Select the checkbox to enable FTP device access. FTP (*File Transfer Protocol*) is the standard protocol for transferring files over a TCP/IP network. FTP requires administrators enter a valid username and password authenticated locally. FTP access is disabled by default.
FTP Username	Specify a username required when logging in to the FTP server. The username cannot exceed 32 characters.
FTP Password	Specify a password required when logging in to the FTP server. Reconfirm the password in the field provided to ensure it has been entered correctly. The password cannot exceed 63 characters.
FTP Root Directory	Provide the complete path to the root directory in the space provided. The default setting has the root directory set to flash:/

7 Set the following **General** parameters:

Idle Session Timeout	Specify an inactivity timeout for management connection attempts (in seconds) from 0 - 4,320.
Message of the Day	Enter *message of the day* text (no longer then 255 characters) displayed at login for clients connecting via the CLI.

8 Set the following **Access Restrictions** parameters:

Filter Type	Select a filter type for access restriction. Options include *IP Access List*, *Source Address* or *None*. To restrict management access to specific hosts, select *Source Address* as the filter type and provide the allowed addresses within the Source Hosts field.
IP Access List	If the selected filter type is IP Access List, select an access list from the drop-down menu or select the *Create* button to define a new one. IP based firewalls function like *Access Control Lists* (ACLs) to filter/ mark packets based on the IP from which they arrive, as opposed to filtering packets on layer 2 ports. IP firewalls implement uniquely defined access control policies, so if you don't have an idea of what kind of access to allow or deny, a firewall is of little value, and could provide a false sense of network security.
Source Hosts	If the selected filter type is Source Address, enter an IP Address or IP Addresses for the source hosts. To restrict management access to specific hosts, select Source Address as the filter type and provide the allowed addresses within the Source Hosts field.
Source Subnets	If the selected filter type is Source Address, enter a source subnet or subnets for the source hosts. To restrict management access to specific subnets, select Source Address as the filter type and provide the allowed addresses within the Source Subnets field.
Logging Policy	If the selected filter is Source Address, enter a logging policy for administrative access. Options includes *None*, *Denied Requests* or *All*.

9 Set the **User Lockout Settings**. Click the **Add Row** button and configure the following role-based user-account lockout and unlock criteria:

Role	Specify the user-role for which account lockout is to be enabled. The options are: • device-provisioning-admin • helpdesk • monitor • network-admin • security-admin • system-admin • vendor-admin • web-suer-admin Note, you can enable account lockout for multiple roles. After specifying the role/roles, set the *Lockout Time* and *Number of Password Attempts*. User-account lockout is individually applied to each account within the specified role/roles. For example, consider the 'monitor' role having two users: 'user1' and 'user2'. The *Number of Password Attempts* and *Lockout Time* is set at '5' attempts and '10' minutes respectively. In this scenario, user2 makes 5 consecutive, failed login attempts, and the user2 account is locked out for 10 minutes. However, during this lockout time the user1 account remains active.
Lockout Time	Specify the maximum time for which an account remains locked. Specify a value from 0 to 600 minutes. The value '0' indicates that the account is permanently locked.
Number of Password Attempts	Specify the maximum number of consecutive, failed attempts allowed before an account is locked. Specify a value from 1 to 100.

10 Select **OK** to update the access control configuration. Select **Reset** to the last saved configuration.

12.1.1.4 Setting the Authentication Configuration

Adding or Editing a Management Access Policy

Refer to the **Authentication** tab to define how user credential validation is conducted on behalf of a Management Access policy. If utilizing an external authentication resource, an administrator can optionally apply a TACACS policy. *Terminal Access Controller Access - Control System+* (TACACS+) is a protocol created by CISCO to provide access control to network devices (routers, network access servers or other networked devices) through one or more centralized servers. TACACS provides separate authentication, authorization, and accounting services running on different servers.

To configure an external authentication resource:

1 Select the **Authentication** tab from the Management Policy screen.

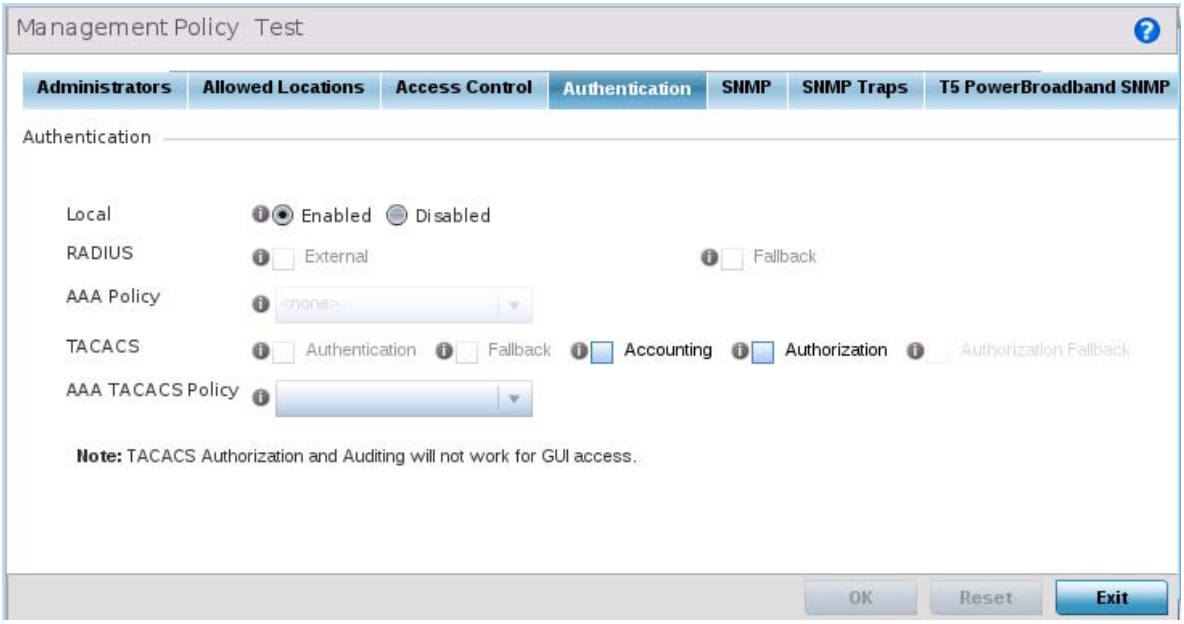


Figure 12-8 *Management Policy screen - Authentication tab*

2 Define the following settings to authenticate management access requests:

Local	Select whether the authentication server resource is centralized (local), or whether an external authentication resource is deployed for validating user access. Local is enabled by default.
RADIUS	If local authentication is disabled, define whether the RADIUS server is *External* or *Fallback*.
AAA Policy	Define the AAA policy used to authenticate user validation requests to the controller or service platform managed network. Select the *Create* icon as needed to define a new AAA policy or select the *Edit* icon to modify an existing policy.
TACACS	If local authentication is *disabled*, optionally select *Authentication* or *Fallback* (only one authentication or fallback option can be selected) or *Accounting* and *Authorization*. TACACS policies control user access to devices and network resources while providing separate accounting, authentication, and authorization services.
AAA TACACS Policy	Select an existing AAA TACACS policy (if available), or select *Create* to define a new policy or *Edit* to modify an existing one.

3 Select **OK** to update the authentication configuration. Select **Reset** to the last saved configuration.

12.1.1.5 Setting the SNMP Configuration

Adding or Editing a Management Access Policy

Optionally use the *Simple Network Management Protocol* (SNMP) to communicate with devices within the network. SNMP is an application layer protocol that facilitates the exchange of management information between the controller or service platform and a managed device. SNMP enabled devices listen on port 162 (by default) for SNMP packets from the controller or service platform's management server. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices. The read-only

community string is used to gather statistics and configuration parameters from a supported wireless device. The read-write community string is used by a management server to *set* device parameters. SNMP is generally used to monitor a system's performance and other parameters.

SNMP Version	Encrypted	Authenticated	Default State
SNMPv1	No	No	Disabled
SNMPv2	No	No	Enabled
SNMPv3	Yes	Yes	Enabled

To configure SNMP Management Access:

1 Select the **SNMP** tab from the Management Policy screen.

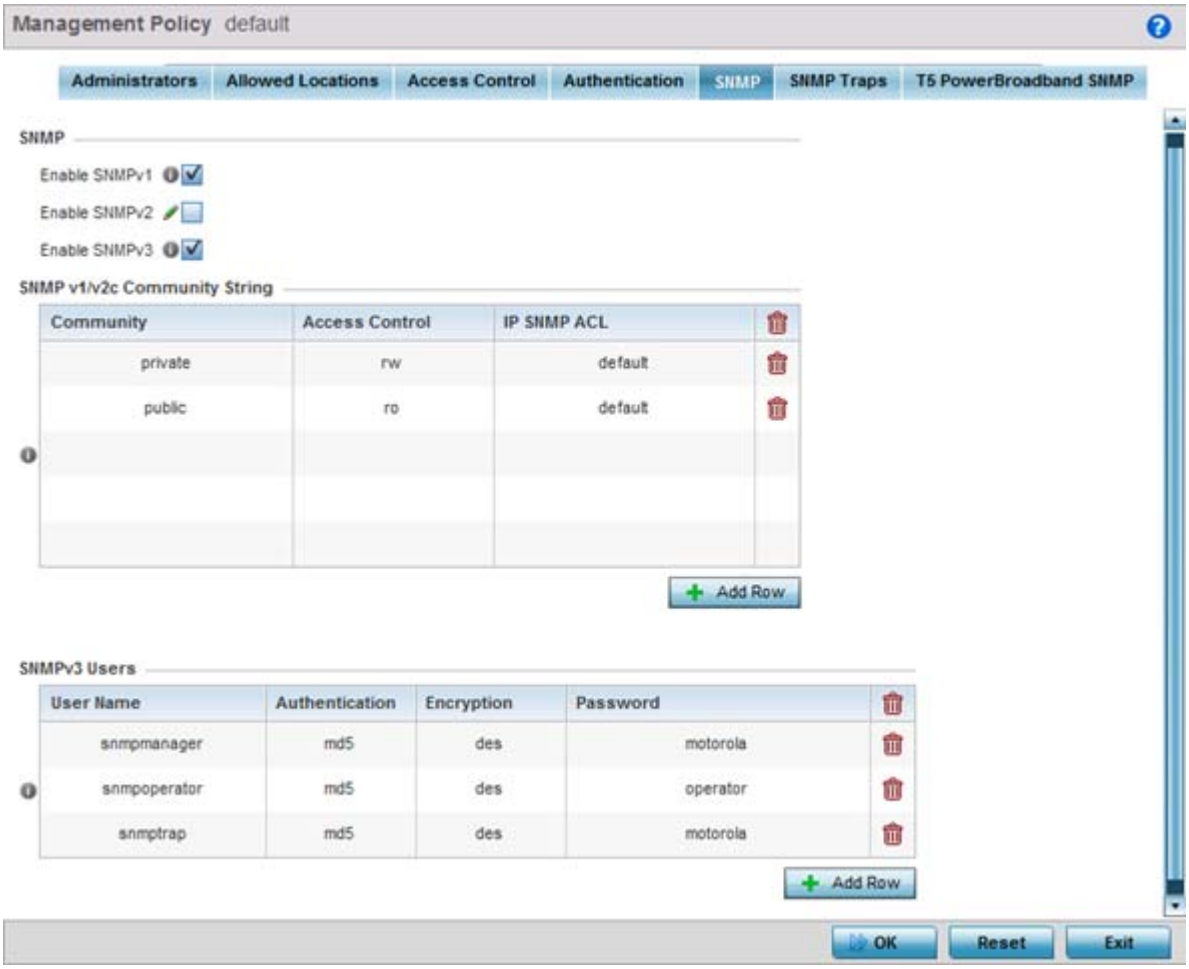


Figure 12-9 *Management Policy screen - SNMP tab*

2 Enable or disable SNMP v1, SNMPv2 and SNMPv3.

Enable SNMPv1	SNMP v1exposes a device's management data so it can be managed remotely. Device data is exposed as variables that can be accessed and modified as text strings, with version 1 being the original (rudimentary) implementation. SNMPv1 is enabled by default.

Enable SNMPv2	Select the checkbox to enable SNMPv2 support. SNMPv2 provides device management using a hierarchical set of variables. SNMPv2 uses *Get*, *GetNext*, and *Set* operations for data management. SNMPv2 is enabled by default.
Enable SNMPv3	Select the checkbox to enable SNMPv3 support. SNMPv3 adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the *user-based security model* (USM) for message security and the *view-based access control model* (VACM) for access control. The architecture supports the concurrent use of different security, access control and message processing techniques. SNMPv3 is enabled by default.

3 Set the **SNMP v1/v2 Community String** configuration. Use the **+ Add Row** function as needed to add additional SNMP v1/2 community strings, or select an existing community string's radio button and select the **Delete** icon to remove it.

Community	Define a *public* or *private* community designation. By default, SNMPv2 community strings on most devices are set to *public,* for the read-only community string, and *private* for the read-write community string.
Access Control	Set the access permission for each community string used by devices to retrieve or modify information. Available options include: *Read Only* - Allows a remote device to retrieve information. *Read-Write* - Allows a remote device to modify settings.
IP SNMP ACL	Set the IP SNMP ACL used along with community string. Use the drop-down menu to select an existing ACL. Use the *Create* icon to create and add a new ACL. Select an existing ACL and the *Edit* icon to update an existing ACL.

4 Set the **SNMPv3 Users** configuration. Use the **+ Add Row** function as needed to add additional SNMPv3 user configurations, or select a SNMP user's radio button and select the **Delete** icon to remove the user.

User Name	Use the drop-down menu to define a user name of *snmpmanager*, *snmpoperator* or *snmptrap*.
Authentication	Displays the authentication scheme used with the listed SNMPv3 user. The listed authentication scheme ensures only trusted and authorized users and devices can access the network.
Encryption	Displays the encryption scheme used with the listed SNMPv3 user.
Password	Provide the user's password in the field provided. Select the *Show* check box to display the actual character string used in the password, while leaving the check box unselected protects the password and displays each character as "*".

5 Select **OK** to update the SNMP configuration. Select **Reset** to revert to the last saved configuration.

12.1.1.6 SNMP Trap Configuration

Adding or Editing a Management Access Policy

The managed network can use SNMP trap receivers for fault notifications. SNMP traps are unsolicited notifications triggered by thresholds (or actions), and are therefore an important fault management tool.

A SNMP trap receiver is the destination of SNMP messages (external to the controller or service platform). A trap is like a Syslog message, just over another protocol (SNMP). A trap is generated when a device consolidates event

information and transmits the information to an external repository. The trap contains several standard items, such as the SNMP version, community etc.

SNMP trap notifications exist for most controller or service platform operations, but not all are necessary for day-to-day operation.

To define a SNMP trap configuration for receiving events at a remote destination:

1 Select the **SNMP Traps** tab from the Management Policy screen.

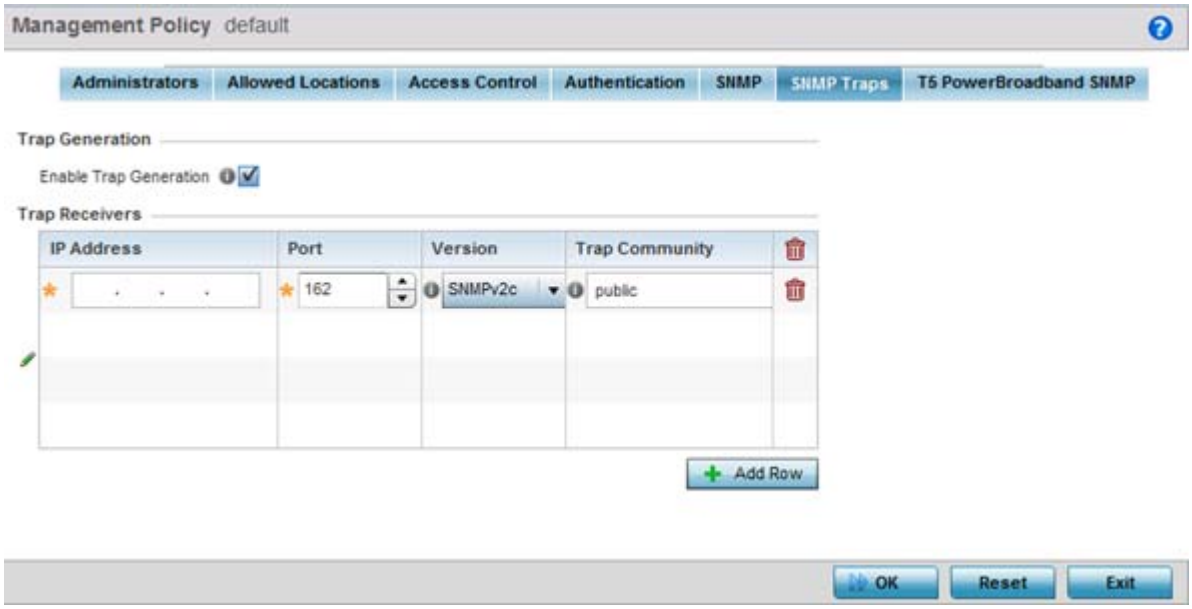


Figure 12-10 *Management Policy screen - SNMP Traps tab*

2 Select the **Enable Trap Generation** checkbox to enable trap generation using the trap receiver configuration defined. This feature is disabled by default.

3 Refer to the **Trap Receiver** table to set the configuration of the external resource dedicated to receiving trap information. Select **Add Row +** as needed to add additional trap receivers. Select the **Delete** icon to permanently remove a trap receiver.

IP Address	Sets the IP address of the external server resource dedicated to receiving the SNMP traps on behalf of the controller or service platform.
Port	Set the port of the server resource dedicated to receiving SNMP traps. The default port is port 162.
Version	Sets the SNMP version to use to send SNMP traps. SNMPv2 is the default.
Trap Community	Provide a 32 character maximum trap community string. The community string functions like a user id or password allowing access to controller or Access Point resources. If the community string is correct, the controller or Access Point provides with the requested information. If the community string is incorrect, the device controller or Access Point discards the request and does not respond. Community strings are used only by devices which support SNMPv1 and SNMPv2c. SNMPv3 uses username/password authentication, along with an encryption key. The default setting is *public*.

4 Select **OK** to update the SNMP Trap configuration. Select **Reset** to revert to the last saved configuration.

12.1.1.7 T5 PowerBroadband SNMP

Adding or Editing a Management Access Policy

A T5 controller, once enabled as a supported external device, can provide data to WiNG to assist in a T5's management within a WiNG supported subnet populated by both types of devices.

To define a T5 controller power broadband SNMP configuration:

1 Select the **T5 Power Broadband** tab from the Management Policy screen.

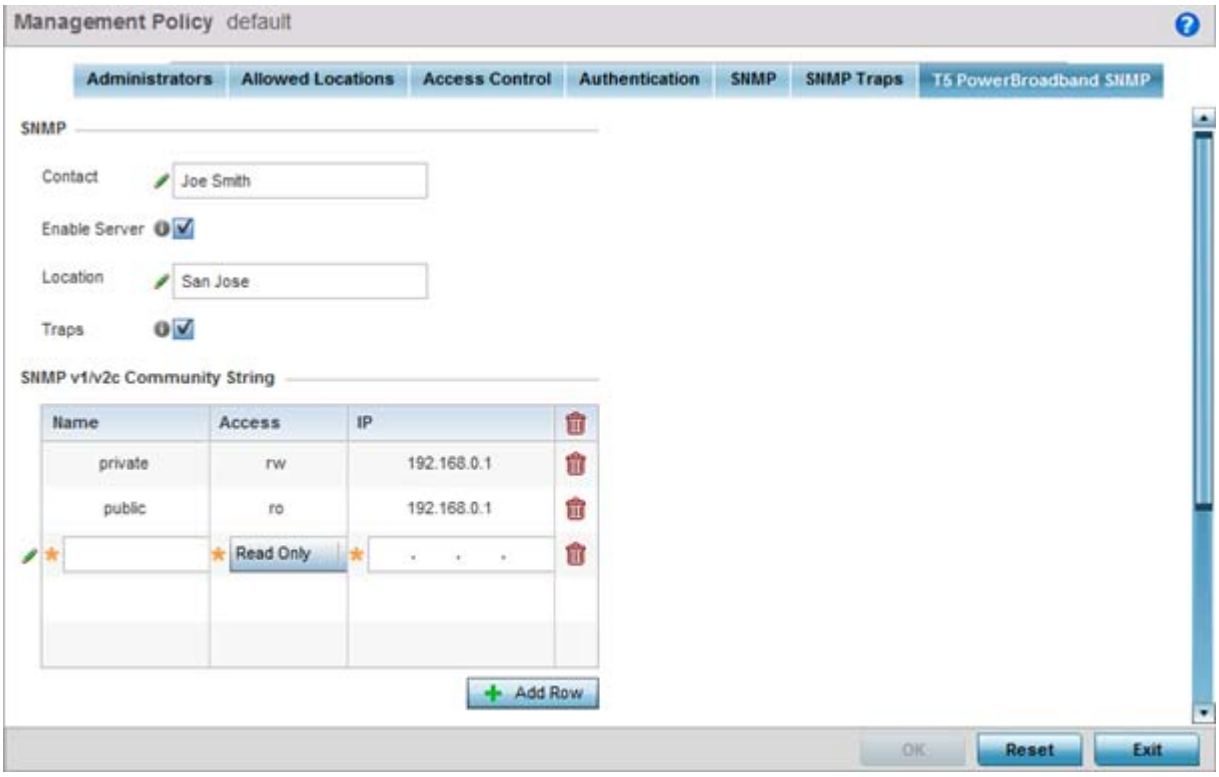


Figure 12-11 *Management Policy screen - T5 PowerBroadband tab*

2 Set the following **SNMP** settings:

Contact	Set a 64 character maximum contact name for the administration of T5 controller SNMP events.
Enable Server	Select this option to enable SNMP event management for the T5 controller. This setting is disabled by default.
Location	Set a 64 character maximum location for the SNMP resource dedicated to T5 controller support.
Traps	Select this option for SNMP trap support for the T5 controller. A trap is like a Syslog message, just over another protocol (SNMP). A trap is generated when a device consolidates event information and transmits the information to an external repository. The trap contains several standard items, such as the SNMP version, community etc.

3 Set the **SNMP v1/v2c Community String** configuration for T5 controller usage. Use the **+ Add Row** function as needed to add additional SNMP v1/2 community strings, or select an existing community string's radio button and select the **Delete** icon to remove it.

Community	Set a 32 character maximum SNMP community string.
Access	Set the access permission for each community string used by devices to retrieve or modify information. Available options include: *Read Only* - Allows a remote device to retrieve information. *Read-Write* - Allows a remote device to modify settings.
IP	Set the IP address of the SNMP manager.

4 Use the **Host** table to define up to 4 SNMP receiver resource IP addresses.

5 Select **OK** to update the configuration. Select **Reset** to revert to the last saved configuration.

12.2 EX3500 Management Policies

The EX3500 series switch is a Gigabit Ethernet Layer 2 switch with either 24 or 48 10/100/1000-BASE-T ports, and four *Small Form Factor Pluggable* (SFP) transceiver slots for fiber connectivity. Each 10/100/1000 Mbps port supports both the IEEE 802.3af and IEEE 802.3at-2009 PoE standards. Each EX3500 series switch includes an SNMP-based management agent, which provides both in-band and out-of-band access for management. An EX3500 series switch utilizes an embedded HTTP Web agent and *command line interface* (CLI) somewhat different from the WiNG operating system, while still enabling the EX3500 series switch to provide WiNG controllers PoE and port management resources.

Going forward NX9600, NX9500, NX7500, NX6500, NX5500, NX4500 WiNG managed services platforms and WiNG VMs can discover, adopt and partially manage EX3500 series Ethernet switches, as DHCP option 193 has been added to support external device adoption. DHCP option 193 is a simplified form of DHCP options 191 and 192 used by WiNG devices currently. DHCP option 193 supports *pool1*, *hello-interval* and a*djacency-hold-time* parameters.

NOTE: WiNG can partially manage an EX3500 without using DHCP option 193. In this case the EX3500 must be directly configured to specify the IPv4 addresses of potential WiNG adopters, using the EX3500 `controller host ip address` CLI command.

WiNG service platforms leave the proprietary operating system running the EX3500 switches unmodified, and partially manage them utilizing standardized WiNG interfaces. WiNG service platforms use a translation layer to communicate with EX3500 series switches.

To set EX3500 management settings for user EX3500 user group creation, authentication, password management and SNMP:

1 Select **Configuration**.

2 Select **Management**.

3 Refer to the upper, left-hand, portion of the UI and select **EX3500 Management Policy.**

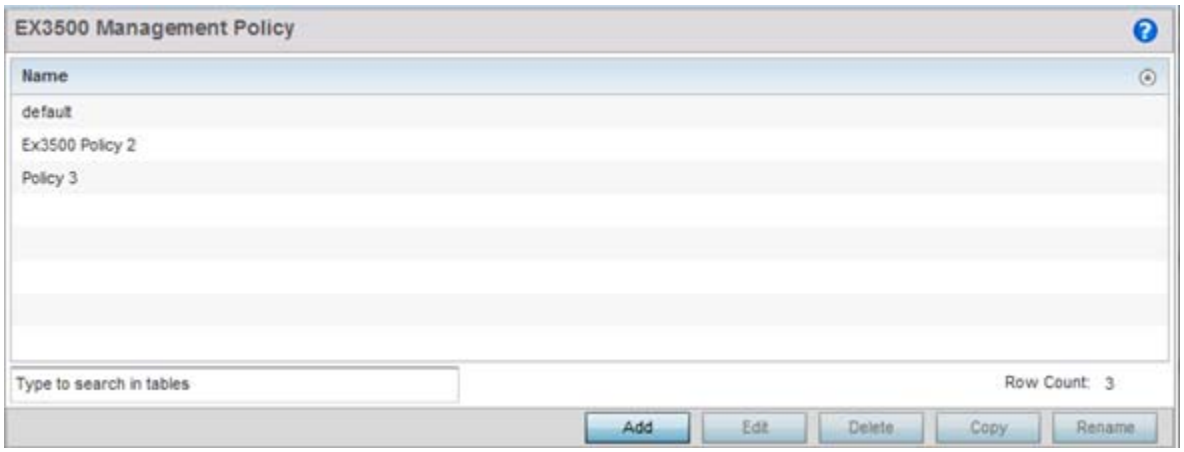


Figure 12-12 *EX3500 Management Policy screen*

The screen lists those EX3500 management policies created thus far. Select **Add** to create a new EX3500 management policy, **Edit** to modify the attributes of a policy or **Delete** to remove an obsolete list from those available. Existing lists can be copied or renamed as needed.

For more information, refer to the following:

- *EX3500 User Groups*
- *EX3500 Authentication*
- *EX3500 Exec Password Management*
- *EX3500 System Settings*
- *EX3500 SNMP Management*
- *EX3500 SNMP Users*

12.2.1 EX3500 User Groups

EX3500 switch user groups are stored in a local database on the WiNG service platform. Each user group can be assigned unique access levels and passswords to provide administrative priority.

To set an EX3500 user group configuration:

1 Select **Configuration**.

2 Select **Management**.

3 Refer to the upper, left-hand, portion of the UI and select **EX3500 Management Policy.**

4 The screen lists those EX3500 management policies created thus far. Select **Add** to create a new EX3500 management policy, **Edit** to modify an existing policy or **Delete** to remove an obsolete policy. Existing lists can be copied or renamed as needed.

5 If creating a new EX35000 user group, assign it a **Name** up to 32 characters. Select **Continue.**

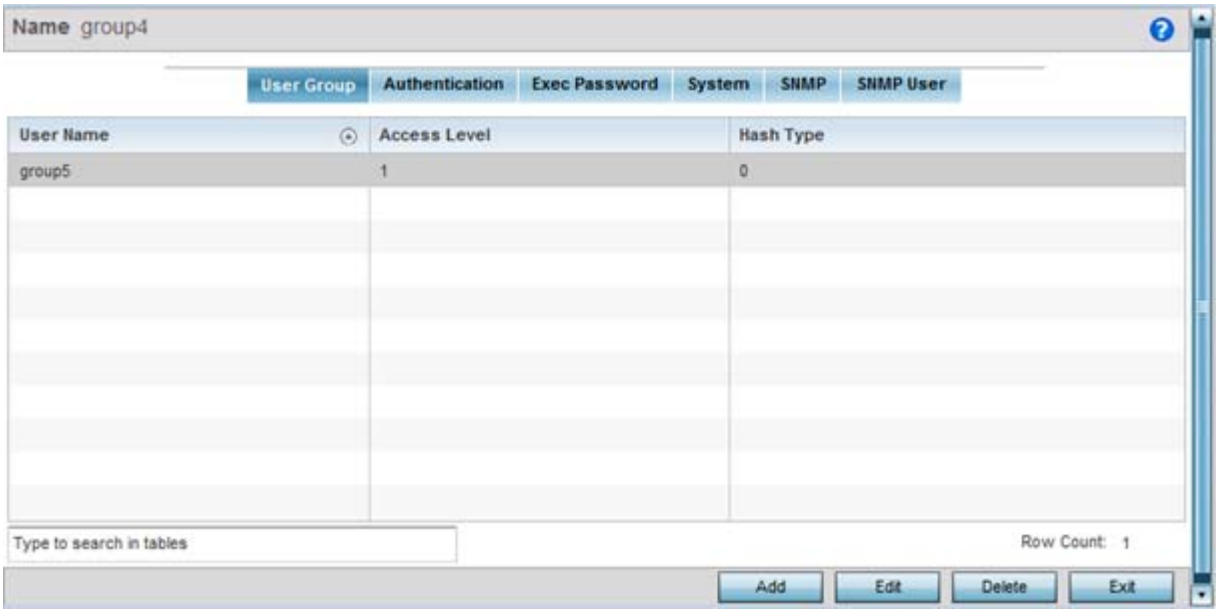


Figure 12-13 *EX3500 Management Policy User Group screen*

6 Select **Add** to create a new EX3500 user group, **Edit** to modify an existing group or **Delete** to remove an obsolete group. Set the following **User Group** attributes:

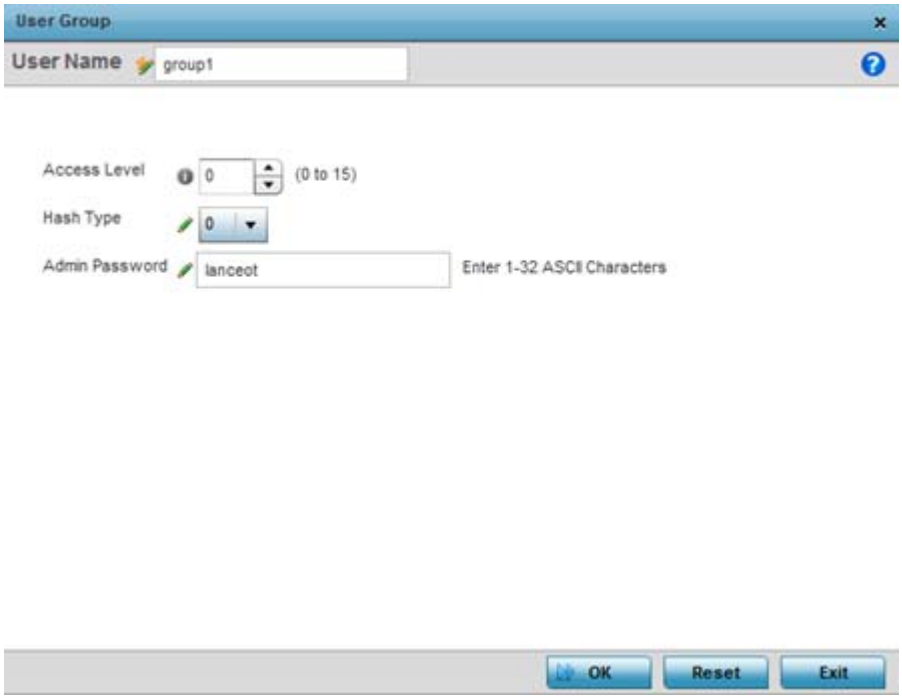


Figure 12-14 *User Group Add/Edit screen*

Access Level	Use the spinner control to set an access level from 0 - 15 serving as the access priority of each user group requesting access and interoperability with an EX3500 switch. Access level 0 corresponds to a guest user with minimal access to commands while access level 15 corresponds to an administrator user with full access to all commands.

Hash Type	Select either 0 or 7 to define the hash in plain text (0) or encrypted characters (7).
Admin Password	Create a 32 character maximum password for the EX3500 user group.

7 Select **OK** when completed to update the EX3500 user group configuration. Select **Reset** to revert the screen back to its last saved configuration.

12.2.2 EX3500 Authentication

Management access to an EX3500 switch can be enabled/disabled as required using separate interfaces and protocols (HTTP, SSH). Disabling un-used and insecure interfaces and unused management services can dramatically reduce an attack footprint and free resources within an EX3500 management policy.

To authenticate an EX3500 management policy:

1 Select **Configuration** from the Web UI.

2 Select **Management**.

3 Refer to the upper, left-hand, portion of the UI and select **EX3500 Management Policy.**

4 The screen lists those EX3500 management policies created thus far. Select **Add** to create a new EX3500 management policy, **Edit** to modify an existing policy or **Delete** to remove an obsolete policy. Existing lists can be copied or renamed as needed.

5 Select the **Authentication** tab.

Figure 12-15 *EX35000 Management Policy Authentication screen*

6 Select the following **HTTP** server settings to authenticating a HTTP connection to an EX3500:

Server	When selected, access the EX3500 using HTTP from any Windows PC, Linux PC or other device that uses HTTP. This setting is enabled by default.
Port	Set the HTTP port number from 1 - 65,535. The default port is 80.
Secure Server	Select this option to secure HTTP over a designated secure port.

Secure Port	Use the spinner control to select a secure port from 1 - 65, 535.

7 Select the following **SSH** server settings to authenticate a SSH connection to an EX3500:

Server	When selected, access the EX3500 using SSH from any Windows PC, Linux PC or other device that uses SSH. This setting is enabled by default.
Retries for SSH	Set the maximum number of retries, from 1 - 5, for connection to the SSH server resource. The default setting is 3.
Server Key	Set the SSH server key length from 512 - 1,024. The default length is 768.
Time Out	Set the inactivity timeout for the SSH server resource from 1 - 120 seconds. When this setting is exceeded, the SSH server resource becomes unreachable and must be reauthenticated. The default value is 120 seconds.

8 Select **OK** when completed to update the EX3500 authentication configuration. Select **Reset** to revert the screen back to its last saved configuration.

12.2.3 EX3500 Exec Password Management

Each EX3500 management policy can have a unique exec password with its own privilege level assigned. Utilize these passwords as specific EX3500 management sessions require priority over others.

To administrate EX3500 management passwords and their privileges:

1 Select **Configuration** from the Web UI.

2 Select **Management**.

3 Refer to the upper, left-hand, portion of the UI and select **EX3500 Management Policy.**

4 The screen lists those EX3500 management policies created thus far. Select **Add** to create a new EX3500 management policy, **Edit** to modify an existing policy or **Delete** to remove an obsolete policy. Existing lists can be copied or renamed as needed.

5 Select the **Exec Password** tab.

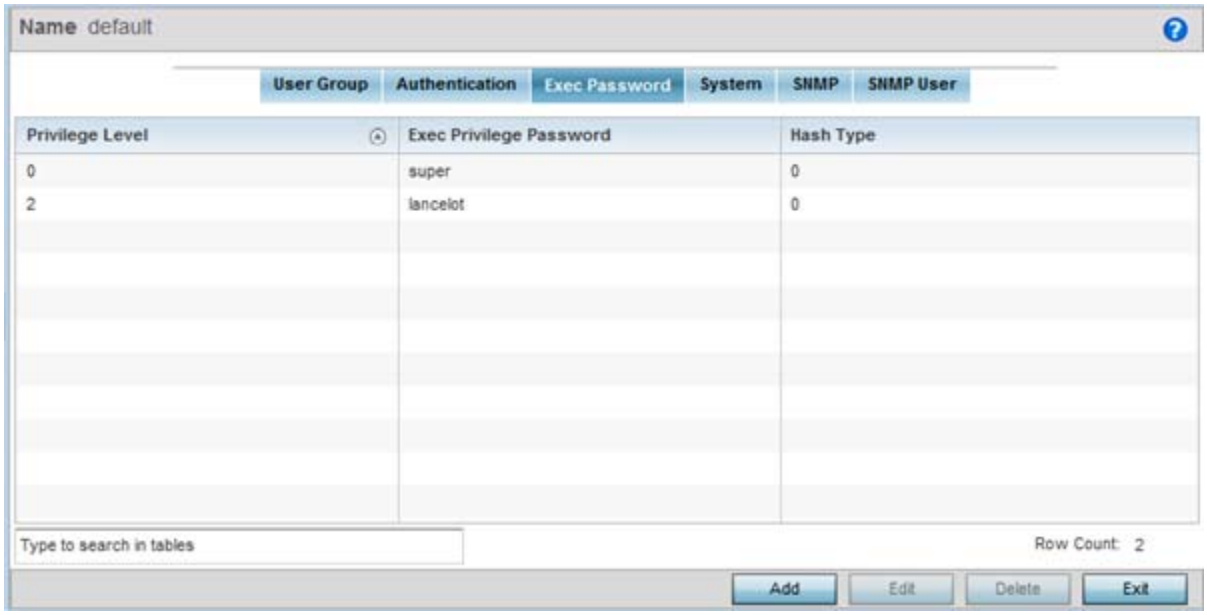


Figure 12-16 *EX35000 Management Policy Exec Password screen*

6 Select **Add** to create a new EX3500 exec password, **Edit** to modify an existing password configuration or **Delete** to remove an obsolete password.

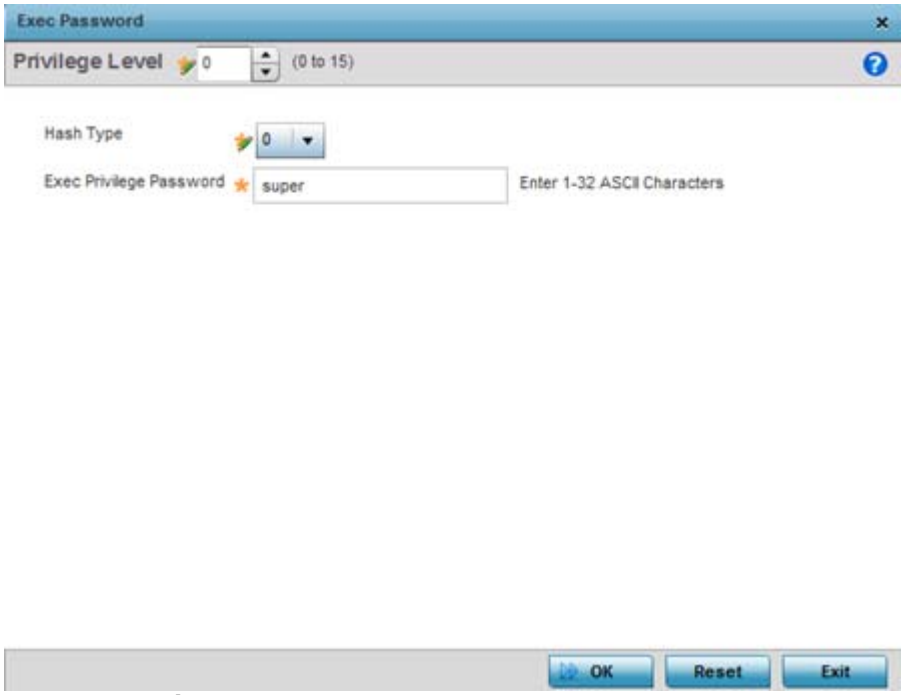


Figure 12-17 *EX35000 Management Policy Exec Password Add/Edit screen*

7 Assign a privilege level from 0 - 15. 0 provides the least access, while level 15 provides the most access. The commands available at each level vary.

8 Select the following **Exec Password** settings:

Hash Type	Select either 0 or 7 to define the hash in plain text (0) or encrypted characters (7).

Exec Privilege Password	Create a 32 character maximum password for the EX3500 exec password.

9 Select **OK** when completed to update the EX3500 exec password. Select **Reset** to revert the screen back to its last saved configuration.

12.2.4 EX3500 System Settings

An EX3500 management policy can be customized to include high and low alarm thresholds for EX3500 memory and CPU utilization.

The **Memory** and **CPU** rising and falling thresholds control when the EX3500 generates SNMP traps if these thresholds are exceeded. A trap is generated when the utilization exceeds the rising threshold, and another trap is generated after the utilization drops below the falling threshold. These thresholds do not protect the resource, they provide notification of an excessive use of the resource.

To administrate EX3500 management policy memory and CPU threshold settings:

1 Select **Configuration** from the Web UI.

2 Select **Management**.

3 Refer to the upper, left-hand, portion of the UI and select **EX3500 Management Policy.**

4 The screen lists those EX3500 management policies created thus far. Select **Add** to create a new EX3500 management policy, **Edit** to modify an existing policy or **Delete** to remove an obsolete policy. Existing lists can be copied or renamed as needed.

5 Select the **System** tab.

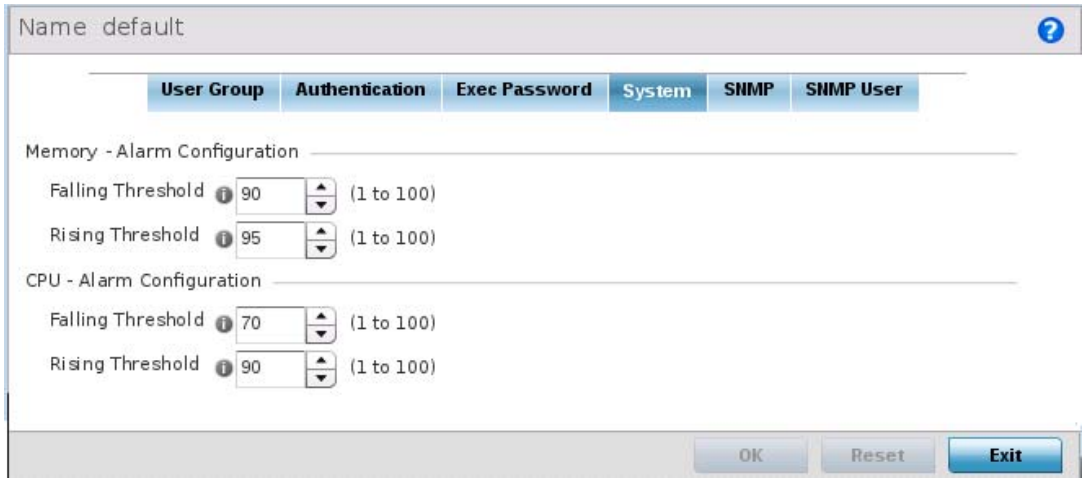


Figure 12-18 *EX35000 Management Policy System screen*

6 Set the following **Memory - Alarm Configuration** threshold settings:

Falling Threshold	Set the threshold for clearing the EX3500 memory utilization alarm. Once the rising threshold is exceeded, the memory utilization must drop below this threshold for the alarm to clear. The threshold is set as a percentage from 1 - 100, with a default of 90.
Rising Threshold	Set the threshold for EX3500 memory utilization as too high. The threshold is set as a percentage from 1 - 100, with a default of 95.

7 Set the following **CPU - Alarm Configuration** threshold settings:

Falling Threshold	Set the threshold for clearing the EX3500 CPU (processor) utilization alarm. Once the rising threshold is exceeded, the CPU (processor) utilization must drop below this threshold for the alarm to clear. The threshold is set as a percentage from 1 - 100, with a default of 70.
Rising Threshold	Set the notification threshold for EX3500 CPU (processor) utilization as too high. The threshold is set as a percentage from 1 - 100, with a default of 90.

8 Select **OK** when completed to update the EX3500 system threshold settings. Select **Reset** to revert the screen back to its last saved configuration.

12.2.5 EX3500 SNMP Management

Optionally use the *Simple Network Management Protocol* (SNMP) with the EX3500 management policy for statistics gathering, or to fully manage the EX3500. SNMP is an application layer protocol that facilitates the exchange of management information between the controller or service platform and a managed device. SNMP enabled devices listen on port 161 (by default) for SNMP packets from the controller or service platform's management server. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices. The read-only community string is used to gather statistics and configuration parameters from a supported wireless device. The read-write community string is used by a management server to set device parameters. SNMP is generally used to monitor a system's performance and other parameters.

To the EX3500's SNMP management policy configuration:

1 Select **Configuration** from the Web UI.

2 Select **Management**.

3 Refer to the upper, left-hand, portion of the UI and select **EX3500 Management Policy.**

4 The screen lists those EX3500 management policies created thus far. Select **Add** to create a new EX3500 management policy, **Edit** to modify an existing policy or **Delete** to remove an obsolete policy. Existing lists can be copied or renamed as needed.

5 Select the **SNMP** tab.

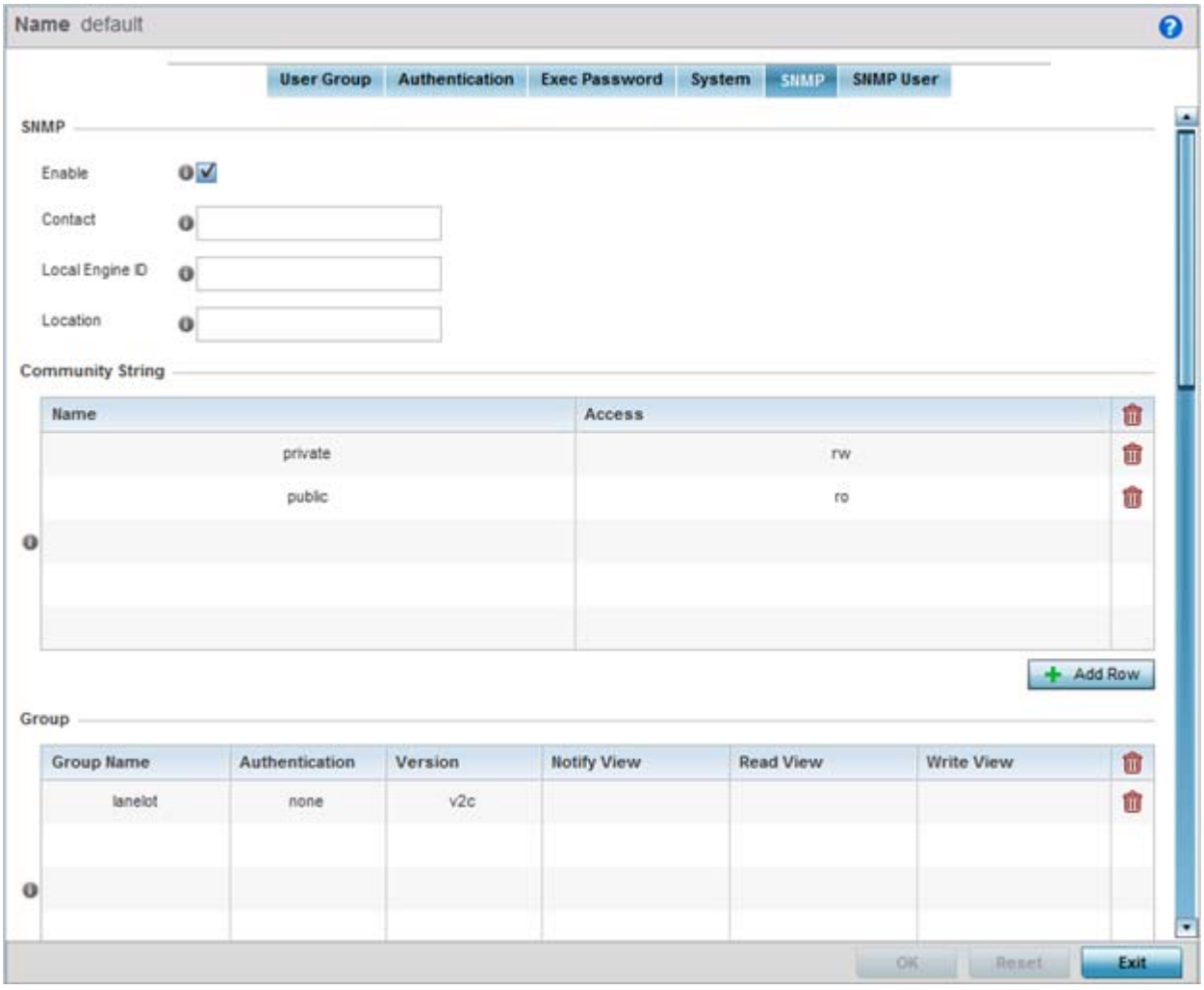


Figure 12-19 *EX35000 Management Policy SNMP screen*

6 Set the following **SNMP** settings:

Enable	Select the checkbox to enable SNMPv1, SNMPv2 or SNMPv3 support. The SNMP version utilized is selected and mapped to a user group within the *Group* table.
Contact	Define a 255 character maximum SNMP contact name for responsible for the WiNG administration of the EX3500 switch.
Local Engine ID	Set a 64 character maximum local engine ID. The local engine ID is the administratively unique identifier of an SNMPv3 engine used for identification, not addressing. There are two parts of an engine ID: *prefix* and *suffix*. The prefix is formatted according to the specifications defined in RFC 3411.
Location	Assign a 255 character maximum EX3500 switch location reflecting the switch's physical deployment location.

7 Select **+ Add Row** and set the following **Community Strings**:

Name	Define a *public* or *private* community designation. By default, SNMPv2 community strings on most devices are set to public, for the read-only community string, and private for the read-write community string.
Access	Set the access permission for each community string used by devices to retrieve or modify information. Available options include: *Read Only* - Allows a remote device to retrieve information. *Read-Write* - Allows a remote device to modify settings.

8 Select **+ Add Row** and set the following **Group** settings for SNMP management of the EX3500:

Group Name	Define a 32 character maximum name for this SNMP group. A maximum of 17 groups can be set for EX3500 model switches.
Authentication	If utilizing SNMPv3 as the version for this group, select whether *auth, noauth* or *priv* is applied to this group as a credential exchange and validation mechanism. This setting is not enabled if utilizing either SNMPv1 or SNMPv2.
Version	Apply either SNMPv1, SNMPv2 or SNMPv3 to this EX3500 SNMP group. SNMP v2 is identical to version 1, but it adds support for 64 bit counters. Most devices support SNMP v2c automatically. However, there are some devices that require you to explicitly enable v2, and that poses no risk. SNMP v3 adds security to the 64 bit counters provided with SNMP v2. SNMP v3 adds both encryption and authentication, which can be used together or separately. Its setup is more complex than just defining a community string. But if you require security, SNMP v3 is recommended.
Notify View	Set a 32 character maximum notify string to restrict and filter the objects in the notification.
Read View	Set an optional 32 character maximum string indicating that users who belong to this group have *read* access to the EX3500 switch.
Write View	Set an optional 32 character maximum string indicating that users who belong to this group have *write* access to the EX3500 switch.

9 Set the following **SNMP Traps** for SNMP event management of the EX3500:

Authentication	Select the checkbox to enable trap generation for user authentication events when accessing a EX3500 switch from a WiNG managed controller. This feature is disabled by default.
Enable SNMP Trap	Select the checkbox to enable EX3500 MAC generation traps. When enabled a trap is generated when a dynamic MAC address is added or removed to/from the switch's address table. This feature is disabled by default.
Link Up Down	Select this option to generate a trap a when either a link is established or broken between the EX3500 switch and a connected device (WiNG managed or not).

10 Refer to the **SNMP View** table and select **+ Add Row** to include or exclude up to 31 SNMP views.

View Name	Enter a 32 alphanumeric character maximum name to identify the EX3500 SNMP MIB view. A view is a set of MIB view subtrees, or a family of subtrees, where each is a subtree within the managed object naming tree. Create MIB views to control the OID range that SNMPv3 users can access.

OID Tree	Provide an OID string to include or exclude from the view. The OID string is 128 characters in length.
View Access	Designate whether view access is *included* or *excluded* for the subtree or family of subtrees from the MIB view. If creating an excluded view subtree, consider creating a corresponding included entry with the same view name to allow subtrees outside of the excluded subtree to be included.

11 Refer to the **Notify Filter** table and select **+ Add Row** to set up to 5 remote resources for archive and retrieval.

Name	Enter a 26 character maximum name for the filter. Notifications indicate erroneous user authentication requests, restarts, connection closures, connection loss to a neighbor router or other events.
Remote Host	Provide a destination IP address for a remote server resource for trap filters.

12 Refer to the **Remote Engine** table and select **+ Add Row** to set up to 5 remote IDs and addresses.

Remote Engine IP	Enter a remote engine IP address for the remote SNMP agent of the device where the user resides.
Remote Engine Id	Provide an Id 9 - 64 characters in length. If configuring the EX3500 management for SNMP V3, is it necessary to configure an engine ID, as passwords are localized using the SNMP ID of the SNMP engine. The remote agent's SNMP engine ID is needed when computing authentication from a password.

13 Refer to the **Host** table and select **+ Add Row** to set the trap receiver host configuration.

Authentication	If using SNMPv3, define the authentication scheme for user credential validation as either *auth, noauth* or *priv.*
Community String	Provide the 1 - 32 character text community strings for accessing EX3500 switch configuration files. SNMP uses read-only and read-write community strings as an authentication mechanism to monitor and configure supported devices.
Inform	Enable this option to enable an EX3500 switch to send inform requests to SNMP managers.Traps are not as reliable than informs since an acknowledgment is not sent from the receiving end when a trap is received. A SNMP manager that receives an inform acknowledges the message with an SNMP response.
IP	Define the trap receiver's IP address.
Retry	Set the number of server connection retries (from 1 - 255). When no response is received after the last retry attempt, the connection session is terminated with the trap receiver IP address.
Timeout	Configures the duration (in seconds) the host connection process is shutdown temporarily before a reset of the process is attempted for the set number of retries.
UDP Port	Set the port of the server resource dedicated to receiving EX3500 switch SNMP traps. The default port is port 162.

Version	Set whether SNMP version 1, 2 or 3 is used with this dedicated host. Versions 1 and 2 provide no data security. SNMPv3 adds security and remote configuration capabilities to previous versions. The SNMPv3 architecture introduces the *user-based security model* (USM) for message security and the *view-based access control model* (VACM) for access control.

12.2.6 EX3500 SNMP Users

An EX3500 SNMP management session utilizes unique SNMP users with specific authentication and privacy parameters.

To administrate EX3500 SNMP users and their permissions:

1 Select **Configuration** from the Web UI.

2 Select **Management**.

3 Refer to the upper, left-hand, portion of the UI and select **EX3500 Management Policy.**

4 The screen lists those EX3500 management policies created thus far. Select **Add** to create a new EX3500 management policy, **Edit** to modify an existing policy or **Delete** to remove an obsolete policy. Existing lists can be copied or renamed as needed.

5 Select the **SNMP User** tab.

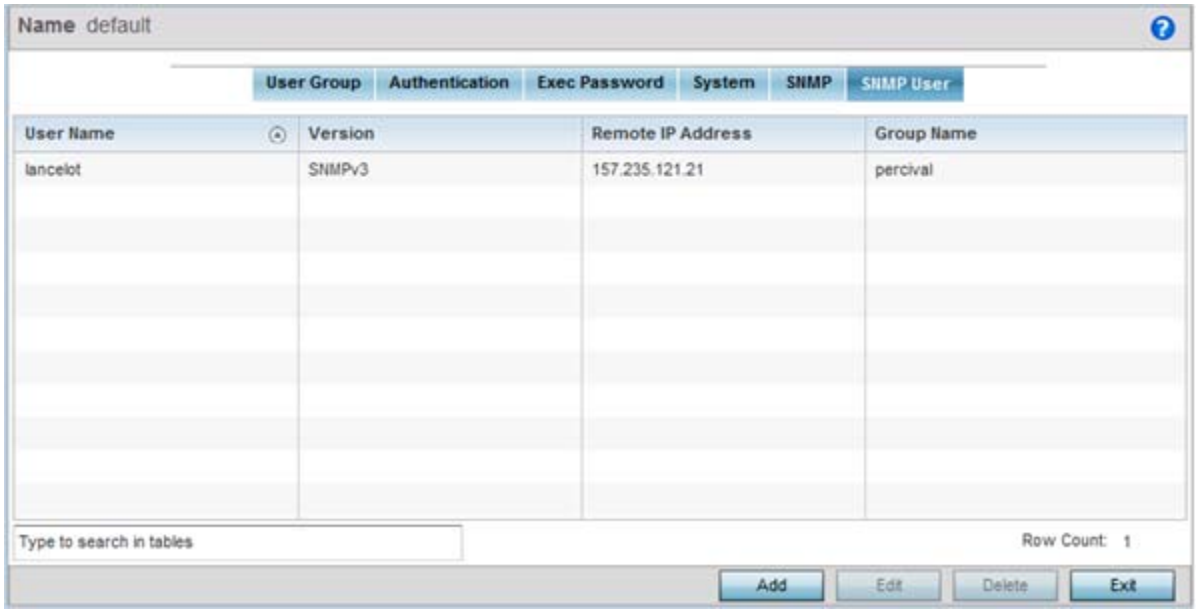


Figure 12-20 *EX3500 SNMP User screen*

6 Review the following EX3500 SNMP user credentials to determine whether a new user requires creation on an existing user configuration needs modification:

User Name	Displays the 32 character maximum SNMP user name assigned the specific SNMP version and remote SNMP server resource listed. More than one user can be assigned to the same EX3500 SNMP user group.

Version	Lists whether SNMPv1, SNMPv2 or SNMPv3 is applied to this EX3500 SNMP user. SNMP v2 is identical to version 1, but it adds support for 64 bit counters. Most devices support SNMP v2c automatically. However, there are some devices that require you to explicitly enable v2, and that poses no risk. SNMP v3 adds security to the 64 bit counters provided with SNMP v2. SNMP v3 adds both encryption and authentication, which can be used together or separately. Its setup is more complex than just defining a community string. But if you require security, SNMP v3 is recommended.
Remote IP Address	Lists the remote server resource designated for receiving SNMP trap and inform event messages for the listed SNMP user.
Group Name	Lists the 32 character maximum name assigned to this SNMP group, as SNMP access rights are organized by groups. The trap group name can be any string and is embedded in the community name field of a trap. A maximum of 17 groups can be set for EX3500 model switches.

7 Select **Add** to create a new user configuration or **Edit** to modify the attributes of an existing EX3500 SNMP user configuration.

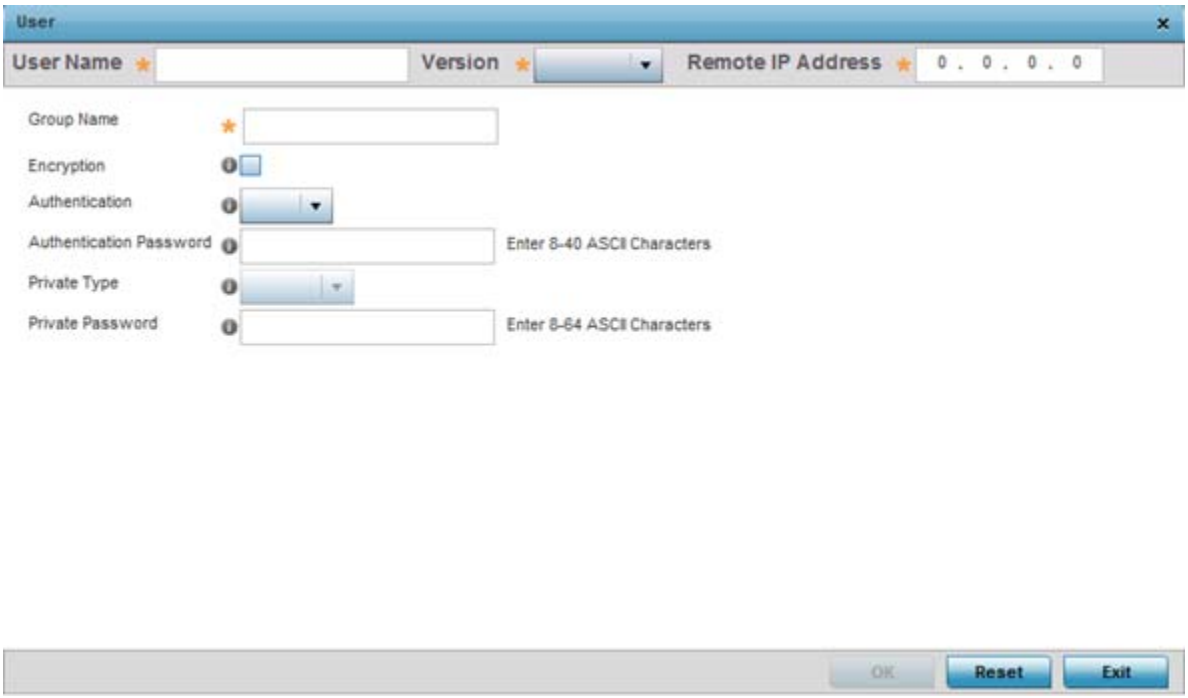


Figure 12-21 *EX3500 SNMP User Add/Edit screen*

8 Set the following SNMP user credentials for the EX3500 SNMP user:.

User Name	Enter a 32 character maximum SNMP user name for EX3500 SNMP session management.
Version	Use the drop-down menu to define whether SNMPv1, SNMPv2 or SNMPv3 is applied to this EX3500 SNMP user configuration. SNMP v2 is identical to version 1, but it adds support for 64 bit counters. Most devices support SNMP v2c automatically. However, there are some devices that require you to explicitly enable v2, and that poses no risk. SNMP v3 adds security to the 64 bit counters provided with SNMP v2. SNMP v3 adds both encryption and authentication, which can be used together or separately. Its setup is more complex than just defining a community string. But if you require security, SNMP v3 is recommended.

Remote IP Address	Set the remote server resource IP address designated for receiving SNMP trap and inform event messages for this SNMP user.
Group Name	Enter a 32 character maximum for a SNMP group. The group name can be any string and is embedded in the community name field of a SNMP trap.
Encryption	When using SNMPv3, the *Encryption* option becomes available to scramble packet contents and prevent them from exposure to unauthorized sources.
Authentication	When using SNMPv3, the *Authentication* option becomes available to ensure messaging is from a valid source. SNMPv3 uses the *user-based security model* (USM) for message security and the *view-based access control model* (VACM) for access control. USM specifies authentication and encryption. VACM specifies access-control rules.
Authentication Password	Enter a 8 - 40 character ASCII authentication password. The selected authentication password ensures only trusted and authorized users can access an EX3500 SNMP management session.
Private Type	Use the drop-down menu to specify the privacy type. The *Advanced Encryption Standard* (AES) is utilized as one of the privacy protocol options for SNMPv3 messages in either an *aes128*, *aes192* or *aes256* format and are recommended. *3DES* and *des56* are also options, but are considered somewhat insecure and vulnerable to *brute-force-attacks*.
Private Password	Enter a 8 - 64 character ASCII password to secure the privacy type selected.

9 Select **OK** when completed to update the EX3500 SNMP user settings. Select **Reset** to revert the screen back to its last saved configuration.

12.3 Hierarchical Tree

Tree Setup is unique because it is not a policy (which is reused in other objects), but rather a global configuration that represents the tree displayed for *Dashboard*, *Operations* and *Statistics*. However since it is set as a configuration, it follows the standard configuration methods, and requires a *Commit* before it taking effect and a *Save* to become persistent across reboots.

ADSP can run as a virtual machine on NX9500 and NX9510 model service platforms. WiNG communicates with ADSP using a *single sign-on* (SSO) authentication mechanism. Once the user is logged in, WiNG gains access to ADSP without being prompted to login again at ADSP. There is no synchronization between the WiNG and ADSP databases. ADSP has its own user database stored locally within its virtual machine. This local database is accessed if a user logs directly into ADSP.

WiNG and ADSP must be consistent in the manner events are reported up through a network hierarchy to ensure optimal interoperability and event reporting. To provide such consistency, WiNG has added support for an ADSP-like hierarchal tree. The tree resides within WiNG, and ADSP reads it from WiNG and displays the network hierarchy in its own ADSP interface. The hierarchal tree can also be used to launch ADSP modules (like Spectrum Analyzer) directly from WiNG.

NOTE: The Hierarchical tree is available on both controllers and service platforms, but not Access Points.

WiNG uses the following *containers* within the tree to be consistent with ADSP's hierarchy conventions:

- *Country*
- *Region*
- *City*
- *Campus*

Hierarchy rules are enforced in the containers. For example, a *city* can be created under a *country* or *region*, but not vice versa. An RF Domain can be placed in any container. However, there cannot be any additional containers under the RF Domain.
WiNG's RF Domain's already use *areas* and *floors*, and these will continue to work as they currently do. Floors are also numbered to be consistent with ADSP's usage.

To configure a hierarchal tree to use with ADSP:

1 Select **Configuration**.

2 Select **Management**.

3 Refer to the upper, left-hand, portion of the UI and select **Tree Setup**.

The **Tree Setup** screen displays with a System node that requires population with the containers to represent the deployment shared between WiNG and ADSP.

The *Country*, *Region*, *City* and *Campus* containers can be defined in any order, but at least one of these containers is required within the hierarchy before the RF Domain can be added and the hierarchy defined as valid.

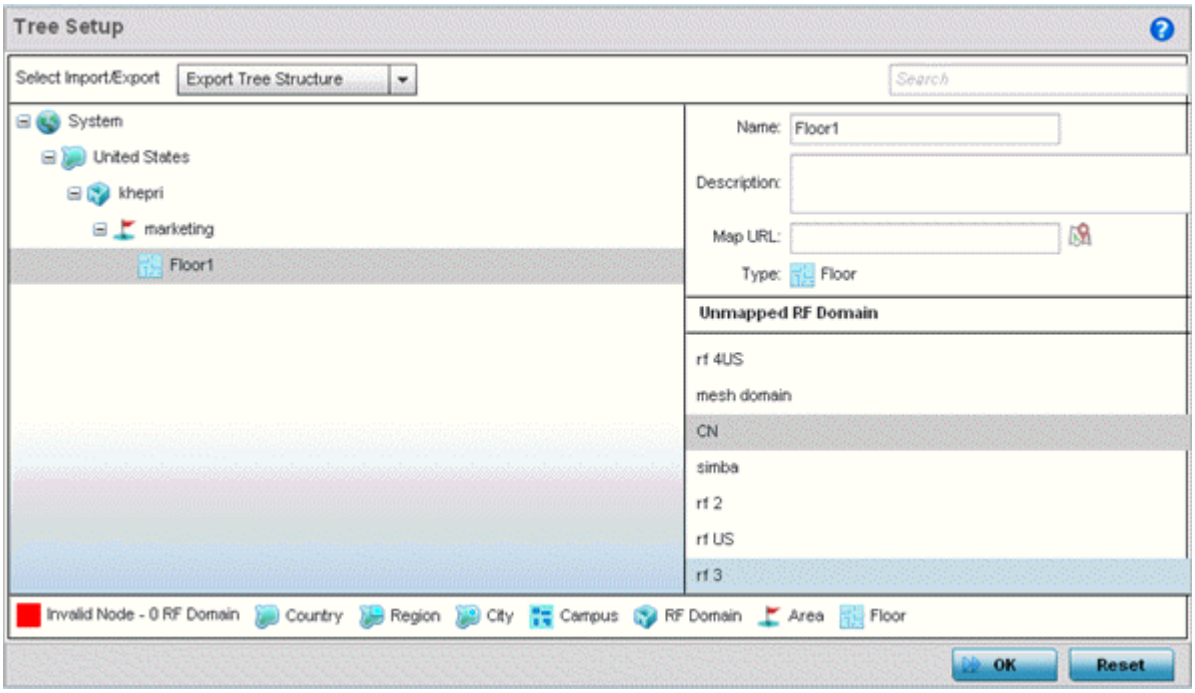


Figure 12-22 *Hierarchal Tree screen*

4 To add a *Country, Region*, *City* or *Campus* to the tree, select **System** from the upper, left-hand, portion of the Tree Setup screen. An add child link displays on the right-hand side of the display.

If adding a **Country**, select a deployment country from the **Type** drop-down menu and use the **Name** drop-down menu to scroll to the country of deployment where the RF Domain resides. Adding a country first is a good idea since regions, city and campus can all be added as child items in the tree structure. However, the selected country is an invalid tree node until a RF Domain is applied.

If adding a region, select **Region** from the **Type** drop-down menu and use the **Name** parameter to enter its name. Select **Add** to display the region. A city and campus can be added as child items in the tree structure under a region. An RF Domain can be mapped anywhere down the hierarchy for a region and not just directly under a Country. For example, a region can have city and campus and one RF Domain mapped.

If adding a **City,** select City from the **Type** drop-down menu and use the **Name** parameter to enter its name. Select **Add** to display the city. Only a campus can be added as a child item under a city. The city is an invalid tree node until a RF Domain is applied somewhere within the directory tree.

If adding a **Campus**, select Campus from the **Type** drop-down menu and use the **Name** parameter to enter its name. Select **Add** to display the campus. A Campus is the last node in the hierarchy before A RF Domain, and it cannot be valid unless it has a RF Domain mapped to it.

NOTE: If a complete tree configuration has been saved and exported for archive to remote location, it can be imported back into the Tree Setup screen and utilized without having to re-configure the containers and RF Domain of that tree. Select **Import** to utilize and existing tree configuration.

NOTE: If a tree container (country, region, city or campus) has a red box around it, it either has invalid attributes or a RF Domain requires addition.

5 Select the add RF Domain link at the right-hand side of any container to display an **Unmapped RF Domain** screen.

6 Provide the default RF Domain name whose deployment area and floor is mapped graphically, and whose events are shared between WiNG and ADSP. Select **Add** to display the RF Domain within its respective place in the tree hierarchy. A default RF Domain can also be dragged into the tree from the right-hand side of the screen.

Once the RF Domain is in the tree, select the add child link at the right-hand side of the RF Domain to display a screen where the RF Domain deployment **Area** and **Floor** are defined. Once define, select **Add** to populate the tree with the Area and Floor.

Provide the **Map URL** to upload the floor plan created under an Area. Each area can have multiple floors

NOTE: While the MAP URL graphic file represents the RF Domain's physical device deployment area, devices cannot be dragged into topology or manipulated. To define a network topology that allows an administrator to add devices and manipulate locations, refer to *Network View on page 4-27*.

7 Edit a tree node at any time by selecting it from amongst the Tree Setup screen, and referring to the right-hand side of the screen where a field displays to modify the container.

8 Optionally, select **Tree Import Export Template** to upload a *template.csv* file if one is needed for container configuration.

A sample of the tree template is provided here for reference.

Row Description

record type (folder),server,Name,Description,Type,Floor Number,Path(slash delimited),Command(add|delete)

Actual Row is CSV file

folder,localhost,US,Country Description,Country,,
folder,localhost,Southeast,Region Description,Region,,US
folder,localhost,Alpharetta,City Description,City,,US/Southeast
folder,localhost,Sanctuary Park,Campus Description,Campus,,US/Southeast/Alpharetta
folder,localhost,The Falls 1125,Domain Description,RFDomain,,US/Southeast/Alpharetta/Sanctuary Park
folder,localhost,Queens,,Area,,US/Southeast/Alpharetta/Sanctuary Park/The Falls 1125
folder,localhost,FloorQLab,,Floor,1,US/Southeast/Alpharetta/Sanctuary Park/The Falls 1125/Queens
folder,localhost,FloorSLab,,Floor,2,US/Southeast/Alpharetta/Sanctuary Park/The Falls 1125/Queens
folder,localhost,FloorTLab,,Floor,3,US/Southeast/Alpharetta/Sanctuary Park/The Falls 1125/Queens

In the CSV file, configure specific tree node properties.

Index 1 : Record Type. This value is always 'folder'. Import/export allows the configuration of folder nodes only. Leaf nodes cannot be configured like devices.

Index 2 : Server Name. This value is always 'localhost' as we are supporting the import/export from localhost only.

Index 3 : Name. This configures the name/label of the tree node. This is the value which is visible to the user in Tree node.

Index 4 : Description. This configures the additional information in form, which user wants to store with the Tree node.

Index 5 : Type. This configures the type of the Tree node. Type can take one of the value "country, region, city, campus, rfdomain, area, floor".

Index 6 : Floor Number. This is configures the floor number. This is applicable only for the floor node.

Index 7 : Path. This is /'(slash delimited) from the 'root'.

Index 8 : add|delete. Allows manipulation of the node. If no value is specified, the default is 'add' . If value is 'delete' then reference node is removed.

9 Select **Import Tree Structure** to optionally import a .csv file with pre-defined the containers and RF Domain. Importing an existing tree saves an administrator from creating a new one from the beginning.

10 Once the tree topology is defined to your satisfaction, select **Export Tree Structure** to archive the tree topology (in .csv file format) to a defined location.

The exported tree topology can be re-imported and automatically displayed within the Tree Setup screen at any time.

11 Select **OK** to update the tree setup configuration. Select **Reset** to revert to the last saved configuration.

NOTE: Since the tree is set as a configuration, it follows standard configuration methods, and requires a *Commit* before it taking effect and A *Save* to become persistent across reboots.

12.4 Management Access Deployment Considerations

Before defining a access control configuration as part of a Management Access policy, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Unused management protocols should be disabled to reduce a potential attack against managed resources. For example, if a device is only being managed by the Web UI and SNMP, there is no need to enable CLI interfaces.
- Use management interfaces providing encryption and authentication. Management services like HTTPS, SSH and SNMPv3 should be used when possible, as they provide both data privacy and authentication.
- By default, SNMPv2 community strings on most devices are set to *public* for the read-only community string and *private* for the read-write community string. Legacy devices may use other community strings by default.
- SNMPv3 should be used for SNMP device management, as it provides both encryption, and authentication.
- Enabling SNMP traps can provide alerts for isolated attacks at both small managed radio deployments or distributed attacks occurring across multiple managed sites.
- Whenever possible, centralized RADIUS management should be enabled. This provides better management and control of management usernames and passwords and allows administrators to quickly change credentials in the event of a security breach.

13 Diagnostics

Resident diagnostic capabilities enable administrators to understand how devices are performing and troubleshoot issues impacting device performance. Performance and diagnostic information is collected and measured on controllers and service platforms for any anomalies potentially causing a key processes to fail.

Numerous tools are available within the Diagnostics menu. Some filter events, others allow you to view logs and manage files generated when hardware or software issues are detected.

The diagnostics are managed as follows:

- *Fault Management*
- *Crash Files*
- *Advanced Diagnostics*

13.1 Fault Management

Fault management enables user's administering multiple sites to assess how individual devices are performing and review issues impacting the network. Use the Fault Management screens to administrate errors generated by the controller or service platform, Access Point or wireless client.

To assess the Fault Management configuration:

1 Select **Diagnostics** > **Fault Management**.

The **Filter Events** screen displays by default. Use this screen to configure how events are tracked. By default, all events are enabled, and an administrator has to turn off events that do not require tracking.

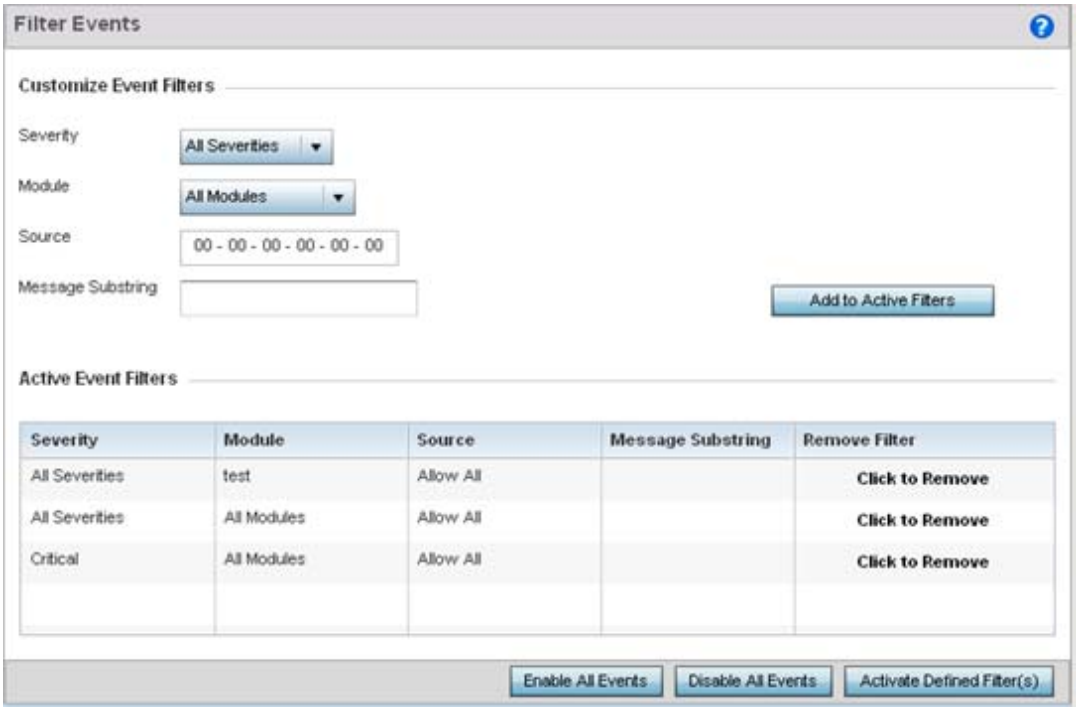


Figure 13-1 *Fault Management Filter Events screen*

Use the **Filter Events** screen to create filters for managing detected events. Events can be filtered based on severity, module received, source MAC, device MAC and client MAC address.

2 Define the following **Customize Event Filters** parameters for the Fault Management configuration:

Severity	Set the filtering severity. Select from the following: *All Severities* – All events are displayed, irrespective of their severity *Critical* – Only critical events are displayed *Error* – Only errors and above are displayed *Warning* – Only warnings and above are displayed *Informational* – Only informational and above events are displayed
Module	Select the module from which events are tracked. When a module is selected, events from other modules are not tracked. Remember this when interested in events generated by a particular module. Individual modules can be selected (such as *TEST*, *LOG*, *FSM* etc.) or all modules can be tracked by selecting *All Modules*.
Source	Set the MAC address of the source device to be tracked. Setting a MAC address of 00:00:00:00:00:00 allows all devices to be tracked.
Message Substring	Optionally append a text message (substring) to the event filter to assist the administrator in distinguishing this filter from others with similar attributes.

NOTE: Leave the fields to a default value of 00:00:00:00:00:00 to track all MAC addresses.

3 Select the **Add to Active Filters** button to create a new filter and add it to the **Active Event Filters** table. When added, the filter uses the current configuration defined in the Customize Event Filters field.

4 Refer to the **Active Event Filters** table to set the following parameters for the Fault Management configuration:

a. To activate all the events in the Active Events Filters table, select the **Enable All Events** button. To stop event generation, select **Disable All Events**.

b. To enable an event in the Active Event Filters table, click the event to select it. Then, select the **Activate Defined Filter(s)** button.

NOTE: Filters cannot be persisted across sessions. They have to be created every time a new session is established.

5 Select **View Events** from the upper, left-hand, side of the **Diagnostics** > **Fault Management** menu.

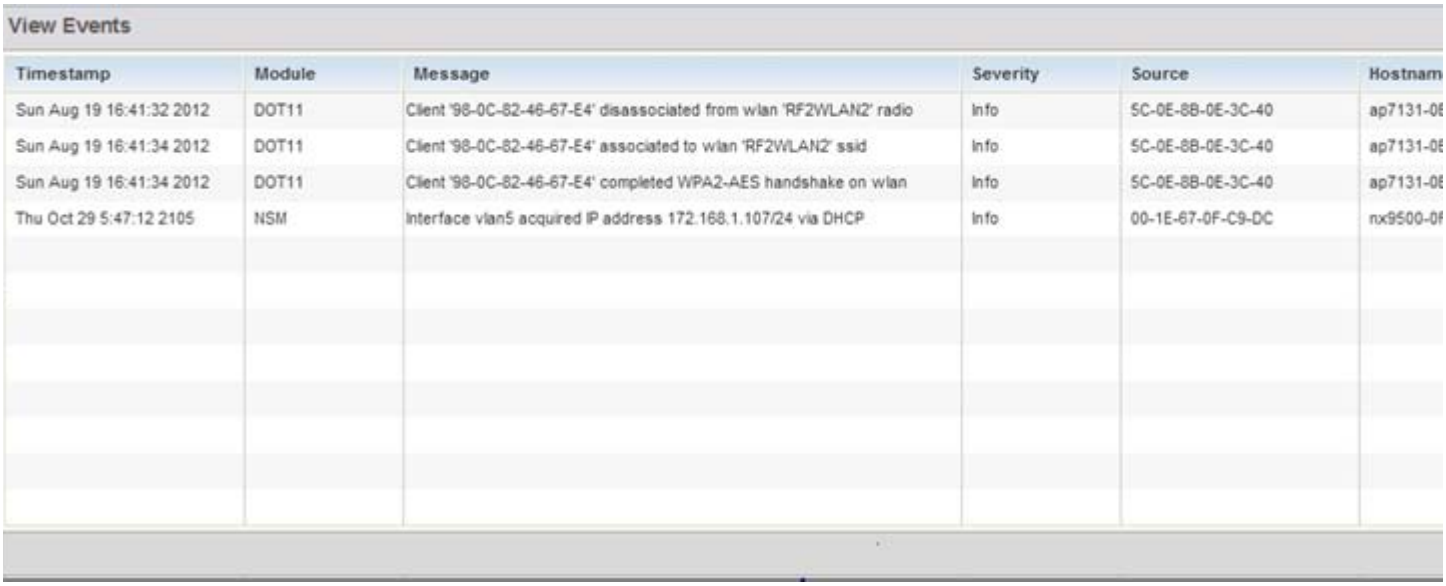


Figure 13-2 *Fault Management View Events screen*

Use the **View Events** screen to track and troubleshoot events using the source and severity levels defined in the Configure events screen.

6 Define the following **Customize Event Filters** parameters for the Fault Management configuration:

Timestamp	Displays the Timestamp (time zone specific) when the fault occurred.
Module	Displays the module used to track the event. Events detected by other module are not tracked.
Message	Displays error or status messages for each event listed.
Severity	Displays the severity of the event as defined for tracking from the Configuration screen. Severity options include: *All Severities* – All events are displayed irrespective of their severity *Critical* – Only critical events are displayed *Error* – Only errors and above are displayed *Warning* – Only warnings and above are displayed *Info* – Only informational and above events are displayed
Source	Displays the MAC address of the tracked source device.
Hostname	Lists the administrator assigned hostname of the tracked source device.

7 Select **Clear All** to clear events and begin new event data gathering.

8 Select **Event History** from the upper, left-hand, side of the **Diagnostics** > **Fault Management** menu.

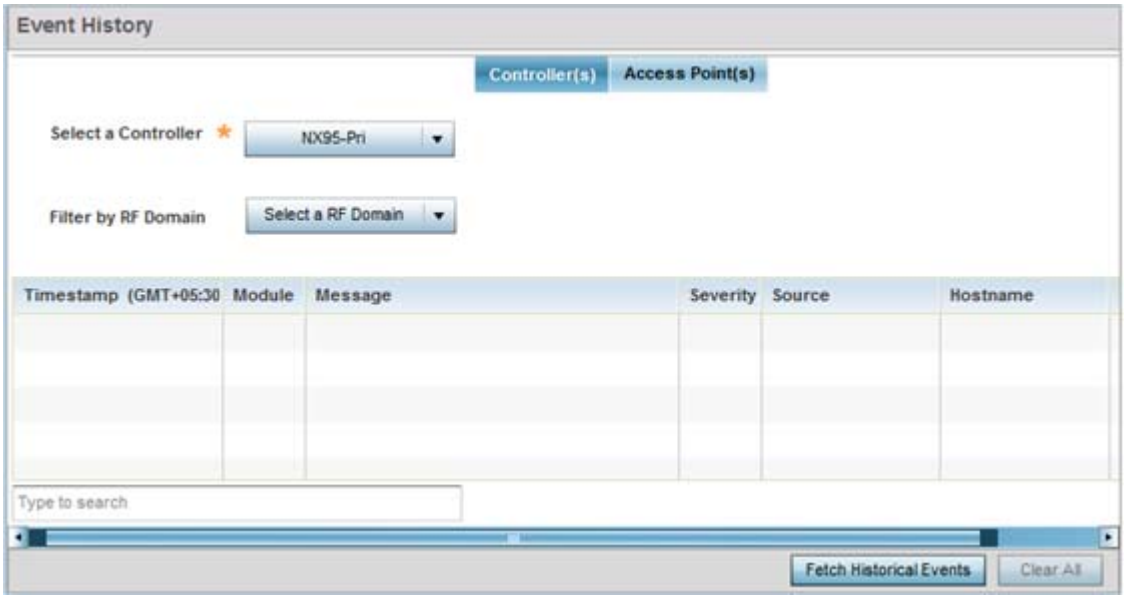


Figure 13-3 *Fault Management Event History screen*

The **Event History** screen displays events for controllers, service platforms and Access Points. The Controller(s) tab displays by default. Information on this tab can be filtered by controllers and service platforms, then further by a RF Domain. Similarly, the Access Point(s) tab displays information for each RF Domain on the Access Point and this information can be further filtered on the devices adopted by this Access Point.

9 Within the *Controller(s)* tab, select the controller from the **Select a Controller** field to filter events to display. To filter messages further, select a RF Domain from the **Filter by RF Domain** field.

10 Within the *Access Point(s)* tab, select the RF Domain from the **Select a RF Domain** field to filter events to display. To filter messages further, select a device from the **Filter by Device** field.

11 Select **Fetch Historical Events** from the lower, right-hand, side of the UI to populate the table with either device or RF Domain events. The following event data is fetched and displayed:

Timestamp	Displays the Timestamp (time zone specific) when the fault occurred.
Module	Displays the module used to track the event. Events detected by other module are not tracked.
Message	Displays error or status messages for each event listed.
Severity	Displays the severity of the event as defined for tracking from the Configuration screen. Severity options include: *All Severities* – All events are displayed irrespective of their severity *Critical* – Only critical events are displayed *Error* – Only errors and above are displayed *Warning* – Only warnings and above are displayed *Info* – Only informational and above events are displayed
Source	Displays the MAC address of the source device tracked by the selected module.
Hostname	Lists the administrator assigned hostname of the source device tracked by the selected module.

RF Domain	Displays the RF Domain membership of the source device tracked by the selected module.

12 Select **Clear All** to clear events and begin new event data gathering.

13.2 Crash Files

Use the **Crash Files** screen to review files created when a controller or service platform encounters a critical error or malfunction. Use crash files to troubleshoot issues specific to the device on which a crash event was generated. These are issues impacting the core (distribution layer). Once reviewed, files can be deleted or transferred for archive. Crash files can be sent to a support team to expedite issues with the reporting device.

1 Select **Diagnostics** > **Crash Files** to display the crash file information.

Once a target device has been selected its crash file information displays in the viewer on the right.

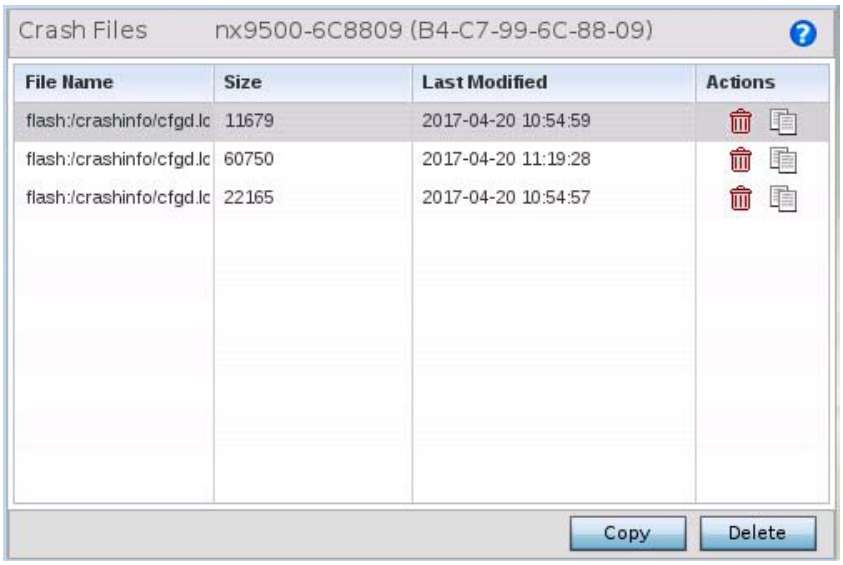


Figure 13-4 *Crash Files information*

2 Refer to the following crash file information for the selected device.

File Name	Displays the name of the file generated when a crash event occurred. This is the file available for copy to an external location for archive and remote administration.
Size	Lists the size of the crash file, as this information is often needed when copying files to an external location.
Last Modified	Displays the Timestamp (time zone specific) when the most recent update to the file occurred.
Actions	Displays the action taken in direct response to the detected crash event.

3 Select **Copy** to copy a selected crash file to an external location. Select **Delete** to remove a selected crash file.

13.3 Advanced Diagnostics

Refer to Advanced UI Diagnostics to review and troubleshoot any potential issue with the resident *User Interface* (UI). The UI Diagnostics screen provides diagnostic tools to identify and correct issues with the UI. Diagnostics can also be performed at the device level for the Access Point radios and connected clients.

13.3.1 UI Debugging

Advanced Diagnostics

Use the UI Debugging screen to view debugging information for a selected device.

To review device debugging information:

1 Select **Diagnostics** > **Advanced** > **UI Debugging** to display the UI Debugging menu options.
The UI debugging information displays within the **NETCONF Viewer** by default.

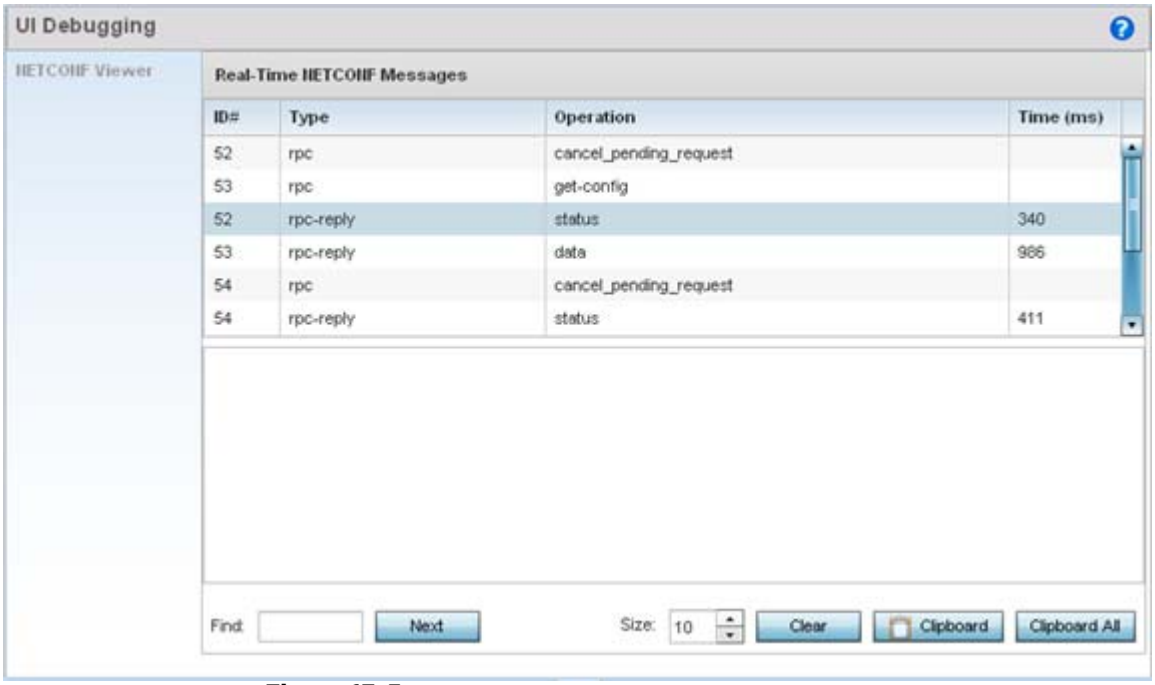


Figure 13-5 *UI Debugging screen - NETCONF Viewer*

2 Use the **NETCONF Viewe**r to review NETCONF information. NETCONF is a proprietary tag-based configuration protocol for devices. Messages are exchanged using XML tags.

3 The **Real Time NETCONF Messages** area lists an XML representation of any message generated by the system. The main display area of the screen is updated in real time.

4 Refer to the **Request Response** and **Time Taken** fields on the bottom of the screen to assess the time to receive and respond to requests. The time is displayed in microseconds.

5 Use the **Clear** button to clear the contents of the Real Time NETCONF Messages area. Use the **Find** parameter and the **Next** button to search for message variables in the Real Time NETCONF Messages area.

13.3.2 Viewing UI Logs

Advanced Diagnostics

Use the UI logs to periodically assess *user interface* (UI) events by type, category and severity to assess whether any administrative corrective actions are warranted.

To view UI log information:

1 Select **Diagnostics** > **Advanced** > **View UI Logs** to display the *Flex Logs* and *Error Logs* screens. The Flex Logs screen displays by default, but both tabs list the same information for either UI logs or UI error logs respectively.

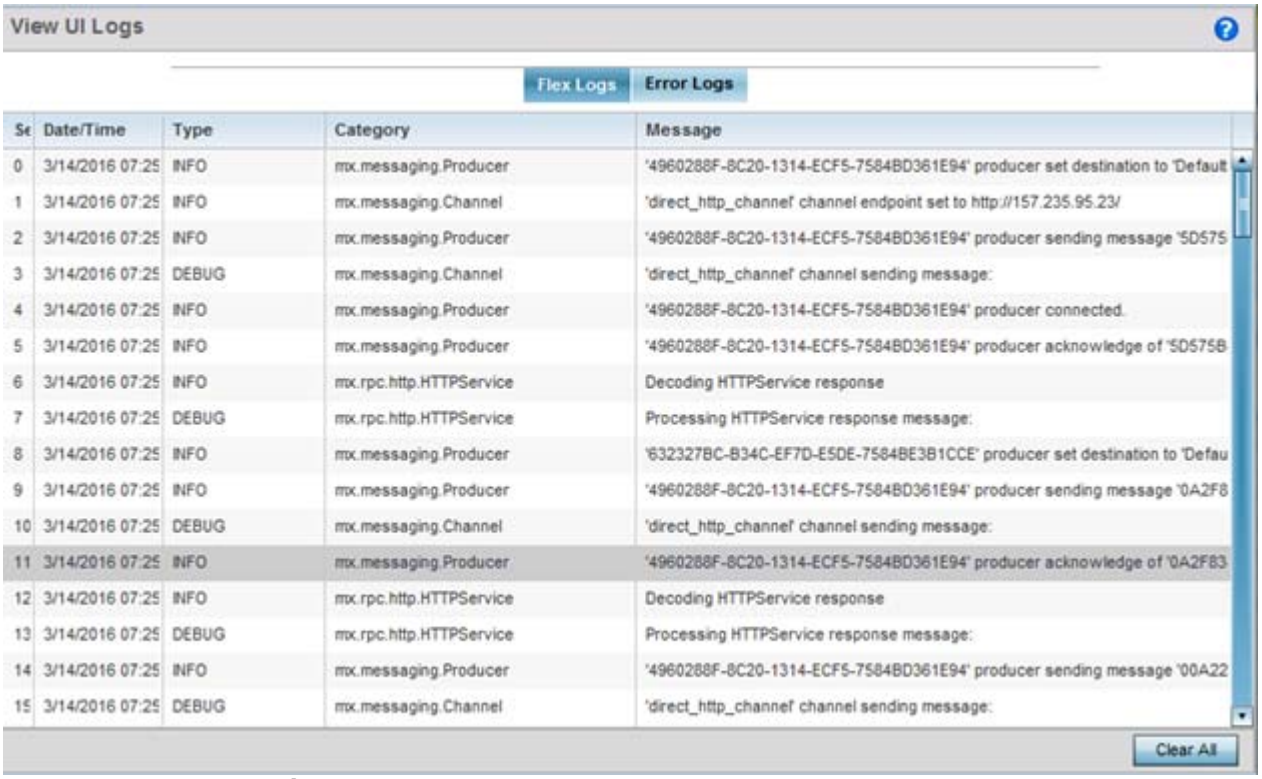


Figure 13-6 *View UI Logs screen - Flex Logs tab*

2 Refer to the following UI event or error log parameters:

Sequence	Displays a numeric number for the generation of the listed UI events. If changing the data display from a sequential display, these numbers can be used to assess the chronology of the UI event generation.
Date/Time	Lists the date and time when each listed UI log event occurred. Use this information to assess whether time was factor in the generation of one or more events and whether their timestamp increases their significance.
Type	Displays each listed log entry's event or error type. Some events are DEBUG while others are INFO. Categorize collectively as specific events warrant additional administration.
Category	Lists each event or error's system defined category as a means of further filtering specific events or system collected error logs. This is helpful when assess whether specific events or errors impact multiple UI functions.

Message	Displays the system generated message for the functions impacted by each listed UI or error. Use this data in combination with the date, type and category to assess whether specific messages are related and their significance worthy of immediate administration.

3 Select **Clear All** to remove all the log or error entries from the screen and begin a new data collection.

13.3.3 Viewing UI Sessions

Advanced Diagnostics

Refer to the **View Sessions** screen to assess specific user interface sessions by individual user.s

To view UI session information:

1 Select **Diagnostics** > **Advanced** > **View Sessions**.

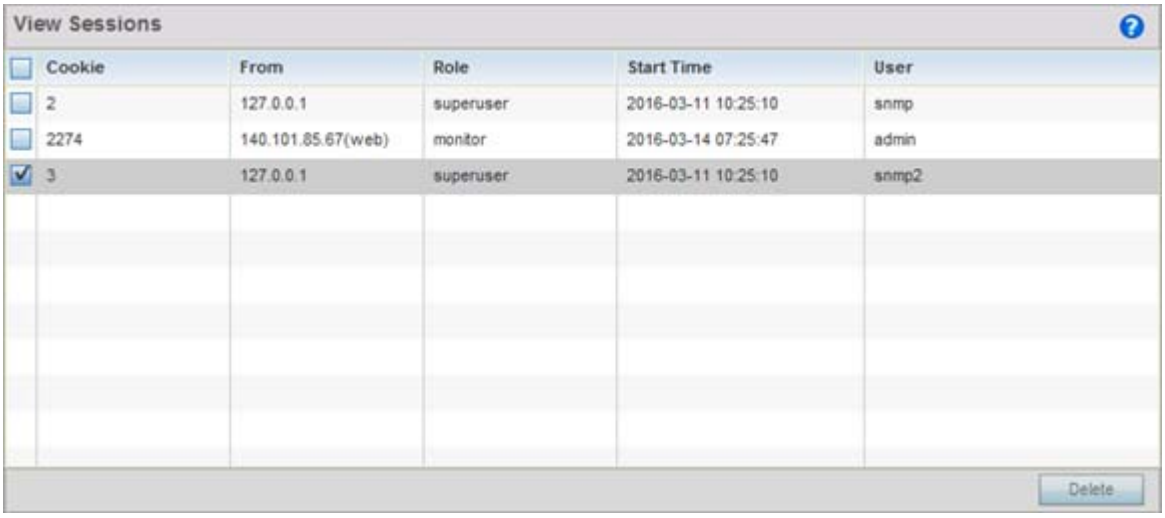


Figure 13-7 *View Sessions Screen*

2 Refer to the following UI session data to assess its significance:

Cookie	Displays a numeric session cookie which identifies the session corresponding to it. This information can be used to further filter specific user sessions to the network route used.
From	Lists the numeric IP address used by each listed user as their network identifier into the WiNG user interface.
Role	Displays each user's defined administrative role. Each role has different access and administrative privileges.
Start Time	Lists the time each listed user began their WiNG interface UI session. Does this start time correspond to a known UI event or error condition?
User	Displays each user's SNMP administrative access protocol and their session permissions.

3 Select a specific user session and **Delete** to remove the selected session from those listed for administration.

14 Operations

The functions within the controller or service platform's *Operations* menu allow firmware and configuration files management and certificate generation for managed devices. In a clustered environment, these operations can be performed on one controller or service platform, then propagated to each member of the cluster and onwards to the devices managed by each cluster member.

A certificate links identity information with a public key enclosed in the certificate. Device certificates can be imported and exported to and from the controller or service platform to a secure remote location for archive and retrieval as they are required for application to other managed devices.

Self Monitoring At Run Time RF Management (Smart RF) is an innovation designed to simplify RF configurations for new deployments, while (over time) providing on-going deployment optimization and radio performance improvements. The Smart RF functionality scans the managed network to determine the best channel and transmit power for each managed Access Point radio. Smart RF policies can be applied to specific RF Domains, to add site specific deployment configurations and self recovery values to groups of devices within pre-defined physical RF coverage areas.

For more information, refer to the following:

- *Device Operations*
- *Certificates*
- *Smart RF*

14.1 Device Operations

Updated device firmware and configuration files are periodically released to the Support Web site. If an Access Point's (or its associated device's) firmware is older than the version on the Web site, update to the latest firmware version for full feature functionality and optimal controller or service platform utilization. Additionally, selected devices can either have a primary or secondary firmware image applied or fallback to a selected firmware image if an error occurs in the update process.

For more information, refer to the following:

- *Operations Summary on page 14-1*
- *Adopted Device Upgrades*
- *Using the File Management Browser*
- *Restarting Adopted Devices*
- *Captive Portal Configuration*
- *Crypto CMP Certificate*
- *RAID Operations*
- *Re-elect Controller*

14.1.1 Operations Summary

Device Operations

The **Summary** screen displays by default when **Operations** is selected from the controller or service platform's main menu bar.

The **Summary** screen displays firmware information for a specific device selected from either the RF Domain or Network tabs on the left-hand side of the screen.

NOTE: When displaying the **Summary** screen at the RF Domain level of the UI's hierarchal tree, the screen does not display a field for a device's **Primary** and **Secondary** firmware image. At the RF Domain level, the Summary screen just lists the *Hostname, MAC Address*, *Online* status, *Device Type* and *Is Controller* designations for the devices comprising the selected RF Domain. A RF Domain must be selected from the hierarchal tree and expanded to list the devices comprising the RF Domain. From there, individual controllers, service platforms and Access Points can be selected and their properties modified.

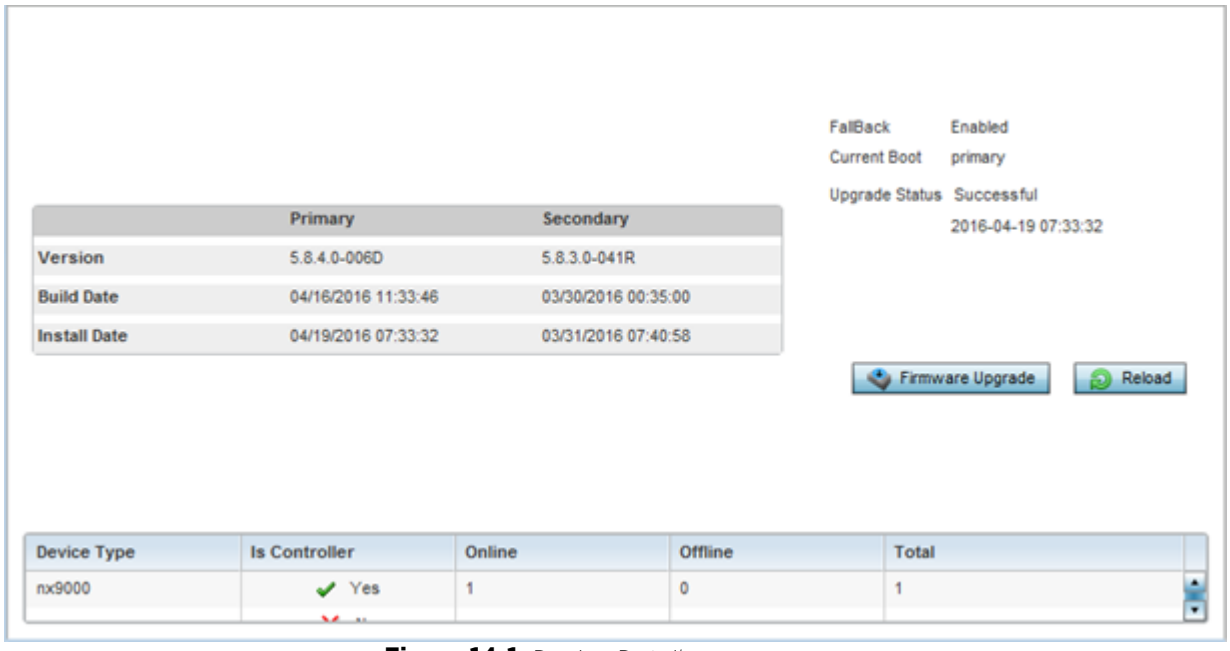


Figure 14-1 *Device Details screen*

1 Refer to the following to determine whether a firmware image needs to be updated for the selected device, or a device requires a restart or revert to factory default settings.

Version	Displays the primary and secondary firmware image version from the wireless controller.
Build Date	Displays the date the primary and secondary firmware image was built for the selected device.
Install Date	Displays the date the firmware was installed for the selected device.
Fallback	Lists whether fallback is currently enabled for the selected device. When enabled, the device reverts back to the last successfully installed firmware image if something were to happen in its next firmware upgrade that would render the device inoperable.
Current Boot	Lists firmware image for the device on the current boot.
Upgrade Status	Displays the status of the last firmware upgrade performed for each listed device managed by this controller or service platform.
Firmware Upgrade	Select this option to display the firmware upgrade window for the selected device. Select the *Apply* button to perform the function.
Reload	Select this option to restart the selected device. Selecting this option restarts the target device using the specified options in the settings window. Restarting a device resets all data collection values to zero. Select the *Reload* button to perform the function.

2 Refer to the device table for basic information for known device types. The device table displays the **Device Type**, **Controller** status, **Online**, **Offline** and **Total** device counts.

14.1.1.1 Upgrading Device Firmware

Operations Summary

Controllers and service platforms can conduct firmware updates on behalf of their managed devices.

To update the firmware of a managed device:

1 Select a device from the browser.

2 Select the **Firmware Upgrade** button.

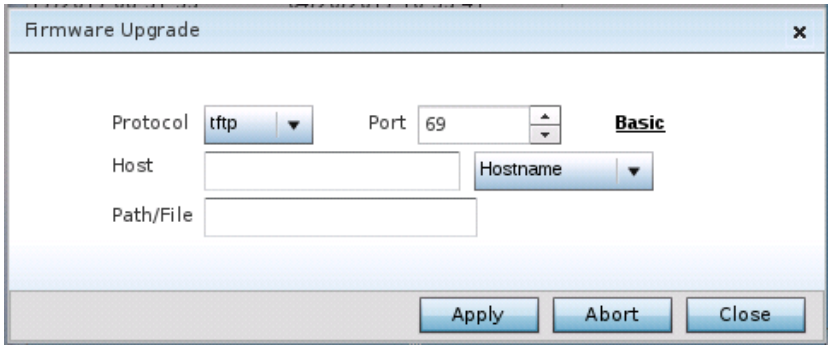


Figure 14-2 *Firmware Update screen*

3 By default, the **Firmware Upgrade** screen displays the server parameters for the target device firmware file.

4 Provide the following information to accurately define the location of the target device firmware file:

Protocol	Select the protocol used for updating the device firmware. Available options include: tftp ftp sftp http cf usb1-4
Port	Use the spinner control or manually enter the value to define the port used by the protocol for firmware updates. This option is not valid for *cf* or *usb1-4*.
Host	Provide the hostname or numeric IPv4 or IPv6 formatted address of the server used to update the firmware. This option is not valid for *cf* and *usb1-4*. A hostname cannot contain an underscore.
User Name	Define the user name used to access either a FTP or SFTP server.
Password	Specify the password for the user account to access a FTP or a SFTP server.
Path/File	Specify the path to the firmware file. Enter the complete relative path to the file on the server.

5 Select **Apply** to start the firmware update. Select **Abort** to terminate the firmware update. Select **Close** to close the upgrade popup. The upgrade continues in the background.

14.1.2 Adopted Device Upgrades

Device Operations

An administrator can designate controllers, service platforms or Access Points as RF Domain managers capable of receiving firmware files from the NOC (NX4500, NX6500, NX7500 or NX9000 series service platforms) then provisioning other devices within their same RF Domain. Controllers, service platforms and Access Points can now all update the firmware of different device models within their RF Domain. However, firmware updates cannot be made simultaneously to devices in different site deployments.

To administer a device upgrade and administrate upgrade status and history:

1 Select the **Operations.**

2 Ensure **Devices** is selected from the Operations menu on the top, left-hand, side of the screen.

3 Expand the System node on the left-hand side of the screen, select a RF Domain and one of its member devices.

4 Select the **Adopted Device Upgrade** tab. The screen displays with the **Device Upgrade List** selected by default.

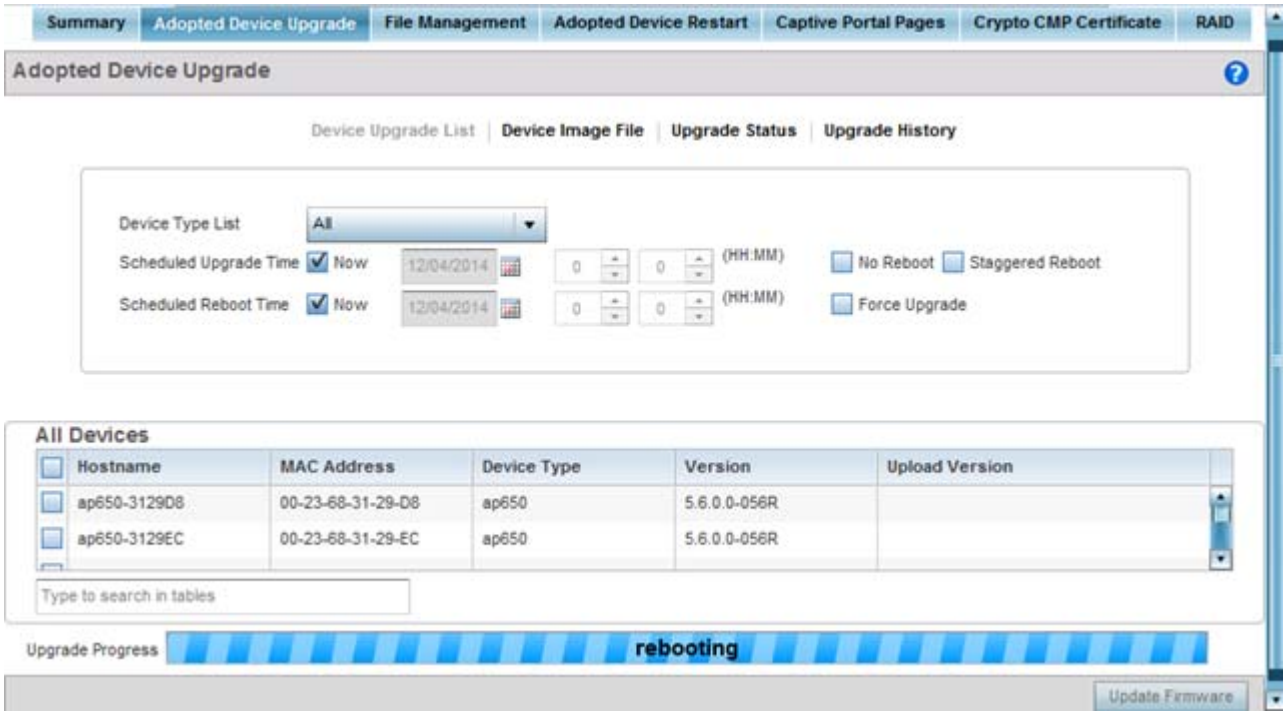


Figure 14-3 *Device Upgrade List screen*

5 Select a controller, service platform or Access Point model from the **Device Type List** drop-down menu. This is the device model intended to provision firmware to the devices selected within the **All Devices** table below.

NOTE: If selecting the **Device Upgrade** screen from the RF Domain level of the UI's hierarchal tree, there's an additional **Upgrade from Controller** option to the right of the *Device Type List*. Select this option to provision selected device models within the same RF Domain from this RF Domain manager. If expanding a RF Domain and selecting a member device, the upgrade tab is entitled **Adopted Device Upgrade**, as an upgrade is made from an elected RF Domain Manager device. There's also an additional **Device Image File** screen to select the device image type and set the transfer protocol.

6 Use the **Scheduled Upgrade Time** option to set when the upgrade occurs. To perform an upgrade immediately, select **Now**. To schedule the upgrade to take place at a specified time, enter a date and time in the appropriate fields.

7 Refer to the **Scheduled Reboot Time** option to schedule when an updated device is rebooted to implement the updated firmware. To reboot immediately, select **Now**. To schedule the reboot to take place at a future time to keep the device in service, enter a date and time in the appropriate fields.

Use the **No Reboot** option to keep from rebooting after an upgrade. Select **Staggered Reboot** to avoid upgrading devices simultaneously and risk bringing down the network. When selected, devices are rebooted incrementally to preserve network availability. Select **Force Upgrade** to initiate an Access Point firmware upgrade and reboot at the present time.

NOTE: The **Scheduled Upgrade Time** and **Scheduled Reboot Time** are your local system's time. They're not the Access Point, controller, service platform or VX time and are not synched with the device.

Use the **All Devices** table to select controller, service platform and Access Point models for firmware updates from the device model selected from the Device Type List.

Refer to the **MAC Address** and **Device Type** values to help determine the specific models available for upgrade within the RF domain. Use the **Version** and **Upload Version** values to assess each listed device's current firmware as well as the firmware version available to a device upgrade.

8 Select **Device Image File**.

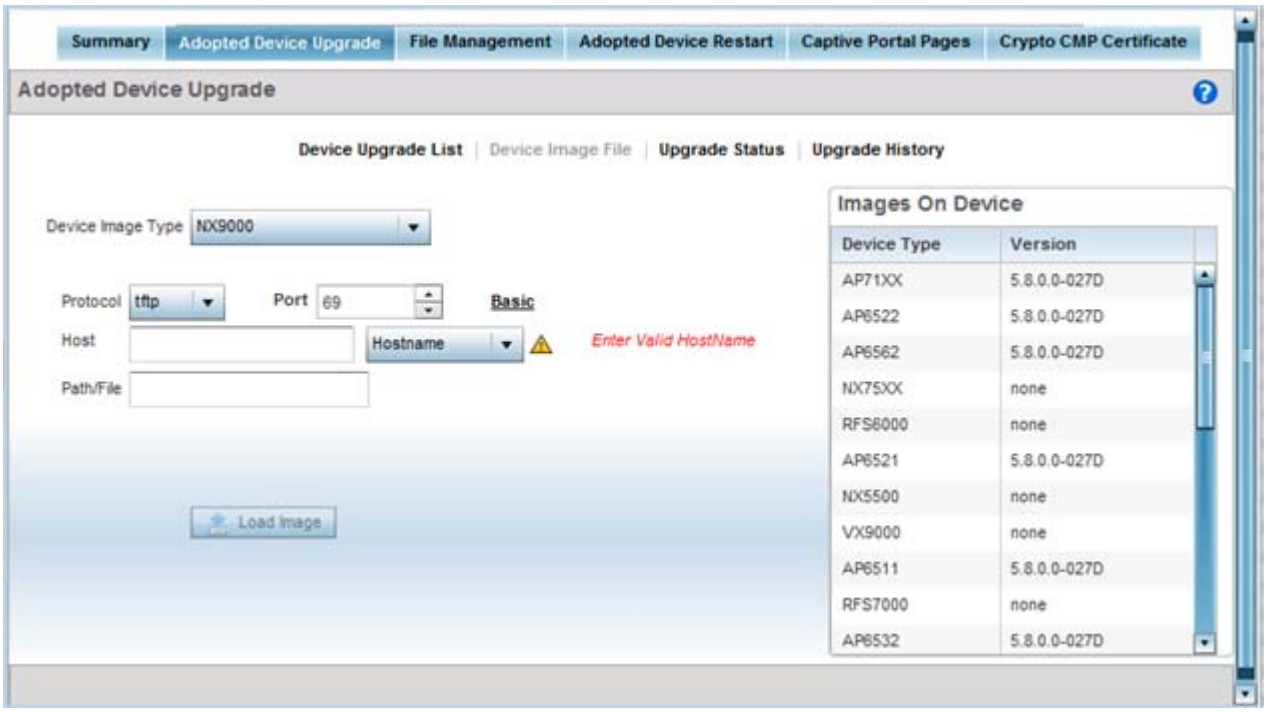


Figure 14-4 *Device Image File screen*

9 Select a controller, service platform or Access Point model from the **Device Image Type** drop-down menu. Selecting **All** makes each controller, service platform and Access Point model images available for updates on those specific models.

10 Select the **Basic** link to enter a **URL** pointing to the location of the controller, service platform or Access Point image files for the device update(s).

11 Selecting Advanced lists additional options for the device's firmware image file location:

Protocol	Select the protocol for device firmware file management and transfer. Available options include: tftp ftp sftp http cf
Port	Designate the port for transferring the firmware files used in the upgrade operation. Enter the port number directly or use the spinner control.

Host	Specify a numerical *IP address* or textual *Hostname* of the resource used to transfer files to the devices designated for a firmware update. A hostname cannot contain an underscore.
Path / File	Define the path to the file on the file repository resource. Enter the complete relative path to the file.

12 Select the **Load Image** button to upload the device firmware in preparation of an upgrade.

The firmware image is loaded to the flash/upgrade directory (not the flash/cache directory). If the NOC pushes the image, then it is loaded to flash/cache/upgrade.

13 Select **Upgrade Status** to assess the administration, scheduling and progress of device firmware updates.

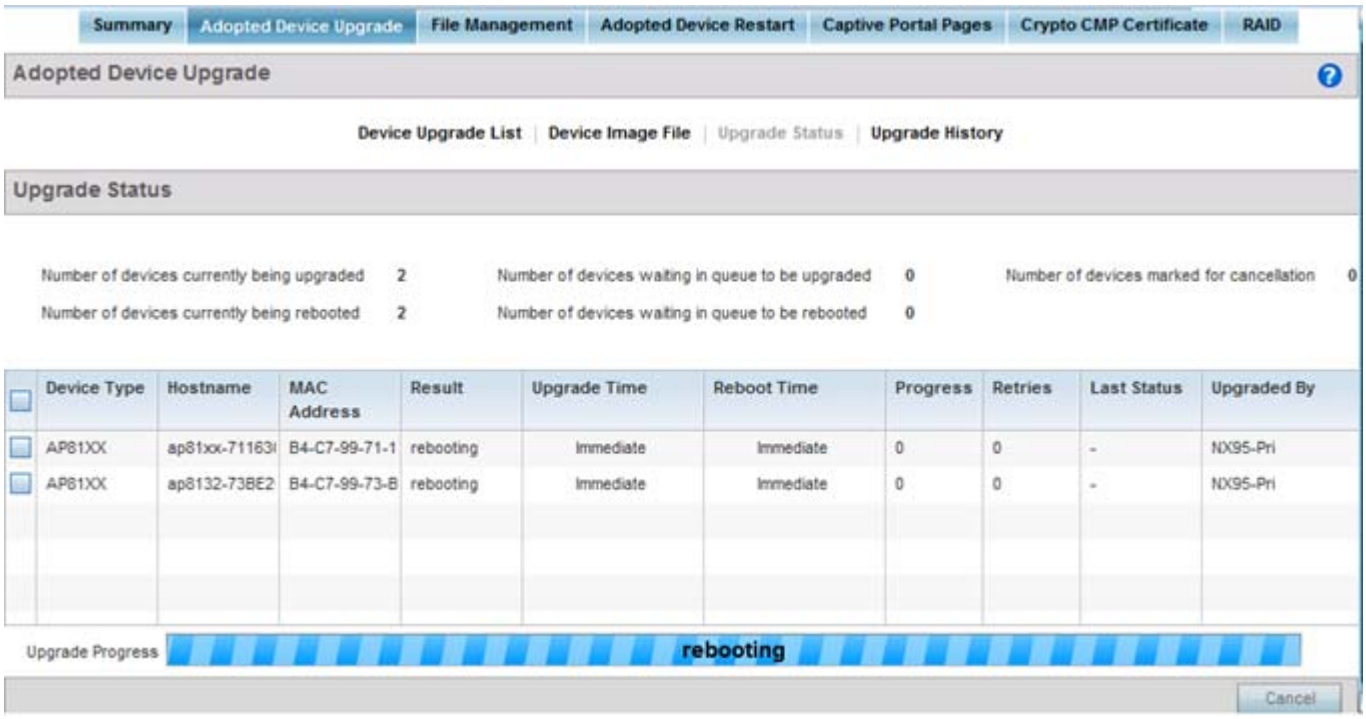


Figure 14-5 *Upgrade Status screen*

14 Refer to the **Upgrade Status** field to assess the completion of in-progress upgrades.

Number of devices currently being upgraded	Lists the number of firmware upgrades currently in-progress and downloading for selected devices. Once the device has the image it requires a reboot to implement the firmware image.
Number of devices currently being booted	Lists the number devices currently booting after receiving an upgrade image. The reboot is required to implement the new image and renders the device offline during that period. Using the *Device Upgrade List*, reboots can be staggered or placed on hold to ensure device remains in service.
Number of devices waiting in queue to be upgraded	Lists the number of devices waiting to receive a firmware image from their provisioning controller, service platform or Access Point. Each device can have its own upgrade time defined, so the upgrade queue could be staggered.

Number of devices waiting in queue to be upgraded	Lists the number of devices waiting to reboot before actively utilizing its upgraded image. The *Device Upgrade List* list allows an administrator to disable or stagger a reboot time, so device reboots may not occur immediately after an upgrade. The reboot operation renders the device offline until completed so reboots can scheduled for periods of reduced load.
Number of devices marked for cancellation	Lists the number of upgrades that have been manually cancelled during the upgrade operation.

15 Refer to the following status reported for each current or scheduled upgrade operation:

Device Type	Displays the model number of devices pending an upgrade. Each listed device is provisioned an image file unique to that model.
Hostname	Lists the factory encoded MAC address of a device either currently upgrading or in the queue of scheduled upgrades.
MAC Address	Lists the factory encoded MAC address of a device either currently upgrading or in the queue of scheduled upgrades.
Result	Lists the state of an upgrade operation (*downloading*, *waiting for a reboot* etc.).
Upgrade Time	Displays whether an upgrade is immediate or set by an administrator for a specific time. Staggering upgrades is helpful to ensure a sufficient number of devices remain in service at any given time while others are upgrading.
Reboot Time	Displays whether a reboot is immediate or time set by an administrator for a specific time. Reboots render the device offline, so planning reboots carefully is central to ensuring a sufficient number of devices remain in service.
Progress	Lists the number of specific device types currently upgrading.
Retries	Displays the number of retries, if any, needed for an in-progress firmware upgrade operation.
Last Status	Lists the last reported upgrade and reboot status of each listed in progress or planned upgrade operation.
Upgraded By	Lists the model of the controller, service platform or Access Point RF Domain manager that's provisioning an image to a listed device.

16 Optionally select **Cancel** (from the lower, right-hand corner of the screen) to cancel the upgrade of devices under the selected RF Domain. The Cancel button is enabled only if there are device undergoing upgrade and they're are selected for cancellation.

17 Select **Upgrade History**.

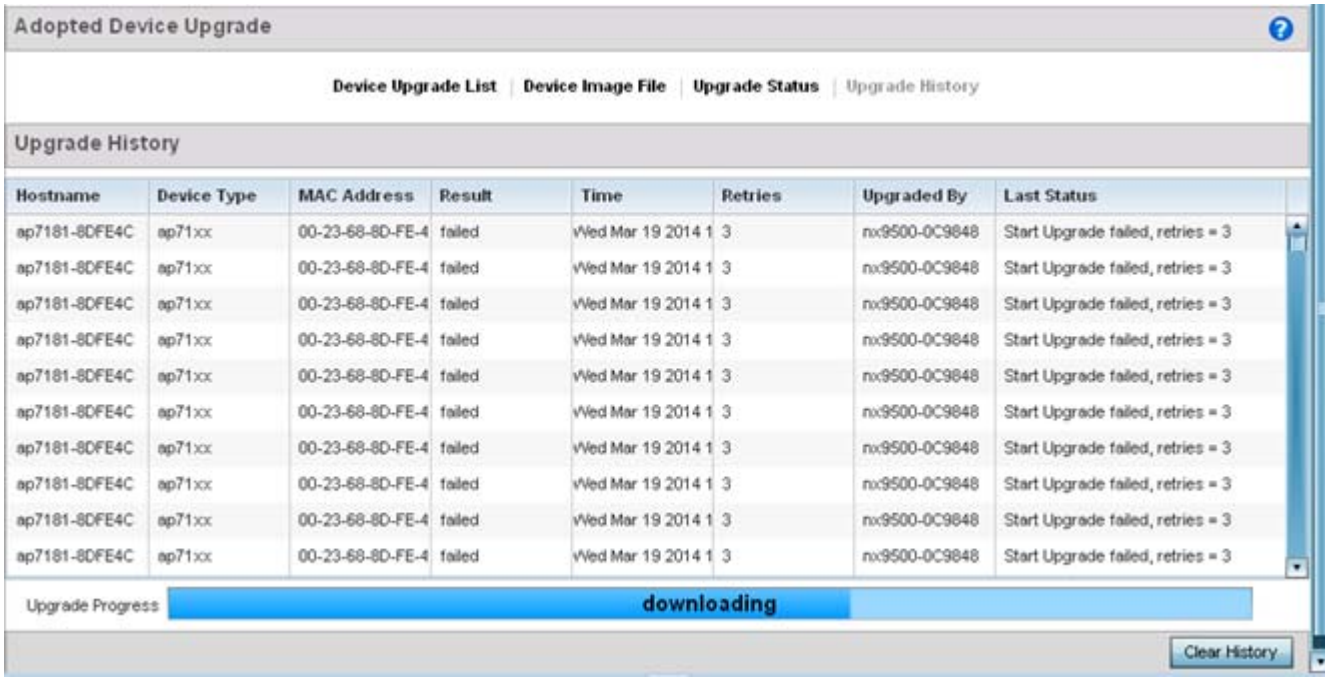


Figure 14-6 *Upgrade History screen*

18 Refer to the following **Upgrade History** status:

Hostname	Displays the administrator assigned Hostname for each listed controller, service platform or Access Point that's received an update.
Device Type	Displays the controller, service platform or Access Point model upgraded by a firmware update operation.
MAC Address	Displays the device *Media Access Control* (MAC) or hardware address for a device that's received an update.
Result	Displays the upgrade result for each listed device.
Time	Displays the time and date of the last status received from an upgraded device.
Retries	Displays the number of retries, if any, needed for the firmware upgrade operation.
Upgraded By	Displays the administrator credentials responsible for initiating each listed upgrade operation.
Last Status	Displays the last status update received for devices that have been upgraded.

19 Select the **Clear History** button to clear the current update information for each listed device and begin new data collections.

14.1.3 Using the File Management Browser

Device Operations

Controllers and service platforms maintain a File Browser allowing an administrator to review the files residing on a controller or service platform's internal or external memory resource. Directories can be created and maintained for each File Browser location and folders and files can be moved and deleted as an administrator interprets necessary.

NOTE: The **File Management** tab is not available at the RF Domain level of the UI's hierarchal tree. A RF Domain must be selected and expanded to display the RF Domain's member devices. Once expanded, selected a RF Domain member device to ensure the File Management UI option is available.

To administer files for managed devices and memory resources:

1 Select the **Operations** > **Devices** > **File Management.**

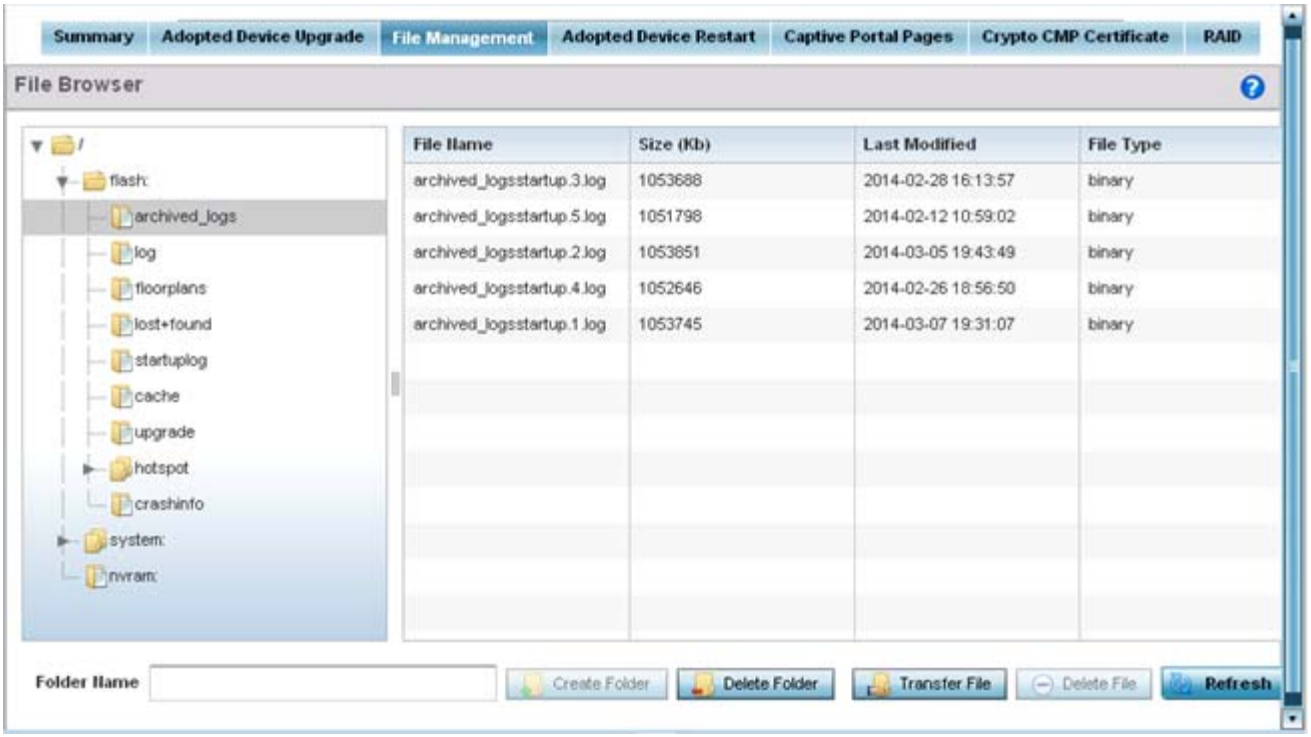


Figure 14-7 *File Browser screen - flash*

2 Refer to the following to determine whether a file needs to be deleted or included in a new folder for the selected internal (flash, system, nvram) or external (cf, USB1-4) memory resource. The following display for each available memory resource:

File Name	Displays the name of the file residing on the selected *flash*, *system*, *nvram* or *usb1-4* location. The name cannot be modified from this location.
Size (Kb)	Displays the size of the file in kb. Use this information to help determine whether the file should be moved or deleted in respect to available system memory.

Last Modified	Lists a timestamp for the last time each listed file was modified. Use this information to determine the file's relevance or whether it should be deleted.
File Type	Displays the type for each file including binary, text or empty.

3 If needed, use the **Create Folder** utility to create a folder that servers as a directory for some or all of the files for a selected memory resource.

4 Select **Transfer File** to invoke a subscreen where the local or server file *source* and *target* (destination) are defined as well as the file transfer protocol and external destination location or resource. For more information, see *Managing File Transfers on page 14-11*.

5 Optionally, use the **Delete Folder** or **Delete File** buttons to remove a folder or file from within the controller, service platform or Access Point's current memory resource.

14.1.3.1 Managing File Transfers

Device Operations

Controllers and service platforms can administer files on managed devices. Transfer files from a device to this controller, to a remote server or from a remote server to the controller. An administrator can transfer logs, configurations and crash dumps.

To administer files for managed devices:

1 Select the **Operations** > **Devices** > **File Management**

2 Select the **Transfer File** button.

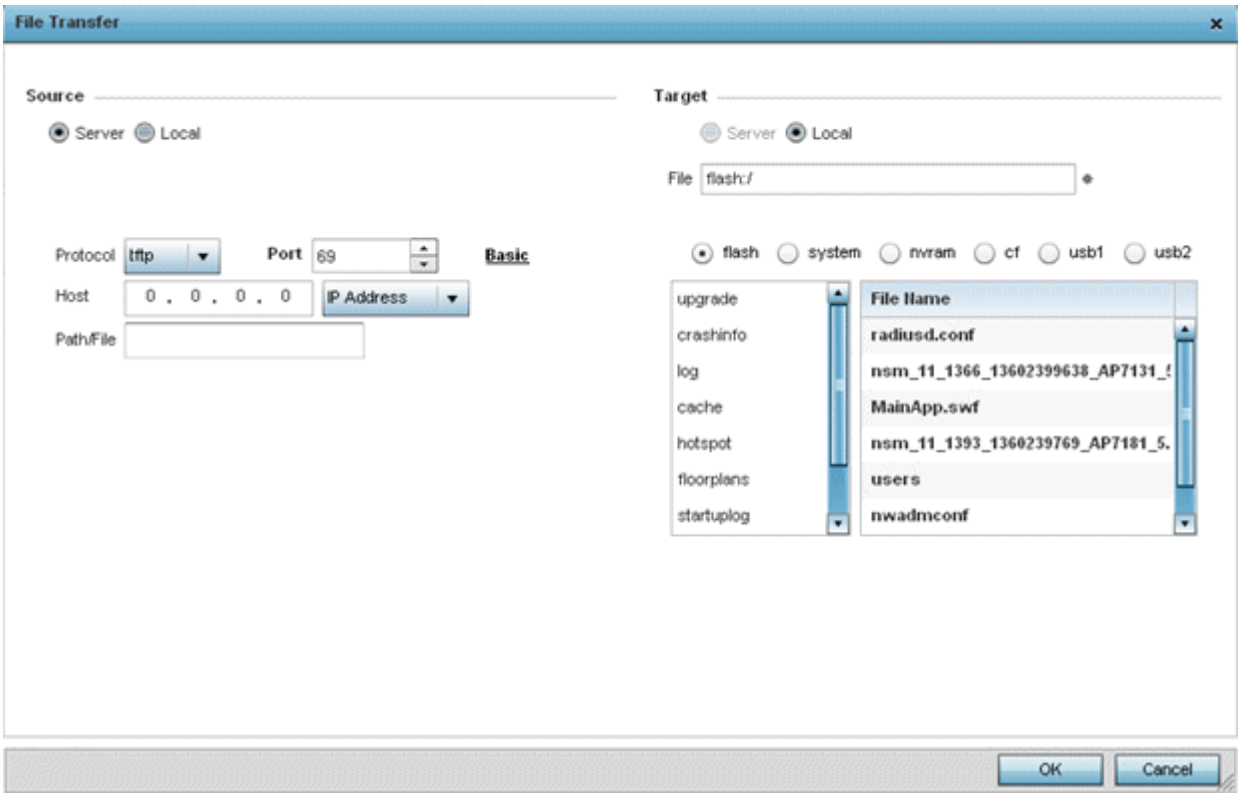


Figure 14-8 *File Transfers screen*

3 Set the following file management source and target directions as well as the configuration parameters of the required file management activity:

Source	Select the source of the file transfer. Select *Server* to indicate the source of the file is a remote server. Select *Local* to indicate the source of the file is local to this controller or service platform.
File	If the source is *Local*, enter the name of the file to be transferred.
Protocol	Select the protocol for file management. Available options include: tftp ftp sftp http cf usb1-4 This parameter is required only when Server is selected as the Source.
Port	Specify the port for transferring files. This option is not available for *cf*, and *usb1-4*. Enter the port number directly or use the spinner control. This parameter is required only when *Server* is selected as the *Source*.
Host	If needed, specify a hostname or numeric IP address of the serve transferring the file. This option is not valid for cf and usb1-4. If a hostname is provided, an *IP Address* is not needed. A hostname cannot contain an underscore. This field is only available when Server is selected in the *From* field.
User Name	Provide a user name to access a FTP or a SFTP server. This parameter is required only when *Server* is selected as the *Source*, and the selected protocol is *ftp* or *sftp*.
Password	Provide a password to access the FTP or SFTP server. This parameter is required only when *Server* is selected as the *Source*, and the selected protocol is *ftp* or *sftp*.
Path / File	Define the path to the file on the server. Enter the complete relative path to the file. This parameter is required only when *Server* is selected as the *Source*.
Target	Select the target destination to transfer the file. Select *Server* if the destination is a remote server, then provide a URL to the location of the server resource or select *Advanced* and provide the same network address information described above. Select *Local* if the destination is this controller or service platform.

4 Select **Copy** to begin the file transfer. Selecting **Reset** reverts the screen to its last saved configuration.

14.1.4 Restarting Adopted Devices

Device Operations

Adopted devices may periodically require restarting to implement firmware updates or other maintenance activities.

NOTE: The **Adopted Device Restart** tab is not available at the RF Domain level of the UI's hierarchal tree. A RF Domain must be selected and expanded to display the RF Domain's member devices. Once expanded, selected a RF Domain member device to ensure the Adopted Device Restart option is available.

To restart controller or service platform adopted Access Points:

1 Select the **Operations** > **Devices** > **Adopted Device Restart.**

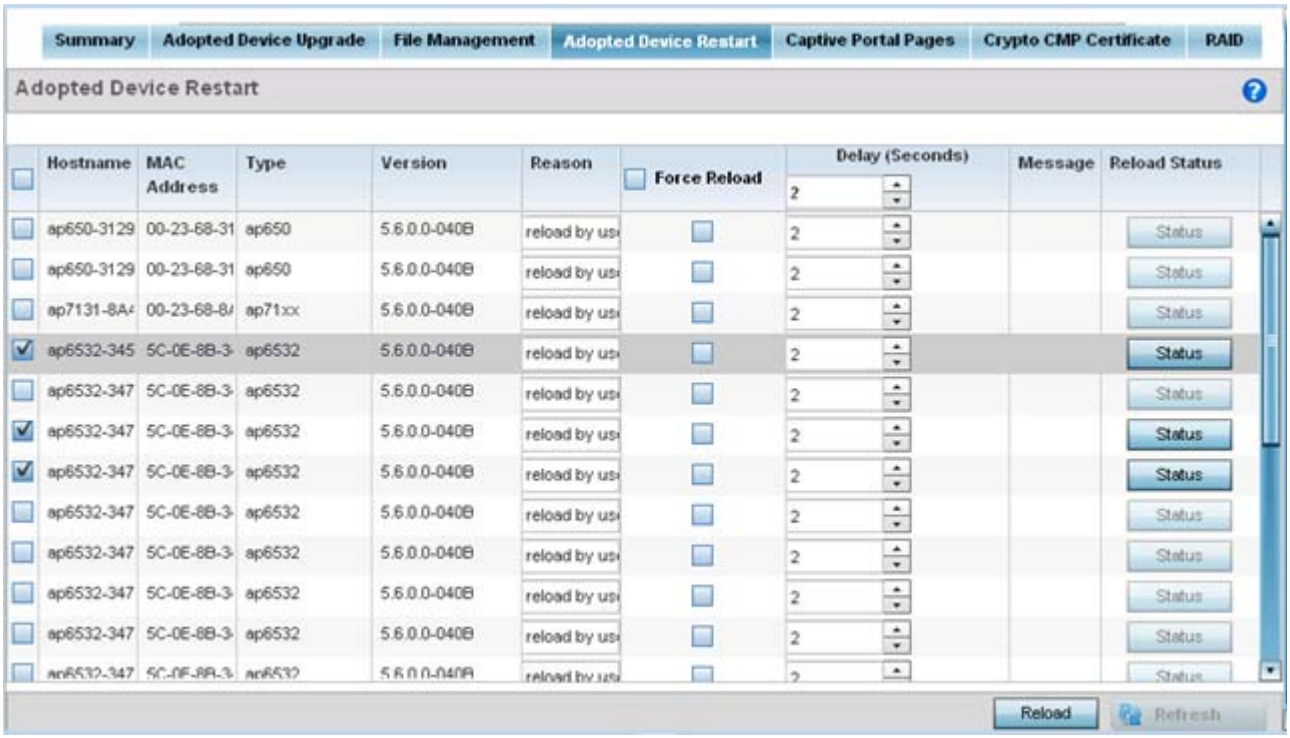


Figure 14-9 *Adopted Device Restart screen*

2 The **Adopted AP Restart** table displays the following information for each Adopted AP:

Hostname	Displays the specified Hostname for each known Access Point.
MAC Address	Displays the primary *Media Access Control* (MAC) or hardware address for each known Access Point.
Type	Displays the Access Point model number for each adopted Access Point.
Version	Displays the current firmware version for each adopted Access Point.
Reason	Lists the administrator defined reason an adopted device has been queued for a restart.

3 To restart an Access Point (or Access Points), select the checkbox to the left of each Access Point to restart and configure the following options:

Force Reload	To force a reload of an Access Point or Access Points, select the *Force Reload* checkbox next to each AP.
Delay (Seconds)	Specify the amount of time, in seconds, before the Access Point restart should be executed. Delaying the restart may allow a selected Access Point to complete its current duty cycle.
Message	Displays any messages associated with each adopted Access Point
Reload Status	Click the *Reload Status* button next to each adopted Access Point to display their current status information.

14.1.5 Captive Portal Configuration

Device Operations

A captive portal is an access policy that provides temporary and restrictive access to the controller or service platform managed wireless network.

A captive portal policy provides secure authenticated access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access the wireless network. Once logged into the captive portal, additional *Terms and Agreement*, *Welcome*, *Fail* and *No Service* pages provide the administrator with a number of options on screen flow and appearance.

Captive portal authentication is used primarily for guest or visitor access to the network, but is increasingly used to provide authenticated access to private network resources when 802.1X EAP is not a viable option. Captive portal authentication does not provide end-user data encryption, but it can be used with static WEP, WPA-PSK or WPA2-PSK encryption.

The **Captive Portal Pages** enable the management of the client access request pages and their transfer to the controller or service platform managed wireless network.

To manage captive portal pages:

1 Select the **Operations** > **Devices** > **Captive Portal Pages.** The **AP Upload List** displays by default.

Use the AP Upload List to provide connected Access Points with specific captive portal configurations so they can successfully provision login, welcome and condition pages to requesting clients attempting to access the wireless network using a captive portal.

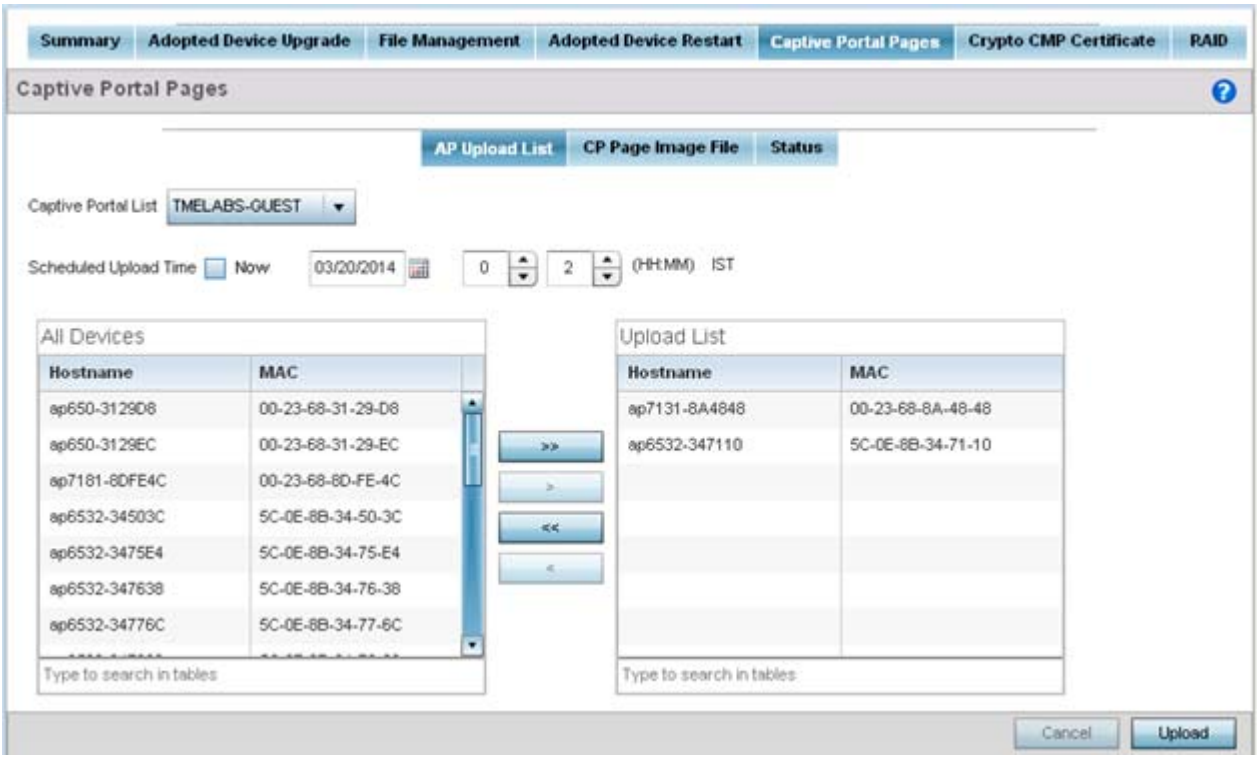


Figure 14-10 *Captive Portal Pages - AP Upload List screen*

2 Use the **Captive Portal List** drop-down menu to select an existing captive portal configuration to upload to an Access Point and display to requesting client devices as they login and adhere to the terms required set for access.

> **NOTE:** If selecting the **Captive Portal Pages** screen from the System and RF Domain levels of the UI's hierarchal tree, there's an additional **Upload from Controller** option to the right of the *Captive Portal List* drop-down menu. Select this option to upload existing captive portal pages from this device's managing controller or service platform.

3 Use **Scheduled Upload Time** to set the time of the captive portal page upload. Select **Now** to immediately start. Use the date, hour and minute spinner controls to set a future date and time for the upload.

> **NOTE:** The **Scheduled Upload Time** is your local system's time. It's not the Access Point, controller, service platform or VX time and it is not synched with the device.

The **All Devices** table lists the hostname and MAC address of devices adopted by this Access Point.

4 At the device level, use the arrow buttons (>> > < <<) to move selected devices from the **All Devices** table to the **Upload List** table. The Upload List table displays the Access Points to which the captive portal pages are applied.

5 Select **Upload** from the lower right-hand side of the screen to upload the captive portal pages to the designated Access Points.

6 Select the **CP Pages Image File** tab.

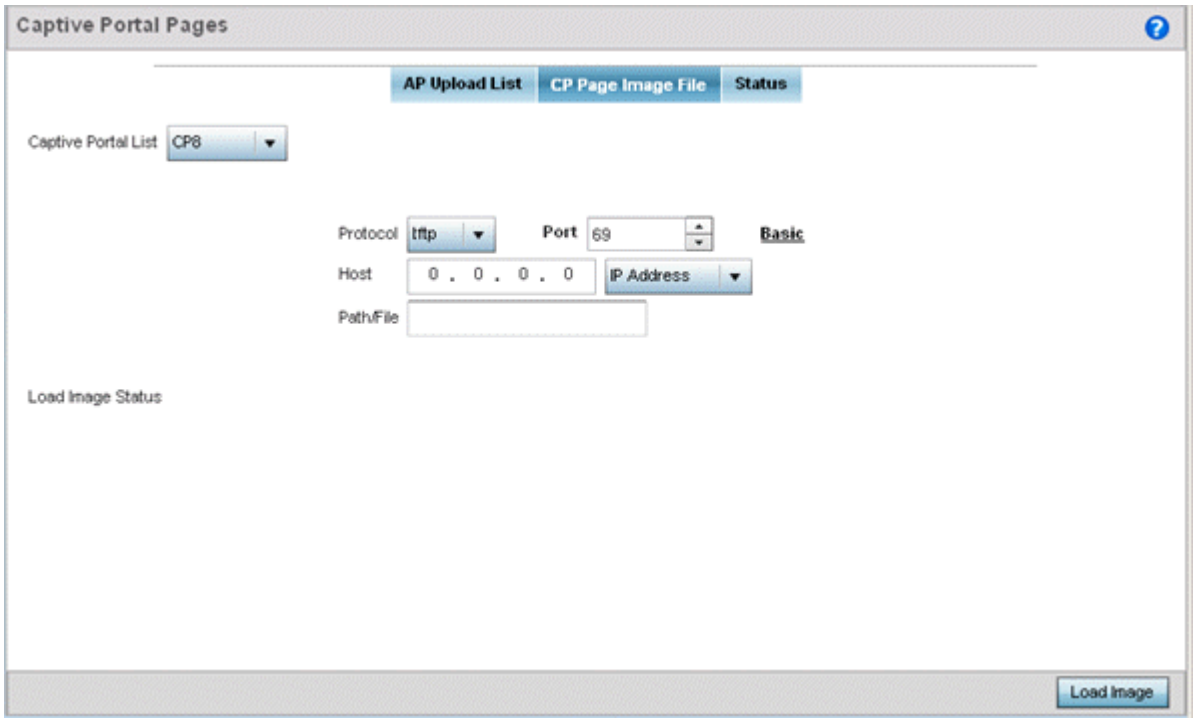


Figure 14-11 *Captive Portal Pages - CP Page Image File screen*

7 Use the **Captive Portal List** drop-down menu to select an existing policy. This policy contains the image (or set of login and conditions pages) requesting clients will navigate and complete before granted access to the network using the unique permissions of the captive portal.

8 Set the following protocols, ports and network address information for sending image files to captive portal provisioning Access Points:

Protocol	Define the protocol (transfer medium) used to forward the image files to the Access Points provisioning captive portal files to requesting clients. Available options include: • tftp • ftp • sftp • http The protocol parameter is required only when Server is selected as the Source and the Advanced option is used.
Host	If needed, specify a Hostname of the server transferring the file. This option is not valid for cf, usb1, and usb2. If a hostname is provided, an *IP Address* is not needed. A hostname cannot contain an underscore. This field is only available when Server is selected in the *From* field.
Port	Specify the port for transferring files. Enter the port number directly or use the spinner control.
User Name	Provide a user name to access the FTP or SFTP server. This parameter is required only when the selected protocol is *ftp* or *sftp*.

Password	Provide a password to access the FTP or SFTP server. This parameter is required only when the selected protocol is *ftp* or *sftp*.
Path/File	Define the path to the file on the server. Enter the complete relative path to the file.

9 Select **Load Image** to upload the image file. Optionally, refer to the **Load Image Status** field to review the status of the current upload.

10 Select the **Status** tab.

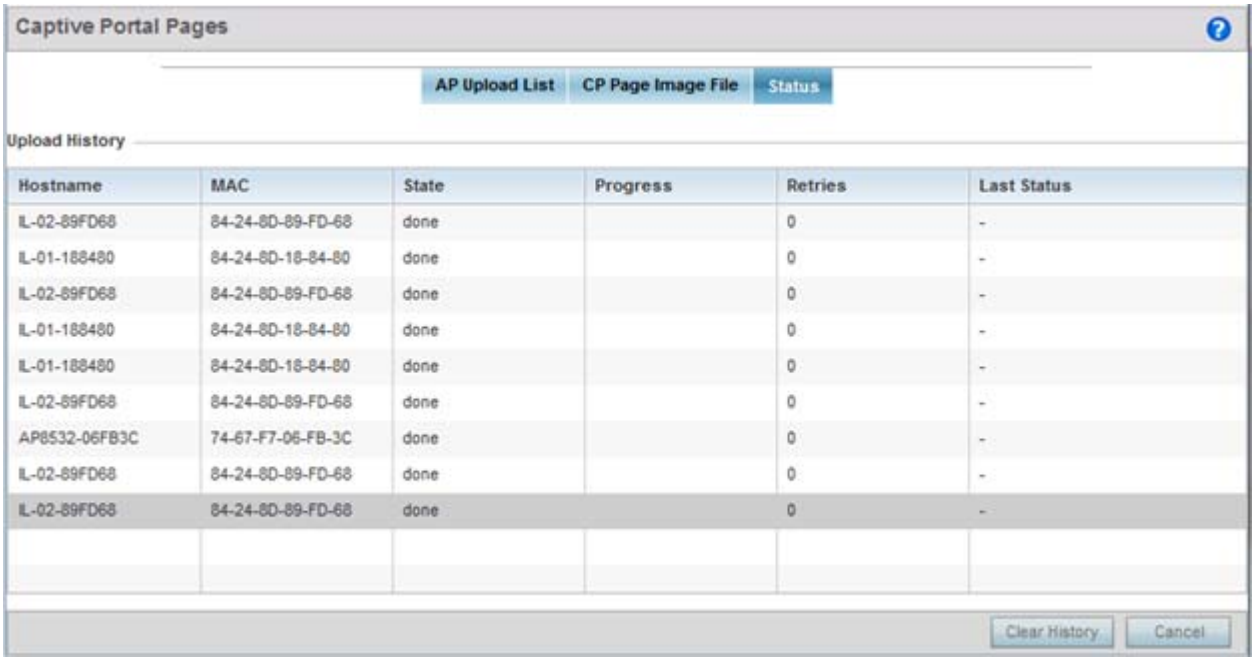


Figure 14-12 *Captive Portal Pages - Status screen*

11 Refer to the **Status** tab to review the progress of Captive Portal Pages upload.

Hostname	Displays the hostname of the recipient device to which the captive portal files are directed.
MAC	Displays the factory encoded MAC address of the recipient device.
State	Displays the target device's current operational state within the controller or service platform managed network.
Progress	Displays the completion progress of each captive portal upload operation.
Retries	Lists the number of retries needed to upload the captive portal files to each listed device.
Last Status	Displays the last known status of the captive portal page uploaded to each listed device.

12 Select **Clear History** to clear the history displayed in the Status tab and begin new data collections.

14.1.6 Crypto CMP Certificate

Device Operations

Certificate Management Protocol (CMP) is an Internet protocol to obtain and manage digital certificates in a *Public Key Infrastructure* (PKI) network. A *Certificate Authority* (CA) issues the certificates using the defined CMP.

Using CMP, a device can communicate to a CMP supported CA server, initiate a certificate request and download the required certificates from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting the certificates from the server. It can also auto update the certificates which are about to expire.

The CMP client on the controller, service platform or Access Point triggers a request for the configured CMS CA server. Once the certificate is validated and confirmed from the CA server it is saved on the device and becomes part of the trustpoint. During the creation of the CMP policy the trustpoint is assigned a name and client information. An administrator can use a manually created trustpoint for one service (like HTTPs) and use the CMP generated trustpoint for RADIUS EAP certificate based authentication.

To assess existing certificates and, if necessary, renew a certificate:

1 Select **Operations** > **Devices** > **Crypto CMP Certificate.** This option is selectable at the controller level.

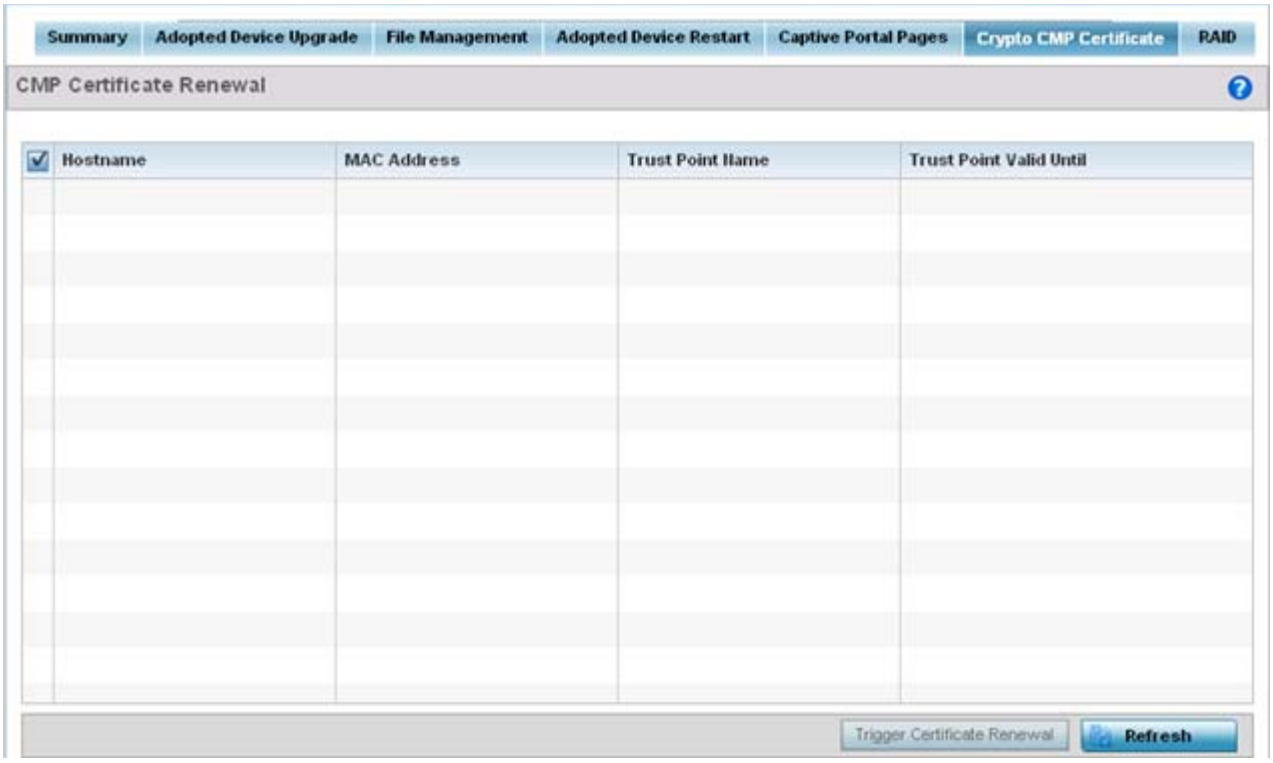


Figure 14-13 *Crypto CMP Certificate screen*

2 Review the following Crypto CMP certificate information to assess whether a certificate requires renewal:

Hostname	Lists the administrator assigned hostname of the CMP resource requesting a certificate renewal from the CMP CA server.
MAC Address	Lists the hardware encoded MAC address of the CMP server resource.

Trust Point Name	Lists the 32 character maximum name assigned to the target trustpoint. A trustpoint represents a CA/identity pair containing the identity of the CA, CA specific configuration parameters, and an association with an enrolled identity certificate.
Trust Point Valid Until	The expiration of the CMP certificate is checked once a day. When a certificate is about to expire a certificate renewal can initiated with the server via an existing IPsec tunnel. If the tunnel is not established, the CMP renewal request is not sent.

3 Select **Trigger Certificate Renewal** to begin update the credentials of the certificate. If a renewal succeeds, the newly obtained certificate overwrites an existing certificate. If the renewal fails, an error is logged.

4 Select **Refresh** to update the screen to the last saved configuration.

14.1.7 RAID Operations

Device Operations

An administrator can configure a NX7530 or a NX9000 series RAID supported service platform with respect to both its collective drive array as well as individual drive behavior and diagnostics. The service platform's array alarm can be silenced, drive LEDs can be illuminated and stopped, drive consistency (integrity) checks can be made and the array can be prepared for drive replacements.

NOTE: RAID controller drive arrays are available within NX7530 and NX9000 series service platforms (NX9000, NX9500 and NX9510 models) only. However, they can be administrated on behalf of a profile by a different model service platform or controller.

To administrate the service platform's drive array and its member drives:

NOTE: The **RAID** tab is not available at the RF Domain level of the UI's hierarchal tree. A RF Domain must be selected and expanded to display the RF Domain's member devices. Once expanded, selected a RF Domain member NX7530, NX9000, NX9500 or NX9510 model device to ensure the RAID option is available.

1 Select **Operations** > **Devices** > **RAID.**

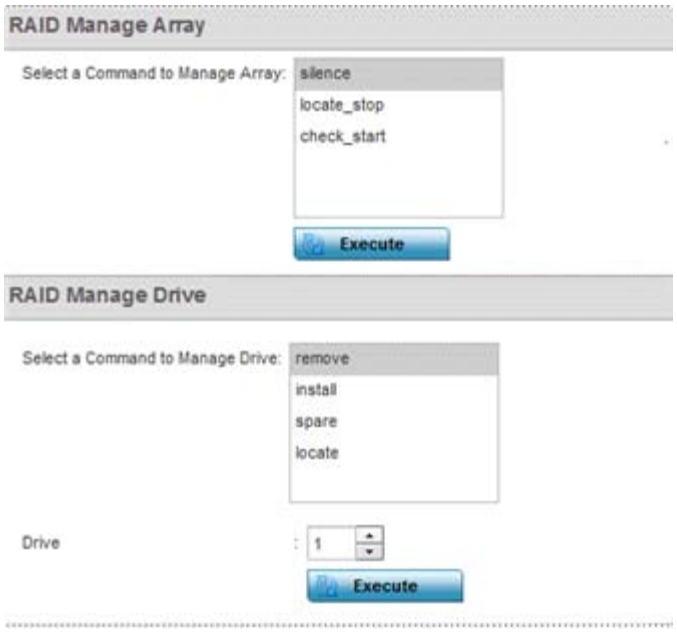


Figure 14-14 *RAID screen*

2 Conduct the following array diagnostic operations from within the **RAID Manage Array** field:

silence	Select *silence* to stop (silence) the service platform's RAID controller array alarm. When a drive is rendered offline for any reason, the service platform's array controller alarm is invoked.
locate-stop	Select *locate-stop* to stop the LEDs of all the drives within the array.
check-start	Select *check-start* to initiate a consistency check on the RAID array.

3 Conduct the following drive diagnostic operations from within the **RAID Manage Drive** field:

remove	Select *remove* to prepare a selected drive for physically removing it from the drive array. The remove command can be applied to either an online or hot spare drive.
install	Once a new drive is installed, it must be prepared for active array utilization. Select *install* to dedicate a selected drive to repair a degraded array and begin an array rebuild operation.
spare	Select *spare* to define a selected unused drive as a hot spare that can be dedicate as an active array drive if one of the two online array drives were to fail.
locate	Select *locate* to flash a selected drive's LED so it can easily located within the drive array.

4 Select **Execute** to initiate the selected command from either the RAID Manage Array or RAID Manage Drive fields.

To view the service platform's current RAID array status, drive utilization and consistency check information, refer to *RAID Statistics on page 15-114*.

14.1.8 Re-elect Controller

Device Operations

Use the **Controller Re-election** screen to identity available Access Point resources within a selected RF Domain and optionally make some, or all, of the Access Points available to initiate tunnel connections.

NOTE: Take care when selecting Access Points for controller re-election, as client connections may be broken on upon re-election. Ensure an elected Access Point's client load can be compensated by another Access Point in the same RF Domain.

To re-elect controller adoption resources for tunnel establishment:

NOTE: The **Re-elect Controller** tab is only available at the RF Domain level of the UI's hierarchal tree and is not available for individual controllers, service platforms and Access Points.

1 Select **Operations.**

2 Ensure a **RF Domain** is selected from the Operations menu on the top, left-hand, side of the screen. Otherwise, the Re-elect Controller screen cannot be located, as it does not display at either the system or device levels of the hierarchal tree.

3 Select the **Re-elect Controller** tab.

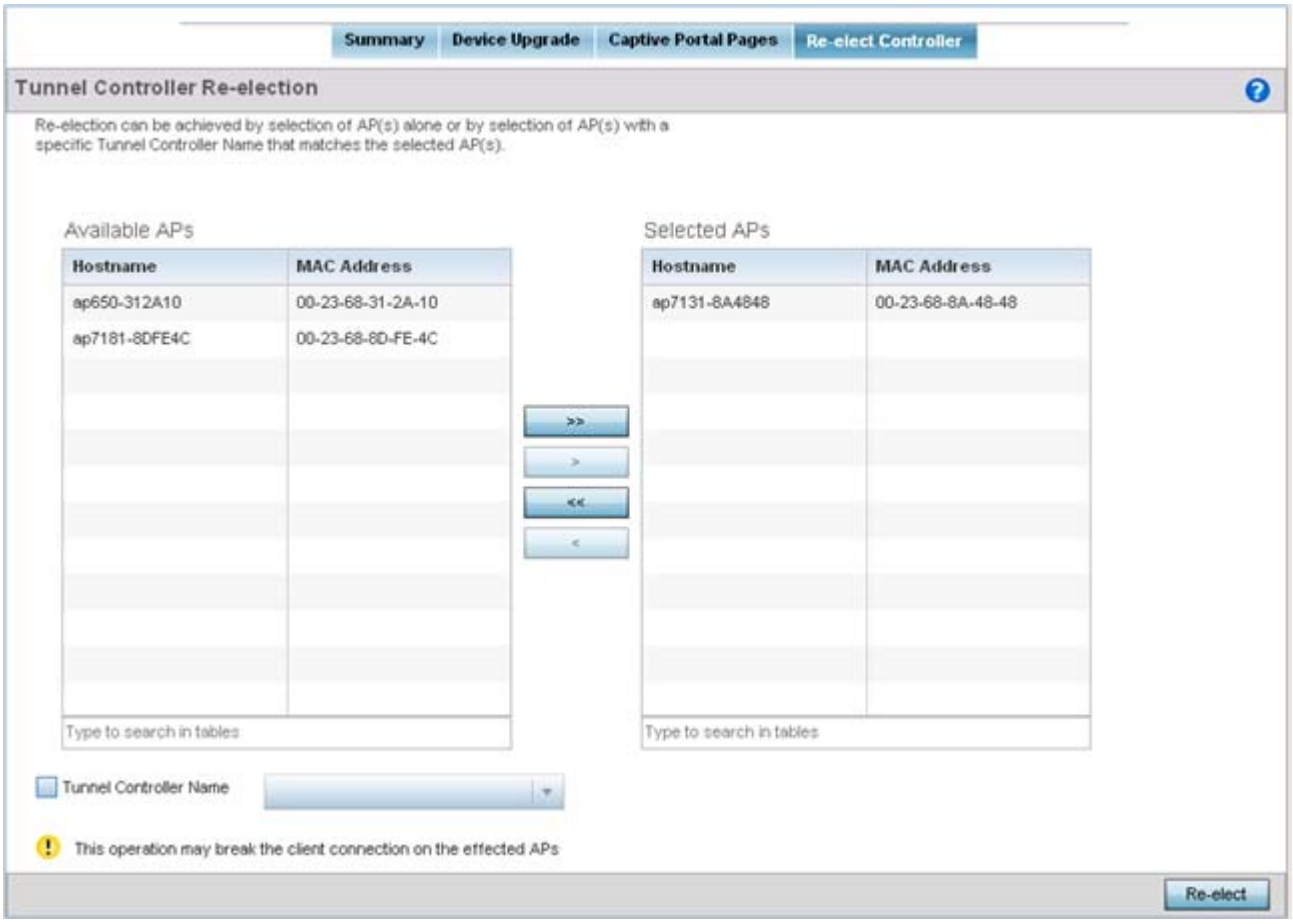


Figure 14-15 *Re-elect Controller screen*

4 Refer to the **Available APs** column, and use the **>** button to move the selected Access Point into the list of **Selected APs** available for RF Domain Manager candidacy. Use the **>>** button to move all listed Access Points into the Selected APs table.

The re-election process can be achieved through the selection of an individual Access Point, or through the selection of several Access Points with a specific Tunnel Controller Name matching the selected Access Points.

5 Select **Re-elect** to designate the Selected AP(s) as resources capable of tunnel establishment.

14.2 Certificates

A certificate links identity information with a public key enclosed in the certificate.

A *certificate authority* (CA) is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate. A browser must contain this CA certificate in its Trusted Root Library so it can trust certificates *signed* by the CA's private key.

Depending on the public key infrastructure, the digital certificate includes the owner's public key, the certificate expiration date, the owner's name and other public key owner information.

Each certificate is digitally signed by a *trustpoint*. The trustpoint signing the certificate can be a certificate authority, corporation or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters and an association with an enrolled identity certificate.

SSH keys are a pair of cryptographic keys used to authenticate users instead of, or in addition to, a username/password. One key is private and the other is public key. *Secure Shell* (SSH) public key authentication can be used by a client to access managed resources, if properly configured. A RSA key pair must be generated on the client. The public portion of the key pair resides with the controller or service platform, while the private portion remains on a secure local area of the client.

For more information on the certification activities support by the controller or service platform, refer to the following:

- *Certificate Management*
- *RSA Key Management*
- *Certificate Creation*
- *Generating a Certificate Signing Request*

14.2.1 Certificate Management

Certificates

If not wanting to use an existing certificate or key with a selected device, an existing *stored* certificate can be leveraged from a different managed device for use with the target device. Device certificates can be imported and exported to and from the controller or service platform to a secure remote location for archive and retrieval as they are required for application to other managed devices.

To configure trustpoints for use with certificates:

1 Select **Operations** > **Manage Certificates.**

2 Select a device from amongst those displayed in either the RF Domain or Network panes on the left-hand side of the screen.

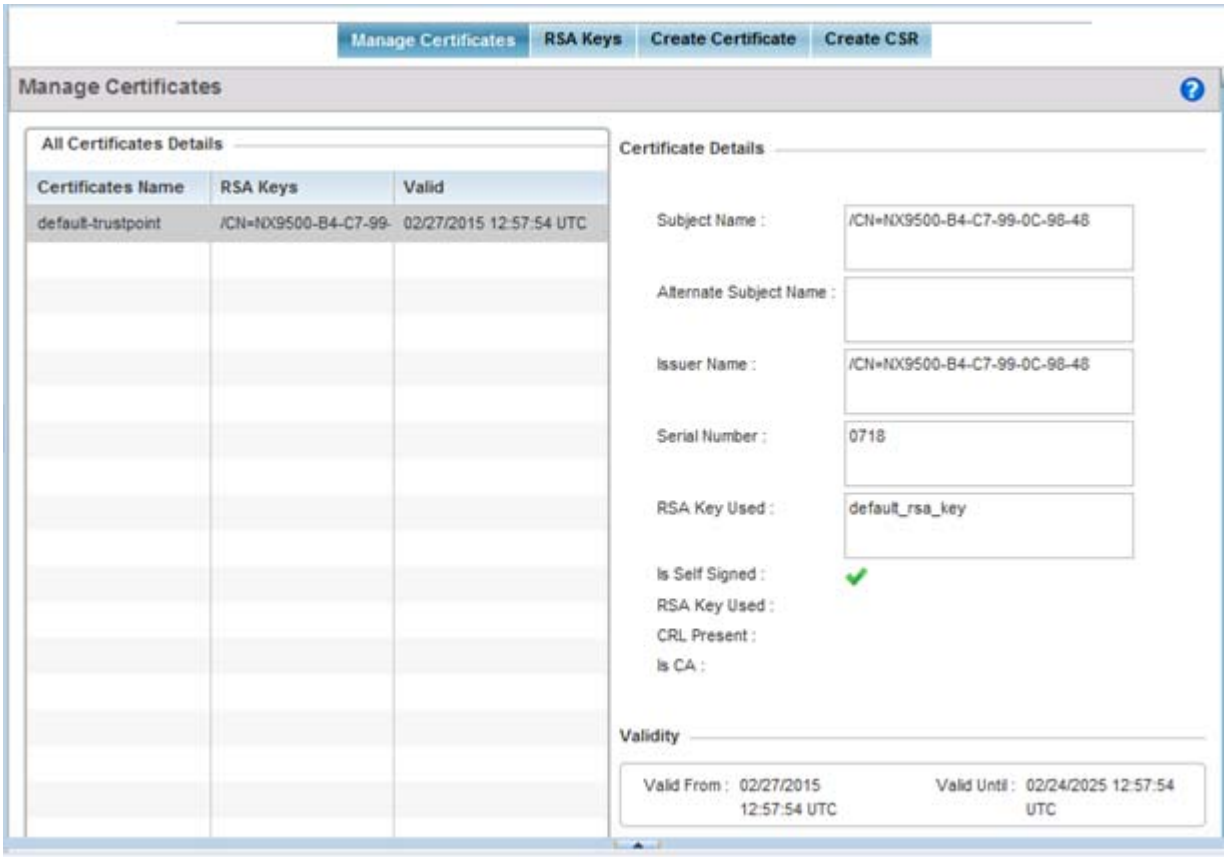


Figure 14-16 *Manage Certificates screen*

3 Select a device from amongst those displayed to review its certificate usage within the controller or service platform managed network.

4 Refer to the **All Certificate Details** to review the certificate's properties, self-signed credentials, validity period and CA information.

5 To import a certificate to the controller or service platform, select the **Import** button from the bottom of the Manage Certificates screen.

An **Import New Trustpoint** screen displays where CA certificates, CRLs and signed certificates can optionally be imported to the controller or service platform once the network credentials of the file transfer have been defined.

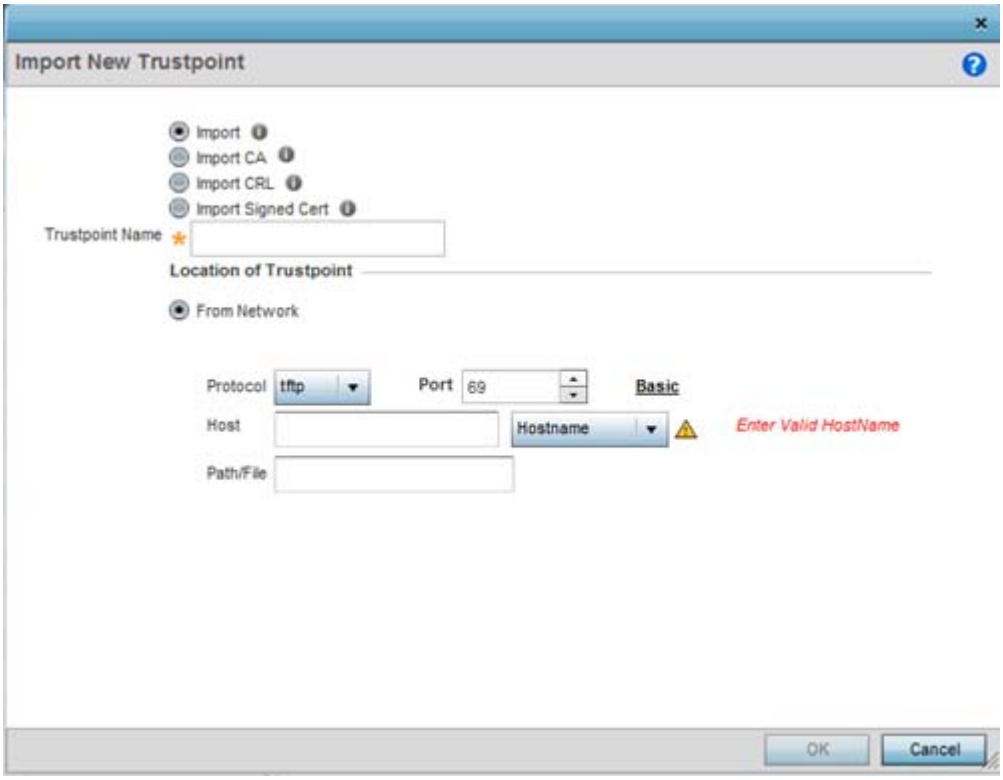


Figure 14-17 *Import New Trustpoint screen*

6 To optionally import a CA certificate to the controller or service platform, select the **Import CA** button from the **Import New Trustpoint** screen.

A CA is a network authority that issues and manages security credentials and public keys for message encryption. The CA signs all digital certificates it issues with its own private key. The corresponding public key is contained within the certificate and is called a CA certificate.

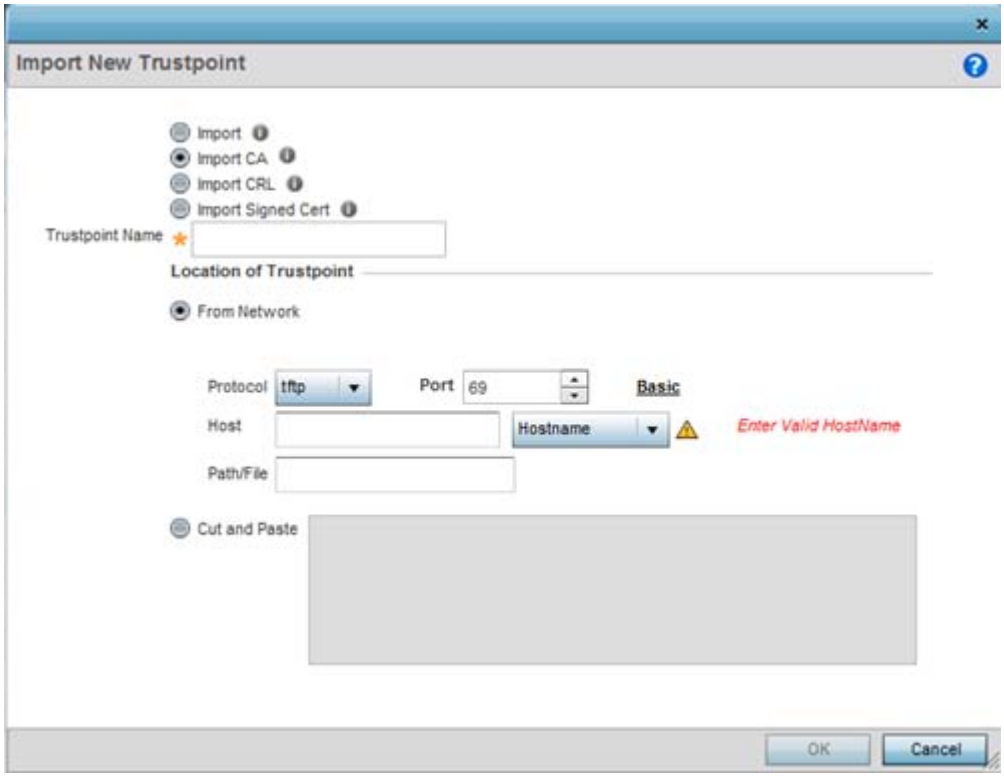


Figure 14-18 *Import New Trustpoint - Import CA screen*

7 Define the following configuration parameters required for the **Import CA** of the CA certificate:

Trustpoint Name	Enter the 32 character maximum name assigned to the target trustpoint signing the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA specific configuration parameters, and an association with an enrolled identity certificate.
URL	Provide the complete URL to the location of the trustpoint. If needed, select *Advanced* to expand the dialog to display network address information to the location of the target trustpoint. The number of additional fields populating the screen is dependent on the selected protocol.
Advanced / Basic	Click the *Advanced* or *Basic* link to switch between a basic URL and an advanced location to specify trustpoint location.
Protocol	Select the protocol used for importing the target CA certificate. Available options include: tftp ftp sftp http cf usb 1-4
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1 - 4*.

Host	Provide the hostname or numeric IP4 or IPv6 formatted IP address of the server used to export the trustpoint. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. Providing a host is not required for cf and usb1-4. A hostname cannot contain an underscore.
Path/File	Specify the path or filename of the CA certificate. Enter the complete relative path to the file on the server.
Cut and Paste	Select the *Cut and Paste* radio button to simply copy an existing trustpoint into the cut and paste field. When pasting, no additional network address information is required.

8 Select **OK** to import the defined CA certificate. Select **Cancel** to revert the screen to its last saved configuration.

9 Select the **Import CRL** button from the **Import New Trustpoint** screen to optionally import a CRL to the controller or service platform.

If a certificate displays within the Certificate Management screen with a CRL, that CRL can be imported into the controller or service platform. A *certificate revocation list* (CRL) is a list of certificates that have been revoked or are no longer valid. A certificate can be revoked if the CA had improperly issued a certificate, or if a private-key is compromised. The most common reason for revocation is the user no longer being in sole possession of the private key.

For information on creating a CRL to use with a trustpoint, refer to *Setting the Profile's Certificate Revocation List (CRL) Configuration on page 8-166*.

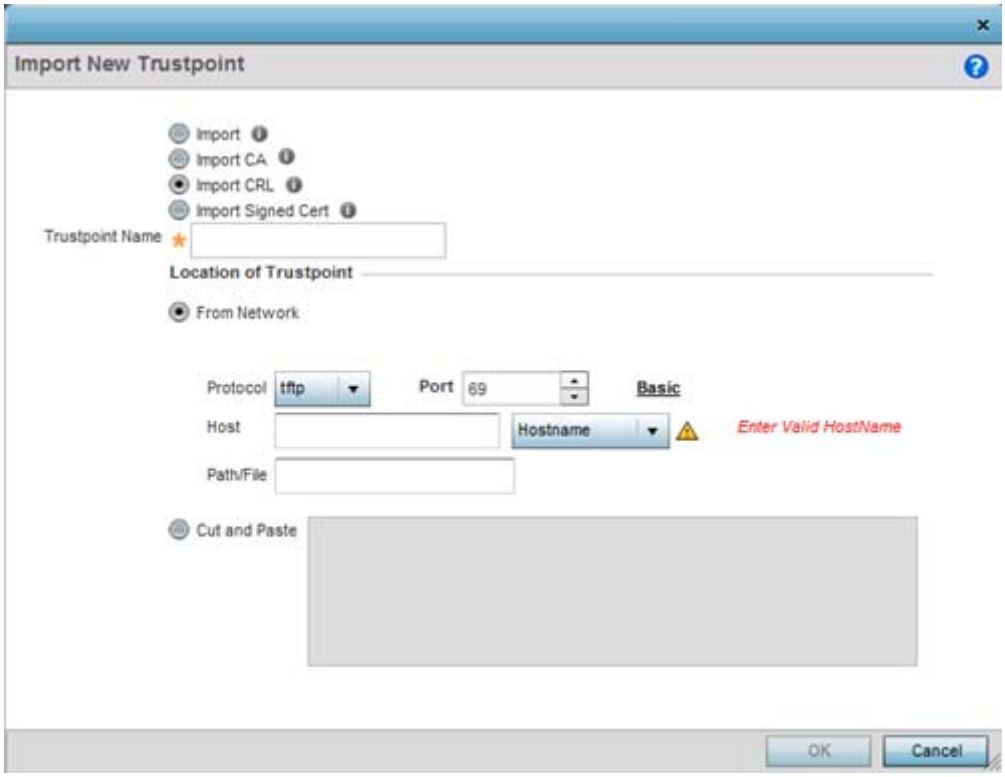


Figure 14-19 *Import New Trustpoint - Import CRL screen*

10 Define the following configuration parameters required for the **Import** of the CRL:

Trustpoint Name	Enter the 32 character maximum name assigned to the target trustpoint signing the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.
From Network	Select the *From Network* radio button to provide network address information to the location of the target CRL. The number of additional fields that populate the screen is also dependent on the selected protocol. This is the default setting.
URL	Provide the complete URL to the location of the CRL. If needed, select *Advanced* to expand the dialog to display network address information to the location of the CRL. The number of additional fields that populate the screen is also dependent on the selected protocol.
Protocol	Select the protocol used for importing the CRL. Available options include: tftp ftp sftp http cf usb1-4
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1-4*.
Host	Provide the hostname or numeric IP4 or IPv6 formatted IP address of the server used to export the trustpoint. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. Providing a host is not required for cf and usb1-4. A hostname cannot contain an underscore.
Path/File	Specify the path to the CRL. Enter the complete relative path to the file on the server.
Cut and Paste	Select the *Cut and Paste* radio button to simply copy an existing CRL into the cut and paste field. When pasting a CRL, no additional network address information is required.

11 Select **OK** to import the CRL. Select **Cancel** to revert the screen to its last saved configuration.

12 To import a signed certificate to the controller or service platform, select **Import Signed Cert** from the **Import New Trustpoint** screen.

Signed certificates (or root certificates) avoid the use of public or private CAs. A self-signed certificate is an identity certificate signed by its own creator, thus the certificate creator also signs off on its legitimacy. The lack of mistakes or corruption in the issuance of self signed certificates is central.

Self-signed certificates cannot be revoked which may allow an attacker who has already gained access to monitor and inject data into a connection to spoof an identity if a private key has been compromised. However, CAs have the ability to revoke a compromised certificate, preventing its further use.

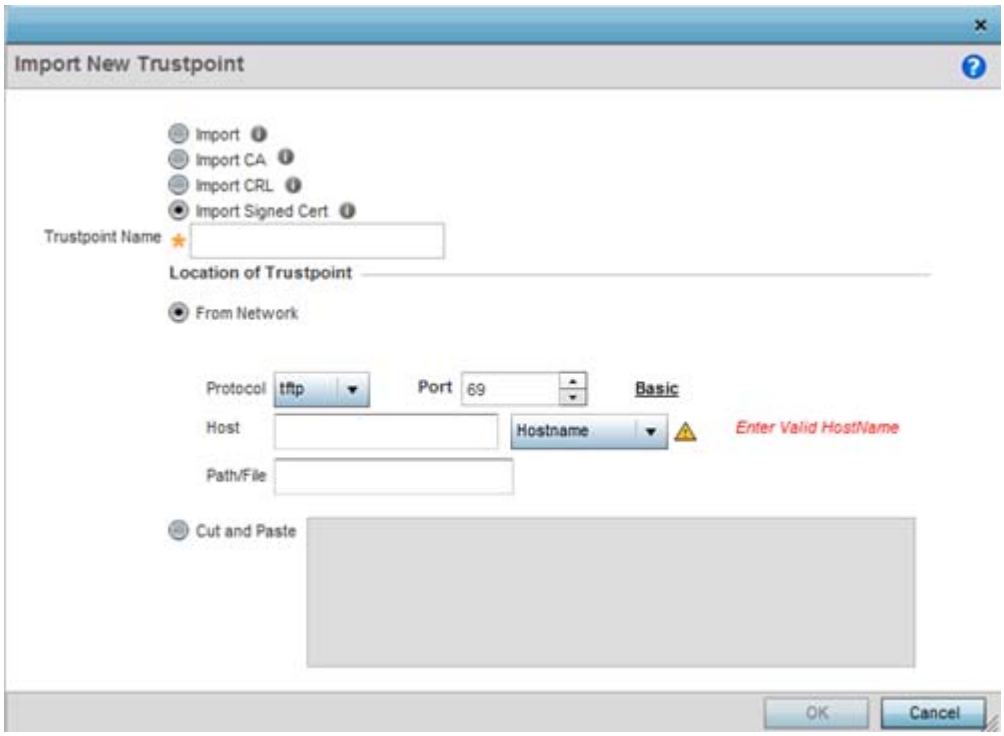


Figure 14-20 *Import New Trustpoint - Import Signed Cert*

13 Define the following parameters required for the **Import** of the Signed Certificate:

Trustpoint Name	Enter the 32 character maximum trustpoint name with which the certificate should be associated.
From Network	Select the *From Network* radio button to provide network address information to the location of the signed certificate. The number of additional fields that populate the screen is dependent on the selected protocol. From Network is the default setting.
URL	Provide the complete URL to the location of the signed certificate. If needed, select *Advanced* to expand the dialog to display network address information to the location of the signed certificate. The number of additional fields populating the screen is dependent on the selected protocol.
Protocol	Select the protocol for importing the signed certificate. Available options include: tftp ftp sftp http cf usb1-4
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1-4*.

Host	Provide the hostname or numeric IP4 or IPv6 formatted IP address of the server used to import the trustpoint. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. Providing a host is not required for cf and usb1-4. A hostname cannot contain an underscore.
Path/File	Specify the path to the signed certificate. Enter the complete relative path to the file on the server.
Cut and Paste	Select the *Cut and Paste* radio button to simply copy an existing signed certificate into the cut and paste field. When pasting a signed certificate, no additional network address information is required.

14 Select **OK** to import the signed certificate. Select **Cancel** to revert the screen to its last saved configuration.

15 To optionally export a trustpoint from the controller or service platform to a remote location, select the **Export** button from the Certificate Management screen.

Once a certificate has been generated on the controller or service platform's authentication server, export the self signed certificate. A digital CA certificate is different from a self signed certificate. The CA certificate contains the public and private key pairs. The self certificate only contains a public key. Export the self certificate for publication on a Web server or file server for certificate deployment or export it in to an active directory group policy for automatic root certificate deployment.

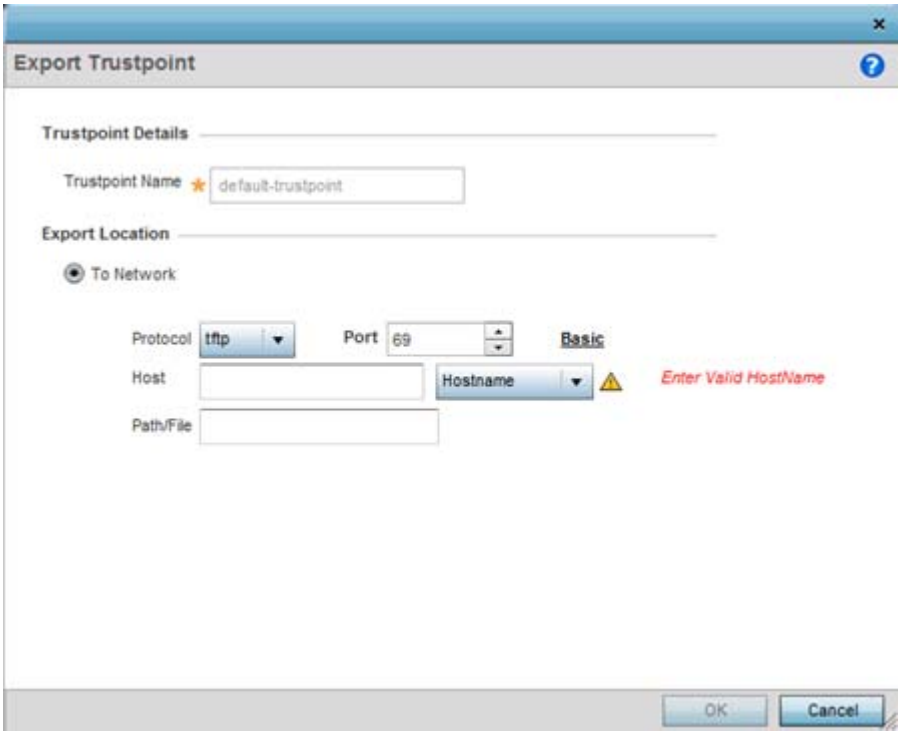


Figure 14-21 *Certificate Management - Export Trustpoint screen*

16 Define the following configuration parameters required for the **Export** of the trustpoint.

Trustpoint Name	Enter the 32 character maximum name assigned to the trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual.

URL	Provide the complete URL to the location of the trustpoint. If needed, select *Advanced* to expand the dialog to display network address information to the location of the trustpoint. The number of additional fields that populate the screen is dependent on the selected protocol.
Protocol	Select the protocol used for exporting the target trustpoint. Available options include: tftp ftp sftp http cf usb1-4
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1-4*.
Host	Provide the hostname or numeric IPv4 or IPv6 formatted address of the server used to export the trustpoint. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. Providing a host is not required for cf and usb1-4. A hostname cannot contain an underscore.
Path/File	Specify the path to the trustpoint. Enter the complete relative path to the file on the server.

17 Select **OK** to export the defined trustpoint. Select **Cancel** to revert the screen to its last saved configuration.

18 To optionally delete a trustpoint, select the **Delete** button from within the Certificate Management screen. Provide the trustpoint name within the **Delete Trustpoint** screen and optionally select **Delete RSA Key** to remove the RSA key along with the trustpoint. Select **OK** to proceed with the deletion, or **Cancel** to revert to the Certificate Management screen.

14.2.2 RSA Key Management

Certificates

Refer to the RSA Keys screen to review existing RSA key configurations applied to managed devices. If an existing key does not meet the needs of a pending certificate request, generate a new key or import/export an existing key to and from a remote location.

Rivest, Shamir, and Adleman (RSA) is an algorithm for public key cryptography. It's an algorithm that can be used for certificate signing and encryption. When a device trustpoint is created, the RSA key is the private key used with the trustpoint.

To review existing device RSA key configurations, generate additional keys or import/export keys to and from remote locations:

1 Select **RSA Keys** tab from the Certificate Management screen.

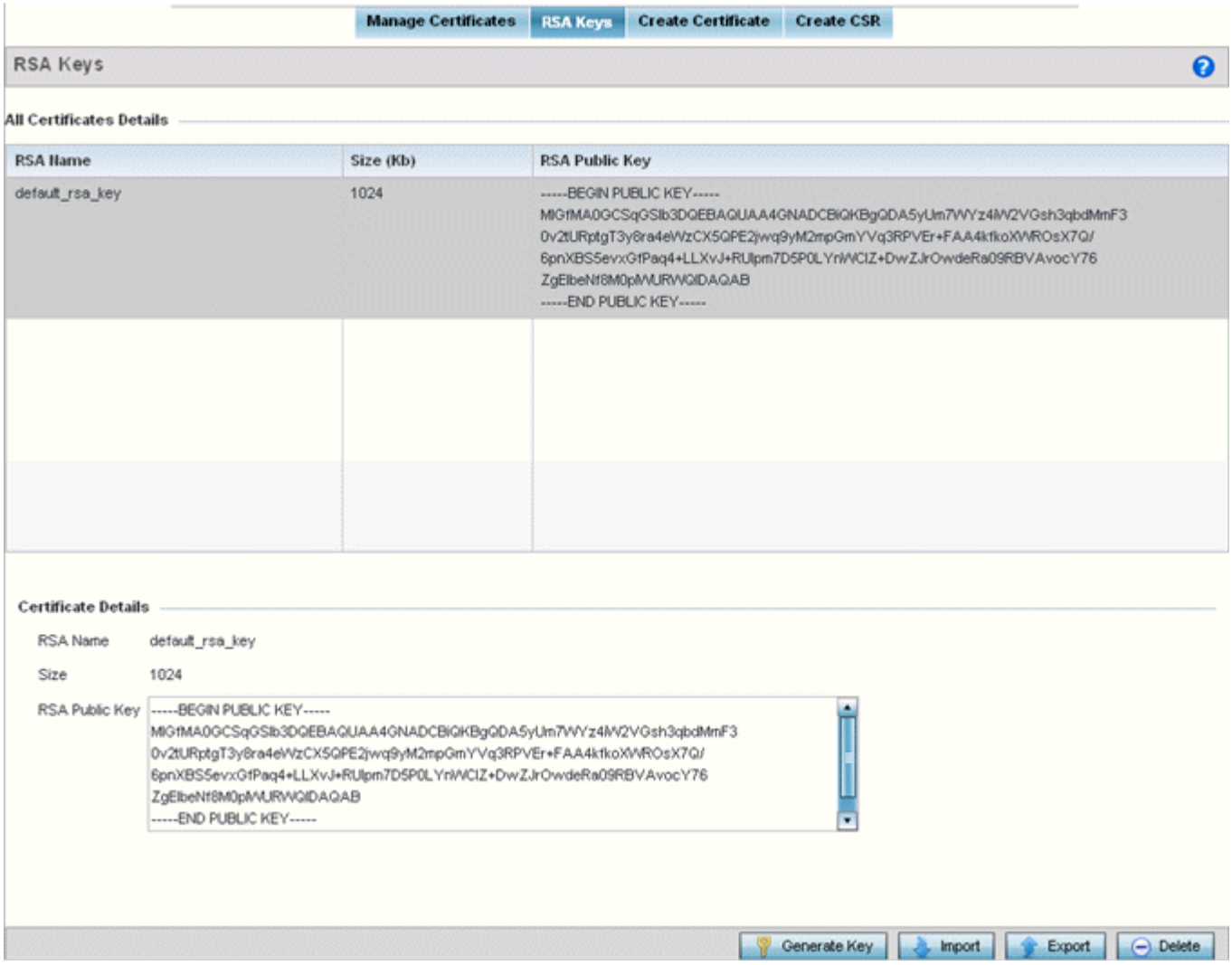


Figure 14-22 *Certificate Management - RSA Keys screen*

2 Select a listed device to review its current RSA key configuration.

Each key can have its size and character syntax displayed. Once reviewed, optionally generate a new RSA key, import a key from a selected device, export a key from the controller or service platform to a remote location or delete a key from a selected device.

3 Select **Generate Key** to create a new key with a defined size.

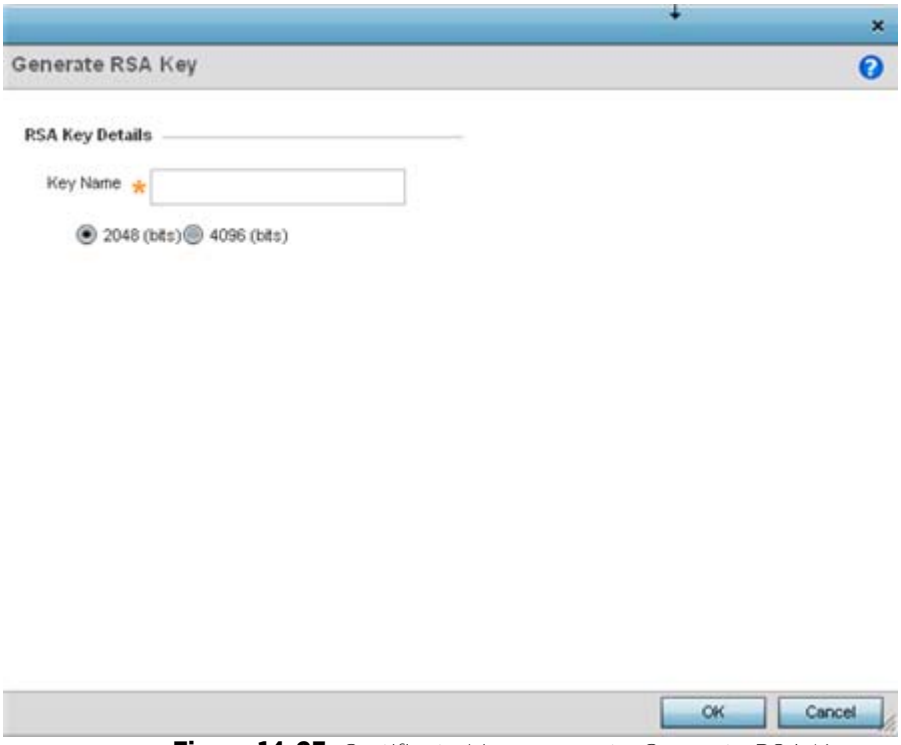


Figure 14-23 *Certificate Management - Generate RSA Keys screen*

4 Define the following configuration parameters required for the **Import** of the key:

Key Name	Enter the 32 character maximum name assigned to the RSA key.
Key Size	Set the size of the key as either *2048 (bits)* or *4096 (bits)*. Leaving this value at the default setting of 2048 is recommended to ensure optimum functionality.

5 Select **OK** to generate the RSA key. Select **Cancel** to revert the screen to its last saved configuration.

6 To optionally import a CA certificate to the controller or service platform, select the **Import** button from the Certificate Management > RSA Keys screen.

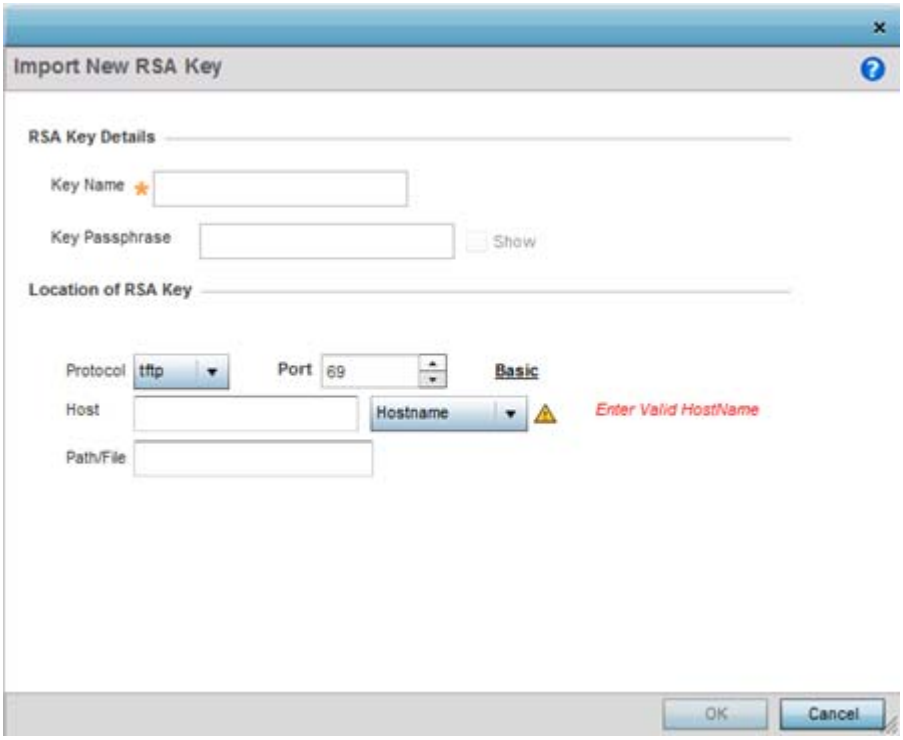


Figure 14-24 *Certificate Management - Import New RSA Key screen*

7 Define the following parameters required for the **Import** of the RSA key:

Key Name	Enter the 32 character maximum name assigned to identify the RSA key.
Key Passphrase	Define the key used by both the controller or service platform and the server (or repository) of the RSA key. Select the *Show* to expose the actual characters used in the passphrase. Leaving the Show unselected displays the passphrase as a series of asterisks "*".
URL	Provide the complete URL to the location of the RSA key. If needed, select *Advanced* to expand the dialog to display network address information to the location of the target key. The number of additional fields that populate the screen is dependent on the selected protocol.
Advanced / Basic	Select either the *Advanced* or *Basic* link to switch between a basic URL and an advanced location to specify key location.
Protocol	Select the protocol used for importing the target key. Available options include: tftp ftp sftp http cf usb1-4
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1-4*.

Host	Provide the hostname or numeric IPv4 or IPv6 formatted address of the server used to import the RSA key. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. Providing a host is not required for cf and usb1-4. A hostname cannot contain an underscore.
Path/File	Specify the path to the RSA key. Enter the complete relative path to the key on the server.

8 Select **OK** to import the defined RSA key. Select **Cancel** to revert the screen to its last saved configuration.

9 To optionally export a RSA key from the controller or service platform to a remote location, select the **Export** button from the Certificate Management > RSA Keys screen.

Export the key to a redundant RADIUS server to import it without generating a second key. If there's more than one RADIUS authentication server, export the certificate and don't generate a second key unless you want to deploy two root certificates.

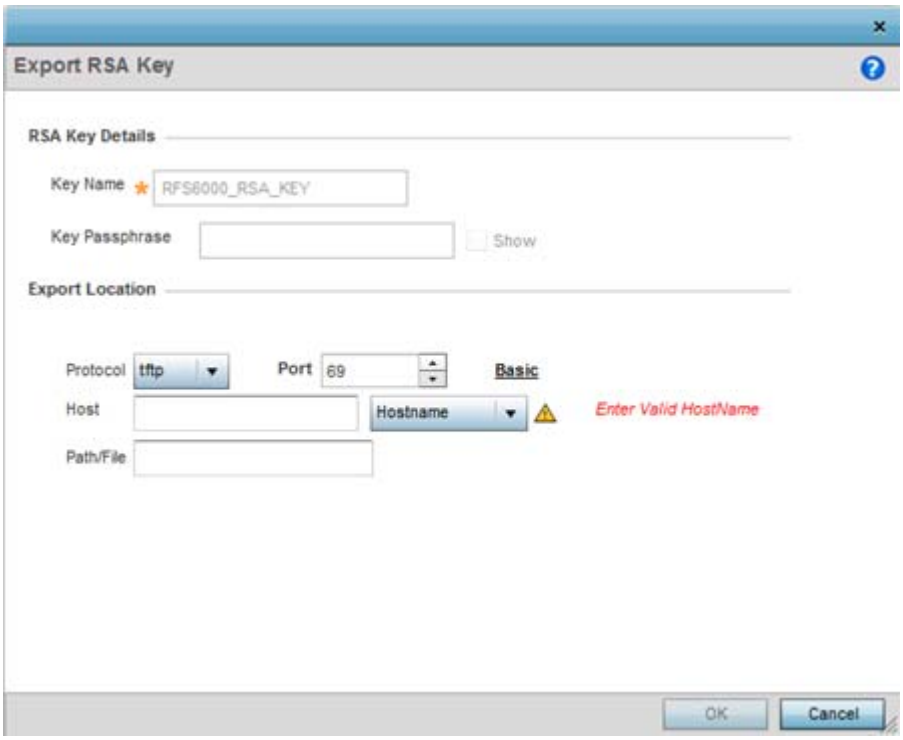


Figure 14-25 *Certificate Management - Export RSA Key screen*

10 Define the following configuration parameters required for the **Export** of the RSA key.

Key Name	Enter the 32 character maximum name assigned to the RSA key.
Key Passphrase	Define the key passphrase used by both the controller or service platform and the server. Select *Show* to expose the actual characters used in the passphrase. Leaving the Show unselected displays the passphrase as a series of asterisks "*".

URL	Provide the complete URL to the location of the key. If needed, select *Advanced* to expand the dialog to display network address information to the location of the target key. The number of additional fields that populate the screen is dependent on the selected protocol.
Protocol	Select the protocol used for exporting the RSA key. Available options include: tftp ftp sftp http cf usb1-4
Port	Use the spinner control to set the port. This option is not valid for *cf* and *usb1-4*.
Host	Provide the hostname or numeric IPv4 or IPv6 formatted address of the server used to export the RSA key. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. Providing a host is not required for cf and usb1-4. A hostname cannot contain an underscore.
Path/File	Specify the path to the key. Enter the complete relative path to the key on the server.

11 Select **OK** to export the defined RSA key. Select **Cancel** to revert the screen to its last saved configuration.

12 To optionally delete a key, select the **Delete** button from within the Certificate Management > RSA Keys screen. Provide the key name within the **Delete RSA Key** screen and select **Delete Certificates** to remove the certificate. Select **OK** to proceed with the deletion, or **Cancel** to revert back to the Certificate Management screen.

14.2.3 Certificate Creation

Certificates

The **Create Certificate** screen provides the facility for creating new self-signed certificates. Self signed certificates (often referred to as root certificates) do not use public or private CAs. A self signed certificate is a certificate signed by its own creator, with the certificate creator responsible for its legitimacy.

To create a self-signed certificate that can be applied to a managed device:

1 Select the **Create Certificate** tab the Certificate Management screen.

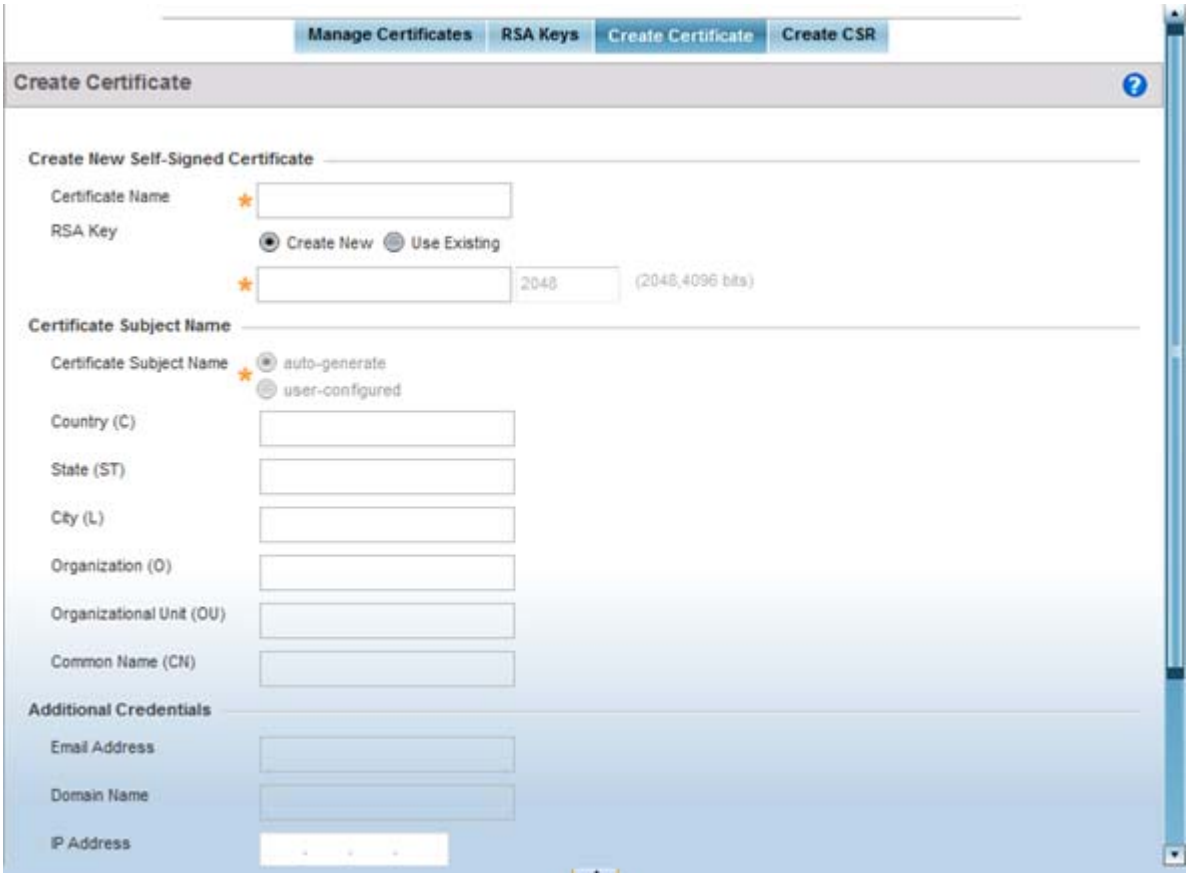


Figure 14-26 *Certificate Management - Create Certificate screen*

2 Define the following configuration parameters required to **Create New Self-Signed Certificate**:

Certificate Name	Enter the 32 character maximum name assigned to identify the name of the trustpoint associated with the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.
RSA Key	To create a new RSA key, select *Create New* to define a 32 character maximum name used to identify the RSA key. Set the size of the key (2048, 4096 bits). Leave this value at the default setting of 2048 to ensure optimum functionality. To use an existing key, select *Use Existing* and select a key from the drop-down menu.

3 Set the following **Certificate Subject Name** parameters required for the creation of the certificate:

Certificate Subject Name	Select either *auto-generate* to automatically create the certificate's subject credentials or *user-configured* to manually enter the credentials of the self signed certificate. The default setting is auto-generate.
Country (C)	Define the *Country* used in the certificate. The field can be modified by the user to other values. This is a required field and must not exceed 2 characters.

State (ST)	Enter a *State/Prov.* for the state or province name used in the certificate. This is a required field.
City (L)	Enter a *City* to represent the city used in the certificate. This is a required field.
Organization (O)	Define an *Organization* for the organization represented in the certificate. This is a required field.
Organizational Unit (OU)	Enter an *Org. Unit* for the organization unit represented in the certificate. This is a required field.
Common Name (CN)	If there's a common name (IP address) for the organizational unit issuing the certificate, enter it here.

4 Select the following **Additional Credentials** required for the generation of the self signed certificate:

Email Address	Provide an *Email Address* used as the contact address for issues relating to this certificate request.
Domain Name	Enter a *fully qualified domain name* (FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely. To distinguish an FQDN from a regular domain name, a trailing period is added. For example, *somehost.example.com*. An FQDN differs from a regular domain name by its absoluteness, since a suffix is not added.
IP Address	Specify the IP address used as the destination for certificate requests.

5 Select the **Generate Certificate** button at the bottom of the Create Certificate screen to produce the certificate.

14.2.4 Generating a Certificate Signing Request

Certificates

A *certificate signing request* (CSR) is a message from a requestor to a certificate authority to apply for a digital identity certificate. The CSR is composed of a block of encrypted text generated on the server the certificate will be used on. It contains information included in the certificate, including organization name, common name (domain name), locality, and country.

A RSA key must be either created or applied to the certificate request before the certificate can be generated. A private key is not included in the CSR, but is used to digitally sign the completed request. The certificate created with a particular CSR only worked with the private key generated with it. If the private key is lost, the certificate is no longer functional.The CSR can be accompanied by other identity credentials required by the certificate authority, and the certificate authority maintains the right to contact the applicant for additional information.

If the request is successful, the CA sends an identity certificate digitally signed with the private key of the CA.

To create a CSR:

1 Select **Operations** > **Certificates.**

2 Select a device from amongst those displayed in either the RF Domain or Network panes on the left-hand side of the screen.

3 Select **Create CSR.**

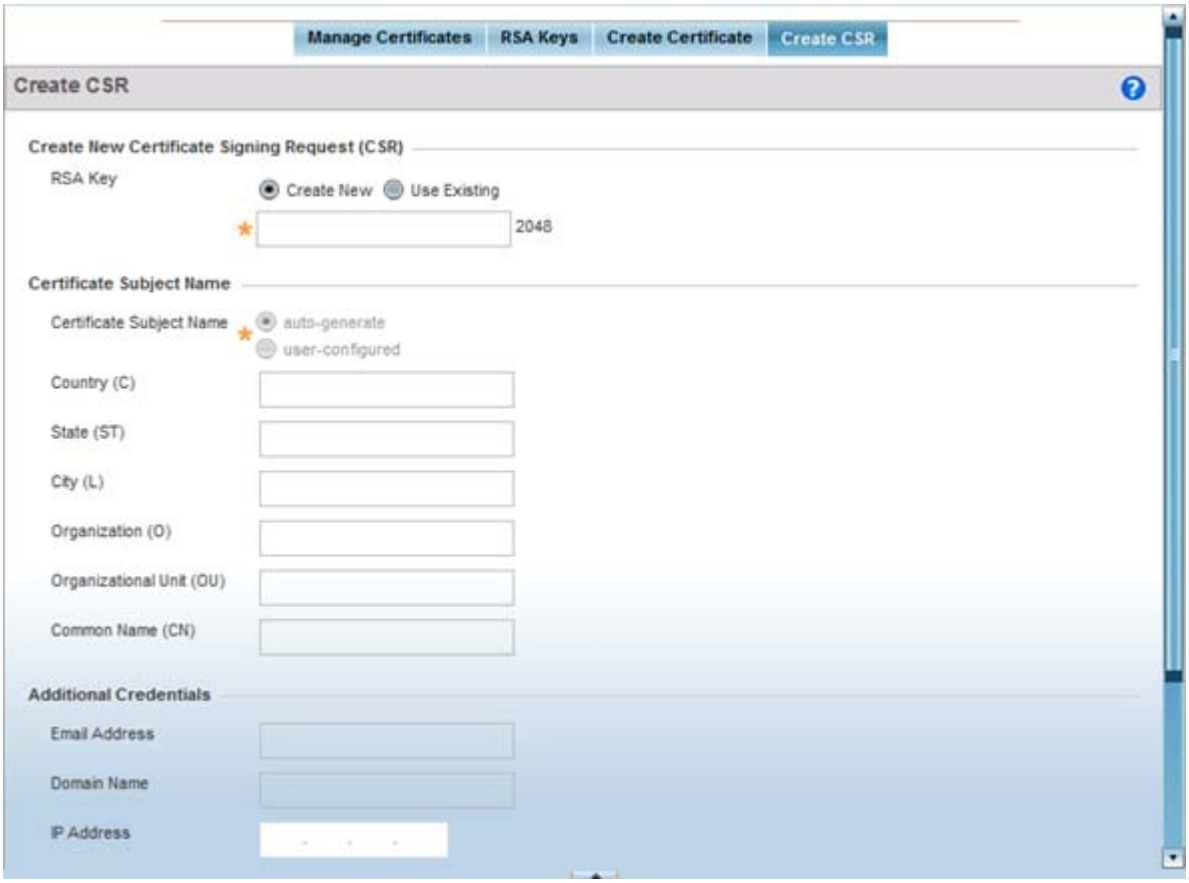


Figure 14-27 *Create CSR screen*

4 Define the following configuration parameters required to **Create New Certificate Signing Request (CSR)**:

RSA Key	To create a new RSA key, select *Create New* to define a 32 character maximum name used to identify the RSA key. Set a 2,048 bit key. To use an existing key, select *Use Existing* and select a key from the drop-down menu.

5 Set the following **Certificate Subject Name** parameters:

Certificate Subject Name	Select either the *auto-generate* radio button to automatically create the certificate's subject credentials or select *user-configured* to manually enter the credentials of the self signed certificate. The default setting is auto-generate.
Country (C)	Define the *Country* used in the CSR. The field can be modified by the user to other values. This is a required field and must not exceed 2 characters.
State (ST)	Enter a *State/Prov.* for the state or province name used in the CSR. This is a required field.
City (L)	Enter a *City* to represent the city name used in the CSR. This is a required field.
Organization (O)	Define an *Organization* for the organization used in the CSR. This is a required field.

Organizational Unit (OU)	Enter an *Org. Unit* for the name of the organization unit used in the CSR. This is a required field.
Common Name (CN)	If there's a common name (IP address) for the organizational unit issuing the certificate, enter it here.

6 Select the following **Additional Credentials** required for the generation of the CSR:

Email Address	Provide an email address used as the contact address for issues relating to this CSR.
Domain Name	Enter a *fully qualified domain name* (FQDN) is an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely. A trailing period is added to distinguish an FQDN from a regular domain name. For example, *somehost.example.com*. An FQDN differs from a regular domain name by its absoluteness, since a suffix is not added.
IP Address	Specify the IP address used as the controller or service platform destination for certificate requests.

7 Select the **Generate CSR** button at the bottom of the screen to produce the CSR.

14.3 Smart RF

Self Monitoring At Run Time RF Management (Smart RF) is an innovation designed to simplify RF configurations for new deployments, while (over time) providing on-going deployment optimization and radio performance improvements.

The Smart RF functionality scans the managed network to determine the best channel and transmit power for each wireless controller managed Access Point radio. Smart RF policies can be applied to specific RF Domains, to apply site specific deployment configurations and self recovery values to groups of devices within pre-defined physical RF coverage areas.

Smart RF also provides self recovery functions by monitoring the managed network in real-time and provides automatic mitigation from potentially problematic events such as radio interference, coverage holes and radio failures. Smart RF employs self recovery to enable a WLAN to better maintain wireless client performance and site coverage during dynamic RF environment changes, which typically require manual reconfiguration to resolve.

Smart RF is supported in standalone and clustered environments. In standalone environments, the individual controller or service platform manages the calibration and monitoring phases. In clustered environments, a single controller or service platform is elected a Smart Scan master and the remaining cluster members operate as Smart RF clients. In cluster operation, the Smart Scan master coordinates calibration and configuration and during the monitoring phase receives information from the Smart RF clients. Smart RF calibration can be triggered manually or continues at run-time, all the time.

Smart RF is supported on wireless controllers managing Access Points in either standalone or clustered environments.

Within the Operations node, Smart RF is managed within selected RF Domains, using the Access Points that comprise the RF Domain and their respective radio and channel configurations as the basis to conduct Smart RF calibration operations.

14.3.1 Managing Smart RF for an RF Domain

Smart RF

When calibration is initiated, Smart RF instructs adopted radios (within a selected RF Domain) to beacon on a specific legal channel, using a specific transmit power setting. Smart RF measures the signal strength of each beacon received from both managed and unmanaged neighboring APs to define a RF map of the neighboring radio coverage area. Smart RF uses this information to calculate each managed radio's RF configuration as well as assign radio roles, channel and power.

Within a well planned RF Domain, any associated radio should be reachable by at least one other radio. The Smart RF feature records signals received from its neighbors. Access Point to Access Point distance is recorded in terms of signal attenuation. The information is used during channel assignment to minimize interference.

To conduct Smart RF calibration for an RF Domain:

1 Select **Operations** > **Smart RF.**

2 Expand the System mode in the upper, left-hand, side of the user interface to display the RF Domains available for Smart RF calibration.

3 Select a RF Domain from amongst those displayed.

The Smart RF screen displays information specific to the devices within the selected RF Domain using data from the last interactive calibration.

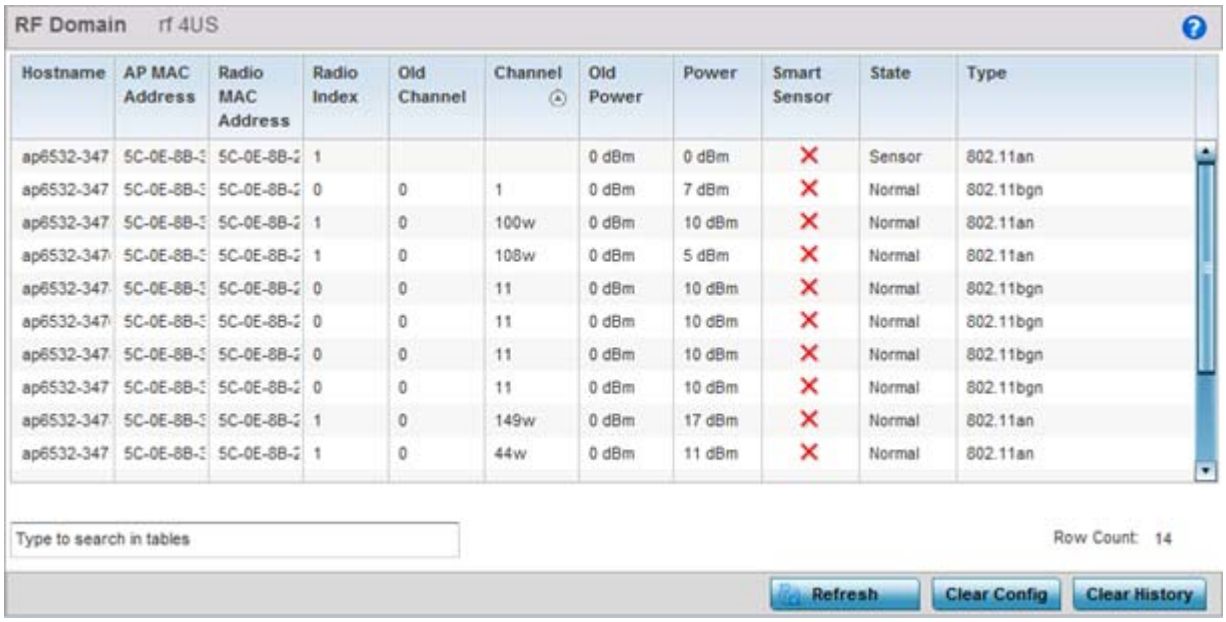


Figure 14-28 *Smart RF screen*

4 Refer to the following to determine whether a Smart RF calibration or an interactive calibration is required:

Hostname	Displays the assigned Hostname for each member of the RF Domain.
AP MAC Address	Displays the hardware encoded MAC address assigned to each Access Point radio within the selected RF Domain. This value cannot be modified as past of a calibration activity.

Radio MAC Address	Displays the hardware encoded MAC address assigned to each Access Point radio within the selected RF Domain. This value cannot be modified as past of a calibration activity.
Radio Index	Displays a numerical index assigned to each listed Access Point radio when it was added to the managed network. This index helps distinguish this radio from others within this RF Domain with similar configurations. This value is not subject to change as a result of a calibration activity, but each listed radio index can be used in Smart RF calibration.
Old Channel	Lists the channel originally assigned to each listed Access Point MAC address within this RF Domain. This value may have been changed as part an Interactive Calibration process applied to this RF Domain. Compare this Old Channel against the Channel value to right of it (in the table) to determine whether a new channel assignment was warranted to compensate for a coverage hole.
Channel	Lists the current channel assignment for each listed Access Point, as potentially updated by an Interactive Calibration. Use this data to determine whether a channel assignment was modified as part of an Interactive Calibration. If a revision was made to the channel assignment, a coverage hole was detected on the channel as a result of a potentially failed or under performing Access Point radio within this RF Domain.
Old Power	Lists the transmit power assigned to each listed Access Point MAC address within this RF Domain. The power level may have been increased or decreased as part an Interactive Calibration process applied to this RF Domain. Compare this Old Power level against the Power value to right of it (in the table) to determine whether a new power level was warranted to compensate for a coverage hole.
Power	This column displays the transmit power level for the listed Access Point MAC address after an Interactive Calibration resulted in an adjustment. This is the new power level defined by Smart RF to compensate for a coverage hole.
Smart Sensor	Defines whether a listed Access Point is smart sensor on behalf of the other Access Point radios comprising the RF Domain.
State	Displays the current state of the Smart RF managed Access Point radio. Possible states include: *Normal*, *Offline* and *Sensor*.
Type	Displays the radio type (802.11an, 802.11bgn etc.) of each listed Access Point radio within the selected RF Domain.

5 Select the **Refresh** button to (as needed) to update the contents of the Smart RF screen and the attributes of the devices within the selected RF Domain.

6 Select the **Clear Config** button to remove a displayed Smart RF configuration.

7 Select the **Clear History** button to revert the statistics counters to zero to begin a new assessment.

15 Statistics

This chapter describes statistics displayed by the *graphical user interface* (GUI). Statistics are available for controllers or service platforms and their managed devices.

A Smart RF statistical history is available to assess adjustments made to device configurations to compensate for detected coverage holes or device failures.

Statistics display detailed information about controller or service platform peers, health, device inventories, wireless clients associations, adopted AP information, rogue APs and WLANs.

Access Point statistics can be exclusively displayed to validate connected Access Points, their VLAN assignments and their current authentication and encryption schemes.

Wireless client statistics are available for an overview of client health. Wireless client statistics includes RF quality, traffic utilization and user details. Use this information to assess if configuration changes are required to improve network performance.

Guest access statistics are also available for the periodic review of wireless clients requesting the required pass code, authentication and access into the WiNG managed guest network.

For more information, see:

- *System Statistics*
- *RF Domain Statistics*
- *Controller Statistics*
- *Access Point Statistics*
- *Wireless Client Statistics*
- *Guest Access Statistics*

NOTE: NOC controllers (NX9000, NX9500, NX9510, NX7500, NX6500, NX6524 and RFS6000) can utilize an analytics developer interface as an additional tool available to administrators to review specific APIs in granular detail. For more information, see *Analytics Developer Interface on page 15-333*.

15.1 System Statistics

Statistics

The **System** screen displays information supporting managed devices or peer controllers. Use this information to asses the overall state of the devices comprising the system. Systems data is organized as follows:

- *Health*
- *Inventory*
- *Adopted Devices*
- *Pending Adoptions*
- *Offline Devices*
- *Device Upgrade*
- *Licenses*
- *WIPS Summary*

15.1.1 Health

System Statistics

The *Health* screen displays the overall performance of the controller or service platform managed network (system). This includes device availability, overall RF quality, resource utilization and network threat perception.

To display the health of the wireless controller managed network:

1 Select the **Statistics** menu from the Web UI.

2 Select the **System** node from the left navigation pane.

3 Select **Health** from the left-hand side of the UI.

Figure 15-1 *System - Health screen*

4 The **Devices** field displays the total number of devices in the controller or service platform managed network. The pie chart is a proportional view of how many devices are functional and currently online. Green indicates online devices and red offline devices detected within the controller or service platform managed network.

5 The **Offline Devices** table displays a list of detected devices in the network that are currently offline but available as potential managed resources.

The table displays the number of offline devices within each impacted RF Domain. Assess whether the configuration of a particular RF Domain is contributing to an excessive number of offline devices.

6 The **Traffic Utilization** table displays the top 5 RF Domains with the most effective resource utilization. Utilization is dependent on the number of devices connected to the RF Domain.

Top 5	Displays the top 5 RF Domains in terms of usage index. Utilization index is a measure of how efficiently the domain is utilized. This value is defined as a percentage of current throughput relative to the maximum possible throughput. The values are: *0-20* – Very low utilization *20-40* – Low utilization *40-60* – Moderate utilization 60 and above – High utilization
RF Domain	Displays the name of the RF Domain.
Client Count	Displays the number of wireless clients associated with the RF Domain.

7 The **Device Types** table displays the kinds of devices detected within the system. Each device type displays the number currently online and offline.

8 Use the **RF Quality** table to isolate poorly performing radio devices within specific RF Domains. This information is a starting point to improving the overall quality of the wireless controller managed network.The **RF Quality** area displays the RF Domain performance. Quality indices are:

- *0 – 50* (Poor)
- *50 – 75* (Medium)
- *75 – 100* (Good).

The RF Quality field displays the following:

Worst 5	Displays five RF Domains with the lowest quality indices in the wireless controller managed network. The value can be interpreted as: *0-50* – Poor quality *50-75* – Medium quality *75-100* – Good quality
RF Domain	Displays the name of the RF Domain wherein system statistics are polled for the poorly performing device.

9 The **System Security** table defines a Threat Level as an integer value indicating a potential threat to the system. It's an average of the threat indices of all the RF Domains managed by the wireless controller.

Threat Level	Displays the threat perception value. This value can be interpreted as: *0-2* – Low threat level *3-4* – Moderate threat level *5* – High threat level
RF Domain	Displays the name of the target RF Domain for which the threat level is displayed.

10 Select **Refresh** at any time to update the statistics counters to their latest values.

15.1.2 Inventory

System Statistics

The *Inventory* screen displays information about the physical hardware managed within the system by its member controller or service platforms. Use this information to assess the overall performance of wireless controller managed devices.

To display the inventory statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select the **System** node from the left navigation pane.

3 Select **Inventory** from the left-hand side of the UI.

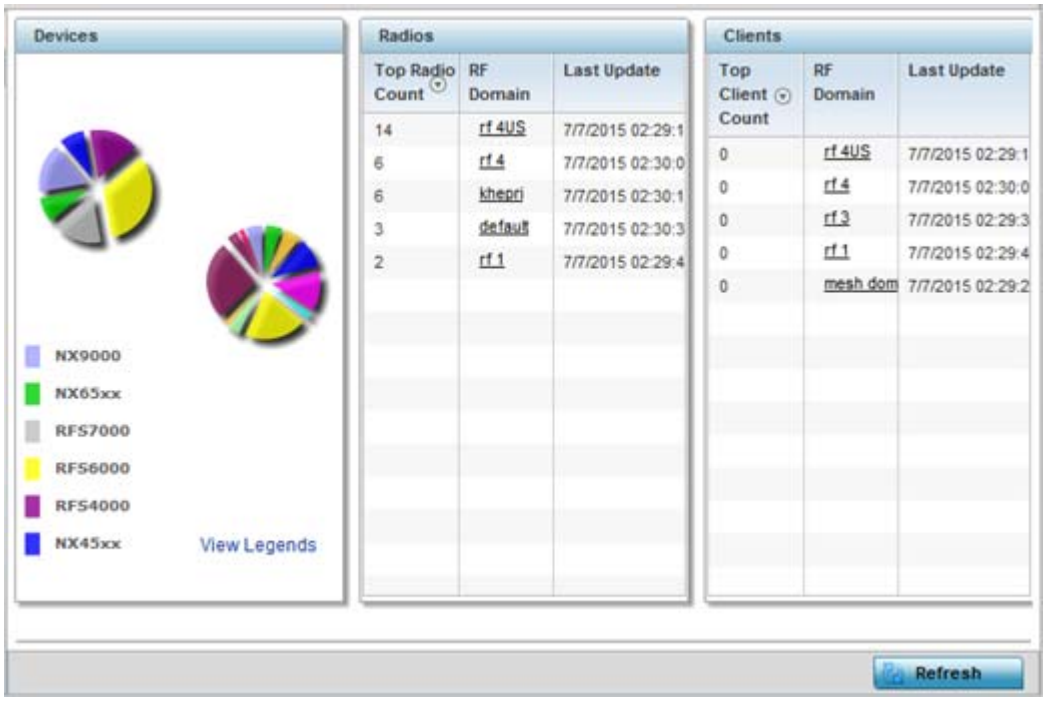


Figure 15-2 *System - Inventory screen*

4 The **Devices** field displays an exploded pie chart depicting controller, service platform and Access Point device type distribution by model. The device on the left displays managing controller models. Select **View Legends** to assess connected Access Points. Use this information to assess whether these are the correct models for the original deployment objective.

5 The **Radios** table displays radios deployed within the wireless controller managed network. This area displays the total number of managed radios and top 5 RF Domains in terms of radio count. The Total Radios value is the total number of radios in this system.

Top Radio Count	Displays the radios index of each listed top radio.
RF Domain	Displays the name of the RF Domain the listed radios belong. The RF Domain displays as a link that can be selected to display configuration and network address information in greater detail.
Last Update	Displays the UTC timestamp when each listed client was last seen on the network.

6 The **Clients** table displays the total number of wireless clients managed by the controller or service platform. This Top Client Count table lists the top 5 RF Domains, in terms of the number of wireless clients adopted:

Top Client Count	Displays the client index of each listed top performing client.
RF Domain	Displays the name of the client RF Domain.
Last Update	Displays the UTC timestamp when the client count was last reported.

7 Select **Refresh** to update the statistics counters to their latest values.

15.1.3 Adopted Devices

System Statistics

The *Adopted Devices* screen displays a list of devices adopted to the wireless controller managed network (entire system). Use this screen to view a list of devices and their current status.

To view adopted AP statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select the **System** node from the left navigation pane.

3 Select Adopted Devices from the left-hand side of the UI.

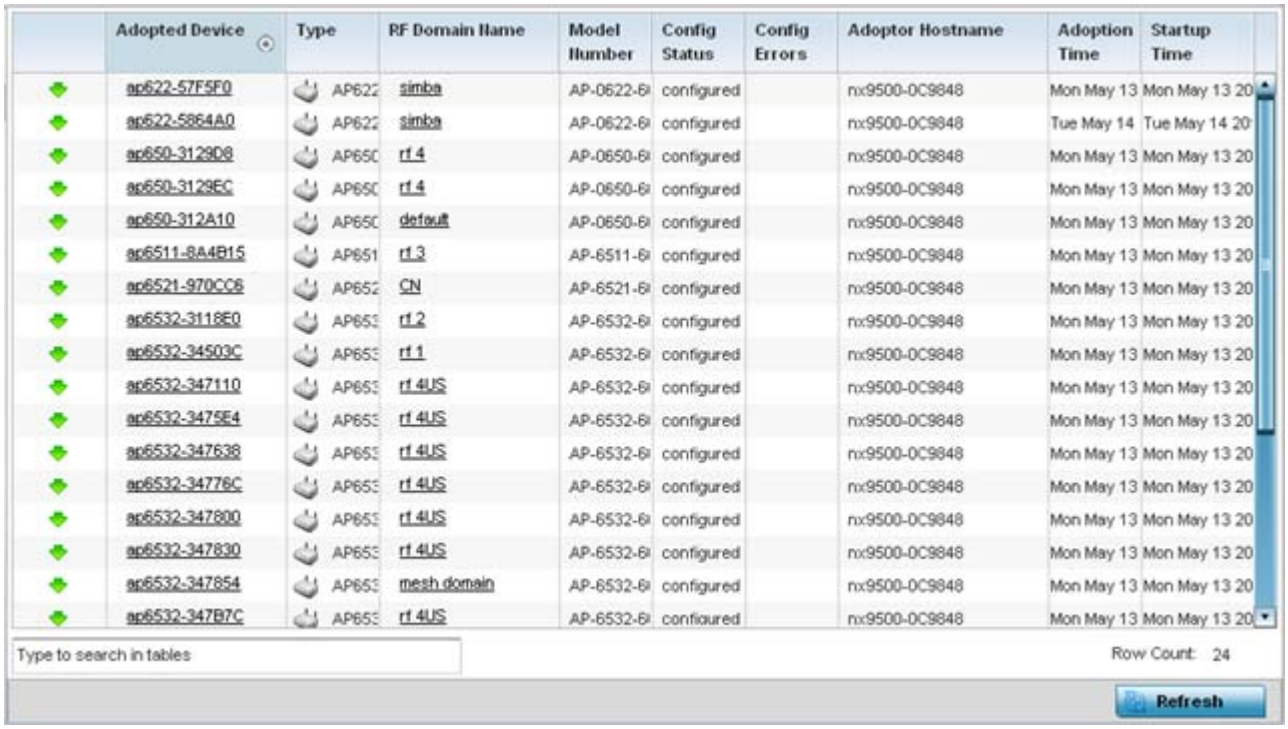


Figure 15-3 *System - Adopted Devices screen*

The **Adopted Devices** screen provides the following:

Adopted Device	Displays administrator assigned hostname of the adopted device. Select the adopted device link to display configuration and network address information in greater detail.
Type	Displays the adopted Access Point's model type.

RF Domain Name	Displays the domain the adopted AP has been assigned to. Select the RF Domain to display configuration and network address information in greater detail.
Model Number	Lists the model number of each AP that's been adopted to the controller or service platform since this screen was last refreshed.
Config Status	Displays the configuration file version in use by each listed adopted device. Use this information to determine whether an upgrade would increase the functionality of the adopted device.
Config Errors	Lists any errors encountered when the listed device was adopted by the controller or service platform.
Adopter Hostname	Lists the administrator hostname assigned to the adopting controller or service platform.
Adoption Time	Displays a timestamp for each listed device that reflects when the device was adopted by the controller or service platform.
Startup Time	Provides a date stamp when the adopted device was restarted post adoption.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

15.1.4 Pending Adoptions

System Statistics

The *Pending Adoptions* screen displays those devices detected within the controller or service platform coverage area, but have yet to be adopted by the controller or service platform. Review these devices to assess whether they could provide radio coverage to wireless clients needing support.

To view pending AP adoptions to the controller or service platform:

1 Select the **Statistics** menu from the Web UI.

2 Select the **System** node from the left navigation pane.

3 Select Pending Adoptions from the left-hand side of the UI.

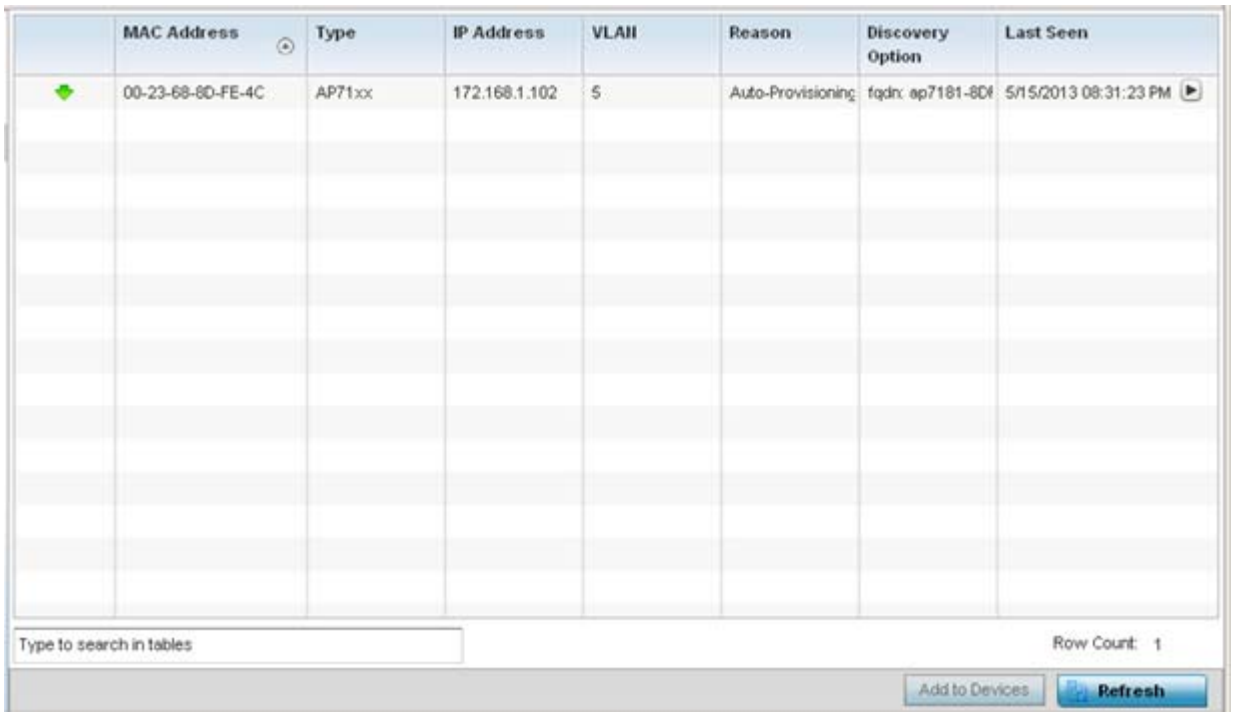


Figure 15-4 *System - Pending Adoptions screen*

The **Pending Adoptions** screen displays the following:

MAC Address	Displays the MAC address of the device pending adoption. Select the MAC address to view device configuration and network address information in greater detail.
Type	Displays the AP type.
IP Address	Displays the current IP Address of the device pending adoption.
VLAN	Displays the VLAN the device pending adoption will use as a virtual interface with its adopting controller or service platform.
Reason	Displays a status (reason) as to why the device is pending adoption.
Discovery Option	Displays the discovery option code for each AP listed pending adoption.
Last Seen	Displays the date and time stamp of the last time the device was seen. Click the arrow next to the date and time to toggle between standard time and UTC.
Add to Devices	Select a listed AP and select the *Add to Devices* button to begin the adoption process for this detected AP.
Refresh	Click the *Refresh* button to update the list of pending adoptions.

15.1.5 Offline Devices

System Statistics

The *Offline Devices* screen displays a list of devices in the controller or service platform managed network or RF Domain that are currently offline. Review the contents of this screen to help determine whether an offline status is still warranted.

To view offline device potentially available for adoption by the controller or service platform:

1 Select the **Statistics** menu from the Web UI.

2 Select the **System** node from the left navigation pane.

3 Select Offline Devices from the left-hand side of the UI.

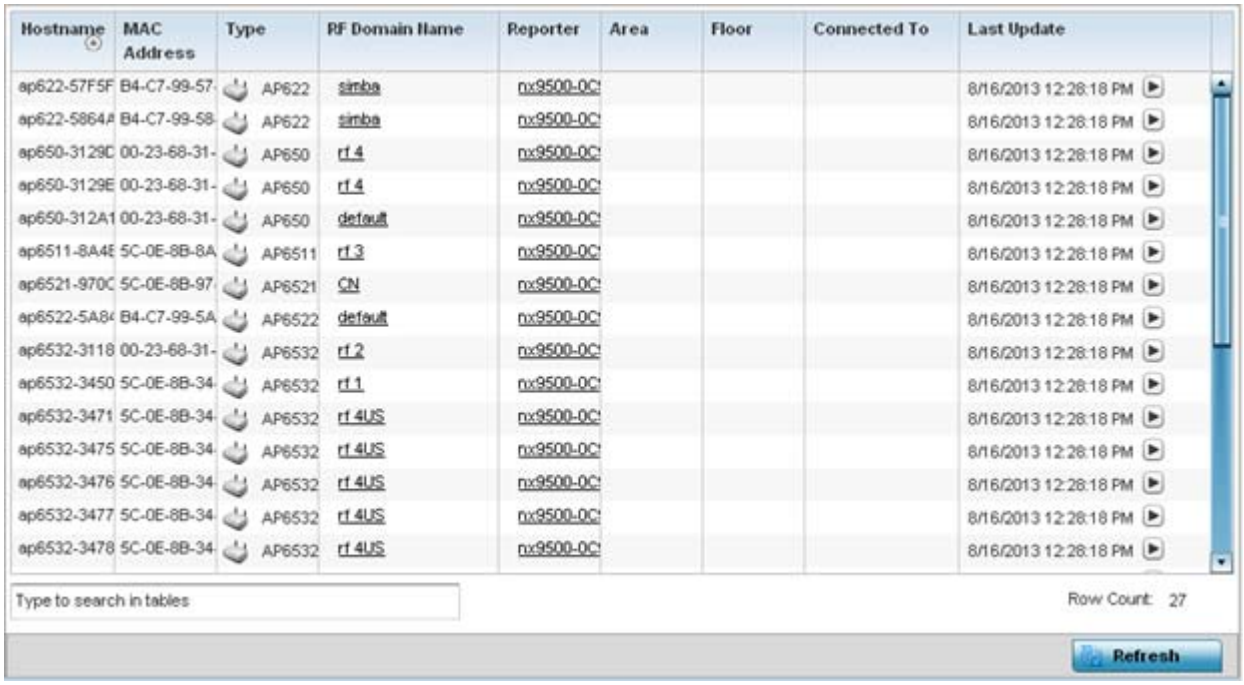


Figure 15-5 *System - Offline Devices screen*

The **Ofp indentfline Devices** screen provides the following:

Hostname	Lists the administrator assigned hostname provided when the device was added to the controller or service platform managed network.
MAC Address	Displays the factory encoded MAC address of each listed offline device.
Type	Displays the offline Access Point's model type.
RF Domain Name	Displays the name of the offline device's RF Domain membership, if applicable. Select the RF Domain to display configuration and network address information in greater detail.
Reporter	Displays the hostname of the device reporting the listed device as offline. Select the reporting device name to display configuration and network address information in greater detail.
Area	Lists the administrator assigned deployment area where the offline device has been detected.
Floor	Lists the administrator assigned deployment floor where the offline device has been detected.
Connected To	Lists the offline's device's connected controller, service platform or peer model Access Point.
Last Update	Displays the date and time stamp of the last time the device was detected within the controller or service platform managed network. Click the arrow next to the date and time to toggle between standard time and UTC.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

15.1.6 Device Upgrade

System Statistics

The *Device Upgrade* screen displays available licenses for devices within a cluster. It displays the total number of AP licenses.

To view a licenses statistics within the controller or service platform managed network:

1 Select the **Statistics** menu from the Web UI.

2 Select the **System** node from the left navigation pane.

3 Select **Device Upgrade** from the left-hand side of the UI.

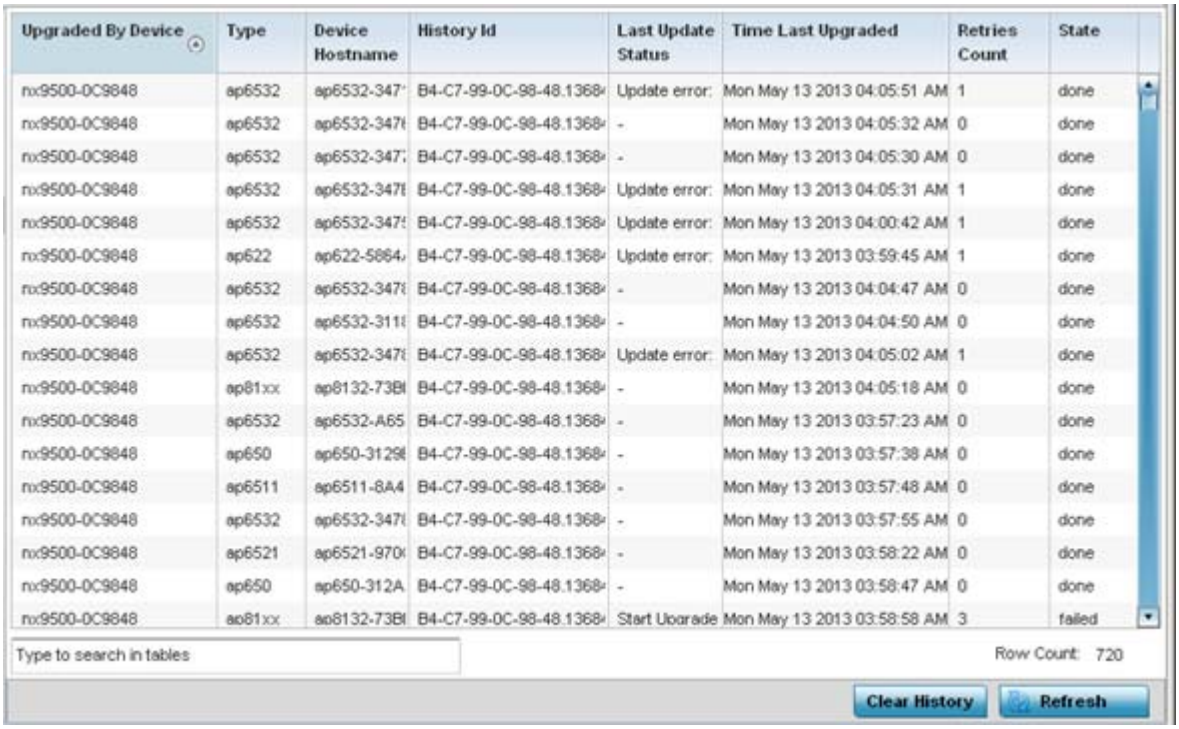


Figure 15-6 *System - Device Upgrade screen*

4 Select **Device Upgrade** from the left-hand side of the UI.

Upgraded By Device	Displays the MAC address of the controller, service platform or peer model Access Point that performed an upgrade.
Type	Displays the model type of the adopting controller, service platform or Access Point. An updating Access Point must be of the same model as the Access Point receiving the update.
Device Hostname	List the administrator assigned hostname of the device receiving an update.
History ID	Displays a unique timestamp for the upgrade event.
Last Update Status	Displays the initiation, completion or error status of each listed upgrade operation.
Time Last Upgraded	Lists the date and time of each upgrade operation.
Retries Count	Displays the number of retries required in an update operation.

State	Displays the *done* or *failed* state of an upgrade operation.
Clear History	Select *Clear History* to clear the screen of its current status and begin a new data collection.
Refresh	Select *Refresh* to update the screen's statistics counters to their latest values.

15.1.7 Licenses

System Statistics

The *Licenses* statistics screen displays available licenses for devices within a cluster. It displays the total number of AP licenses. **Native** (local) and **Guest** license utilization can now be separately tracked as well.

To view a licenses statistics within the controller or service platform managed network:

1 Select the **Statistics** menu from the Web UI.

2 Select the **System** node from the left navigation pane.

3 Select **Licenses** from the left-hand side of the UI.

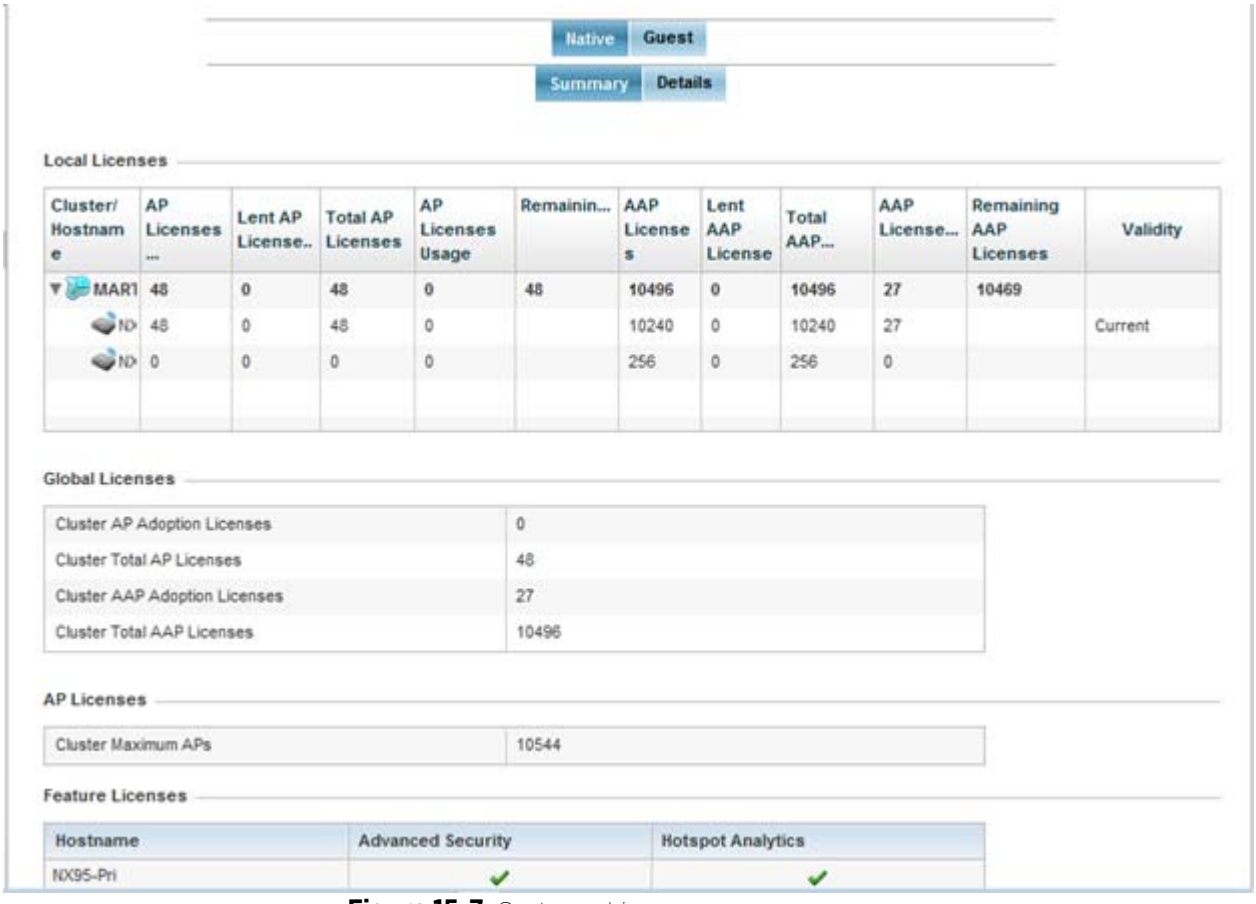


Figure 15-7 *System - Licenses screen*

4 The **Local Licenses** table provides the following information:

Cluster/Hostname	Lists the administrator assigned cluster hostname whose license count and utilization is tallied in this Local Licenses table.

AP Licenses Installed	Lists the number of Access Point connections available to this controller or service platform under the terms of the current license.
Lent AP Licenses	Displays the number of Access Point licenses lent (from this controller or service platform) to a cluster member to compensate for an Access Point's license deficiency.
Total AP Licenses	Displays the total number of Access Point connection licenses currently available to this controller or service platform.
AP License Usage	Lists the number of Access Point connections currently utilized by this controller or service platform out of the total available under the terms of the current license.
Remaining AP Licenses	Lists the remaining number of AP licenses available from the pooled license capabilities of all the members of the cluster.
AAP Licenses Installed	Lists the number of Adaptive Access Point connections available to this controller or service platform under the terms of the current license.
Lent AAP Licenses	Displays the number of Adaptive Access Point licenses lent (from this controller or service platform) to a cluster member to compensate for an Access Point licenses deficiency.
Total AAP Licenses	Displays the total number of Adaptive Access Point connection licenses currently available to this controller or service platform.
AAP Licenses Usage	Lists the number of Adaptive Access Point connections currently utilized by this controller or service platform out of the total available under the terms of the current license.
Remaining AAP Licenses	Lists the remaining number of AAP licenses available from the pooled license capabilities of all the members of the cluster.
Validity	Displays validity information for the license's legal usage with the controller or service platform.

5 The **Global Licenses** table provides the following information:

Cluster AP Adoption Licenses	Displays the current number of Access Point adoption licenses utilized by controller or service platform connected Access Points within a cluster.
Cluster Total AP Licenses	Displays the total number of Access Point adoption licenses available to controller or service platform connected Access Points within a cluster.
Cluster AAP Adoption Licenses	Displays the current number of Adaptive Access Point adoption licenses utilized by controller or service platform connected Access Points within a cluster.
Cluster Total AAP Licenses	Displays the total number of Adaptive Access Point adoption licenses available to controller or service platform connected Access Points within a cluster.

6 The **AP Licenses** table provides the following information:

Cluster Maximum AP	Lists the maximum number of Access Points permitted in a cluster under the terms of the current license.

7 The **Featured Licenses** area provides the following information:

Hostname	Displays the administrator assigned hostname of the controller, service platform or Access Point whose potentially implemented a advanced security, WIPS or Analytics feature licenses.

Advanced Security	Displays whether the separately licensed Advanced Security application is installed for each hostname.
Hotspot Analytics	Displays whether a separately licensed Analytics application is installed for supported NX9500 and NX9510 service platforms.

8 Select the **Details** tab.

Refer to the **Details** screen to further assess the total number of cluster member licenses available, cluster memberships, current utilization versus total licenses available, borrowed licenses, remaining licenses and license validity.

9 Refer to the following license utilization data:

Cluster/Hostname	Lists the administrator assigned cluster hostname whose license count and utilization is listed and tallied for member controllers, service platforms or Access Points.
AP Licenses Installed	Lists the number of Access Point connections available to this controller or service or peer Access Point under the terms of the current license.
Borrowed AP Licenses	Displays the number of Access Point licenses temporarily borrowed from a cluster member to compensate for an AP license deficiency.
Total AP Licenses	Displays the total number of Access Point connection licenses currently available to clustered devices.
AP Licenses Usage	Lists the number of Access Point connections currently utilized out of the total available under the terms of current licenses.
Remaining AP Licenses	Lists the remaining number of AP licenses available from the pooled license capabilities of cluster members.
AAP Licenses Installed	Lists the number of Adaptive Access Point connections available under the terms of current licenses.
Borrowed AAP Licenses	Displays the number of Adaptive Access Point licenses temporarily borrowed from a cluster member to compensate for an AAP license deficiency.
Total AAP Licenses	Displays the total number of Adaptive Access Point connection licenses currently available to clustered devices.
AAP Licenses Usage	Lists the number of Adaptive Access Point connections currently utilized out of the total available under the terms of the current licenses.
Remaining AAP Licenses	Lists the remaining number of AAP licenses available from the pooled license capabilities of all the members of the cluster.
Validity	Displays validity information for the license's legal usage by cluster member devices.
Refresh	Select *Refresh* to update the screen's statistics counters to their latest values.

15.1.8 WIPS Summary

System Statistics

The *Wireless Intrusion Protection System* (WIPS) provides continuous protection against wireless threats and acts as an additional layer of security complementing wireless VPNs and existing encryption and authentication policies. Controllers and service platforms support WIPS through the use of dedicated sensor devices, designed to

actively detect and locate unauthorized AP devices. After detection, they use mitigation techniques to block devices using manual termination, air lockdown or port suppression.

The **WIPS Summary** screen lists RF Domains residing in the system and reports the number of unauthorized and interfering devices contributing to the potential poor performance of the RF Domain's network traffic. Additionally, the number of WIPS events reported by each RF Domain is also listed to help an administrator better mitigate risks to the network.

To review and assess the impact of rogue and interfering Access Points, as well as the occurrence of WIPS events within the controller or service platform's managed system:

1 Select the **Statistics** menu from the Web UI.

2 Select the **System** node from the left navigation pane.

3 Select **WIPS Summary** from the left-hand side of the UI.

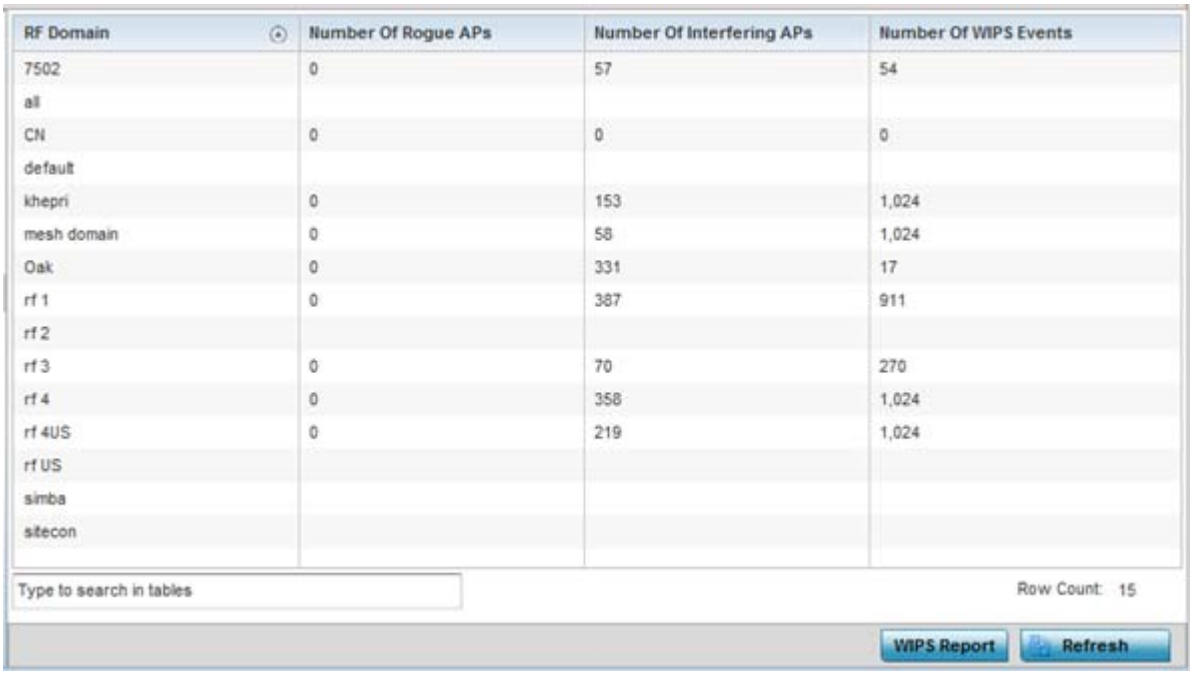


Figure 15-8 *System - WIPS Summary screen*

4 Refer to the following WIPS data reported for each RF Domain in the system:

RF Domain	Lists the RF Domain within the system reporting rogue and interfering Access Point event counts. Use this information to assess whether a particular RF Domain is reporting an excessive number of events or a large number of potentially invasive rogue Access Points versus the other RF Domains within the controller, service platform or Access Point managed system.
Number of Rogue APs	Displays the number of unsanctioned devices in each listed RF Domain. Unsanctioned devices are those devices detected within the listed RF Domain, but have not been deployed by a administrator as a known and approved controller or service platform managed device.

Number of Interfering APs	Displays the number of devices exceeding the interference threshold in each listed RF Domain. Each RF Domain utilizes a WIPS policy with a set interference threshold (from -100 to -10 dBm). When a device exceeds this *noise* value, its defined as an interfering Access Point capable of disrupting the signal quality of other sanctioned devices operating below an approved RSSI maximum value.
Number of WIPS Events	Lists the number of devices triggering a WIPS event within each listed RF Domain.Each RF Domain utilizes a WIPS policy where excessive, MU and AP events can have their individual values set for event generation. An administrator can *enable* or *disable* the filtering of each listed event and set the thresholds required for the generation of the event notification and filtering action.

5 Select the **WIPS Report** button to launch a sub-screen to filter how WIPS reports are generated for the system.

Figure 15-9 *System - WIPS Summary screen*

Select **Summary** to capture all WIPS data or just select *Only Rogue APs*, *Only Interferer APs* for *All APs* to refine event reporting to a specific type of WIPS activity. Select **Generate Report** to compile and archive the results of the query.

6 Select **Refresh** to update the screen's statistics counters to their latest values.

15.2 RF Domain Statistics

Statistics

The RF Domain screens display status for a selected RF domain. This includes the RF Domain *health* and *device inventory, wireless clients* and *Smart RF* functionality. RF Domains allow administrators to assign regional, regulatory and RF configuration to devices deployed in a common coverage area such as on a building floor, or site. Each RF Domain contains regional, regulatory and sensor server configuration parameters and may also be assigned policies that determine Access, SMART RF and WIPS configuration.

Use the following information to obtain an overall view of the performance of the selected RF Domain and troubleshoot issues with the domain or any member device.

- *Health*
- *Inventory*
- *Devices*
- *AP Detection*
- *Wireless Clients*
- *Device Upgrade*
- *Wireless LANs*

- *Radios*
- *Bluetooth*
- *Mesh*
- *Mesh Point*
- *SMART RF*
- *WIPS*
- *Captive Portal*
- *Application Visibility (AVC)*
- *Coverage Hole Summary*
- *Coverage Hole Details*

15.2.1 Health

- *RF Domain Statistics*

The *Health* screen displays general status information for a selected RF Domain, including data polled from all its members.

To display the health of a controller or service platform's RF Domain:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **Health** from the RF Domain menu.

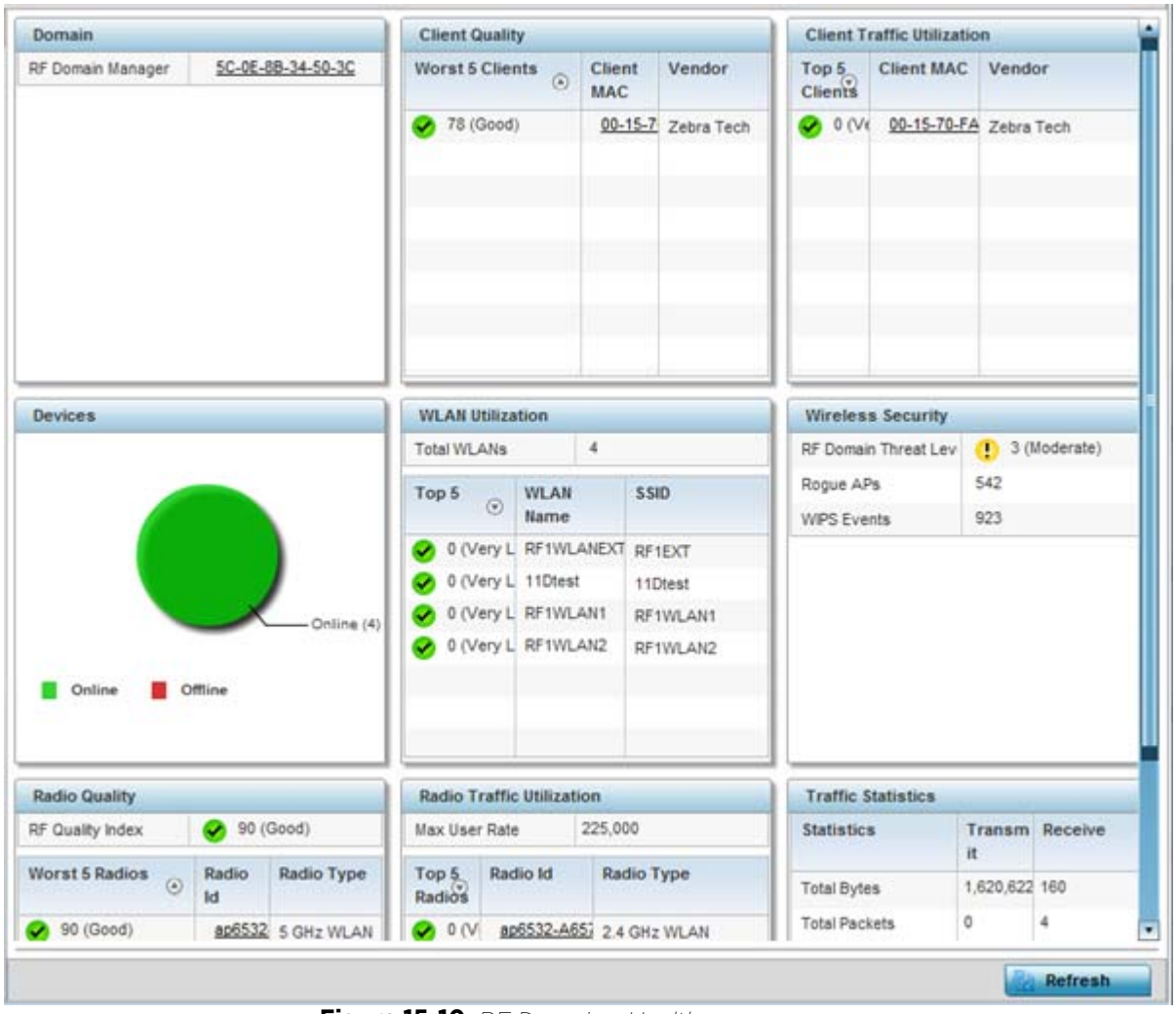


Figure 15-10 *RF Domain - Health screen*

4 The **Domain** field displays the name of the RF Domain manager. The RF Domain manager is the focal point for the radio system and acts as a central registry of applications, hardware and capabilities. It also serves as a mount point for all the different pieces of the hardware system file.

5 The **Devices** field displays the total number of online versus offline devices in the RF Domain, and an exploded pie chart depicts their status.

6 The **Radio Quality** field displays information *on the RF Domain*'s RF quality. The RF quality index is the overall effectiveness of the RF environment as a percentage of the connect rate in both directions, as well as the retry and error rate. This area also lists the worst 5 performing radios in the RF Domain.

The RF Quality Index can be interpreted as:

- *0-20* – Very poor quality
- *20-40* – Poor quality
- *40-60* – Average quality
- *60-100* – Good quality

7 Refer to the **Radio Quality** table for RF Domain member radios requiring administration to improve performance:

Worst 5 Radios	Displays five radios with the lowest average quality in the RF Domain.
Radio ID	Lists each radio's administrator defined hostname and its radio designation (radio 1, radio 2 or radio 3).
Radio Type	Displays the radio type as either 5 GHz or 2.4 GHz.

8 Refer to the **Client Quality** table for RF Domain connected clients requiring administration to improve performance:

Worst 5 Clients	Displays the five clients having the lowest average quality indices.
Client MAC	Displays the hardcoded radio MAC of the wireless client.
Vendor	Displays the vendor name of the wireless client.

9 Refer to the **WLAN Utilization** field to assess the following:

Total WLANs	Displays the total number of WLANs managed by RF Domain member Access Points.
Top 5	Displays the five RF Domain utilized WLANs with the highest average quality indices.
WLAN Name	Displays the WLAN Name for each of the Top 5 WLANs in the Access Point RF Domain.
SSID	Lists the SSD utilized by each listed top 5 performing RF Domain WLANs.

10 The **Radio Traffic Utilization** area displays the following:

Max. User Rate	Displays the maximum recorded user rate in kbps.
Top 5 Radios	Displays five radios with the best average quality in the RF Domain.
Radio ID	Lists each radio's administrator defined hostname and its radio designation (radio 1, radio 2 or radio 3).
Radio Type	Displays the radio type as either 5 GHz or 2.4 GHz.

11 Refer to the **Client Traffic Utilization** table:

Top 5 Clients	Displays the five clients having the highest average quality indices.
Client MAC	Displays the client's hardcoded MAC address used a hardware identifier.
Vendor	Lists each client's manufacturer.

12 The **Wireless Security** area indicates the security of the transmission between WLANs and the wireless clients they support. This value indicates the vulnerability of the WLANs.

RF Domain Threat Level	Indicates the threat from the wireless clients trying to find network vulnerabilities within the Access Point RF Domain. The threat level is represented by an integer.

Rogue APs	Lists the number of unauthorized Access Points detected by RF Domain member devices.
WIPS Events	Lists the number of WIPS events generated by RF Domain member devices.

13 The **Traffic Statistics** statistics table displays the following information for transmitted and received packets:

Total Bytes	Displays the total bytes of data transmitted and received within the Access Point RF Domain.
Total Packets	Lists the total number of data packets transmitted and received within the Access Point RF Domain.
User Data Rate	Lists the average user data rate within the Access Point RF Domain.
Bcast/Mcast Packets	Displays the total number of broadcast/multicast packets transmitted and received within the Access Point RF Domain.
Management Packets	This is the total number of management packets processed within the Access Point RF Domain.
Tx Dropped Packets	Lists total number of dropped data packets within the Access Point RF Domain.
Rx Errors	Displays the number of errors encountered during data transmission within the Access Point RF Domain. The higher the error rate, the less reliable the connection or data transfer.

14 The **SMART RF Activity** area displays the following:

Time Period	Lists the time period when Smart RF calibrations or adjustments were made to compensate for radio coverage holes or interference.
Power Changes	Displays the total number of radio transmit power changes that have been made using SMART RF within the Access Point RF Domain.
Channel Changes	Displays the total number of radio transmit channel changes that have been made using SMART RF within the Access Point RF Domain.
Coverage Changes	Displays the total number of radio coverage area changes that have been made using SMART RF within the Access Point RF Domain.

15.2.2 Inventory

RF Domain Statistics

The *Inventory* screen displays an inventory of RF Domain member Access Points, connected wireless clients, wireless LAN utilization and radio availability.

To display RF Domain inventory statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **Inventory** from the RF Domain menu.

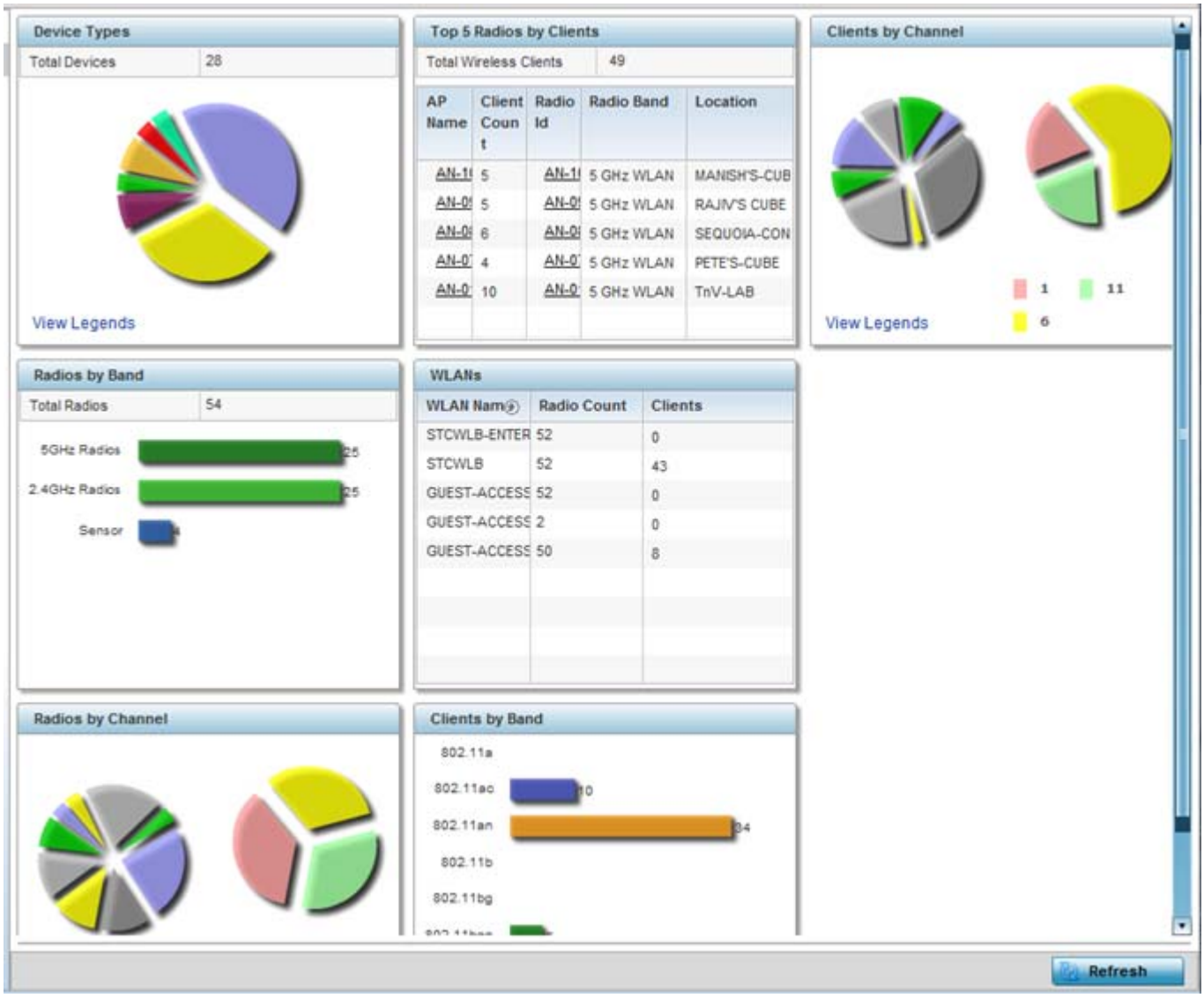


Figure 15-11 *RF Domain - Inventory screen*

4 The **Device Types** table displays the total members in the RF Domain. The exploded pie chart depicts the distribution of RF Domain members by controller and Access Point model type.

5 The **Radios by Band** field displays the total number of radios using 802.11an and 802.11bgn bands within the RF Domain. The number of radios designated as sensors is also represented.

6 The **Radios by Channel** field displays the radio channels utilized by RF Domain member devices in two separate charts. One chart displays for 5 GHz channels and the other for 2.4 GHz channels.

7 The **Top 5 Radios by Clients** table displays the highest 5 performing wireless clients connected to RF Domain members.

Total Wireless Clients	Displays the total number of clients connected to RF Domain members.
AP Name	Displays the clients connected and reporting Access Point. The name displays as a link that can be selected to display Access Point data in greater detail.

Client Count	List the number of connected clients to each listed RF Domain member Access Point.
Radio Id	Lists each radio's administrator defined hostname and its radio designation (radio 1, radio 2 etc.). The name displays as a link that can be selected to display Access Point data in greater detail.
Radio Band	Lists each client's operational radio band.
Location	Displays system assigned deployment location for the client.

8 Refer to the **WLANs** table to review RF Domain WLAN, radio and client utilization. Use this information to help determine whether the WLANs within this RF Domain have an optimal radio and client utilization.

9 The **Clients by Band** bar graph displays the total number of RF Domain member clients by their IEEE 802.11 radio type.

10 The **Clients by Channel** pie charts displays the channels used by RF Domain member clients using 5GHz and 2.4GHz radios.

11 Periodically select **Refresh** to update the contents of the screen to their latest values.

15.2.3 Devices

RF Domain Statistics

The **Devices** screen displays RF Domain member hardware data, connected client counts, radio data and network IP address.

To display RF Domain member device statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **Devices** from the RF Domain menu.

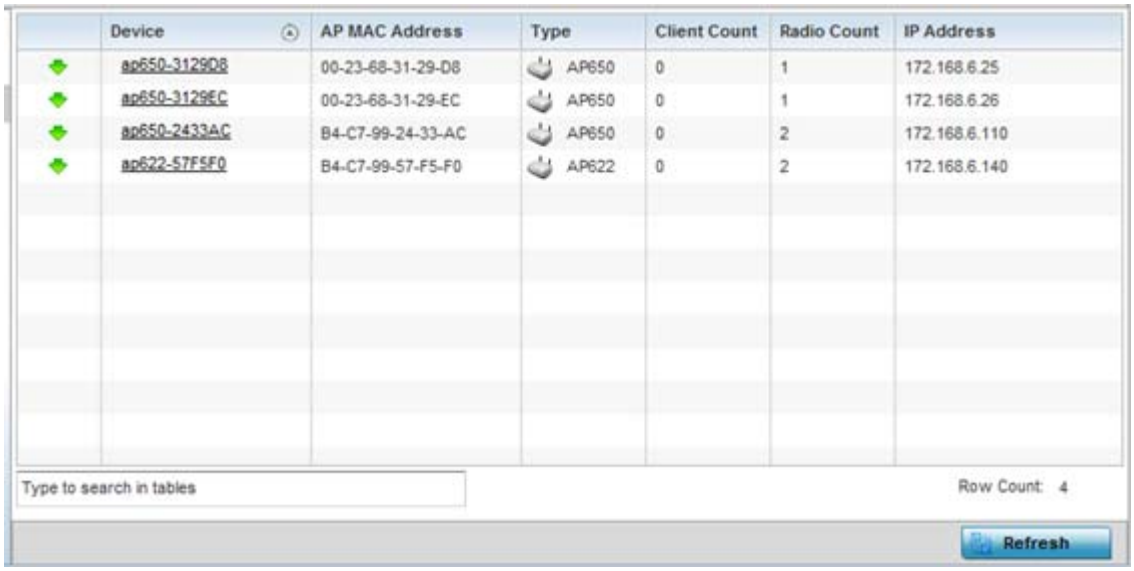


Figure 15-12 *RF Domain - Devices screen*

Device	Displays the system assigned name of each device that's a member of the RF Domain. The name displays as a link that can be selected to display configuration and network address information in greater detail.
AP MAC Address	Displays each device's factory encoded MAC address as its hardware identifier.
Type	Displays each device model within the selected RF Domain.
Client Count	Displays the number of clients connected with each listed device. Supported Access Point models support up to 256 clients per Access Point, with the exception of AP6521 model, which only supports 128.
Radio Count	Displays the number of radios on each listed device.
IP Address	Displays the IP address each listed device is using as a network identifier.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.4 AP Detection

RF Domain Statistics

The *AP Detection* screen displays information about detected Access Points that are not members of a RF Domain. They could be authorized devices or potential rogue devices.

To view device information on detected Access Points:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **AP Detection** from the RF Domain menu.

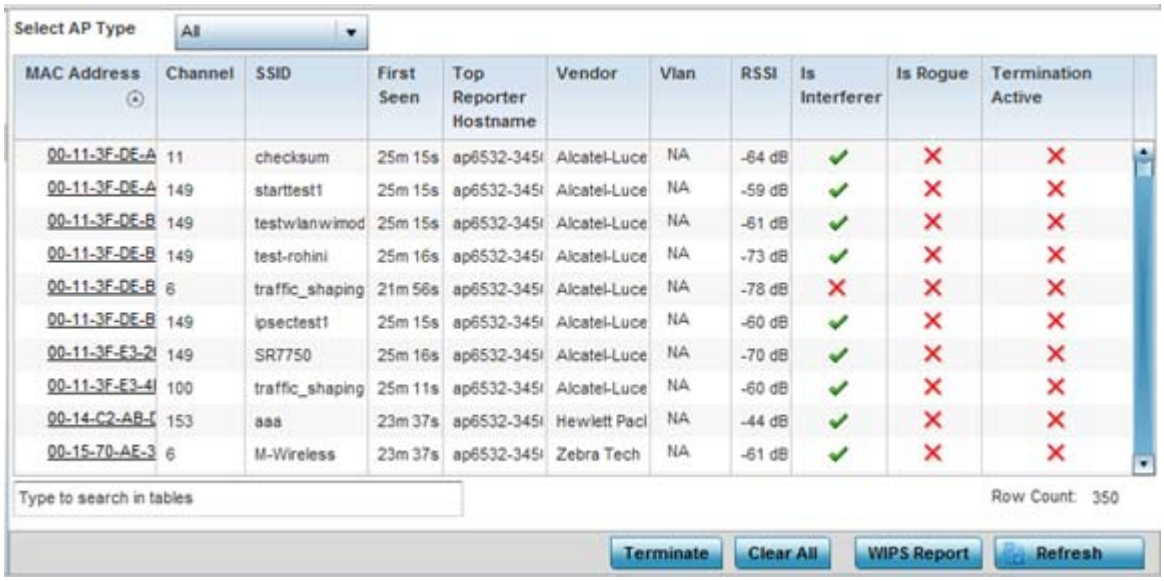


Figure 15-13 *RF Domain - AP Detection screen*

The **AP Detection** screen displays the following:

MAC Address	Displays the hardware encoded MAC address of each listed Access Point detected by a RF Domain member device. The MAC address is set at the factory and cannot be modified via the management software. The MAC address displays as a link that can be selected to display RF Domain member device information in greater detail.
Channel	Displays the channel of operation used by the detected Access Point. The channel must be utilized by both the Access Point and its connected client and be approved for the target deployment country.
SSID	Displays the *Service Set ID* (SSID) of the network to which the detected Access Point belongs.
First Seen	Provides a timestamp when the detected Access Point was first detected by a RF Domain member device.
Top Reporter Hostname	Lists the administrator assigned hostname of the top performing RF Domain member detecting the listed Access Point MAC address. Consider this top performer the best resource for information on the detected Access Point and its potential threat.
Vendor	Lists the manufacturer of the detected Access Point as an additional means of assessing its potential threat to the members of this RF Domain and its potential for interoperability with RF Domain device members.
VLAN	Lists the numeric VLAN ID (virtual interface) the detected Access Point was detected on by members of this RF Domain.
RSSI	Displays the *Received Signal Strength Indicator* (RSSI) of the detected Access Point. Use this variable to help determine whether a device connection would improve network coverage or add noise.
Is Interferer	Lists whether the detected device exceeds the administrator defined RSSI threshold (from -100 to -10 dBm) determining whether a detected Access Point is classified as an interferer.

Is Rogue	Displays whether the detected device has been classified as a rogue device whose detection threatens the interoperation of RF Domain member devices.
Termination Active	Lists whether Air Termination is active and applied to the detected Access Point. Air termination lets you terminate the connection between your wireless LAN and any Access Point or client associated with it. If the device is an Access Point, all clients dis-associated with the Access Point. If the device is a client, its connection with the Access Point is terminated. Air Termination is disabled by default.
Terminate	Select the *Terminate* button to remove the selected Access Point from RF Domain membership.
Clear All	Select *Clear All* to reset the statistics counters to zero and begin a new data collection.
WIPS Report	Select *WIPS Report* launch a subscreen to save a WIPS report (in PDF format) to a specified location. This is a recommended practice to capture RF Domain member Access Point client connection terminations in a format that can be archived externally.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.5 Wireless Clients

RF Domain Statistics

The *Wireless Clients* screen displays device information for wireless clients connected to RF Domain member Access Points. Review this content to determine whether a client should be removed from Access Point association within the selected RF Domain.

To review a RF Domain's connected wireless clients:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **Wireless Clients** from the RF Domain menu.

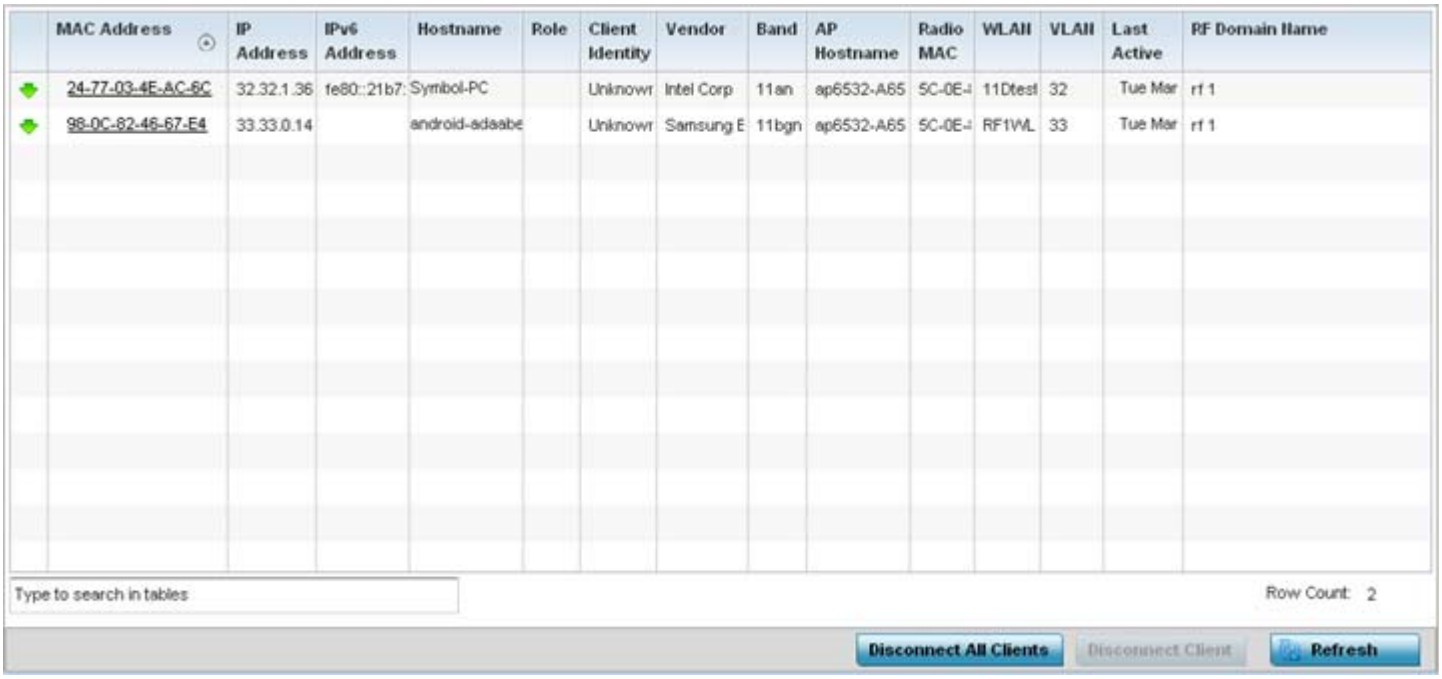


Figure 15-14 *RF Domain - Wireless Clients screen*

The **Wireless Clients** screen displays the following:

MAC Address	Displays the hostname (MAC address) of each listed wireless client. This address is hard-coded at the factory and can not be modified. The address displays as a link that can be selected to display RF Domain member device and network address information in greater detail.
IP Address	Displays the current IP address the wireless client is using for a network identifier.
IPv6 Address	Displays the current IPv6 formatted IP address a listed wireless client is using as a network identifier. IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Hostname	Displays the unique administrator assigned hostname when the client's configuration was originally set.
Role	Lists the role assigned to each controller, service platform or Access Point managed client.
Client Identity	Lists the client's operating system vendor identity (Android, Windows etc.)
Vendor	Displays the vendor (or manufacturer) of the wireless client.
Band	Lists the 2.4 or 5 GHz radio band the listed client is currently utilizing with its connected Access Point, controller or service platform within the RF Domain.
AP Hostname	Displays the administrator assigned hostname of the Access Point to which the client is connected.
Radio MAC	Lists the hardware encoded MAC address of the Access Point radio to which the client is currently connected within the RF Domain.
WLAN	Displays the name of the WLAN the wireless client is currently using for its interoperation within the RF Domain.

VLAN	Displays the VLAN ID the client's connected Access Point has defined for use as a virtual interface.
Last Active	Displays the time when this wireless client was last detected by a RF Domain member.
RF Domain Name	Lists each client's RF Domain membership as defined by its connected Access Point and associated controller or service platform.
Disconnect All Clients	Select the *Disconnect All Clients* button to terminate each listed client's connection and RF Domain membership.
Disconnect Client	Select a specific client MAC address and select the *Disconnect Client* button to terminate this client's connection and RF Domain membership.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.6 Device Upgrade

RF Domain Statistics

The *Device Upgrade* screen reports information about devices receiving updates the RF Domain member provisioning the device. Use this screen to assess version data and upgrade status.

To view wireless device upgrade data for RF Domain members:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **Device Upgrade** from the RF Domain menu.

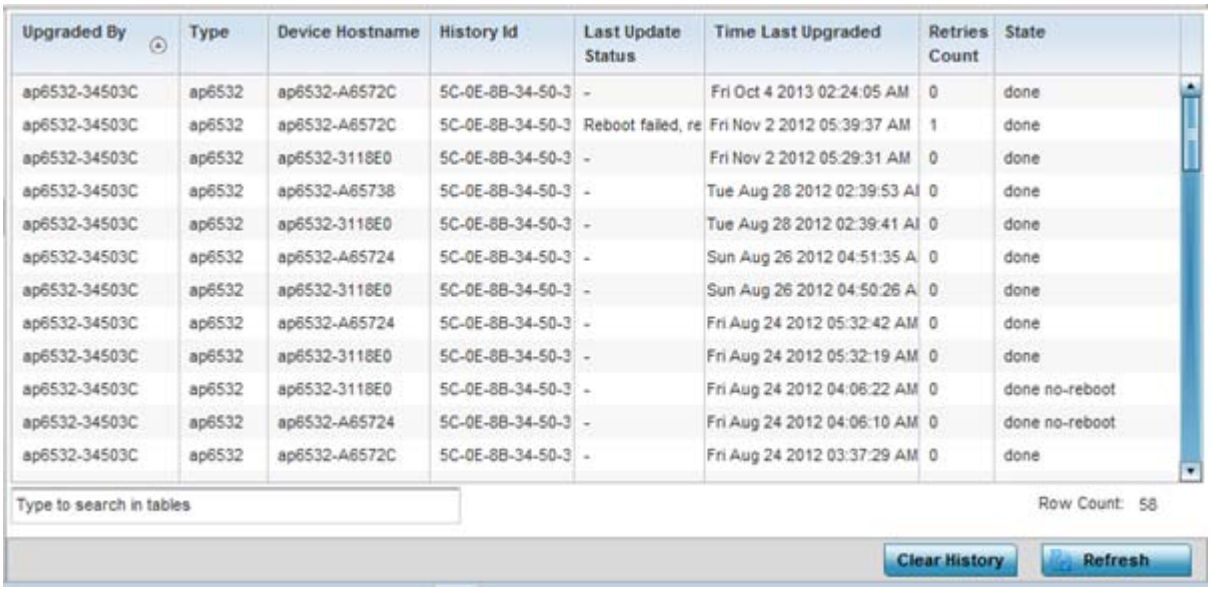


Figure 15-15 *RF Domain - Device Upgrade screen*

The **Device Upgrade** screen displays the following for RF Domain member devices:

Upgraded By	Lists the name of the device performing an update on behalf of a RF Domain member peer device.

Type	Displays the model of the device receiving an update. An updating Access Point must be of the same model as the Access point receiving the update.
Device Hostname	Lists the administrator assigned hostname of each device receiving an update from a RF Domain member.
History Id	Lists the RF Domain member device's MAC address along with a history ID appended to it for each upgrade operation.
Last Update Status	Displays the last status message from the RF Domain member device performing the upgrade operation.
Time Last Upgrade	Displays a timestamp for the last successful upgrade.
Retries Count	Lists the number of retries needed for each listed RF Domain member update operation.
State	Lists whether the upgrade operation is completed, in-progress, failed or whether an update was made without a device reboot.
Clear History	Select *Clear History* to remove the upgrade records for RF Domain member devices. Unlike the Refresh function (that updates existing data), Clear History removes the update record from the screen.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.7 Wireless LANs

RF Domain Statistics

The *Wireless LANs* screen displays the name, network identification and radio quality information for the WLANs currently being utilized by RF Domain members.

To view wireless LAN statistics for RF Domain members:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **Wireless LANs** from the RF Domain menu.

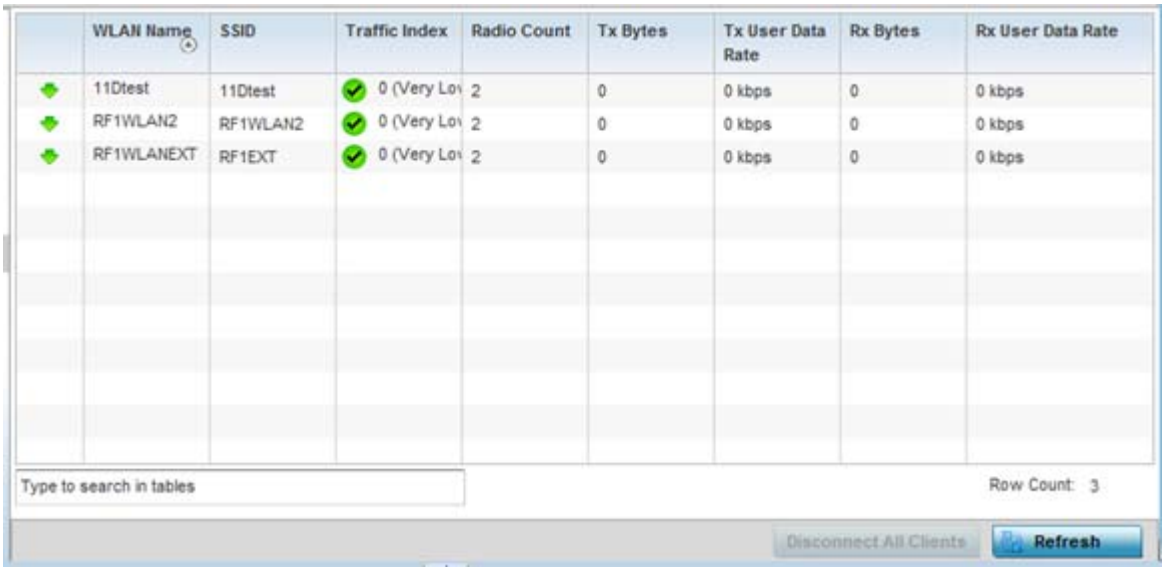


Figure 15-16 *RF Domain - Wireless LANs screen*

The **Wireless LANs** screen displays the following:

WLAN Name	Displays the name assigned to each WLAN upon its creation within the controller or service platform managed network.
SSID	Displays the *Service Set ID* (SSID) assigned to the WLAN upon its creation within the controller or service platform managed network.
Traffic Index	Displays the traffic utilization index of each listed WLAN, which measures how efficiently the traffic medium is used. It's defined as the percentage of current throughput relative to the maximum possible throughput. Traffic indices are: *0 – 20* (very low utilization), *20 – 40* (low utilization), *40 – 60* (moderate utilization), and *60 and above* (high utilization).
Radio Count	Displays the number of radios deployed in each listed WLAN by RF Domain member devices.
Tx Bytes	Displays the average number of packets (in bytes) sent on each listed RF Domain member WLAN.
Tx User Data Rate	Displays the average data rate per user for packets transmitted on each listed RF Domain member WLAN.
Rx Bytes	Displays the average number of packets (in bytes) received on each listed RF Domain member WLAN.
Rx User Data Rate	Displays the average data rate per user for packets received on each listed RF Domain member WLAN.
Disconnect All Clients	Select the *Disconnect All Clients* button to terminate each listed client's WLAN membership from this RF Domain.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.8 Radios

RF Domain Statistics

The **Radio** screens displays information on RF Domain member Access Point radios. Use these screens to troubleshooting radio issues negatively impacting RF Domain performance.

For more information, refer to the following:

- *Status*
- *RF Statistics*
- *Traffic Statistics*

15.2.8.1 Status

To view the RF Domain radio statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Expand **Radios** from the RF Domain menu and select **Status.**

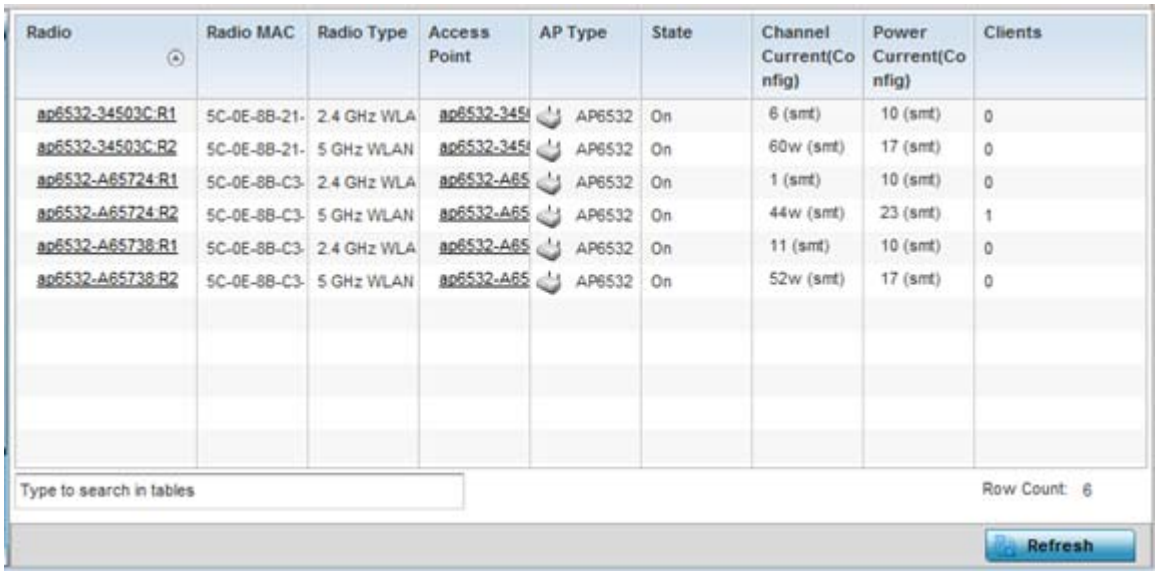


Figure 15-17 *RF Domain - Radio Status screen*

The **Radio Status** screen displays the following:

Radio	Displays the name assigned to each listed RF Domain member Access Point radio. Each name displays as a link that can be selected to display radio information in greater detail.
Radio MAC	Displays the MAC address as a numerical value factory hardcoded to each listed RF Domain member Access Point radio.
Radio Type	Defines whether the radio is operating within the 2.4 or 5 GHz radio band.
Access Point	Displays the user assigned name of the RF Domain member Access Point to which the radio resides.
AP Type	Lists the model type of each RF Domain member Access Point.
State	Displays the radio's current operational state.

Channel Current (Config)	Displays the current channel each listed RF Domain member Access Point radio is broadcasting on.
Power Current (Config)	Displays the current power level the radio is using for its transmissions.
Clients	Displays the number of clients currently connected to each listed RF Domain member Access Point radio. Supported models can manage up to 256 clients per radio, with the exception of AP6511 and AP6521 models, which only support up to 128 clients per their single radio.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.8.2 RF Statistics

To view the RF Domain radio statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Expand **Radios** from the RF Domain menu and select **RF Statistics.**

Figure 15-18 *RF Domain - Radio RF Statistics screen*

The **RF Statistics** screen displays the following:

Radio	Displays the name assigned to each listed RF Domain member radio. Each name displays as a link that can be selected to display radio information in greater detail.
Signal	Displays the power of listed RF Domain member radio signals in dBm.
Noise	Lists the level of noise (in - X dbm format) reported by each listed RF Domain member Access Point.
SNR	Displays the *signal to noise ratio* (SNR) of each listed RF Domain member radio.
Tx Physical Layer Rate	Displays the data transmit rate for each RF Domain member radio's physical layer. The rate is displayed in Mbps.

Rx Physical Layer Rate	Displays the data receive rate for each RF Domain member radio's physical layer. The rate is displayed in Mbps.
Avg Retry Number	Displays the average number of retries for each RF Domain member radio.
Error Rate	Displays the average number of retries per packet. A high number indicates possible network or hardware problems.
RF Quality Index	Displays an integer (and performance icon) that indicates the overall RF performance for each listed radio. The RF quality indices are: *0 – 50* (Poor) *50 – 75* (Medium) *75 – 100* (Good)
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.8.3 Traffic Statistics

The **Traffic Statistics** screen displays transmit and receive data as well as data rate and packet drop and error information for RF Domain member radios. Individual RF Domain member radios can be selected and to information specific to that radio as troubleshoot requirements dictate.

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Expand **Radios** from the RF Domain menu and select **Traffic Statistics.**

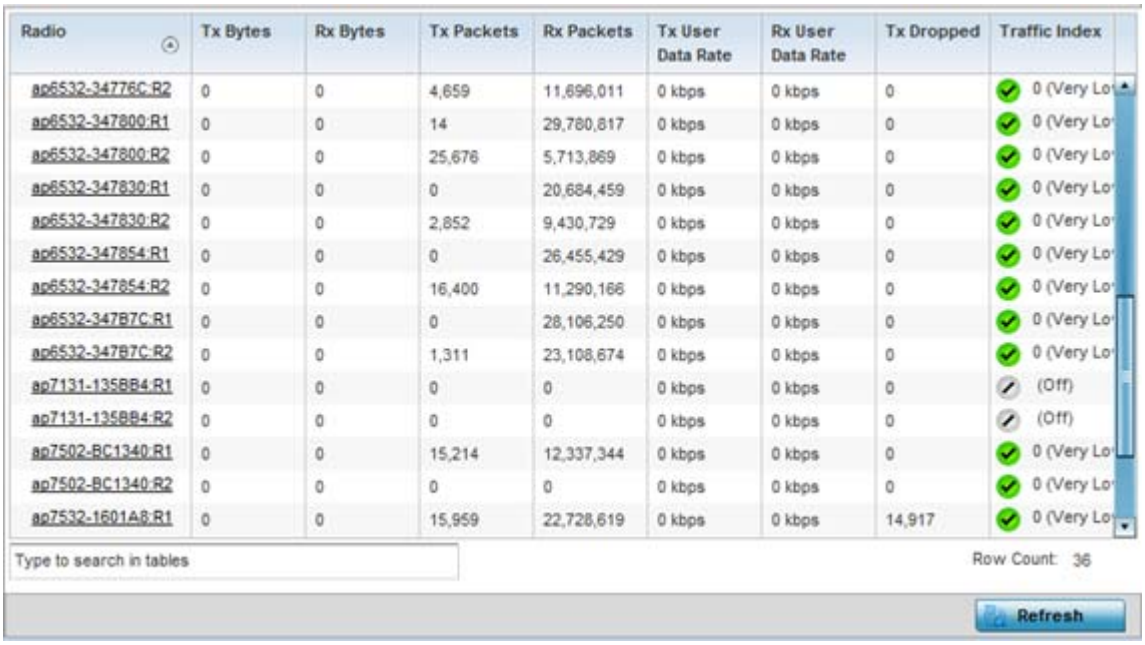


Figure 15-19 *RF Domain - Radio Traffic Statistics screen*

The **Radio Traffic** screen displays the following:

Radio	Displays the name assigned to each listed RF Domain member Access Point radio. Each name displays as a link that can be selected to display radio information in greater detail.

Tx Bytes	Displays the total number of bytes transmitted by each RF Domain member Access Point radio. This includes all user data as well as any management overhead data.
Rx Bytes	Displays the total number of bytes received by each RF Domain member Access Point radio. This includes all user data as well as any management overhead data.
Tx Packets	Displays the total number of packets transmitted by each RF Domain member Access Point radio. This includes all user data as well as any management overhead packets.
Rx Packets	Displays the total number of packets received by each RF Domain member Access Point radio. This includes all user data as well as any management overhead packets.
Tx User Data Rate	Displays the rate (in kbps) user data is transmitted by each RF Domain member Access Point radio. This rate only applies to user data and does not include any management overhead.
Rx User Data Rate	Displays the rate (in kbps) user data is received by each RF Domain member Access Point radio. This rate only applies to user data and does not include any management overhead.
Tx Dropped	Displays the total number of transmitted packets which have been dropped by each RF Domain member Access Point radio. This includes all user data as well as any management overhead packets that were dropped.
Traffic Index	Displays the traffic utilization index of RF Domain member Access Point radios, which measures how efficiently the traffic medium is utilized within this RF Domain. It's defined as the percentage of current throughput relative to the maximum possible throughput. Traffic indices are: 0 – 20 (very low utilization), 20 – 40 (low utilization), 40 – 60 (moderate utilization) and 60 and above (high utilization).
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.9 Bluetooth

RF Domain Statistics

AP-8432 and AP-8533 model Access Points utilize a built in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network. AP-8432 and AP-8533 models support both Bluetooth *classic* and Bluetooth *low energy* technology. These platforms can use their Bluetooth classic enabled radio to sense other Bluetooth enabled devices and report device data (MAC address, RSSI and device calls) to an ADSP server for intrusion detection. If the device presence varies in an unexpected manner, ADSP can raise an alarm.

AP-8432 and AP-8533 model Access Points support Bluetooth beaconing to emit either iBeacon or Eddystone-URL beacons. The Access Point's Bluetooth radio sends non-connectable, undirected *low-energy* (LE) advertisement packets on a periodic basis. These advertisement packets are short, and sent on Bluetooth advertising channels that conform to already-established iBeacon and Eddystone-URL standards.

To view Bluetooth radio statistics for RF Domain member Access Points:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **Bluetooth**.

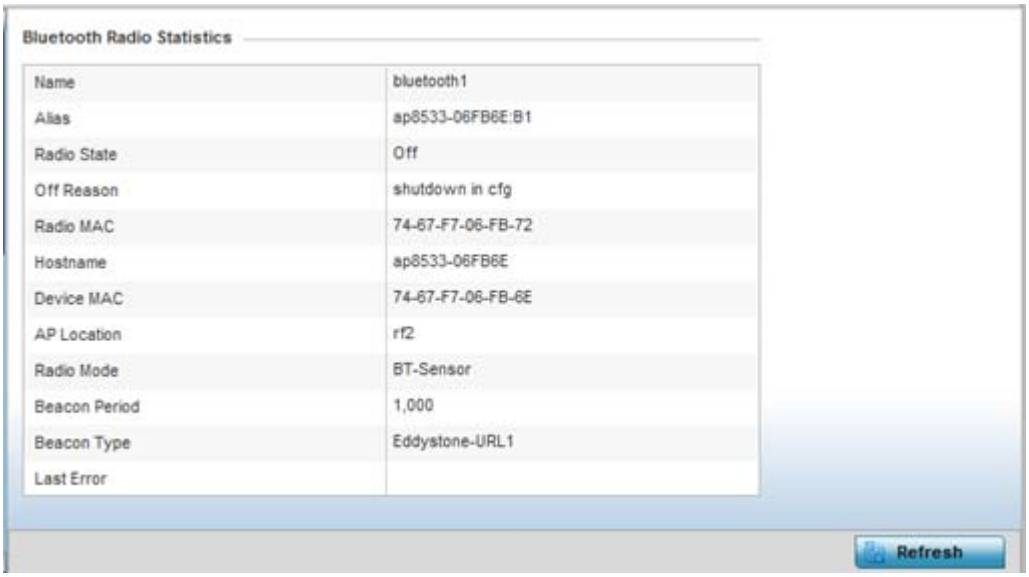


Figure 15-20 *RF Domain - Bluetooth screen*

The RF Domain **Bluetooth** screen displays the following:

Name	Lists the name of the Access Point's Bluetooth radio.
Alias	If an alias has been defined for the Access Point its listed here. The alias value is expressed in the form of <hostname>: B<Bluetooth_radio_number>. If the administrator has defined a hostname for the Access Point, it's used in place of the Access Point's default hostname.
Radio State	Displays the current operational state (On/Off) of the Bluetooth radio.
Off Reason	If the Bluetooth radio is offline, this field states the reason.
Radio MAC	Lists the Bluetooth radio's factory encoded MAC address serving as this device's hardware identifier on the network.
Hostname	Lists the hostname set for the Access Point as its network identifier.
Device MAC	Lists the Access Point's factory encoded MAC address serving as this device's hardware identifier on the network.
AP Location	Lists the Access Point's administrator assigned deployment location.
Radio Mode	Lists an Access Point's Bluetooth radio functional mode as either *bt-sensor* or *le-beacon*.
Beacon Period	Lists the Bluetooth radio's beacon transmission period from 100 -10,000 milliseconds.
Beacon Type	Lists the type of beacon currently configured.
Last Error	Lists descriptive text on any error that's preventing the Bluetooth radio from operating.
Refresh	Select *Refresh* to update the screen's statistics counters to their latest values.

15.2.10 Mesh

RF Domain Statistics

Mesh networking enables users to wirelessly access broadband applications anywhere (even in a moving vehicle). Initially developed for secure and reliable military battlefield communications, mesh technology supports public safety, public access and public works. Mesh technology reduces the expense of wide-scale networks, by leveraging Wi-Fi enabled devices already deployed.

To view Mesh statistics for RF Domain member Access Point and their connected clients:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **Mesh**.

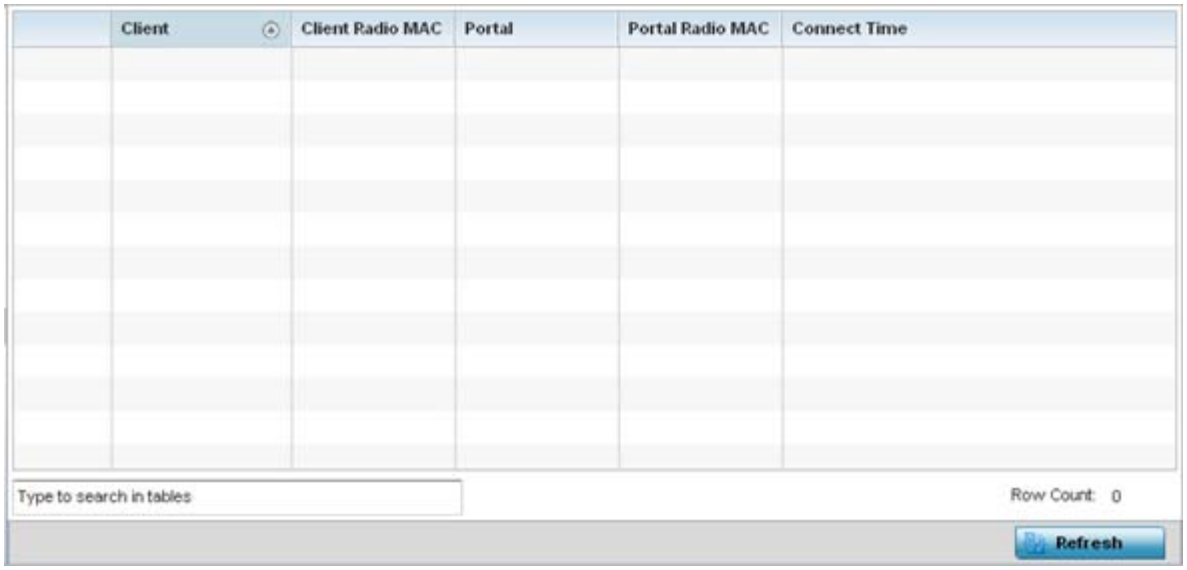


Figure 15-21 *RF Domain - Mesh screen*

The RF Domain **Mesh** screen displays the following:

Client	Displays the configured hostname for each mesh client connected to a RF Domain member Access Point.
Client Radio MAC	Displays the hardware encoded MAC address for each mesh client connected to a RF Domain member Access Point.
Portal	Displays a numerical portal Index ID for the each mesh client connected to a RF Domain member Access Point.
Portal Radio MAC	Displays the hardware encoded MAC address for each radio in the RF Domain mesh network.
Connect Time	Displays the total connection time for each listed client in the RF Domain mesh network.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.11 Mesh Point

RF Domain Statistics

To view *Mesh Point* statistics for RF Domain member Access Point and their connected clients:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **Mesh Point**.
The **MCX Geographical View** displays by default.

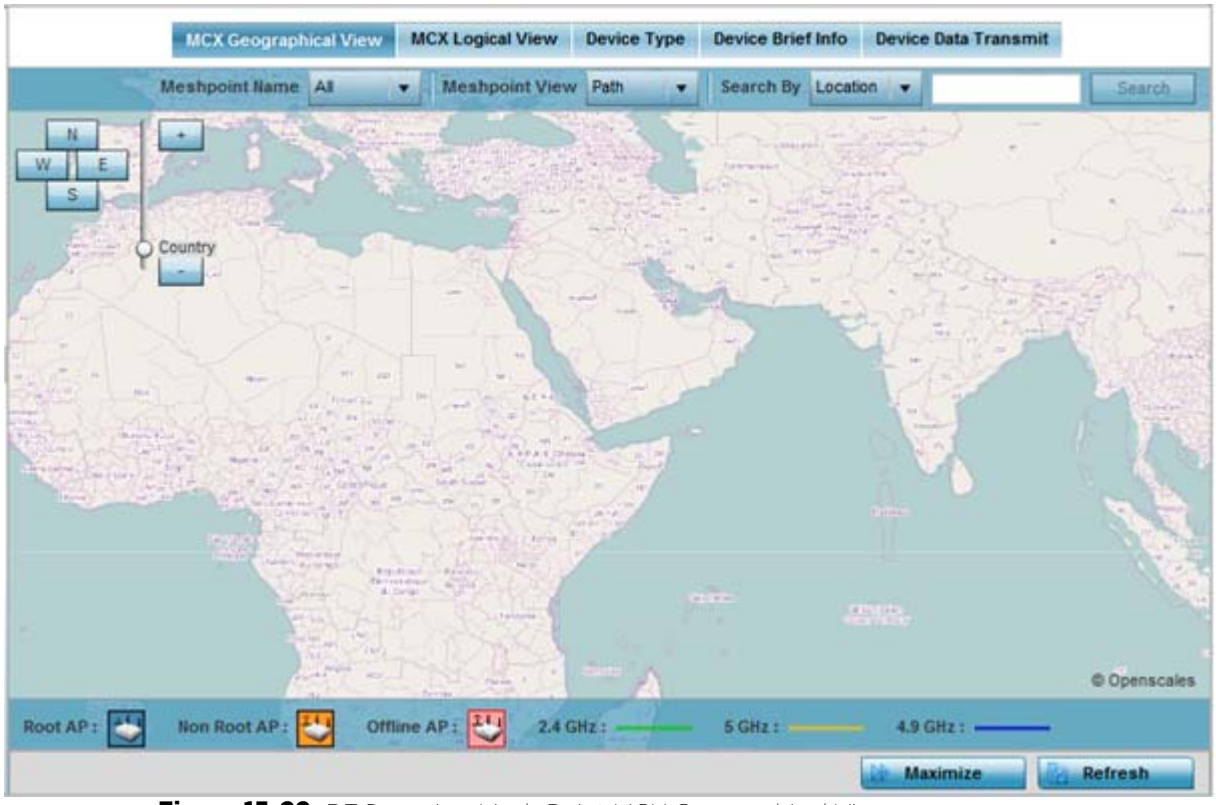


Figure 15-22 *RF Domain - Mesh Point MCX Geographical View screen*

The **MCX Geographical View** screen displays a map where icons of each device in the RF Domain are overlaid. This provides a geographical overview of the location of each RF Domain member device.

4 Use the *N*, *W*, *S* and *E* buttons to move the map in the North, West, South and East directions respectively. The slider next to these buttons enables zooming in and out of the view. The available fixed zoom levels are *World*, *Country*, *State*, *Town*, *Street* and *House*.

5 Use the **Maximize** button to maximize this view to occupy the complete screen. Use the Refresh button to update the status of the screen.

6 Select the **MCX Logical View** tab to view a logical representation of the Meshpoint.

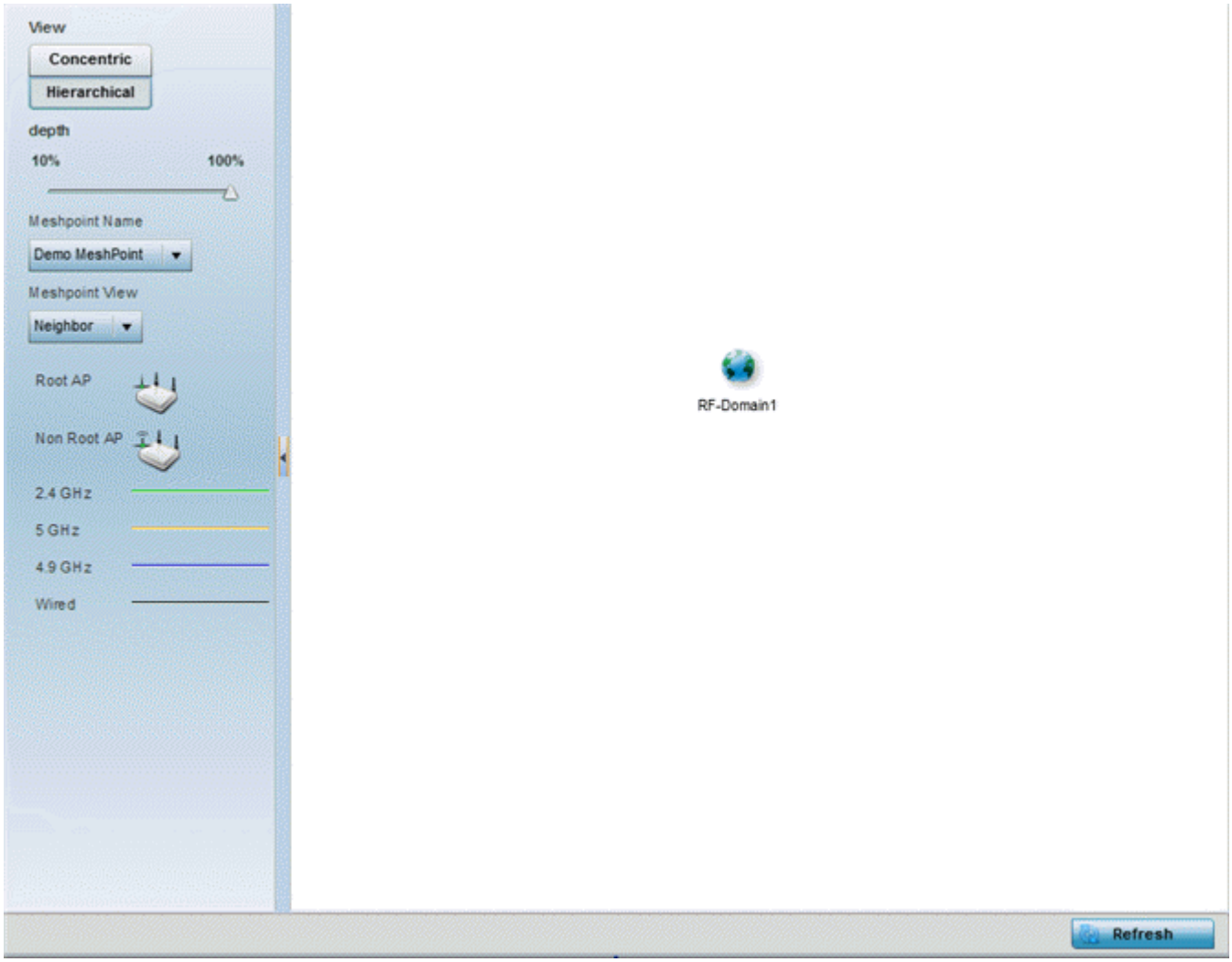


Figure 15-23 *RF Domain - Mesh Point MCX Logical View screen*

The **Concentric** and **hierarchical** buttons define how the mesh point is displayed in the MCX Logical View screen. In the Concentric mode, the mesh is displayed as a concentric arrangement of devices with the root mesh at the centre and the other mesh device arranged around it.

In the hierarchical arrangement, the root node of the mesh is displayed at the top of the mesh tree and the relationship of the mesh nodes are displayed as such.

Use the **Meshpoint Name** drop down to select a mesh point to see the graphical representation of that mesh point. The view can further be filtered based on the values Neighbor or Path selected in the Meshpoint View field.

7 Select the **Device Type** tab.

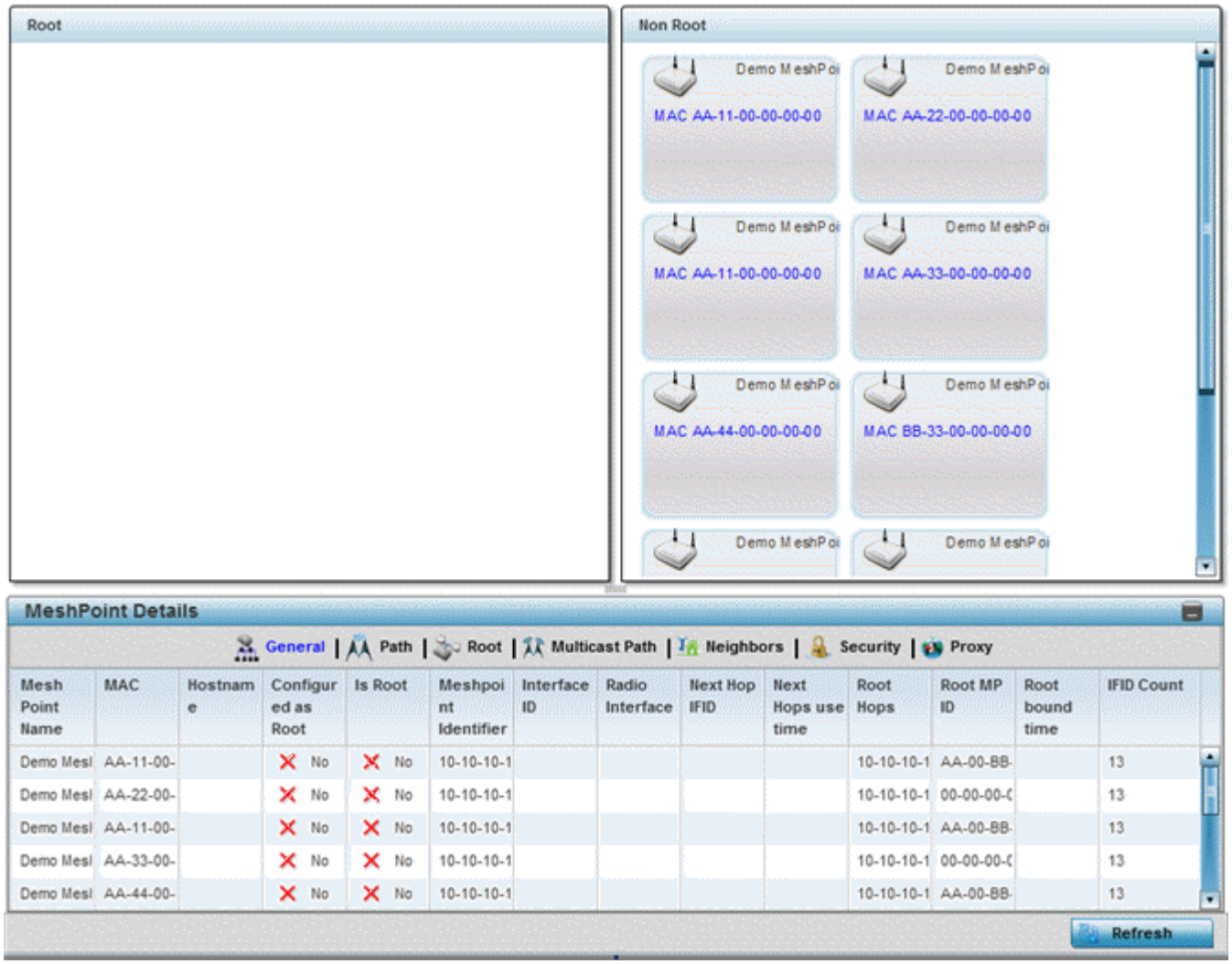


Figure 15-24 *RF Domain - Mesh Point Device Type screen*

The **Root** field displays the Mesh ID and MAC Address of the configured root mesh points in the RF Domain.

8 The **Non Root** field displays the Mesh ID and MAC Address of all configured non-root mesh points in the RF Domain. displays the Mesh ID and MAC Address of all configured non-root mesh points in the RF Domain.

9 The **Mesh Point Details** field on the bottom portion of the screen displays tabs for *General*, *Path*, *Root*, *Multicast Path*, *Neighbors*, *Security* and *Proxy*. Refer to the following:

The **General** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
MAC	Displays the MAC Address of each configured mesh point in the RF Domain.
Hostname	Displays the administrator assigned hostname for each configured mesh point in the RF Domain.
Configured As Root	Indicates whether a mesh point is configured to act as a root device. (Yes/No).
Is Root	A root mesh point is defined as a mesh point connected to the WAN and provides a wired backhaul to the network (Yes/No).

Meshpoint Identifier	The MP identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration.
Interface ID	The IFID uniquely identifies an interface associated with the MPID. Each mesh point on a device can be associated with one or more interfaces.
Radio Interface	Uniquely identifies the radio interface on which the Mesh Point operates.
Next Hop IFID	Lists the ID of the interface on which the next hop for the mesh network can be found.
Next Hops Use Time	Lists the time when the next hop in the mesh network topology was last utilized.
Root Hops	Number of hops to a root and should not exceed 4 in general practice. If using the same interface to both transmit and receive, then you will get approximately half the performance every additional hop out.
Root MP ID	Displays the ID of the root device for this mesh point.
Root Bound Time	Displays the duration this mesh point has been connected to the mesh root.
IFID Count	Displays the number of *Interface IDs* (IFIDs) associated with all the configured mesh points in the RF Domain.

The **Path** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
Meshpoint Identifier	The identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration.
Destination Addr	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
Next Hop IFID	The Interface ID of the mesh point that traffic is being directed to.
Is Root	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network (Yes/No).
MiNT ID	Displays the MiNT Protocol ID for the global mint area identifier. This area identifier separates two overlapping mint networks and need only be configured if the administrator has two mint networks that share the same packet broadcast domain.
Hops	Number of hops to a root and should not exceed 4 in general practice. If using the same interface to both transmit and receive, then you will get approximately half the performance every additional hop out.
Mobility	Displays whether the mesh point is a mobile or static node. Displays *True* when the device is mobile and *False* when the device is not mobile.
Metric	A measure of the quality of the path. A lower value indicates a better path.
State	Indicates whether the path is currently Valid of Invalid.
Binding	Indicates whether the path is bound or unbound.

Timeout	The timeout interval in mili-seconds. The interpretation this value will vary depending on the value of the state.
Sequence	The sequence number also known as the destination sequence number. It is updated whenever a mesh point receives new information about the sequence number from RREQ, RREP, or RERR messages that may be received related to that destination.

The **Root** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
Recommended	Displays the root that is recommended by the mesh routing layer.
Root MPID	The MP identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration.
Next Hop IFID	The IFID of the next hop. The IFID is the MAC Address on the destination device.
Radio Interface	This indicates the interface that is used by the device to communicate with this neighbor. The values are 2.4 and 5.8, indicating the frequency of the radio that is used to communicate with the neighbor.
Bound	Indicates whether the root is bound or unbound.
Metric	Displays the computed path metric between the neighbor and their root mesh point.
Interface Bias	This field lists any bias applied because of the Preferred Root Interface Index.
Neighbor Bias	This field lists any bias applied because of the Preferred Root Next-Hop Neighbor IFID.
Root Bias	This field lists any bias applied because of the Preferred Root MPID.

The **Multicast Path** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
Subscriber Name	The identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration.
Subscriber MPID	Lists the subscriber ID to distinguish between other mesh point neighbor devices in the RF Domain.
Group Address	Displays the MAC address used for the Group in the mesh point.
Timeout	The timeout interval in seconds. The interpretation this value will vary depending on the value of the state. If the state is Init or In Progress, the timeout duration has no significance. If the state is Enabled, the timeout duration indicates the amount of time left before the security validity check is initiated. If the state is Failed, the timeout duration is the amount of time after which the system will retry.

The **Neighbors** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.

Destination Addr	Displays the MeshID (MAC Address) of each mesh point in the RF Domain.
Neighbor MP ID	The MAC Address that the device uses to define the mesh point in the device that the neighbor is a part of. It is used to distinguish the device that is the neighbor.
Neighbor IFID	The MAC Address used by the interface on the neighbor device to communicate with this device. This may define a particular radio or Ethernet port that communicates with this device over the mesh.
Root MP ID	The MAC Address of the neighbor's root mesh point.
Is Root	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. Yes if the mesh point that is the neighbor is a root mesh point or No if the mesh point that is the neighbor is not a root mesh point.
Mobility	Displays whether the Mesh Point is a mobile or static node. Displays *True* when the device is mobile and *False* when the device is not mobile.
Radio Interface	This indicates the interface that is used by the device to communicate with this neighbor. The values are 2.4 and 5.8, indicating the frequency of the radio that is used to communicate with the neighbor.
Mesh Root Hops	The number of devices between the neighbor and its root mesh point. If the neighbor is a root mesh point, this value will be 0. If the neighbor is not a root mesh point but it has a neighbor that is a root mesh point, this value will be 1. Each mesh point between the neighbor and its root mesh point is counted as 1 hop.
Resourced	Displays whether the mesh point has been resourced or not. The Mesh Connex neighbor table can contain more neighbors than the AP supports. If the neighbor is resourced, it will take away a one of the resources for a wireless client device to be used for meshing. Displays True when the device is resourced and False when the device is not.
Link Quality	An abstract value depicting the quality of the mesh link between the device and the neighbor. The range is from 0 (weakest) to 100 (strongest).
Link Metric	This value shows the computed path metric from the device to the neighbor mesh point using this interface. The lower the number the better the possibility that the neighbor will be chosen as the path to the root mesh point.
Root Metric	The computed path metric between the neighbor and their root mesh point.

Rank	The rank is the level of importance and is used for automatic resource management. *8* – The current next hop to the recommended root. *7* – Any secondary next hop to the recommended root to has a good potential route metric. *6* – A next hop to an alternate root node. *5* – A downstream node currently hopping through to get to the root. *4* – A downstream node that could hop through to get to the root, but is currently not hopping through any node (look at authentication, as this might be an issue). *3* – A downstream node that is currently hopping through a different node to get to the root, but could potentially have a better route metric if it hopped through this node. *2* – Reserved for active peer to peer routes and is not currently used. *1* - A neighbor bound to the same recommended root but does not have a potential route metric as good as the neighbors ranked 8 and 7. *0* – A neighbor bound to a different root node. *-1* – Not a member of the mesh as it has a different mesh ID. All client devices hold a rank of 3 and can replace any mesh devices lower than that rank.
Age	Displays the number of miliseconds since the mesh point last heard from this neighbor.

The **Security** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
Mesh Point Identifier	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
Radio Interface	This indicates the interface that is used by the device to communicate with this neighbor. The values are 2.4 and 5.8, indicating the frequency of the radio that is used to communicate with the neighbor.
Interface ID	The IFID uniquely identifies an interface associated with the MPID. Each mesh point on a device can be associated with one or more interfaces.
State	Displays the Link State for each mesh point: *Init* - indicates the link has not been established or has expired. *Enabled* - indicates the link is available for communication. *Failed* - indicates the attempt to establish the link failed and cannot be retried yet. *In Progress* - indicates the link is being established but is not yet available.
Timeout	Displays the maximum value in seconds that the link is allowed to stay in the *In Progress* state before timing out.

Keep Alive	*Yes* indicates that the local MP will act as a supplicant to authenticate the link and not let it expire (if possible). *No* indicates that the local MP does not need the link and will let it expire if not maintained by the remote MP.

The **Proxy** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
Destination Addr	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
Proxy Address	Displays the MAC Address of the proxy used in the mesh point.
Age	Displays the age of the proxy connection for each of the mesh points in the RF Domain.
Proxy Owner	The owner's (MPID) is used to distinguish the neighbor device.
Persistence	Displays the persistence (duration) of the proxy connection for each of the mesh points in the RF Domain.
VLAN	The VLAN ID used as a virtual interface with this proxy. A value of 4095 indicates that there is no VLAN ID.

10 Select the **Device Brief Info** tab from the top of the screen.

The Device Brief Info screen is divided into 2 fields, **All Roots and Mesh Points** and **MeshPoint Details**.

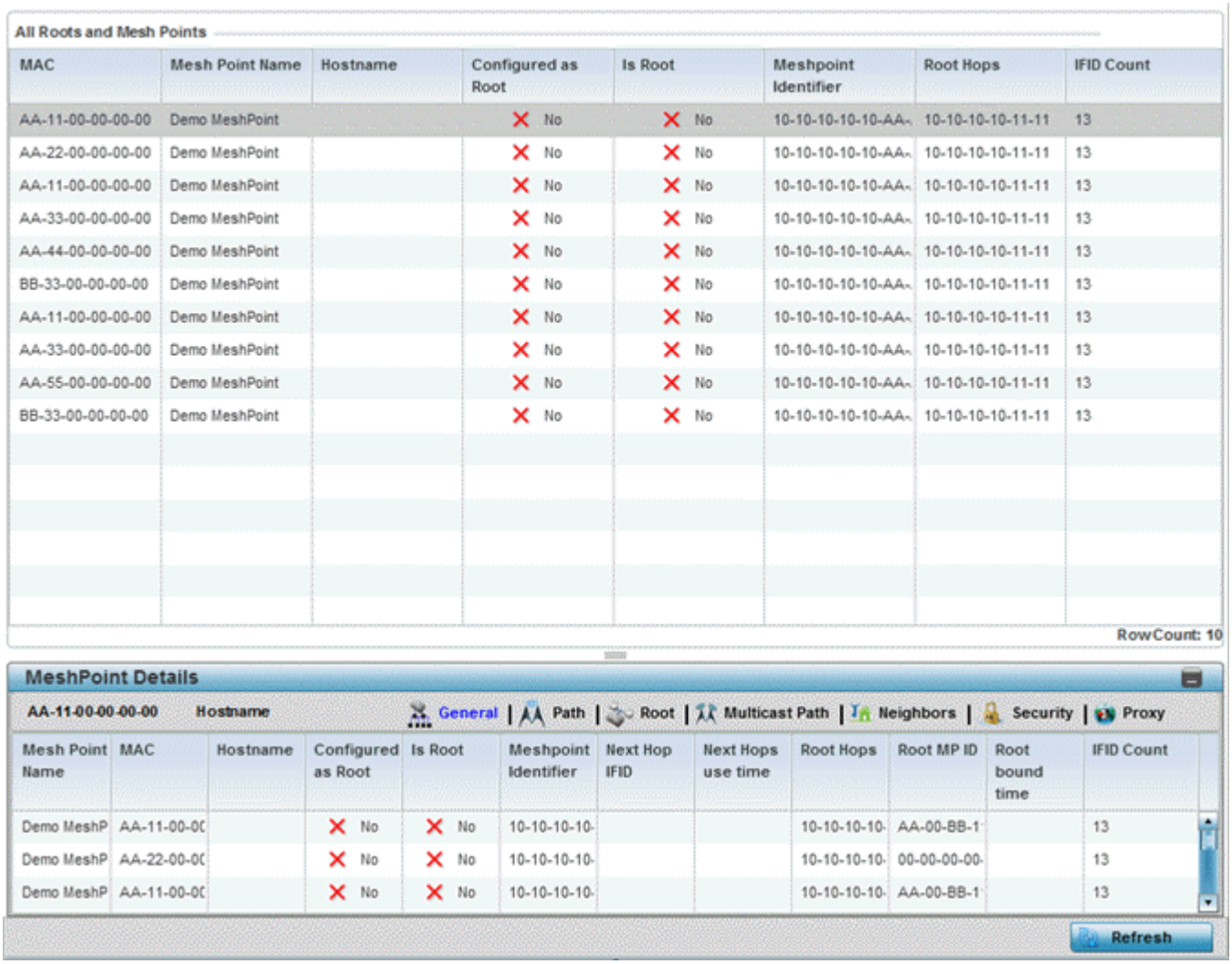


Figure 15-25 *RF Domain - Mesh Point Device Brief Info screen*

The **All Roots and Mesh Points** field displays the following:

MAC	Displays the MAC Address of each configured mesh point in the RF Domain.
Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
Hostname	Displays the administrator assigned hostname for each configured mesh point in the RF Domain.
Configured as Root	A root mesh point is defined as a mesh point connected to the WAN, providing a wired backhaul to the network (Yes/No).
Is Root	Indicates whether the current mesh point is a root meshpoint (Yes/ No).
Destination Addr	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
Root Hops	The number of devices between the selected mesh point and the destination device.
IFID Count	Displays the number of Interface IDs (IFIDs) associated with all the configured mesh points in the RF Domain.

11 The **MeshPoint Details** field on the bottom portion of the screen displays tabs for *General*, *Path*, *Root*, *Multicast Path*, *Neighbors*, *Security* and *Proxy*. Refer to the following:

The **General** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
MAC	Displays the MAC Address of each configured mesh point in the RF Domain.
Hostname	Displays the hostname for each configured mesh point in the RF Domain.
Configured as Root	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network (Yes/No).
Is Root	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network (Yes/No).
Mesh Point Identifier	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
Next Hop IFID	Identifies the ID of the interface on which the next hop for the mesh network can be found.
Next Hops Use Time	Lists the time when the next hop in the mesh network topology was last utilized.
Root Hops	Number of hops to a root and should not exceed 4 in general practice. If using the same interface to both transmit and receive, then you will get approximately half the performance every additional hop out.
Root MP ID	Lists the interface ID of the interface on which the next hop for the mesh network can be found.
Root Bound time	Displays the duration this mesh point has been connected to the mesh root.
IFID Count	Displays the number of *Interface IDs* (IFIDs) associated with all the configured mesh points in the RF Domain.

The **Path** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
Destination Addr	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
Destination	The MAC Address used by the interface on the neighbor device to communicate with this device. This may define a particular radio or Ethernet port that communicates with this device over the mesh.
Is Root	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network (Yes/No).
MiNT ID	Displays the MiNT Protocol ID for the global mint area identifier. This area identifier separates two overlapping mint networks and need only be configured if the administrator has two mint networks that share the same packet broadcast domain.
Next Hop IFID	The Interface ID of the mesh point that traffic is being directed to.
Hops	Number of hops to a root and should not exceed 4 in general practice. If using the same interface to both transmit and receive, then you will get approximately half the performance every additional hop out.

Mobility	Displays whether the mesh point is a mobile or static node. Displays *True* when the device is mobile and *False* when the device is not mobile.
Metric	A measure of the quality of the path. A lower value indicates a better path.
State	Indicates whether the path is currently Valid of Invalid.
Binding	Indicates whether the path is bound or unbound.
Timeout	The timeout interval in seconds. The interpretation this value will vary depending on the value of the state. If the state is Init or In Progress, the timeout duration has no significance. If the state is Enabled, the timeout duration indicates the amount of time left before the security validity check is initiated. If the state is Failed, the timeout duration is the amount of time after which the system will retry.
Sequence	The sequence number also known as the destination sequence number. It is updated whenever a mesh point receives new information about the sequence number from RREQ, RREP, or RERR messages that may be received related to that destination.

The **Root** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
Recommended	Displays the root that is recommended by the mesh routing layer.
Root MPID	The MP identifier is used to distinguish between other mesh points both on the same device and on other devices. This is used by a user to setup the preferred root configuration.
Next Hop IFID	The IFID of the next hop. The IFID is the MAC Address on the destination device.
Radio Interface	This indicates the interface that is used by the device to communicate with this neighbor. The values are 2.4 and 5.8, indicating the frequency of the radio that is used to communicate with the neighbor.
Bound	Indicates whether the root is *bound* or *unbound*.
Metric	Displays the computed path metric between the neighbor and their root mesh point.
Interface Bias	This field lists any bias applied because of the preferred root Interface Index.
Neighbor Bias	This field lists any bias applied because of the preferred root next-hop Neighbor IFID.
Root Bias	This field lists any bias applied because of the preferred root MPID.

The **Multicast Path** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
Subscriber Name	Lists the subscriber name is used to distinguish between other mesh point neighbors both on the same device and on other devices.
Subscriber MPID	Lists the subscriber ID to distinguish between other mesh point neighbors both on the same device and on other devices.
Group Address	Displays the MAC address used for the Group in the mesh point.

Path Timeout	The timeout interval in seconds. The interpretation this value will vary depending on the value of the state. If the state is Init or In Progress, the timeout duration has no significance. If the state is *Enabled*, the timeout duration indicates the amount of time left before the security validity check is initiated. If the state is *Failed*, the timeout duration is the amount of time after which the system will retry.

The **Neighbors** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
Mesh Point Identifier	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
Neighbor MP ID	The MAC Address that the device uses to define the mesh point in the device that the neighbor is a part of. It is used to distinguish the device that is the neighbor.
Neighbor IFID	The MAC Address used by the interface on the neighbor device to communicate with this device. This may define a particular radio or Ethernet port that communicates with this device over the mesh.
Root MP ID	The mesh point ID of the neighbor's root mesh point.
Is Root	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network. Yes if the mesh point that is the neighbor is a root mesh point or No if the mesh point that is the neighbor is not a root mesh point.
Mobility	Displays whether the mesh point is a mobile or static node. Displays *True* when the device is mobile and *False* when the device is not mobile.
Radio Interface	This indicates the interface that is used by the device to communicate with this neighbor. The values are 2.4 and 5.8, indicating the frequency of the radio that is used to communicate with the neighbor.
Mesh Root Hops	The number of devices between the neighbor and its root mesh point. If the neighbor is a root mesh point, this value will be 0. If the neighbor is not a root mesh point but it has a neighbor that is a root mesh point, this value will be 1. Each mesh point between the neighbor and its root mesh point is counted as 1 hop.
Resourced	Displays whether the mesh point has been resourced or not. The Mesh Connex neighbor table can contain more neighbors than the AP supports. If the neighbor is resourced, it will take away a one of the resources for a wireless client device to be used for meshing. Displays True when the device is resourced and False when the device is not.
Link Quality	An abstract value depicting the quality of the mesh link between the device and the neighbor. The range is from 0 (weakest) to 100 (strongest).
Link Metric	This value shows the computed path metric from the device to the neighbor mesh point using this interface. The lower the number the better the possibility that the neighbor will be chosen as the path to the root mesh point.
Root Metric	The computed path metric between the neighbor and their root mesh point.

Rank	The rank is the level of importance and is used for automatic resource management. *8* – The current next hop to the recommended root. *7* – Any secondary next hop to the recommended root to has a good potential route metric. *6* – A next hop to an alternate root node. *5* – A downstream node currently hopping through to get to the root. *4* – A downstream node that could hop through to get to the root, but is currently not hopping through any node (look at authentication, as this might be an issue). *3* – A downstream node that is currently hopping through a different node to get to the root, but could potentially have a better route metric if it hopped through this node. *2* – Reserved for active peer to peer routes and is not currently used. *1* - A neighbor bound to the same recommended root but does not have a potential route metric as good as the neighbors ranked 8 and 7. *0* – A neighbor bound to a different root node. *-1* – Not a member of the mesh as it has a different mesh ID. All client devices hold a rank of 3 and can replace any mesh devices lower than that rank.
Age	Displays the number of miliseconds since the mesh point last heard from this neighbor.

The **Security** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
Mesh Point Identifier	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
Radio Interface	This indicates the interface that is used by the device to communicate with this neighbor. The values are 2.4 and 5.8, indicating the frequency of the radio that is used to communicate with the neighbor.
Interface ID	The IFID uniquely identifies an interface associated with the MPID. Each mesh point on a device can be associated with one or more interfaces.
State	Displays the Link State for each mesh point: *Init* - indicates the link has not been established or has expired. *Enabled* - indicates the link is available for communication. *Failed* - indicates the attempt to establish the link failed and cannot be retried yet. *In Progress* - indicates the link is being established but is not yet available.
Timeout	Displays the maximum value in seconds that the link is allowed to stay in the In Progress state before timing out.

Keep Alive	*Yes* indicates the local MP acts as a supplicant to authenticate the link and not let it expire (if possible). *No* indicates that the local MP does not need the link and will let it expire if not maintained by the remote MP.

The **Proxy** tab displays the following:

Mesh Point Name	Displays the name of each configured mesh point in the RF Domain.
Mesh Point Identifier	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
Proxy Address	Displays the MAC Address of the proxy used in the mesh point.
Age	Displays the age of the proxy connection for each of the mesh points in the RF Domain.
Proxy Owner	The owner (MPID) is used to distinguish the device that is the neighbor.
VLAN	The VLAN ID used as a virtual interface with this proxy. A value of 4095 indicates that there is no VLAN ID.

12 Select **Device Data Transmit**.

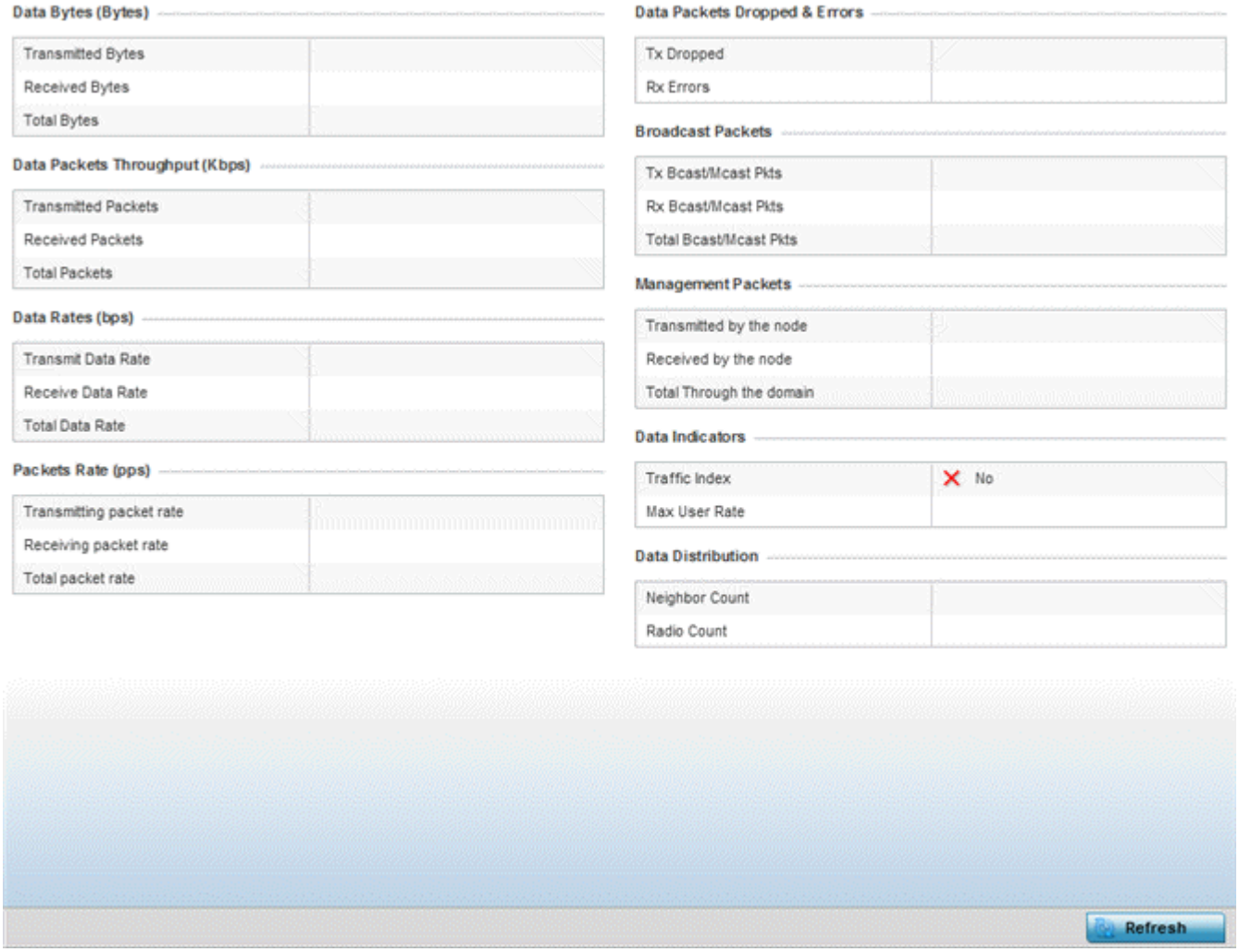


Figure 15-26 *RF Domain - Mesh Point Device Data Transmit screen*

13 Review the following transmit and receive statistics for Mesh nodes:

Data Bytes (Bytes): Transmitted Bytes	Displays the total amount of data, in Bytes, transmitted by mesh points in the RF Domain.
Data Bytes (Bytes): Received Bytes	Displays the total amount of data, in Bytes, received by mesh points in the RF Domain.
Data Bytes (Bytes): Total Bytes	Displays the total amount of data, in Bytes, transmitted and received by mesh points in the RF Domain.
Data Packets Throughput (Kbps): Transmitted Packets	Displays the total amount of data, in packets, transmitted by mesh points in the RF Domain.
Data Packets Throughput (Kbps): Received Packets	Displays the total amount of data, in packets, received by mesh points in the RF Domain.
Data Packets Throughput (Kbps): Total Packets	Displays the total amount of data, in packets, transmitted and received by mesh points in the RF Domain.

Data Rates (bps): Transmit Data Rate	Displays the average data rate, in kbps, for all data transmitted by mesh points in the RF Domain.
Data Rates (bps): Receive Data Rate	Displays the average data rate, in kbps, for all data received by mesh points in the RF Domain.
Data Rates (bps): Total Data Rate	Displays the average data rate, in kbps, for all data transmitted and received by mesh points in the RF Domain.
Packets Rate (pps): Transmitting Packet rate	Displays the average packet rate, in packets per second, for all data transmitted and received by mesh points in the RF Domain.
Packets Rate (pps): Received Packet rate	Displays the average packet rate, in packets per second, for all data received and received by mesh points in the RF Domain.
Packets Rate (pps): Total Packet Rate	Displays the average data packet rate, in packets per second, for all data transmitted and received by mesh points in the RF Domain.
Data Packets Dropped and Errors: Tx Dropped	Displays the total number of transmissions that were dropped mesh points in the RF Domain.
Data Packets Dropped and Errors: Rx Errors	Displays the total number of receive errors from mesh points in the RF Domain.
Broadcast Packets: Tx Bcast/Mcast Pkts	Displays the total number of broadcast and multicast packets transmitted from mesh points in the RF Domain.
Broadcast Packets: Rx Bcast/Mcast Pkts	Displays the total number of broadcast and multicast packets received from mesh points in the RF Domain.
Broadcast Packets: Total Bcast/Mcast Pkts	Displays the total number of broadcast and multicast packets transmitted and received from mesh points in the RF Domain.
Management Packets: Transmitted by the node	Displays the total number of management packets transmitted through the mesh point node.
Management Packets: Received by the node	Displays the total number of management packets received through the mesh point node.
Management Packets: Total Through the domain	Displays the total number of management packets that were transmitted and received through the mesh point node.
Data Indicators: Traffic Index	Displays *True* of *False* to indicate whether or not a traffic index is present.
Data Indicators: Max User Rate	Displays the maximum user throughput rate for mesh points in the RF Domain.
Data Distribution: Neighbor Count	Displays the total number of neighbors known to the mesh points in the RF Domain.
Data Distribution: Radio Count	Displays the total number of neighbor radios known to the mesh points in the RF Domain.

15.2.12 SMART RF

RF Domain Statistics

When invoked by an administrator, *Self-Monitoring At Run Time* (Smart RF) instructs Access Point radios to change to a specific channel and begin beaconing using the maximum available transmit power. Within a well-planned deployment, any RF Domain member Access Point radio should be reachable by at least one other radio. Smart RF records signals received from its neighbors as well as signals from external, un-managed radios. AP-to-

AP distance is recorded in terms of signal attenuation. The information from external radios is used during channel assignment to minimize interference.

To view the Smart RF summary for RF Domain member Access Point radios:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **SMART RF** from the RF Domain menu.

4 Expand the SMART RF menu and select **Summary.**

The summary screen enables administrators to assess the efficiency of RF Domain member device channel distributions, sources of interference potentially requiring Smart RF adjustments, top performing RF Domain member device radios and the number of power, channel and coverage changes required as part of a Smart RF performance compensation activity.

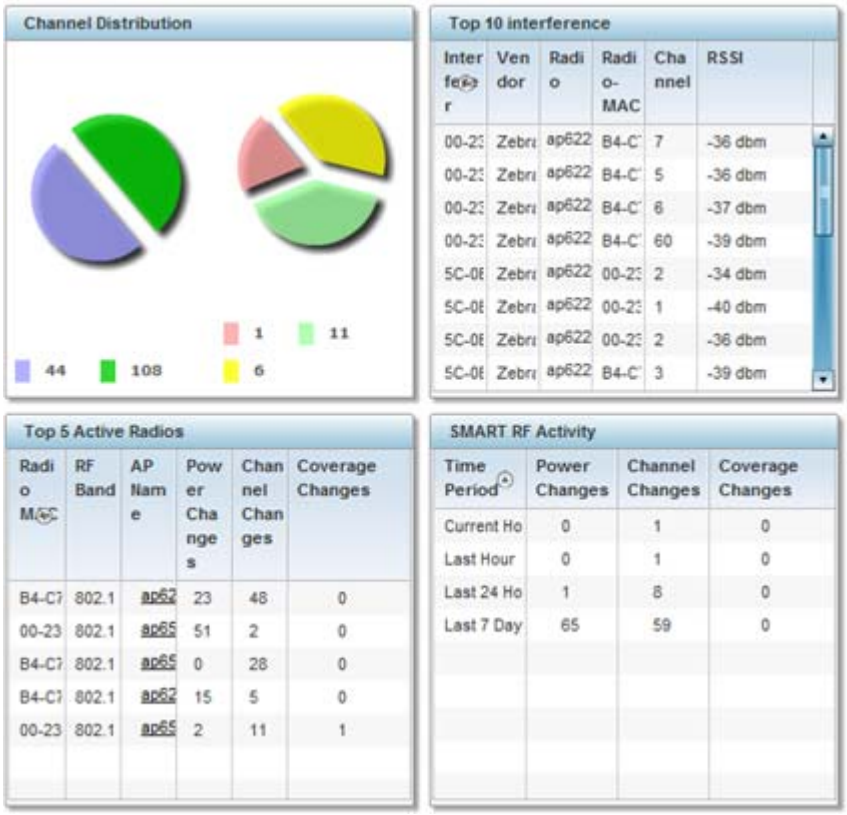


Figure 15-27 *RF Domain - Smart RF Summary screen*

5 The **Channel Distribution** field lists how RF Domain member devices are utilizing different channels to optimally support connect devices and avoid congestion and interference with neighboring devices. Assess whether the channel spectrum is being effectively utilized and whether channel changes are warranted to improve RF Domain member device performance.

6 Review the **Top 10 interference** table to assess RF Domain member devices whose level of interference exceeds the threshold set (from -100 to -10 dBm) for acceptable performance.

Interferer	Lists the administrator defined name of the interfering RF Domain member device.

Vendor	Displays the vendor name (manufacturer) of the interfering RF Domain member device radio.
Radio	Lists each offending device's radio name contributing to the top 10 interference listing.
Radio MAC	Displays the factory encoded hardware MAC address assigned to the RF Domain member device radio.
Channel	Displays the channel each of the 10 poorly performing RF Domain member devices was detected on. Numerous interfering devices on the same channel could define the need for better channel segregation to reduce the levels of detected interference.
RSSI	Lists a *relative signal strength indication* (RSSI) in dBm for those RF Domain member devices falling into the poorest performing 10 devices based on the administrator defined threshold value.

7 Review the **Top 5 Active Radios** to assess the significance of any Smart RF initiated compensations versus their reported top performance.

Radio MAC	Lists the hardware encoded MAC address of each listed top performing RF Domain member device radio.
RF Band	Displays the top performing radio's operation band. This may help administrate whether more changes were required in the 2.4 GHz band then 5 GHz or vice versa.
AP Name	Lists the administrator assigned Access Point name used to differentiate from other RF Domain member Access Point radios. The name displays in the form of a link that can be selected to display device information in greater detail.
Power Changes	Displays the number of Smart RF initiated power level changes reported for this top performing RF Domain member radio.
Channel Changes	Displays the number of Smart RF initiated channel changes reported for this top performing RF Domain member radio.
Coverage Changes	Displays the number of Smart RF initiated coverage changes reported for this top performing RF Domain member radio.

8 Refer to the **SMART RF Activity** table to view the trending of Smart RF compensations.

Time Period	Lists the frequency Smart RF activity is trended for the RF Domain. Trending periods include the *Current Hour*, *Last 24 Hours* or the *Last Seven Days*. Comparing Smart RF adjustments versus the last seven days enables an administrator to assess whether periods of interference and poor performance were relegated to just specific periods.
Power Changes	Displays the number of Smart RF initiated power level changes needed for RF Domain member devices during each of the three trending periods. Determine whether power compensations were relegated to known device outages or if compensations were consistent over the course of a day or week.

Channel Changes	Lists the number of Smart RF initiated channel changes needed for RF Domain member devices during each of the three trending periods. Determine if channel adjustments were relegated to known device count increases or decreases over the course of a day or week.
Coverage Changes	Displays the number of Smart RF initiated coverage changes needed for RF Domain member devices during each of the three trending periods. Determine if coverage changes were relegated to known device failures or known periods of interference over the course of a day or week.

9 Select **Refresh** to update the Summary to its latest RF Domain Smart RF information.

10 Select **Details** from the RF Domain menu.

Refer to the **General** field to review the radio's factory encoded hardware MAC address, the radio index assigned by the administrator, the 802.11 radio type, its current operational state, the radio's AP hostname assigned by an administrator, its current operating channel and power.

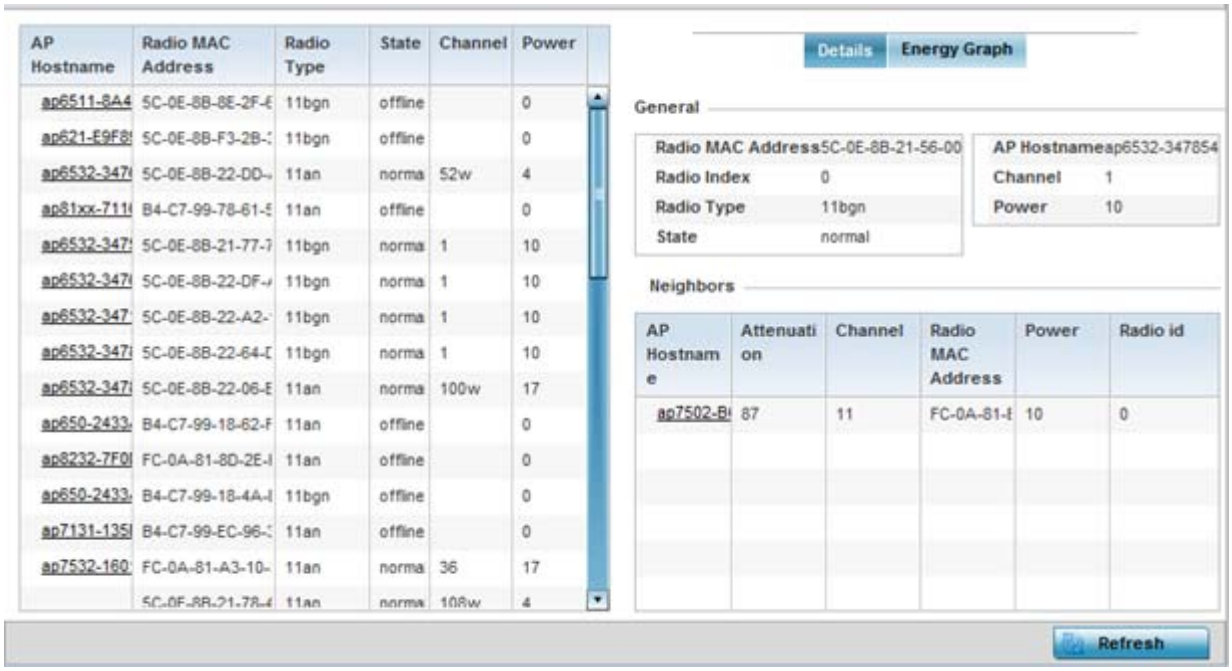


Figure 15-28 *RF Domain - Smart RF Details screen*

Refer to the **Neighbors** table to review the attributes of neighbor radio resources available for Smart RF radio compensations for other RF Domain member device radios. Individual Access Point hostnames can be selected and the RF Domain member radio can be reviewed in greater detail. *Attenuation* is a measure of the reduction of signal strength during transmission. Attenuation is the opposite of amplification, and is normal when a signal is sent from one point to another. If the signal attenuates too much, it becomes unintelligible. Attenuation is measured in decibels. The radio's current operating channel is also displayed, as is the radio's hard coded MAC address transmit power level and administrator assigned ID. Select **Refresh** at any time to update the Details screen to its latest values.

11 Select the **Energy Graph** tab

Use the **Energy Graph** to review the radio's operating channel, noise level and neighbor count. This information helps assess whether Smart RF neighbor recovery is needed in respect to poorly performing radios.

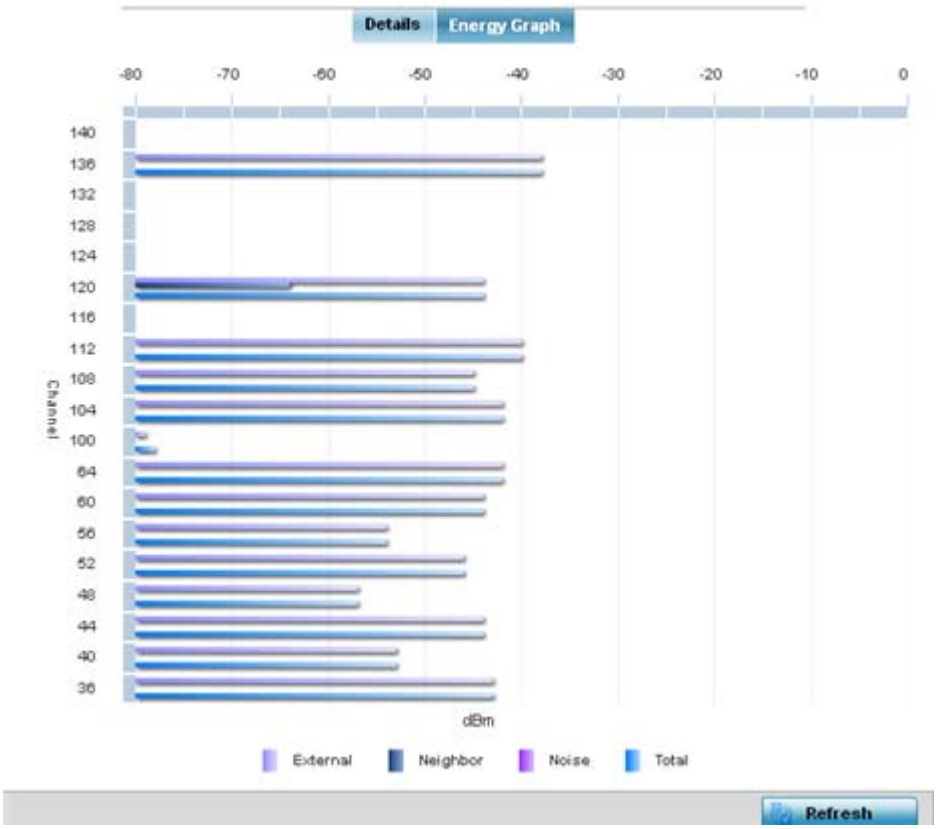
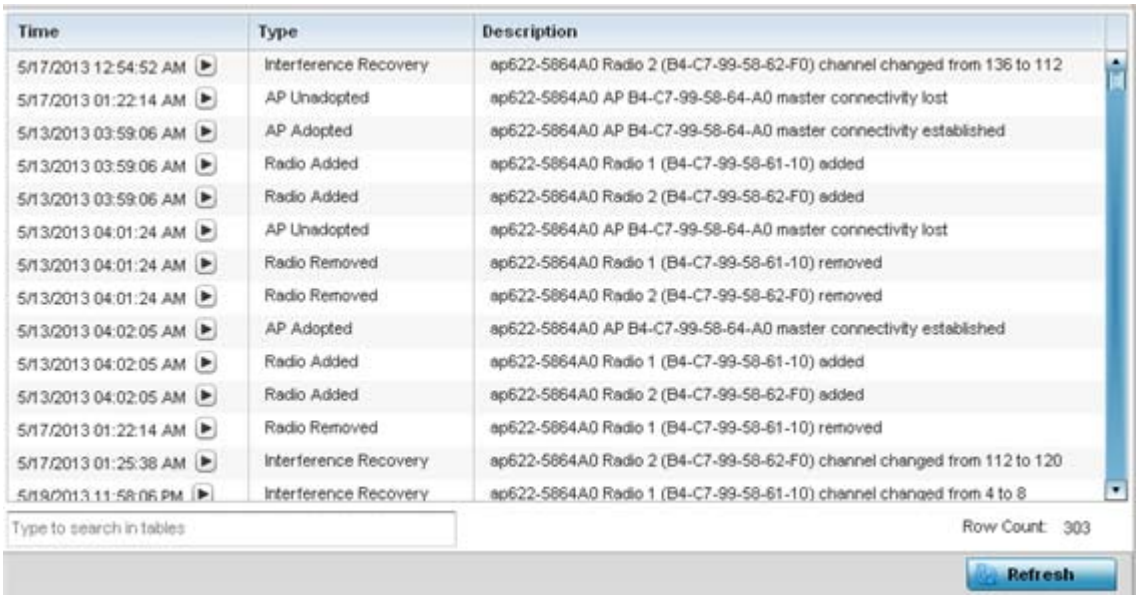


Figure 15-29 *RF Domain - Smart RF Energy Graph*

12 Select **Smart RF History** to review the descriptions and types of Smart RF events impacting RF Domain member devices.



Time	Type	Description
5/17/2013 12:54:52 AM	Interference Recovery	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) channel changed from 136 to 112
5/17/2013 01:22:14 AM	AP Unadopted	ap622-5864A0 AP B4-C7-99-58-64-A0 master connectivity lost
5/13/2013 03:59:06 AM	AP Adopted	ap622-5864A0 AP B4-C7-99-58-64-A0 master connectivity established
5/13/2013 03:59:06 AM	Radio Added	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) added
5/13/2013 03:59:06 AM	Radio Added	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) added
5/13/2013 04:01:24 AM	AP Unadopted	ap622-5864A0 AP B4-C7-99-58-64-A0 master connectivity lost
5/13/2013 04:01:24 AM	Radio Removed	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) removed
5/13/2013 04:01:24 AM	Radio Removed	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) removed
5/13/2013 04:02:05 AM	AP Adopted	ap622-5864A0 AP B4-C7-99-58-64-A0 master connectivity established
5/13/2013 04:02:05 AM	Radio Added	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) added
5/13/2013 04:02:05 AM	Radio Added	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) added
5/17/2013 01:22:14 AM	Radio Removed	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) removed
5/17/2013 01:25:38 AM	Interference Recovery	ap622-5864A0 Radio 2 (B4-C7-99-58-62-F0) channel changed from 112 to 120
5/19/2013 11:58:06 PM	Interference Recovery	ap622-5864A0 Radio 1 (B4-C7-99-58-61-10) channel changed from 4 to 8

Type to search in tables

Row Count: 303

Refresh

Figure 15-30 *RF Domain - Smart RF History screen*

The **SMART RF History** screen displays the following RF Domain member historical data:

Time	Displays a time stamp when Smart RF status was updated on behalf of a Smart RF adjustment within the selected RF Domain.
Type	Lists a high-level description of the Smart RF activity initiated for a RF Domain member device.
Description	Provides a more detailed description of the Smart RF event in respect to the actual Smart RF calibration or adjustment made to compensate for detected coverage holes and interference.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.13 WIPS

RF Domain Statistics

Refer to the *Wireless Intrusion Protection Software* (WIPS) screens to review a client blacklist and events reported by a RF Domain member Access Point.

For more information, see:

- *WIPS Client Blacklist*
- *WIPS Events*

15.2.13.1 WIPS Client Blacklist

WIPS

The *Client Blacklist* displays clients detected by WIPS and removed from RF Domain utilization. Blacklisted clients are not allowed to associate to RF Domain member Access Point radios.

To view the WIPS client blacklist:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Expand the **WIPS** menu item and select **Client Blacklist**.

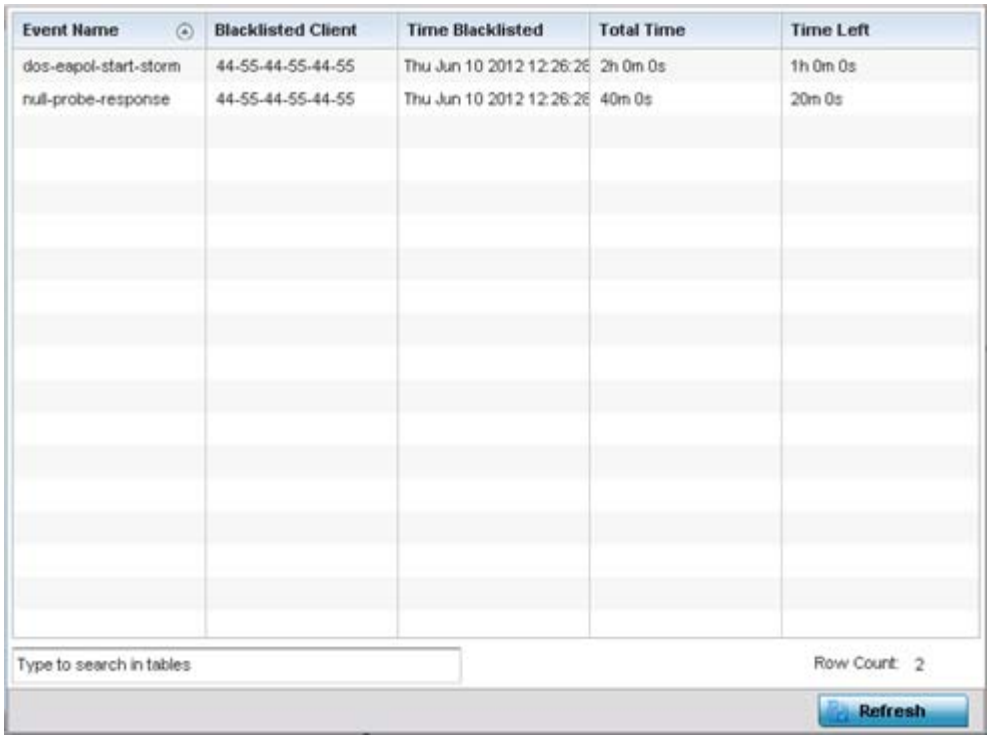


Figure 15-31 *RF Domain - WIPS Client Blacklist screen*

The WIPS **Client Blacklist** screen displays the following:

Event Name	Displays the name of the blacklisting wireless intrusion event detected by a RF Domain member Access Point.
Blacklisted Client	Displays the MAC address of the unauthorized (blacklisted) client intruding the RF Domain.
Time Blacklisted	Displays the time when the wireless client was blacklisted by a RF Domain member Access Point.
Total Time	Displays the time the unauthorized (now blacklisted) device remained in the RF Domain.
Time Left	Displays the time the blacklisted client remains on the list.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.13.2 WIPS Events

WIPS

Refer to the *WIPS Events* screen to assess WIPS events detected by RF Domain member Access Point radios and reported to the controller or service platform.

To view the rogue Access Point statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Expand the **WIPS** menu item and select **WIPS Events.**

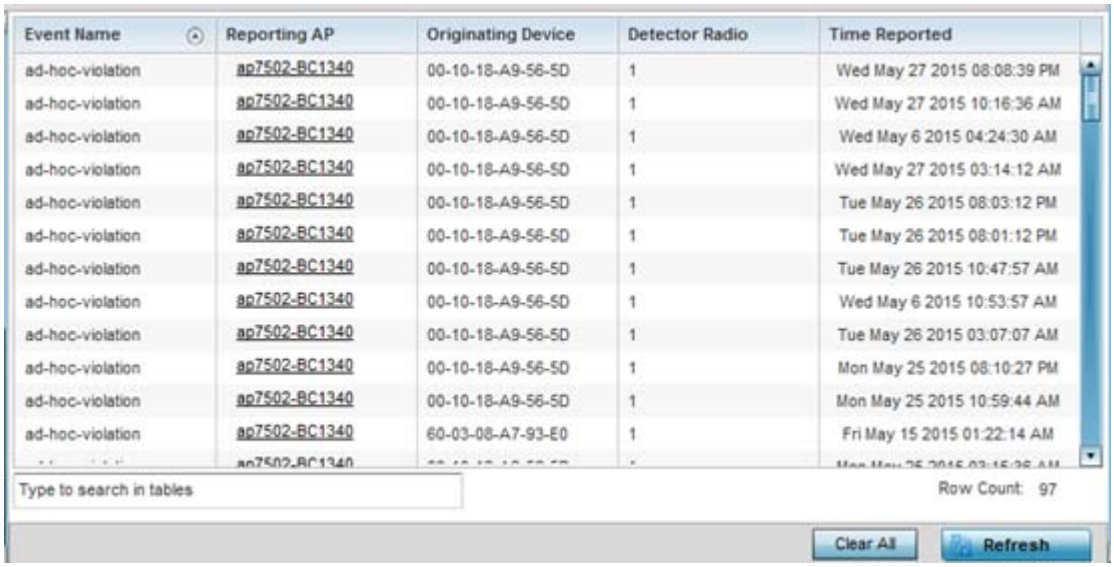


Figure 15-32 *RF Domain - WIPS Events screen*

The **WIPS Events** screen displays the following:

Event Name	Displays the event name of the intrusion detected by a RF Domain member Access Point.
Reporting AP	Displays the MAC address of the RF Domain member Access Point reporting the event.
Originating Device	Displays the MAC address of the device generating the event.
Detector Radio	Displays the radio number detecting the WIPS event.
Time Reported	Displays a time stamp of when the event was reported by the RF Domain member Access Point radio.
Clear All	Select the *Clear All* button to clear the statistics counters and begin a new data collection.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.14 Captive Portal

RF Domain Statistics

A captive portal is guest access policy for providing guests temporary and restrictive access to the controller or service platform managed wireless network. Captive portal authentication is used primarily for guest or visitor access to the network, but is increasingly being used to provide authenticated access to private network resources when 802.1X EAP is not a viable option. Captive portal authentication does not provide end-user data encryption, but it can be used with static WEP, WPA-PSK or WPA2-PSK encryption.

To view the RF Domain captive portal statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **Captive Portal** from the RF Domain menu.

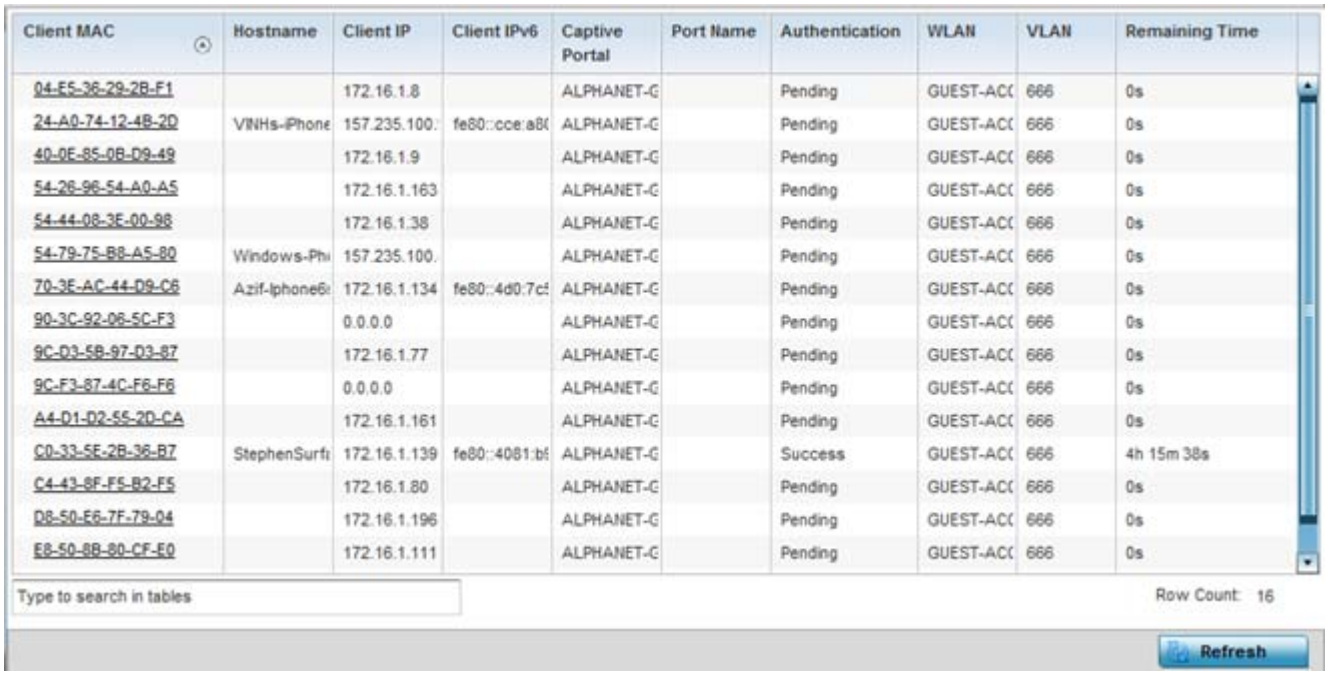


Figure 15-33 *RF Domain - Captive Portal*

The screen displays the following **Captive Portal** data for requesting clients:

Client MAC	Displays the MAC address of each listed client requesting captive portal access to the controller or service platform managed network. This address can be selected to display client information in greater detail.
Hostname	Lists the administrator assigned hostname of the device requesting captive portal access to network's RF Domain resources.
Client IP	Displays the IPv4 formatted address of each listed client using its connected RF Domain member Access Point for captive portal access.
Client IPv6	Displays any IPv6 formatted address of any listed client using its connected RF Domain member Access Point for captive portal access. IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Captive Portal	Lists the name of the RF Domain captive portal currently utilized by each listed client.
Port Name	Lists the name virtual port used for captive portal session direction.
Authentication	Displays the authentication status of requesting clients attempting to connect to the controller or service platform via the captive portal.
WLAN	Displays the name of the WLAN the requesting client would use for interoperation with the controller or service platform.
VLAN	Displays the name of the VLAN the client would use as a virtual interface for captive portal operation with the controller or service platform.

Remaining Time	Displays the time after which a connected client is disconnected from the captive portal.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.15 Application Visibility (AVC)

RF Domain Statistics

RF Domain member devices inspect every byte of each application header packet allowed to pass through the WiNG managed network. When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that specific application. For information on categorizing, filtering and logging the application data allowed to proliferate the WiNG managed network, refer to *Application Policy on page 7-54* and *Application on page 7-58*.

To view the RF Domain application utilization statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **Application Visibility (AVC)** from the RF Domain menu.

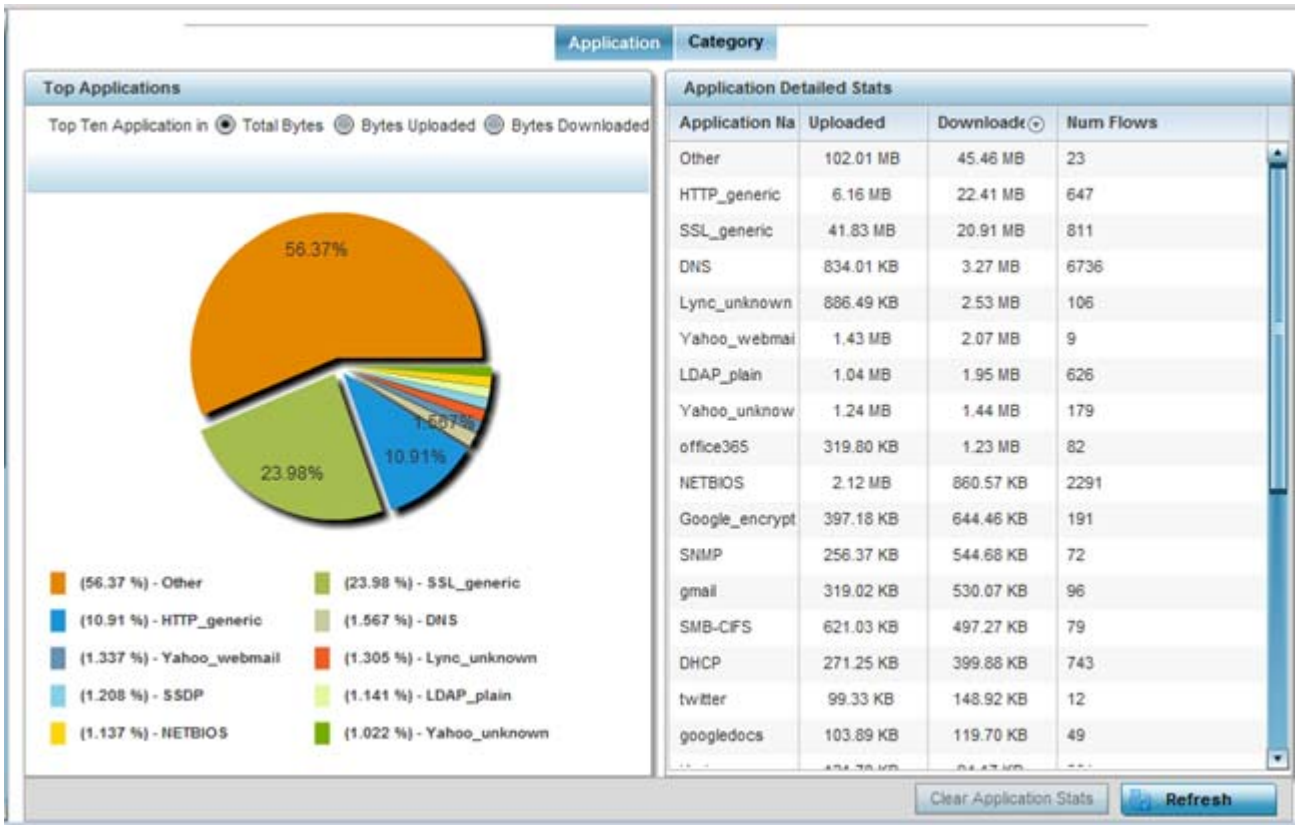


Figure 15-34 *RF Domain - Application Visibility*

4 Refer to the **Top Applications** graph to assess the most prolific, and allowed, application data passing through RF Domain member devices.

Total Bytes	Displays the top ten RF Domain member utilized applications in respect to total data bytes passing through the RF Domain member WiNG managed network. These are only the administrator *allowed* applications approved for proliferation within the RF Domain member device.
Bytes Uploaded	Displays the top ten RF Domain member applications in respect to total data bytes uploaded through the RF Domain member WiNG managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).
Bytes Downloaded	Displays the top ten RF Domain member applications in respect to total data bytes downloaded from the RF Domain member WiNG managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).

5 Refer to the **Application Detailed Stats** table to assess specific application data utilization:

Application Name	Lists the RF Domain member allowed application name whose data (bytes) are passing through the WiNG managed network.
Uploaded	Displays the number of uploaded application data (in bytes) passing the through the WiNG managed network.
Downloaded	Displays the number of downloaded application data (in bytes) passing the through the WiNG managed network.
Num Flows	Lists the total number of application data flows passing through RF Domain member devices for each listed application. An application flow can consist of packets in a specific connection or media stream. Application packets with the same source address/port and destination address/port are considered one flow.
Clear Application Stats	Select this option to clear the application assessment data counters and begin a new assessment.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

6 Select the **Category** tab.

Categories are existing WiNG or user defined application groups (video, streaming, mobile, audio etc.) that assist administrators in filtering (allowing or denying) application data. For information on categorizing application data, refer to *Application Policy on page 7-54* and *Application on page 7-58*.

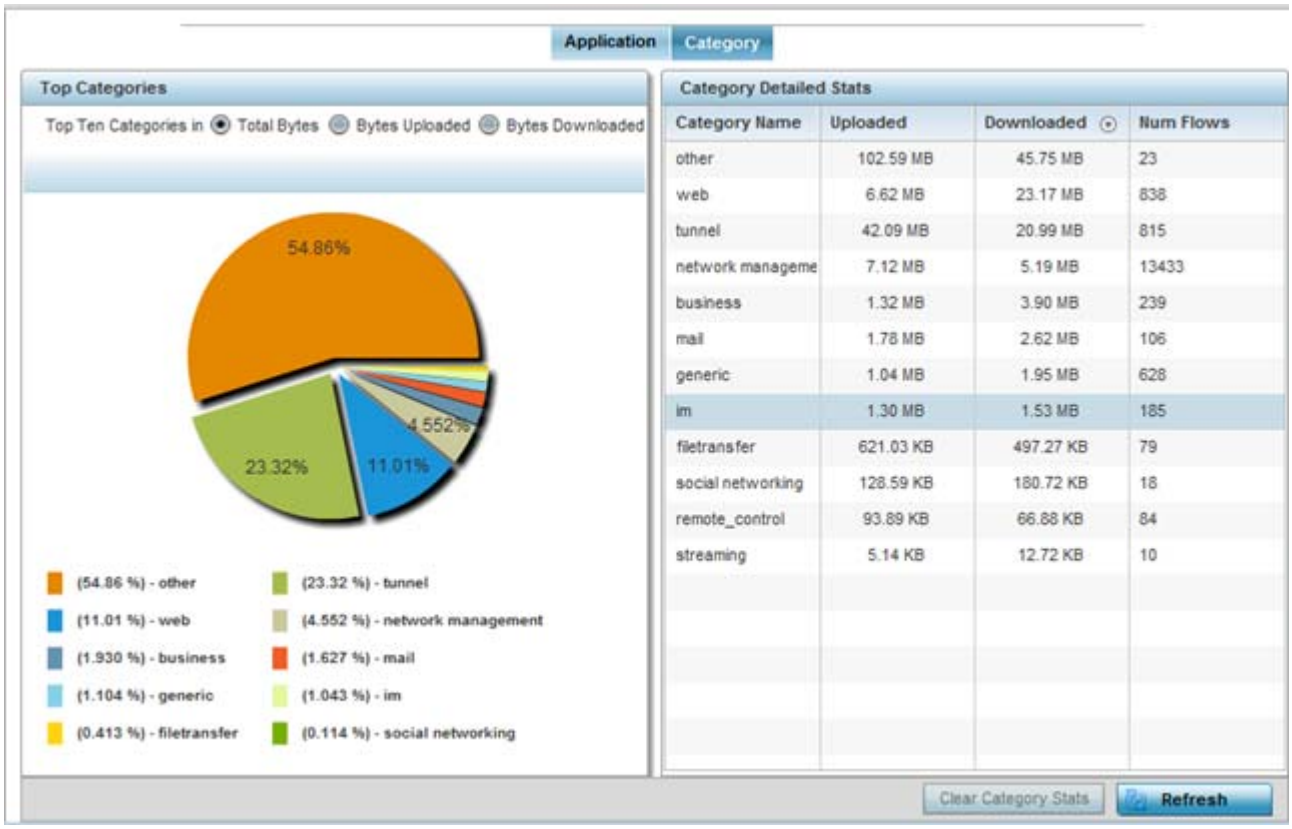


Figure 15-35 *RF Domain - Application Category Visibility*

7 Refer to the **Top Categories** graph to assess the most prolific, and allowed, application data categories utilized by RF Domain member devices.

Total Bytes	Displays the top ten RF Domain member application categories in respect to total data bytes passing through the RF Domain member WiNG managed network. These are only the administrator *allowed* application categories approved for proliferation within the RF Domain.
Bytes Uploaded	Displays the top ten RF Domain member application categories in respect to total data bytes uploaded through the RF Domain member WiNG managed network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories or adjusting their precedence (priority).
Bytes Downloaded	Displays the top ten RF Domain member application categories in respect to total data bytes downloaded from the RF Domain member WiNG managed network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories and categories or adjusting their precedence (priority).

8 Refer to the **Category Detailed Stats** table to assess specific application category data utilization:

Category Name	Lists the RF Domain member allowed category whose application data (in bytes) is passing through the WiNG managed network.

Uploaded	Displays the number of uploaded application category data (in bytes) passing the through the WiNG managed network.
Downloaded	Displays the number of downloaded application category data (in bytes) passing the through the WiNG managed network.
Num Flows	Lists the total number of application category data flows passing through RF Domain member devices. A category flow can consist of packets in a specific connection or media stream. Packets with the same source address/port and destination address/port are considered one flow.
Clear Application Stats	Select this option to clear the application category assessment data counters and begin a new assessment.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.16 Coverage Hole Summary

RF Domain Statistics

Periodically refer to a selected RF Domain's coverage hole summary to assess the RF Domain member Access Point radios reporting coverage hole adjustments. When coverage hole recovery is enabled and a deployment area radio coverage hole is detected, Smart RF determines the radio's power increase compensation required based on a reporting client's *signal to noise* (SNR) ratio. If a client's SNR is above the administrator threshold, its connected Access Point's transmit power is increased until the noise rate falls below the threshold.

To view a RF Domain's coverage hole summary:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **Coverage Hole Detection** from the RF Domain menu and expand this item to display its submenu options.

4 Select **Summary**.

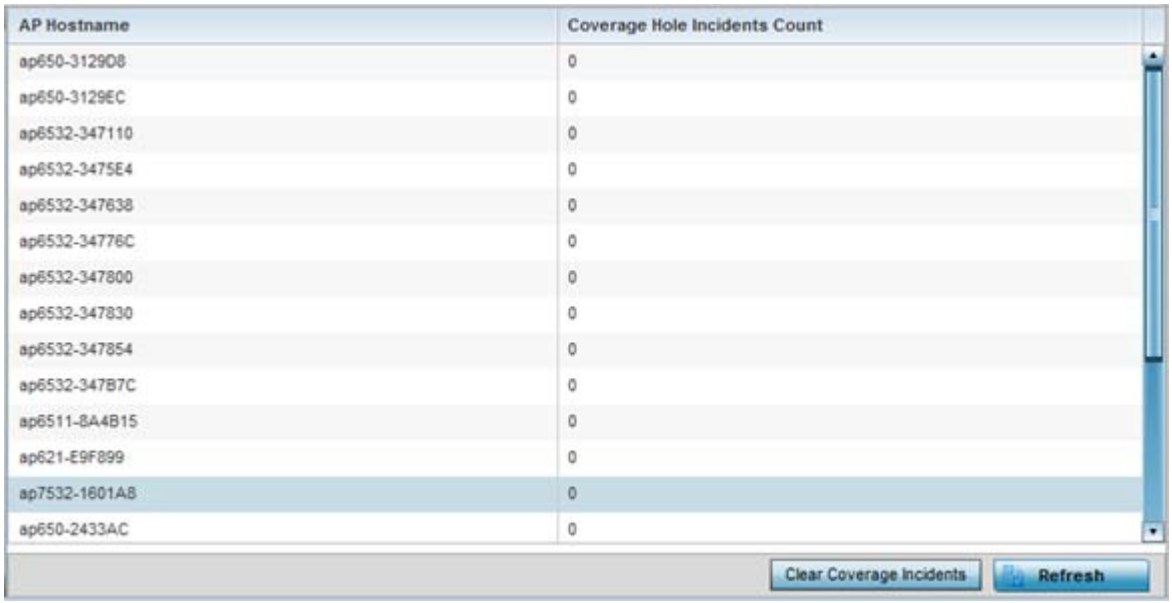


Figure 15-36 *RF Domain - Coverage Hole Summary*

The screen displays the following RF Domain coverage hole summarization data:

AP Hostname	Displays each RF Domain member Access Point hostname reporting a coverage hole compensation event. This can be helpful in assessing whether specific Access Points consistently report coverage holes and whether additional Access Point placements are required to compensate for poorly performing radios.
Coverage Hole Incidents Count	Lists each reporting Access Point's coverage hole incident count since the screen was last cleared. Periodically assess whether a specific Access Point's high incident count over a trended repeatable period warrants additional Access Point placements in that same radio coverage area to reduce a coverage hole.
Clear Coverage Incidents	Select this option to clear the statistics counters and begin a new coverage hole summary for RF Domain member Access Point radios.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.2.17 Coverage Hole Details

RF Domain Statistics

In addition to the RF Domain's Coverage Hole Summary, a specific Access Point's coverage hole history can be reviewed in detail. Consider using different RF Domain member Access Points or their connected clients to help validate the data reported before compensating for the coverage hole by increasing the radio transmit power of neighboring Access Points.

To review specific RF Domain member Access Point coverage hole information:

1 Select the **Statistics** menu from the Web UI.

2 Select a RF Domain from under the System node on the top, left-hand side, of the screen.

3 Select **Coverage Hole Detection** from the RF Domain menu and expand this item to display its submenu options.

4 Select **Detail**.

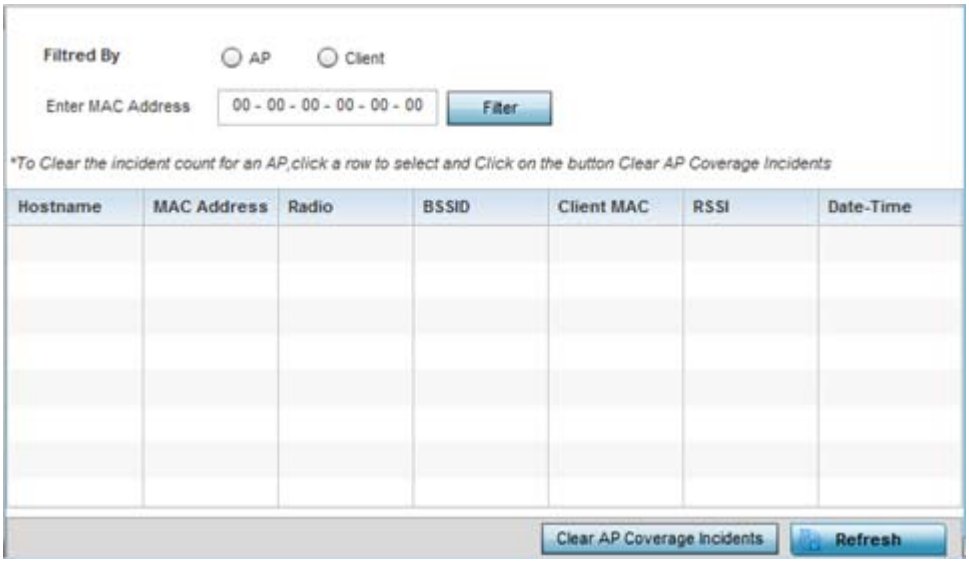


Figure 15-37 *RF Domain - Coverage Hole Details*

5 Use the **Filtered By** option to define whether the RF Domain's coverage hole details are provided by a selected Access Point (**AP**) or by a specific RF Domain member Access Point's connected **Client**. Consider filtering by different RF Domain member devices to validate the accuracy of a reported coverage hole before increasing the transmit power of neighboring radios to compensate.

6 Refer to the **Enter MAC Address** parameter to define a RF Domain member Access Point MAC address or Hostname or just a client MAC address. This is the selected device reporting coverage hole details to the listed RF Domain member Access Point.

7 Select **Filter** to begin the coverage hole data collection using the Access Point or client details provided. Refer to the following to review the data reported:

Hostname	Lists the administrator assigned hostname used as each listed Access Point's network identifier. This is the Access Point whose client(s) are reporting coverage hole RSSI data.
Radio	Lists the Access Point radio receiving and reporting coverage hole RSSI data from the listed client MAC. Each supported Access Point has at least two radios, with the exception of AP6521 model, which is a single-radio model.
BSSID	Displays the *basic service set identifier* (BSSID) included in an Access Point's wireless packet transmissions. Packets need to go to their correct destination. While a SSID keeps packets within the correct WLAN there's usually multiple Access Points within each WLAN. A BSSID identifies the correct Access Point and its connected clients.
Client MAC	Lists each connected client's hardware encoded MAC address. This is the client reporting coverage hole RSSI data to its connected Access Point radio.
RSSI	Displays the *Received Signal Strength Indicator* (RSSI) of the detecting Access Radio or client.

Date-Time	Displays the date and time when each listed Access Point received its coverage hole indecent information.
Clear Coverage Incidents	Select this option to clear the statistics counters and begin a new coverage hole assessment for RF Domain member Access Point radios.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.3 Controller Statistics

▸ *Statistics*

The Wireless Controller screen displays information about peer controllers or service platforms and their connected Access Points. As members of a cluster, a controller or service platform manages its own network and is ready to assume the load of an offline peer. The screen displays detailed statistics which include network health, inventory of devices, wireless clients, adopted APs, rogue APs and WLANs. For more information, refer to the following:

- *Health*
- *Device*
- *Cluster Peers*
- *Web-Filtering*
- *Application Visibility (AVC)*
- *Application Policy*
- *Device Upgrade*
- *Mirroring*
- *Adoption*
- *AP Detection*
- *Guest User*
- *Wireless LANs*
- *Policy Based Routing*
- *Radios*
- *Mesh*
- *Interfaces*
- *RAID Statistics*
- *Border Gateway Protocol (BGP) Statistics*
- *Power Status*
- *PPPoE*
- *OSPF*
- *L2TPv3*
- *VRRP*
- *Critical Resources*
- *LDAP Agent Status*
- *Mint Links*
- *Guest Users*
- *GRE Tunnels*
- *Dot1x*
- *Network*
- *DHCPv6 Relay & Client*

- *DHCP Server*
- *Firewall*
- *VPN*
- *Viewing Certificate Statistics*
- *WIPS Statistics*
- *Sensor Server*
- *Bonjour Services*
- *Captive Portal Statistics*
- *Network Time*

15.3.1 Health

Controller Statistics

The *Health* screen displays details such as hostname, device name, RF Domain name, radio RF quality and client RF quality.

To view controller or service platform device health data:

1 Select the Statistics tab from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select Health from the left-hand side of the UI.

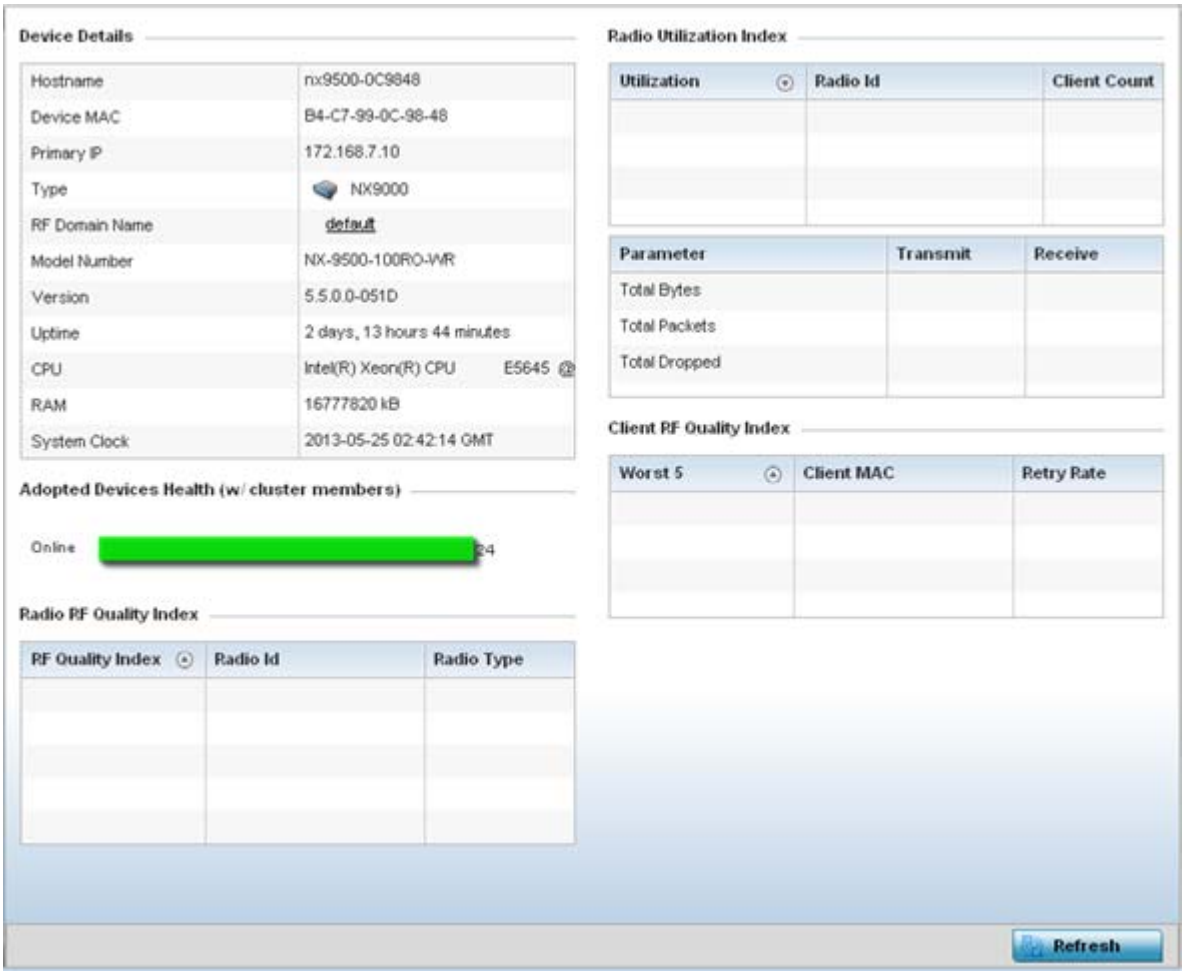


Figure 15-38 *Wireless Controller - Health screen*

The **Device Details** field displays the following:

Hostname	Displays the administrator assigned hostname of the controller or service platform.
Device MAC	Displays the MAC address of the controller.
Primary IP	Lists the network address used by this controller or service platform as a network identifier.
Type	Displays the RFS series controller or NX series service platform type.
RF Domain Name	Displays the controller's domain membership. The name displays in the form of a link that can be selected to display a detailed description of the RF Domain configuration.
Model Number	Displays the RFS series controller or NX series service platform type.
Version	Displays the version of the image running on the controller or service platform.
Uptime	Displays the cumulative time since the controller or service platform was last rebooted or lost power.
CPU	Displays the controller or service platform processor name.
RAM	Displays the CPU memory in use.

System Clock	Displays the system clock information.

The Access Point **Health (w/ cluster members)** chart shows how many Access Points are online and how many are offline. These are APs with cluster members directly managed by the wireless controller. This data does not include Access Points associated to other controllers or service platforms in the same cluster.

The **Radio RF Quality Index** field displays RF quality (overall effectiveness of the RF environment). Use this table to assess radio performance for improvement ideas.

The **RF Quality Index** field displays the following:

RF Quality Index	Displays the five radios with the lowest average quality.
Radio Id	Displays the hardware encoded MAC address of the radio.
Radio Type	Displays the radio type used by this Access Point.

The **Radio Utilization Index** field measures how efficiently the traffic medium is used. It's defined as the percentage of the current throughput relative to the maximum relative possible throughput:

Total Bytes	Displays the total bytes of data transmitted and received by the controller or service platform since the screen was last refreshed.
Total Packets	Lists the total number of data packets transmitted and received by the controller or service platform since the screen was last refreshed.
Total Dropped	List the number of dropped data packets by a controller or service platform managed Access Point radio since the screen was last refreshed.

The **Client RF Quality Index** field displays the RF quality of the clients. Use this table to troubleshoot radios not optimally performing:

Worst 5	Displays the five client radios with the lowest quality indices.
Client MAC	Displays the MAC address of the client.
Retry Rate	Displays the excessive retry rate of each listed controller or service platform managed client.

4 Select **Refresh** to update the statistics counters to their latest values.

15.3.2 Device

Controller Statistics

The *Device* statistics screen provides detailed information about the selected device.

To view controller or service platform device statistics:

1 Select the Statistics tab from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select Device from the left-hand side of the UI.

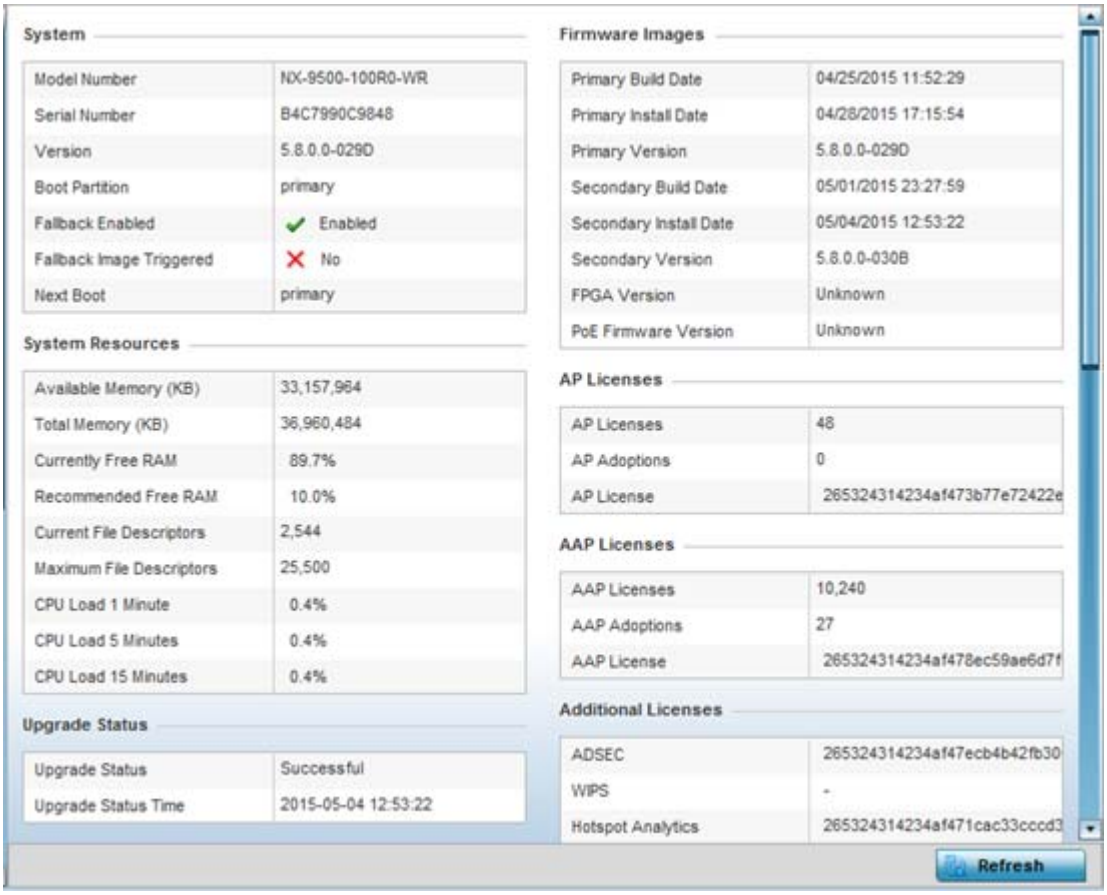


Figure 15-39 *Wireless Controller - Device screen*

The **System** field displays the following:

Model Number	Displays the model number for the selected controller or service platform.
Serial Number	Displays the serial number factory encoded on the controller or service platform at the factory.
Version	Displays the unique alphanumeric firmware version name for the controller or service platform firmware.
Boot Partition	Displays the boot partitioning type.
Fallback Enabled	Displays whether fallback is enabled. The fallback feature enables a user to store both a legacy and new firmware version in memory. You can test the new software and use an automatic fallback mechanism, which loads the old version, if the new version fails.
Fallback Image Triggered	Displays whether the fallback image has been triggered. The fallback is a legacy software image stored in device memory. This allows an user to test a new version and revert to the older version if needed.
Next Boot	Designates this version as the version used the next time the controller or service platform is booted.

The **System Resources** field displays the following:

Available Memory (MB)	Displays the available memory (in MB) available on the selected controller or service platform.

Total Memory (MB)	Displays the controller or service platform's total memory.
Currently Free RAM	Displays the Access Point's free RAM space. If its very low, free up some space by closing some processes.
Recommended Free RAM	Displays the recommended RAM required for routine operation.
Current File Descriptors	Displays the controller or service platform's current file description.
Maximum File Current File Descriptors	Displays the controller or service platform's maximum file description.
CPU Load 1 Minute	Lists the typical controller or service platform processor load over 1 minute.
CPU Load 5 Minutes	Lists the typical controller or service platform processor load over 5 minutes.
CPU Load 15 Minutes	Lists the typical controller or service platform processor load over 15 minutes.

The **Upgrade Status** field displays firmware upgrade statistics. The table provides the following:

Upgrade Status	Displays whether the image upgrade was successful.
Upgrade Status Time	Displays the time of the upgrade.

The **IP Domain** field displays the following:

IP Domain Name	Displays the name of the IP Domain service used with the selected controller or service platform.
IP Domain Lookup state	Lists the current state of the lookup operation.

The **Fan Speed** field displays the following:

Number	Displays the number of fans supported on the this controller or service platform.
Speed (Hz)	Displays the fan speed in Hz.

The **Temperature** field displays the following:

Number	Displays the number of temperature elements used by the controller or service platform.
Temperature	Displays the current temperature (in Celsius) to assess a potential Access Point overheat condition.

The **Kernal Buffers** field displays the following:

Buffer Size	Lists the sequential buffer size.
Current Buffers	Displays the current buffers available to the selected controller or service platform.
Maximum Buffers	Lists the maximum buffers available to the selected controller or service platform.

The **Firmware Images** field displays the following:

Primary Build Date	Displays the build date when this version was created.
Primary Install Date	Displays the date this version was installed on the controller or service platform.
Primary Version	Displays the primary version string.
Secondary Build Date	Displays the build date when this secondary version was created.
Secondary Install Date	Displays the date this secondary version was installed on the controller or service platform.
Secondary Version	Displays the secondary version string.
FGPA Version	Displays the version of FGPA firmware used by the controller or service platform.
PoE Version Firmware	Lists the *Power-Over-Ethernet* (PoE) version firmware.

The **AP Licenses** field displays the following:

AP Licenses	Displays the number of AP licenses currently available on the controller or service platform. This value represents the maximum number of licenses the controller or service platform can adopt.
AP Adoptions	Displays the number of Access Points adopted by this controller or service platform.
AP License	Displays the license string of the AP.

The **AAP Licenses** field displays the following:

AAP Licenses	Displays the number of AAP licenses currently available on the controller or service platform. This value represents the maximum number of licenses the controller or service platform can adopt.
AAP Adoptions	Displays the number of adaptive Access Points adopted by this controller or service platform.
AAP License	Displays the license string of the adaptive Access Point.

The **Additional Licenses** area displays the following information:

ADSEC	Displays Advanced Security licenses. This enables the Role Based firewall and increases the number of IP Sec VPN tunnels. The maximum number of IP Sec VPN tunnels varies by platform.
WIPS	Displays the number of WIPS licenses utilized by the controller or service platform.
Hotspot Analytics	Displays whether an advanced hotspot analytics license is in use and applied to the controller or service platform.

The **IP Name Servers** table displays the following:

Name Server	Displays any custom Name Server mappings on the controller or service platform.
Type	Displays the type of DNS mapping, if any, on the controller or service platform.

The **IPv6 Name Servers** table displays the following:

Name Server	Displays any custom IPv6 formatted IP address Name Server mappings on the controller or service platform.
Type	Displays the type of DNS mapping, if any, on the controller or service platform.

The **IPv6v Hop Limit** table displays the following:

Hop Limit	Lists the maximum number of times IPv6 traffic can hop. The IPv6 header contains a hop limit field that controls the number of hops a datagram can be sent before being discarded (similar to the TTL field in an IPv4 header).

The **IPv6 Delegated Prefixes** table displays the following:

IPv6 Delegated Prefix	If IPv6, prefix delegation is used to assign a network address prefix, configuring the controller or service platform with the prefix.
Prefix Name	Lists the 32 character maximum name for the IPv6 delegated prefix used as an easy to remember alias for an entire IPv6 address.
DHCPv6 Client State	Displays the current DHCPv6 client state as impacted by the IPv6 delegated prefix.
Interface Name	Lists the interface over which IPv6 prefix delegation occurs.
T1 timer (seconds)	Lists the amount of time in seconds before the DHCP T1 (delay before renew) timer expires.
T2 timer (seconds)	Lists the amount of time in seconds before the DHCP T2 (delay before rebind) timer expires.
Last Refreshed (seconds)	Lists the time, in seconds, since IPv6 prefix delegation has been updated.
Preferred Lifetime (seconds)	Lists is the time in seconds (relative to when the packet is sent) the IPv6 formatted addresses remains in a preferred state on the selected interface. The preferred lifetime must always be less than or equal to the valid lifetime.
Valid Lifetime (seconds)	Displays the time in seconds (relative to when the packet is sent) the IPv6 formatted address remains in a valid state on the selected interface. The valid lifetime must always be greater than or equal to the preferred lifetime.

15.3.3 Cluster Peers

Controller Statistics

Refer to the *Cluster Peers* screen to review device address and version information for peer devices within a cluster.

To view controller or service platform cluster peer statistics:

1 Select the **Statistics** tab from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Cluster Peers** from the left-hand side of the UI.

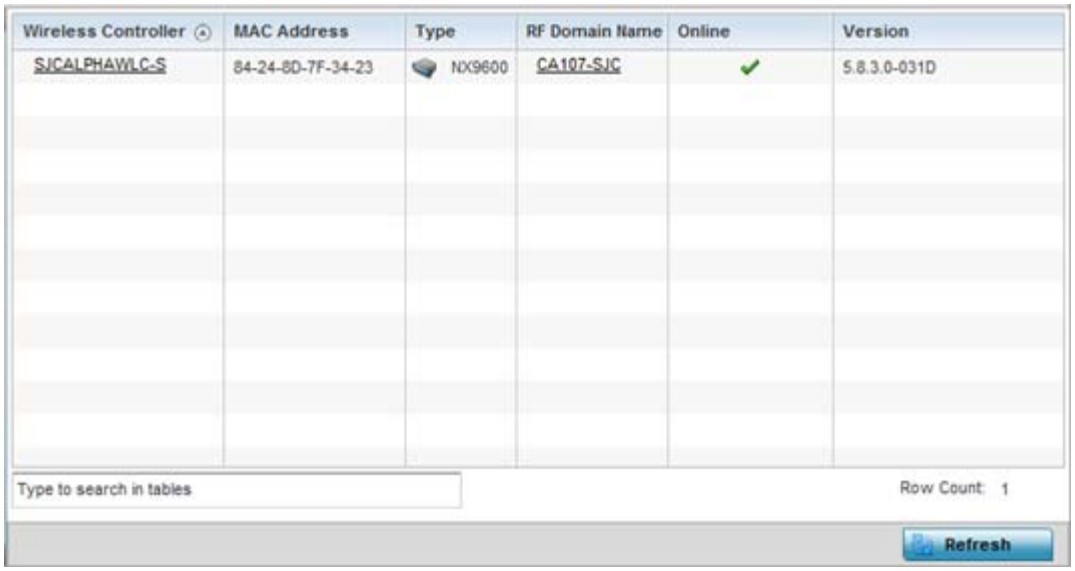


Figure 15-40 *Wireless Controller - Cluster Peers screen*

The **Cluster Peers** screen displays the following:

Wireless Controller	Displays the IP addresses of current cluster member controller or service platform. The name displays in the form of a link that can be selected to display a detailed description of the controller or service platform's configuration.
MAC Address	Displays the MAC addresses of current cluster members.
Type	Displays the type of cluster peer (by controller or service platform model).
RF Domain Name	Displays each member's RF Domain name. The name displays in the form of a link that can be selected to display a detailed description of the RF Domain's configuration.
Online	Displays whether a controller or service platform is online. If online, a green check mark displays, if it is offline a red X displays.
Version	Displays the numeric firmware version currently running on the controller or service platform. Use this version as the basis for comparison on whether newer versions are available from the support site that may provide increased functionality and a broader feature set.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.4 Web-Filtering

Controller Statistics

The *Web-Filtering* screen displays information on Web requests for content and whether the requests were blocked or approved based on URL filter settings defined for the selected controller or service platform. A URL filter is comprised of several filter rules. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.

To view this controller's Web filter statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Web-Filtering**.

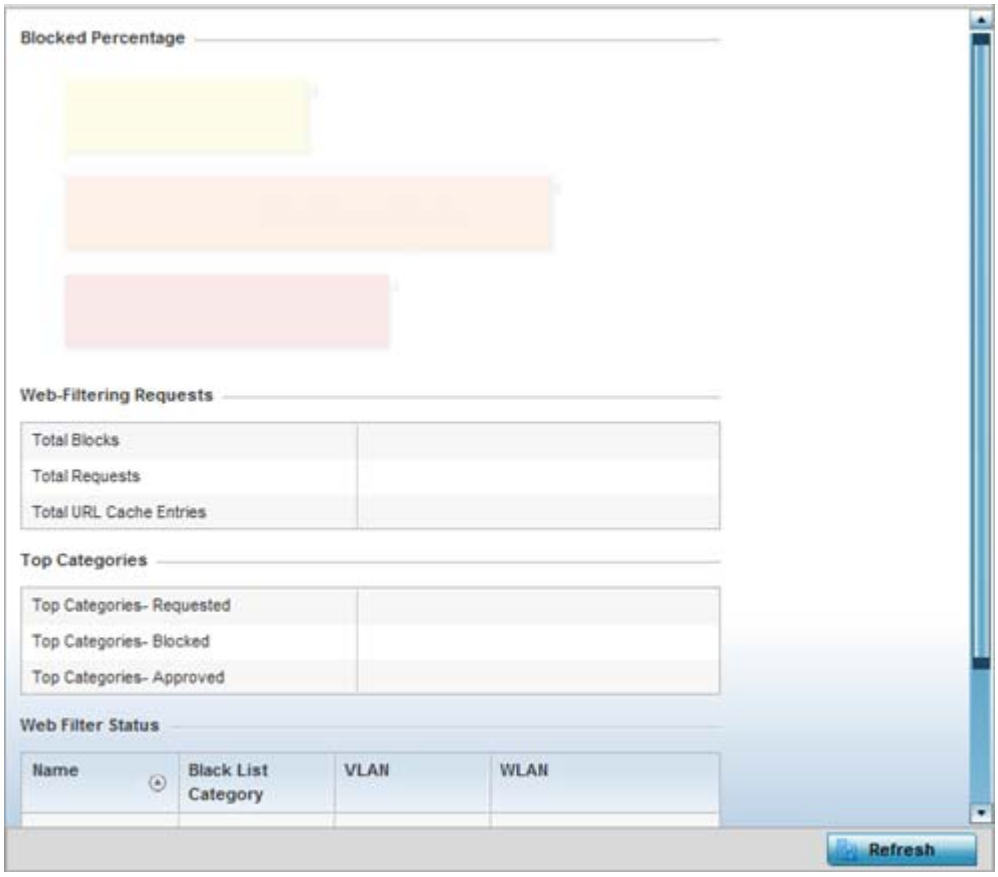


Figure 15-41 *Wireless Controller - Web Filtering screen*

The **Web-Filtering Requests** field displays the following information:

Total Blocks	Lists the number of Web request hits against content blocked in the URL blacklist.
Total Requests	Lists the total number of requests for URL content cached locally on this controller or service platform.
Total URL Cache Entries	Displays the number of chached URL data entries made on this controller or service platform on the request of requesting clients requiring URL data managed by the controller or service platform and their respective whitelist or blacklist.

The **Top Categories** field helps administrators assess the content most requested, blocked and approved based on the defined whitelist and blacklist permissions:

Top Categories - Requested	Lists those Web content categories most requested by clients managed by this controller or service platform. Use this information to assess whether the permissions defined in the blacklist and whitelist optimally support these client requests for cached Web content.

Top Categories - Blocked	Lists those Web content categories blocked most often for requesting clients managed by this controller or service platform. Use this information to periodically assess whether the permissions defined in the blacklist and whitelist still restrict the desired cached Web content from requesting clients. Remember, a whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.
Top Categories - Approved	Lists those Web content categories approved most often on behalf of requesting clients managed by this controller or service platform. Periodically review this information to assess whether this cached and available Web content still adhere's to your organization's standards for client access.

The **Web Filter Status** field displays the following information:

Name	Displays the name of the filter whose URL rule set has been invoked.
Blacklist Category	Lists the blacklist category whose URL filter rule set has caused data to be filtered to a requesting client. Periodically assess whether these rules are still relevant to the data requirements of requesting clients.
VLAN	Lists the impacted controller or service platform VLAN whose Web data traffic has been filtered based on the restrictions in the listed blacklist category.
WLAN	Lists the impacted controller or service platform WLAN whose Web data traffic has been filtered based on the restrictions in the listed blacklist category. Periodically assess whether clients are segregated to the correct WLAN based on their cached Web data requirements and impending filter rules.

4 Periodically select **Refresh** to update this screen to its latest values.

15.3.5 Application Visibility (AVC)

Controller Statistics

Controllers and service platforms can inspect every byte of each application header packet allowed to pass their managed radio devices. When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that specific application. For information on categorizing, filtering and logging the application data allowed to proliferate the controller or service platform managed network, refer to *Application Policy on page 7-54* and *Application on page 7-58*.

To view controller or service platform application utilization statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Application Visibility (AVC).**

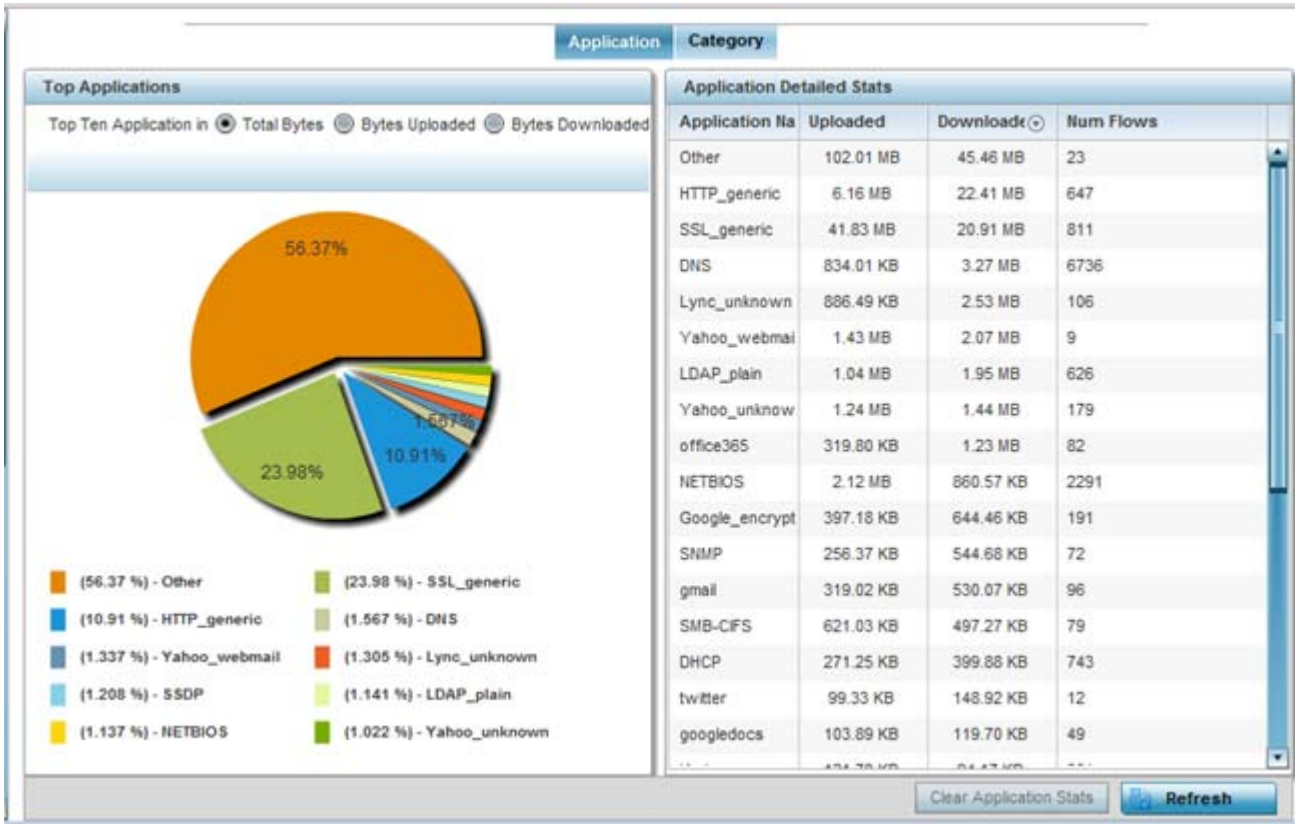


Figure 15-42 *Controller - Application Visibility*

4 Refer to the **Top Applications** graph to assess the most prolific, and allowed, application data passing through the controller and service platform.

Total Bytes	Displays the top ten utilized applications in respect to total data bytes passing through the controller or service platform managed network. These are only the administrator *allowed* applications approved for proliferation within the controller or service platform managed network.
Bytes Uploaded	Displays the top ten applications in respect to total data bytes uploaded through the controller or service platform managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).
Bytes Downloaded	Displays the top ten applications in respect to total data bytes downloaded from the controller or service platform managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).

5 Refer to the **Application Detailed Stats** table to assess specific application data utilization:

Application Name	Lists the allowed application name whose data (bytes) are passing through the controller or service platform managed network
Uploaded	Displays the number of uploaded application data (in bytes) passing the through the controller or service platform managed network.

Downloaded	Displays the number of downloaded application data (in bytes) passing the through the controller or service platform managed network.
Num Flows	Lists the total number of application data flows passing through the controller or service platform for each listed application. An application flow can consist of packets in a specific connection or media stream. Application packets with the same source address/port and destination address/port are considered one flow.
Clear Application Stats	Select this option to clear the application assessment data counters and begin a new assessment. Selecting this option will not clear category stats, just application stats.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

6 Select the **Category** tab.

Categories are existing WiNG or user defined application groups (video, streaming, mobile, audio etc.) that assist administrators in filtering (allowing or denying) application data. For information on categorizing application data, refer to *Application Policy on page 7-54* and *Application on page 7-58*.

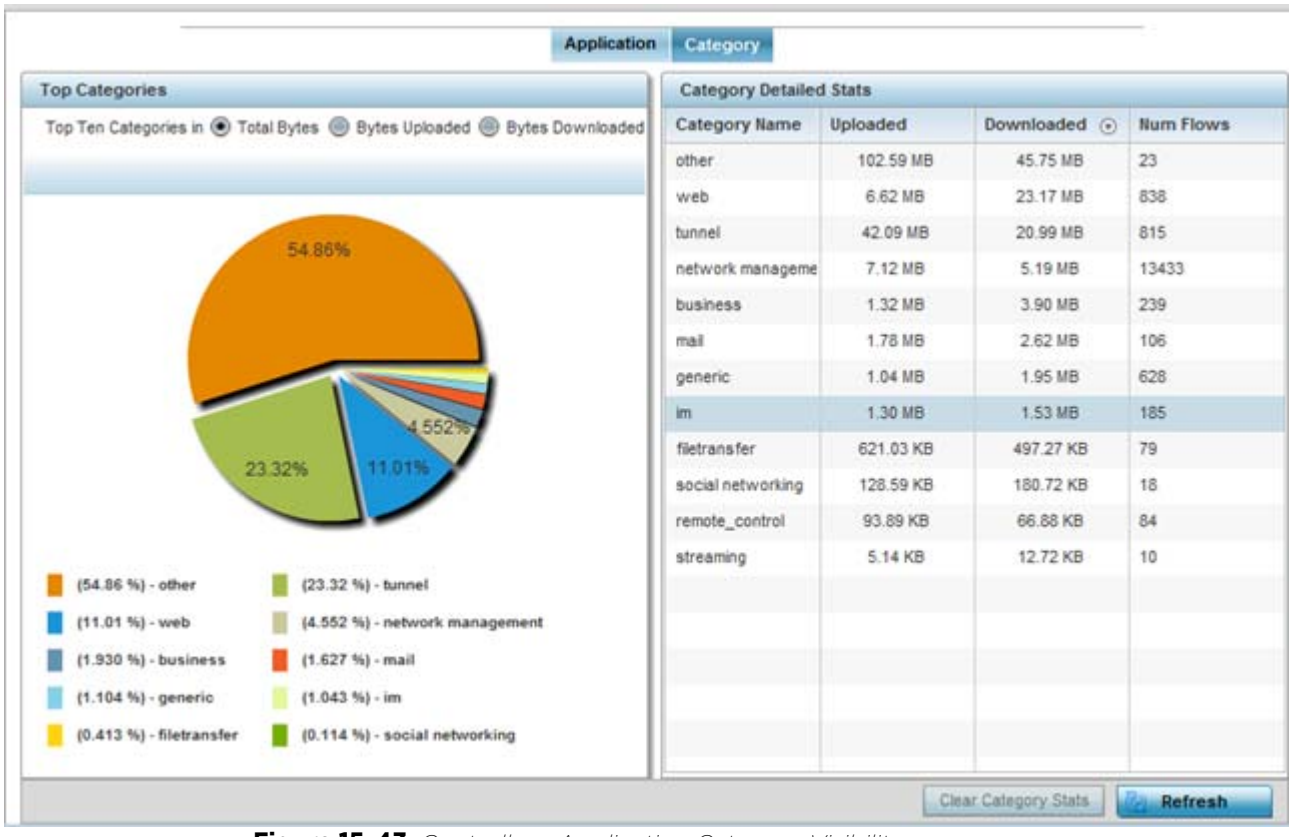


Figure 15-43 *Controller - Application Category Visibility*

7 Refer to the **Top Categories** graph to assess the most prolific, and allowed, application data categories utilized by the controller or service platform.

Total Bytes	Displays the top ten application categories in respect to total data bytes passing through the controller or service platform managed network. These are only the administrator *allowed* application categories approved for proliferation within the controller or service platform managed network.
Bytes Uploaded	Displays the top ten application categories in respect to total data bytes uploaded through the controller or service platform managed network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories or adjusting their precedence (priority).
Bytes Downloaded	Displays the top ten application categories in respect to total data bytes downloaded from the controller or service platform managed network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories and categories or adjusting their precedence (priority).

8 Refer to the **Category Detailed Stats** table to assess specific application category data utilization:

Category Name	Lists the allowed category whose application data (in bytes) is passing through the controller or service platform network.
Uploaded	Displays the number of uploaded application category data (in bytes) passing the through the controller or service platform managed network.
Downloaded	Displays the number of downloaded application category data (in bytes) passing the through the controller or service platform managed network.
Num Flows	Lists the total number of application category data flows passing through controller or service platform managed devices. A category flow can consist of packets in a specific connection or media stream. Packets with the same source address/port and destination address/port are considered one flow.
Clear Category Stats	Select this option to clear the application category assessment data counters and begin a new assessment. Selecting this option will not clear application stats, just category stats.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.3.6 Application Policy

Controller Statistics

When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that specific application. An application policy defines the rules or actions executed on recognized HTTP (Facebook), enterprise (Webex) and peer-to-peer (gaming) applications or application-categories.

For each rule defined, a precedence is assigned to resolve conflicting rules for applications and categories. A deny rule is exclusive, as no other action can be combined with a deny. An allow rule is redundant with other actions,

since the default action is allow. An allow rule is useful when wanting to deny packets for a category, but wanting to allow a few applications in the same category to proceed. In such a cases, add an allow rule for applications with a higher precedence then a deny rule for that category.

Mark actions mark packets for a recognized application and category with DSCP/8021p values used for QoS. Rate-limits create a rate-limiter applied to packets recognized for an application and category. Ingress and egress rates need to be specified for the rate-limiter, but both are not required. Mark and rate-limit are the only two actions that can be combined for an application and category. All other combinations are invalid.

To view controller or service platform application policy statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Application Policy**.

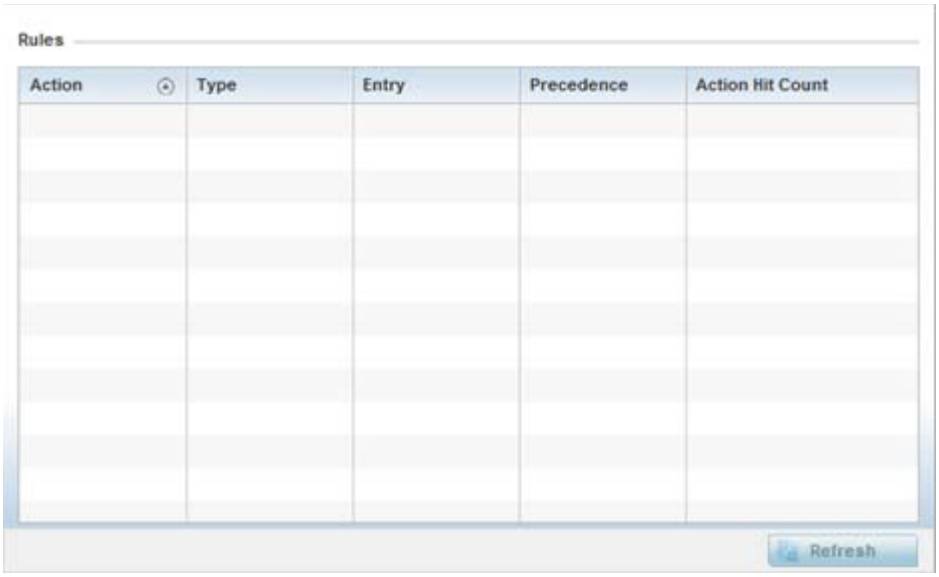


Figure 15-44 *Controller - Application Policy*

4 Refer to the **Rules** table to review the results of the application policies put in place thus far from this managing controller or service platform.

Action	Displays the action executed on the listed application. *Allow* - Allows packets for a specific application and its defined category type (social networking etc.). This is the default *Deny* - Denies (restricts) the action applied to a specific application or a specific application category *Mark* - Marks recognized packets with DSCP/8021p value *Rate-limit* - Rate limits packets from specific application types.
Type	Displays the application policy type applied.
Precedence	Lists the priority (from 1 - 256) for the application policy rule. The lower the value, the higher the priority assigned to this rule's enforcement action and the category and application assigned. A precedence also helps resolve conflicting rules for applications and categories.

Action Hit Count	Displays the number of times each listed application policy action has been triggered.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.3.7 Device Upgrade

Controller Statistics

The *Device Upgrade* screen displays information about the devices receiving updates within the controller or service platform managed network. Use this screen to gather version data, install firmware images, boot an image and upgrade status.

Controllers, service platforms or Access Points can be RF domain managers capable of receiving device firmware files from the NOC (NX4500, NX6500, NX7500 or NX9000 series service platforms) then provisioning other devices within their same RF domain. Controllers, service platforms and Access Points can now all update the firmware of different device models within their RF domain. However, firmware updates cannot be made simultaneously to devices in different site deployments.

To view the upgrade statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Device Upgrade**.

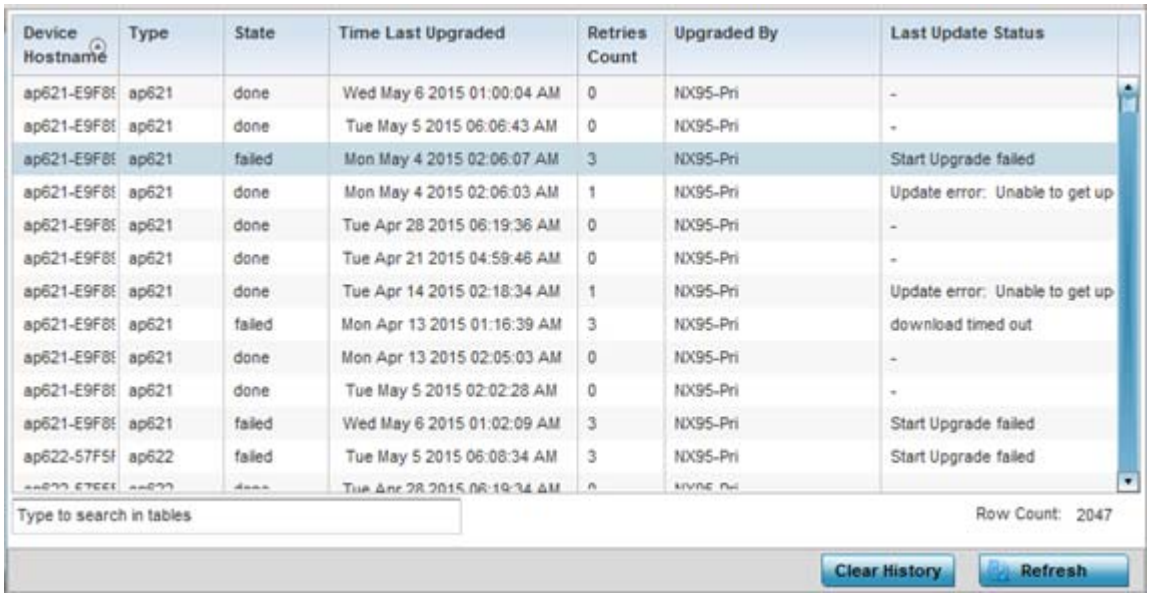


Figure 15-45 *Wireless Controller - Device Upgrade screen*

The **Upgrade** screen displays the following information:

Device Hostname	Displays the administrator assigned hostname of the device receiving the update.
Type	Displays the model type of the device receiving a firmware update from the provisioning controller or service platform.
State	Displays the current state of the Access Point upgrade (*done*, *failed* etc.).

Time Last Upgraded	Displays the date and time of the last successful upgrade operation.
Retries Count	Displays the number of retries made in an update operation.
Upgraded By	Displays the MAC address of the controller or service platform that performed the upgrade operation.
Last Update Status	Displays the status of the last upgrade operation (Start Upgrade, Update error etc.).
Clear History	Select the *Clear History* button to clear the screen of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.8 Mirroring

Controller Statistics

NX4524 and NX6524 model service platforms have the ability to mirror data packets transmitted or received on any of their GE ports (GE port 1 - 24). Both transmit and receive packets can be mirrored from a source to a destination port as needed to provide traditional spanning functionality on the 24 GE ports.

Port mirroring is not supported on NX4500 or NX6500 models, as they only utilize GE ports 1 - 2. Additionally, port mirroring is not supported on uplink (up) ports or wired ports on any controller or service platform model.

To view NX4524 or NX6524 model service platform port mirroring statistics:

1 Select the **Statistics** tab from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Mirroring** from the left-hand side of the UI.

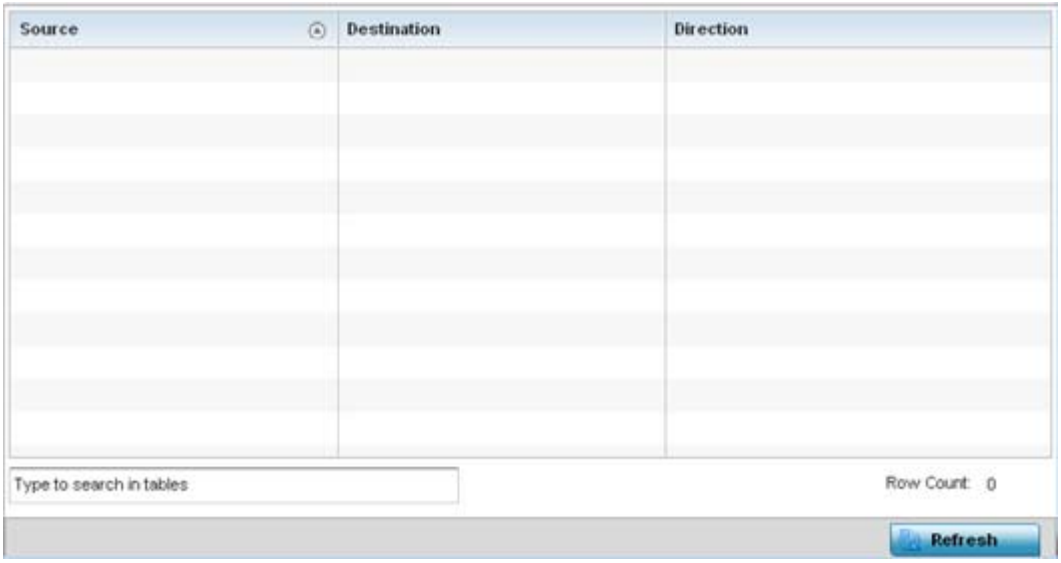


Figure 15-46 *Wireless Controller - Mirroring screen*

The **Mirroring** screen displays the following statistical data:

Source	Lists the GE port (1 - 24) used as the data source to span packets to the selected destination port. The packets spanned from the selected source to the destination depend on whether *Inbound*, *Outbound* or *Any* was selected as the direction. A source port cannot be a destination port.
Destination	Displays the GE port (1 - 24) used as the port destination to span packets from the selected source. The destination port serves as a duplicate image of the source port and can be used to send packets to a network diagnostic without disrupting the behavior on the original port. The destination port transmits only mirrored traffic and does not forward received traffic. Additionally, address learning is disabled on the destination port.
Direction	Lists the direction data packets are spanned from the selected source to the defined destination. Packets spanned from the source to the destination depend on whether *Inbound* (received packets only), *Outbound* (transmitted packets only) or *Any* (packets in either direction) was selected.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.9 Adoption

Controller Statistics

The *Adoption* screens lists Access Points adopted by the controller or service platform, and includes model, RF Domain membership, configuration status and device uptime information. For additional AP adoption information, including an adoption history and pending adoptions, see:

- *AP Adoption History*
- *Pending Adoptions*

To view device adoption statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Adoption > Adopted Devices** from the left-hand side of the UI.

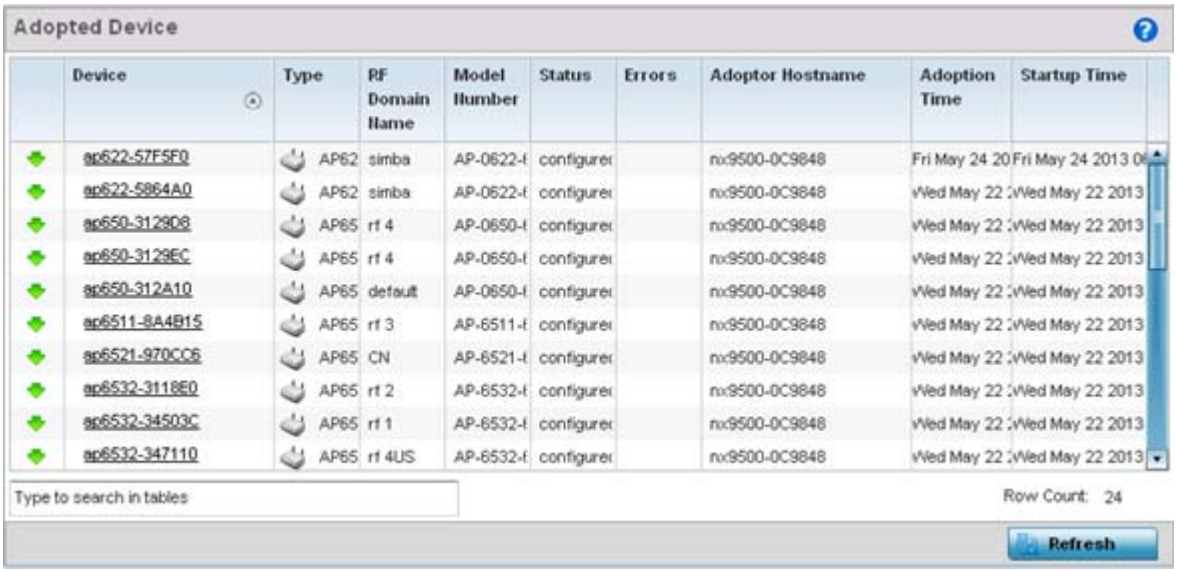


Figure 15-47 *Wireless Controller - Adopted Devices screen*

The **Adopted Devices** screen displays the following:

Device	Displays the name assigned to the adopted device by the management software. The Access Point name displays as a link that can be selected to display configuration and network address information in greater detail.
Type	Lists the model type of each Access Point managed by the selected controller or service platform (the controller or service platform listed in the Adopter Hostname column).
RF Domain Name	Displays the RF Domain memberships of each listed adopted device.
Model Number	Displays the model number of the adopted device.
Status	Lists whether an adopted Access Point has been configured (provisioned) by its connected Access Point or service platform.
Errors	Lists any errors encountered when the each listed Access Point was adopted by the controller or service platform.
Adopter Hostname	Lists the hostname assigned to the adopting controller or service platform.
Adoption Time	Displays a timestamp for each listed Access Point reflecting when the device was adopted by the controller or service platform.
Startup Time	Lists the time the adopted device was last started up and detected on the network.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.9.1 AP Adoption History

Controller Statistics

The *AP Adoption History* screen displays a list of devices adopted to the controller or service platform managed network. Use this screen to view a list of devices and their current status.

To view adopted AP Adoption History statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Adoption > AP Adoption History** from the left-hand side of the UI.

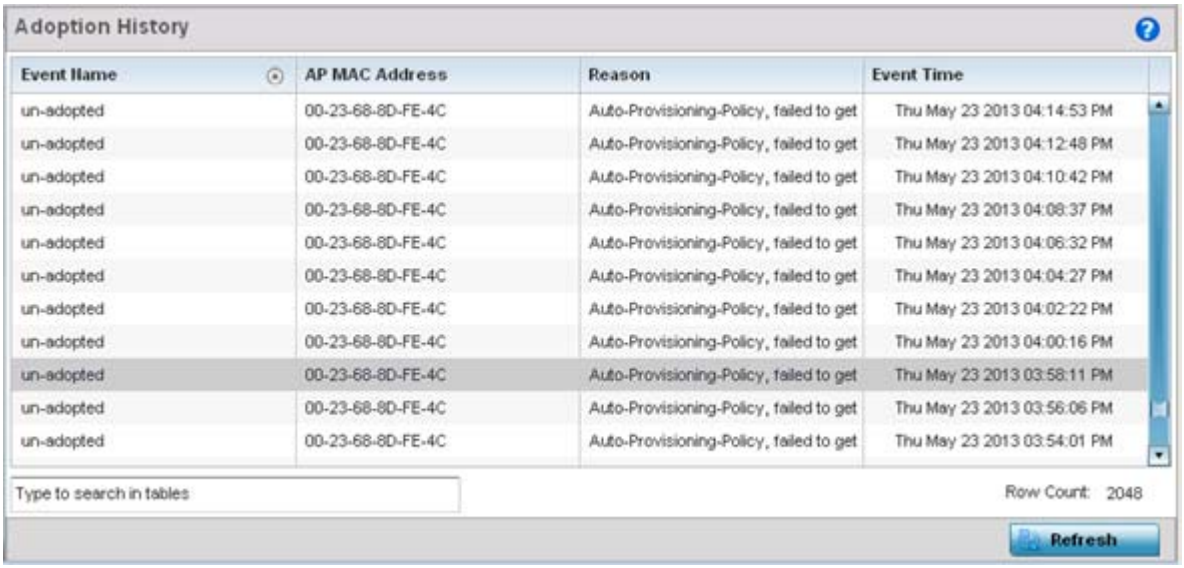


Figure 15-48 *Wireless Controller - AP Adoption History screen*

The **AP Adoption History** screen displays the following

Event Name	Displays the current adoption status of each AP as either *adopted* or *un-adopted*.
AP MAC Address	Displays the *Media Access Control* (MAC) address of each Access Point that the controller or service platform has attempted to adopt.
Reason	Displays the adoption reason message string for each event in the adoption history statistics table.
Event Time	Displays the day, date and time for each Access Point adoption attempt by this controller or service platform.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.9.2 Pending Adoptions

Controller Statistics

The *Pending Adoptions* screen displays devices still pending (awaiting) adoption to the controller or service platform managed network. Review this data to assess whether adoption is still beneficial and to troubleshoot issues preventing adoption.

To view adopted AP statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Adoption > Pending Adoptions** from the left-hand side of the UI.

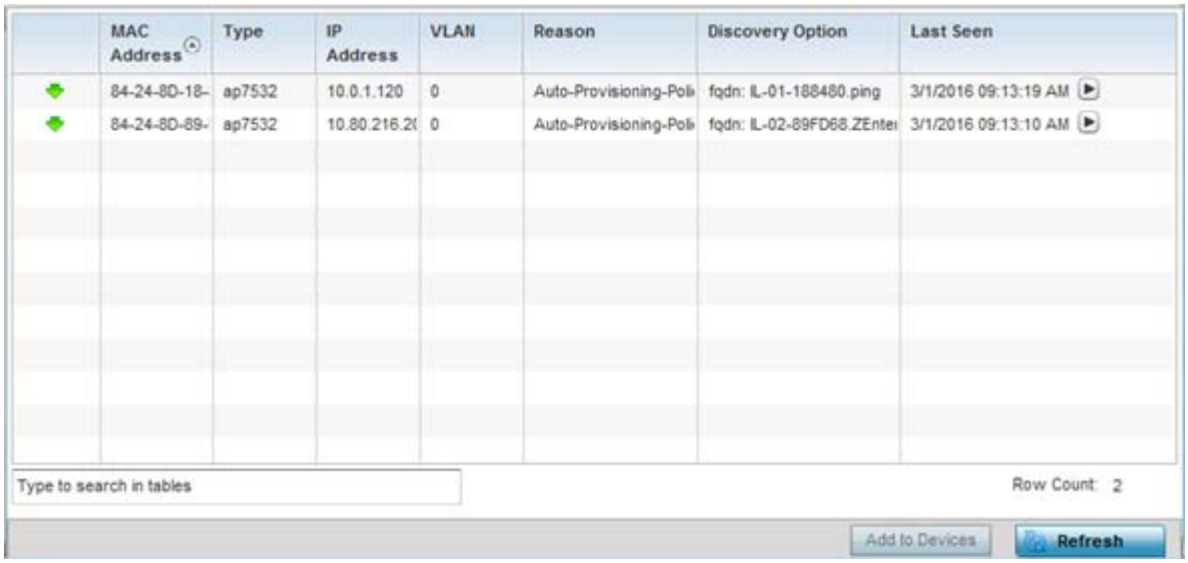


Figure 15-49 *Wireless Controller - Pending Adoptions screen*

The **Pending Adoptions** screen provides the following

MAC Address	Displays the MAC address of the device pending adoption.
Type	Displays the AP's model type.
IP Address	Displays the current IP address of the device pending adoption.
VLAN	Displays the current VLAN number (virtual interface ID) of the device pending adoption.
Reason	Displays the status code as to why the device is still pending adoption.
Discovery Option	Displays the discovery option code for each AP listed pending adoption.
Last Seen	Displays the date and time stamp of the last time the device was seen. Click the arrow next to the date and time to toggle between standard time and UTC.
Add to Devices	Select a device from amongst those displayed and select *Add to Devices* to validate the adoption of the selected device and begin the process of connecting the device to the controller or service platform managed network.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

15.3.10 AP Detection

Controller Statistics

The *AP Detection* screen displays potentially hostile Access Points, their SSIDs, reporting AP, and so on. Continuously revalidating the credentials of detected devices reduces the possibility of an Access Point hacking into the controller or service platform managed network.

To view AP detection statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **AP Detection** from the left-hand side of the UI.

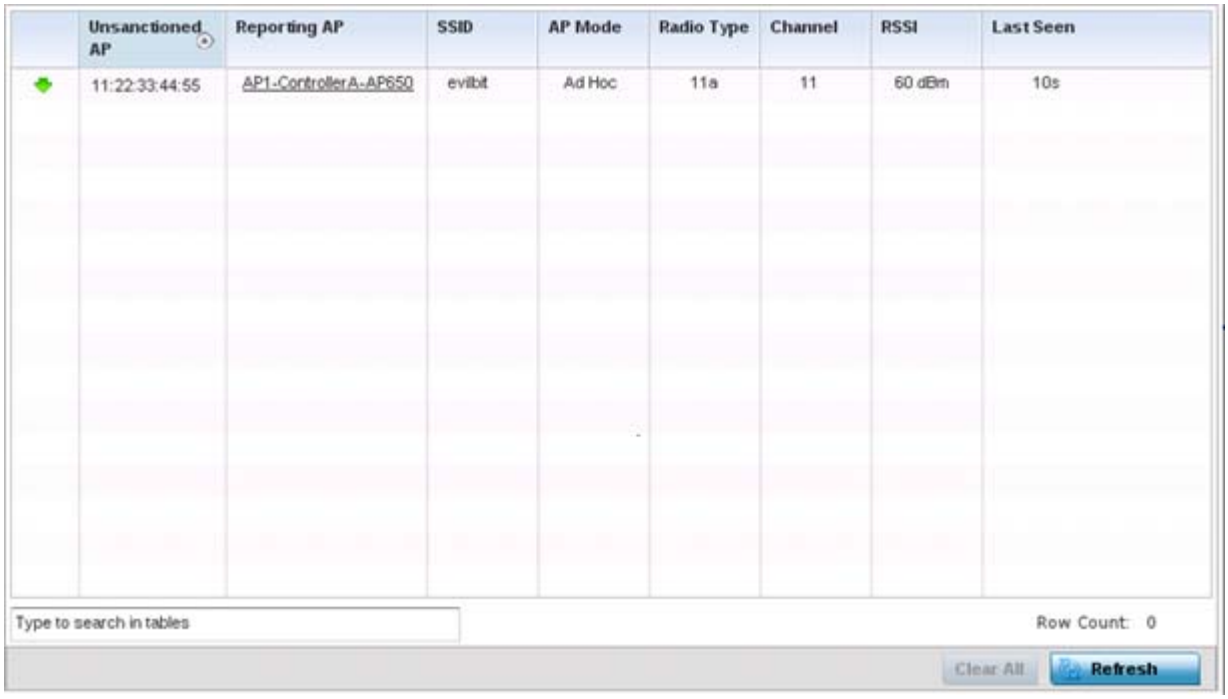


Figure 15-50 *Wireless Controller - AP Detection screen*

The **AP Detection** screen displays the following:

Unsanctioned AP	Displays the MAC address of unsanctioned APs detected within the controller or service platform radio coverage area. Unsanctioned APs are detected APs without deployment approval.
Reporting AP	Lists the Access Point whose radio detected the unsanctioned AP. The Access Point displays as a link that can be selected to display configuration and network address information in greater detail.
SSID	Displays the SSID of each unsanctioned AP.
AP Mode	Displays the operating mode of the unsanctioned device.
Radio Type	Displays the unsanctioned AP's radio type. The radio can be 802.11b, 802.11bg, 802.1bgn, 802.11a or 802.11an.
Channel	Displays the channel where the unsanctioned AP was detected.
RSSI	Lists the *Received Signal Strength Indicator* (RSSI) for each listed AP.

Last Seen	Displays when the unsanctioned AP was last seen by the detecting AP.
Clear All	Select *Clear All* to clear all the screen's statistic counters and begin detecting new Access Points.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

15.3.11 Guest User

Controller Statistics

The *Guest User* screen displays read only device information for guest clients associated with the selected controller or service platform. Use this information to assess if configuration changes are required to improve network performance.

To view a controller or service platform's connected guest user client statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Guest User** from the left-hand side of the UI.

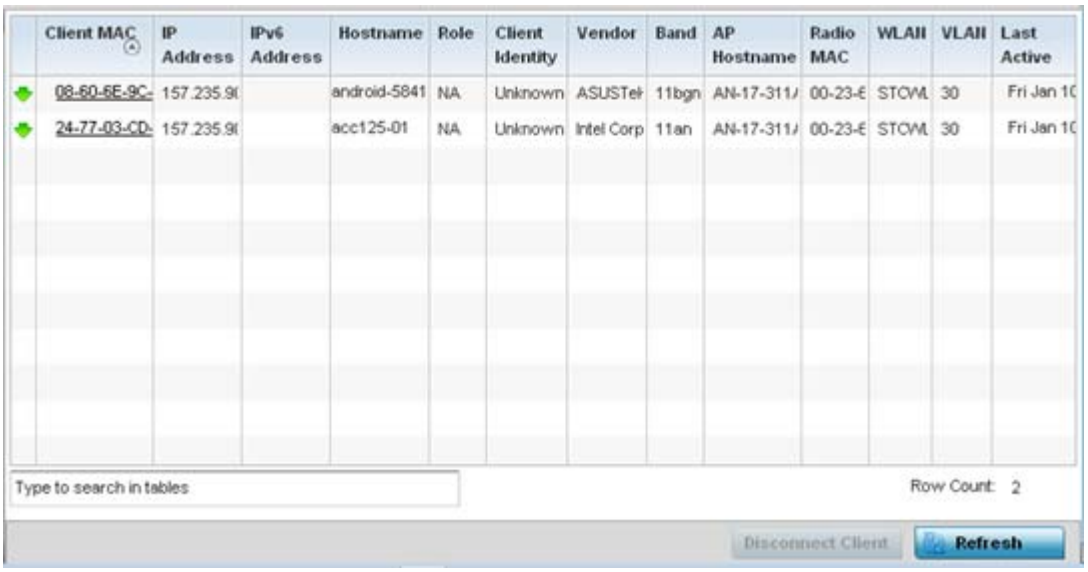


Figure 15-51 *Wireless Controller - Guest User screen*

The **Guest User** screen displays the following:

Client MAC	Displays the hardcoded MAC address assigned to the guest client at the factory and can not be modified. The address displays as a link that can be selected to display configuration and network address information in greater detail.
IP Address	Displays the unique IP address of the guest client. Use this address as necessary throughout the applet for filtering and device intrusion recognition and approval.
IPv6 Address	Displays the current IPv6 formatted IP address a listed guest client is using as a network identifier. IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

Hostname	Displays the hostname (MAC addresses) of connected guest clients. The hostname displays as a link that can be selected to display configuration and network address information in greater detail.
Role	Lists the guest client's defined role within the controller or service platform managed network.
Client Identity	Displays the unique vendor identity of the listed device as it appears to its adopting controller or service platform.
Vendor	Displays the name of the client vendor (manufacturer).
Band	Displays the 2.4 or 5 GHz radio band on which the listed guest client operates.
AP Hostname	Displays the administrator assigned hostname of the Access Point to which this guest client is associated.
Radio MAC	Displays the MAC address of the radio which the guest client is connected.
WLAN	Displays the name of the WLAN the guest client is currently assigned for its Access Point interoperation.
VLAN	Displays the VLAN ID the guest client's connected Access Point has defined as a virtual interface.
Last Active	Displays the time when this guest client was last seen (or detected) by a device within the controller or service platform managed network.
Disconnect Client	Select a specific client and select the *Disconnect Client* button to terminate this guest client's connection to its controller or service platform connected Access Point radio.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

15.3.12 Wireless LANs

Controller Statistics

The *Wireless LANs* statistics screen displays performance statistics for each controller or service platform managed WLAN. Use this information to assess if configuration changes are required to improve connected Access Point and client performance.

To view the wireless LAN statistics for the controller or service platform:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Wireless LANs** from the left-hand side of the UI.

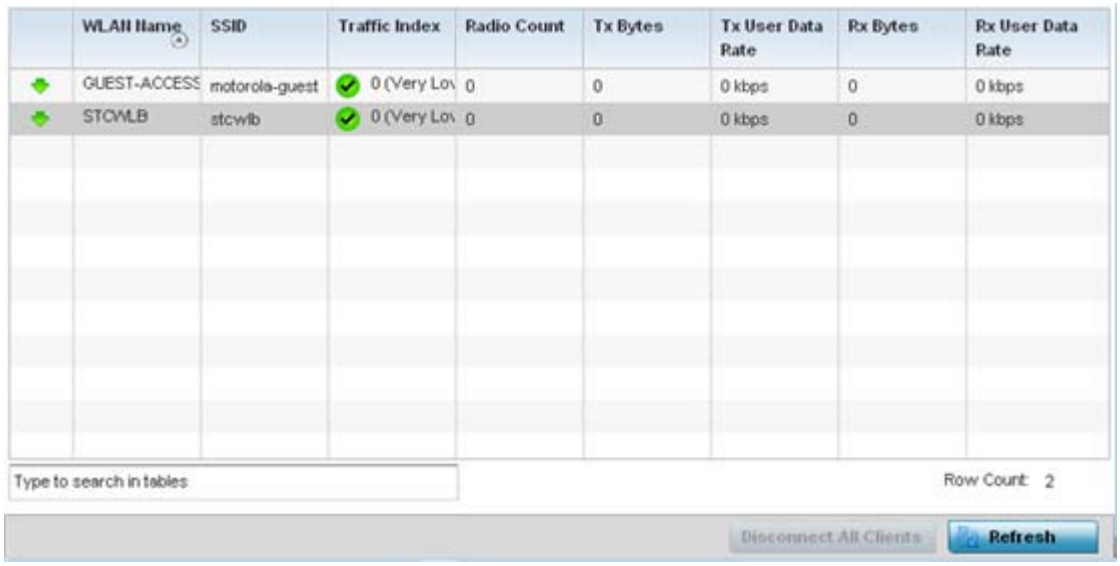


Figure 15-52 *Wireless Controller - Wireless LANs screen*

The **Wireless LANs** screen displays the following:

WLAN Name	Displays the name of the WLANs the controller or service platform is currently utilizing for client connections and QoS segregation.
SSID	Displays the Service Set ID each listed WLAN is using as an identifier.
Traffic Index	Displays the traffic utilization index, which measures how efficiently the traffic medium is used. It's defined as the percentage of current throughput relative to the maximum possible throughput. Traffic indices are: *0 – 20* (very low utilization) *20 – 40* (low utilization) *40 – 60* (moderate utilization) *60 and above* (high utilization)
Radio Count	Displays the number of radios currently in use by devices utilizing the listed controller or service platform managed WLAN.
Tx Bytes	Displays data transmit activity (in bytes) on each listed WLAN.
Tx User Data Rate	Displays the average user data rate on each listed WLAN.
Rx Bytes	Displays the data received in bytes on each listed WLAN.
Rx User Data Rate	Displays the average user data rate for packets received by controller or service platform connected devices using this WLAN.
Disconnect All Clients	Select *Disconnect All Clients* to terminate the all client WLAN memberships.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

15.3.13 Policy Based Routing

Controller Statistics

The *Policy Based Routing* statistics screen displays statistics for selective path packet redirection. PBR can optionally mark traffic for preferential services (QoS). PBR is applied to incoming routed packets, and a route-map

is created containing a set of filters and associated actions. Based on the actions defined in the route-map, packets are forwarded to the next relevant hop. Route-maps are configurable under a global policy called *routing-policy*, and applied to profiles and devices.

To review controller PBR statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Policy Based Routing**.

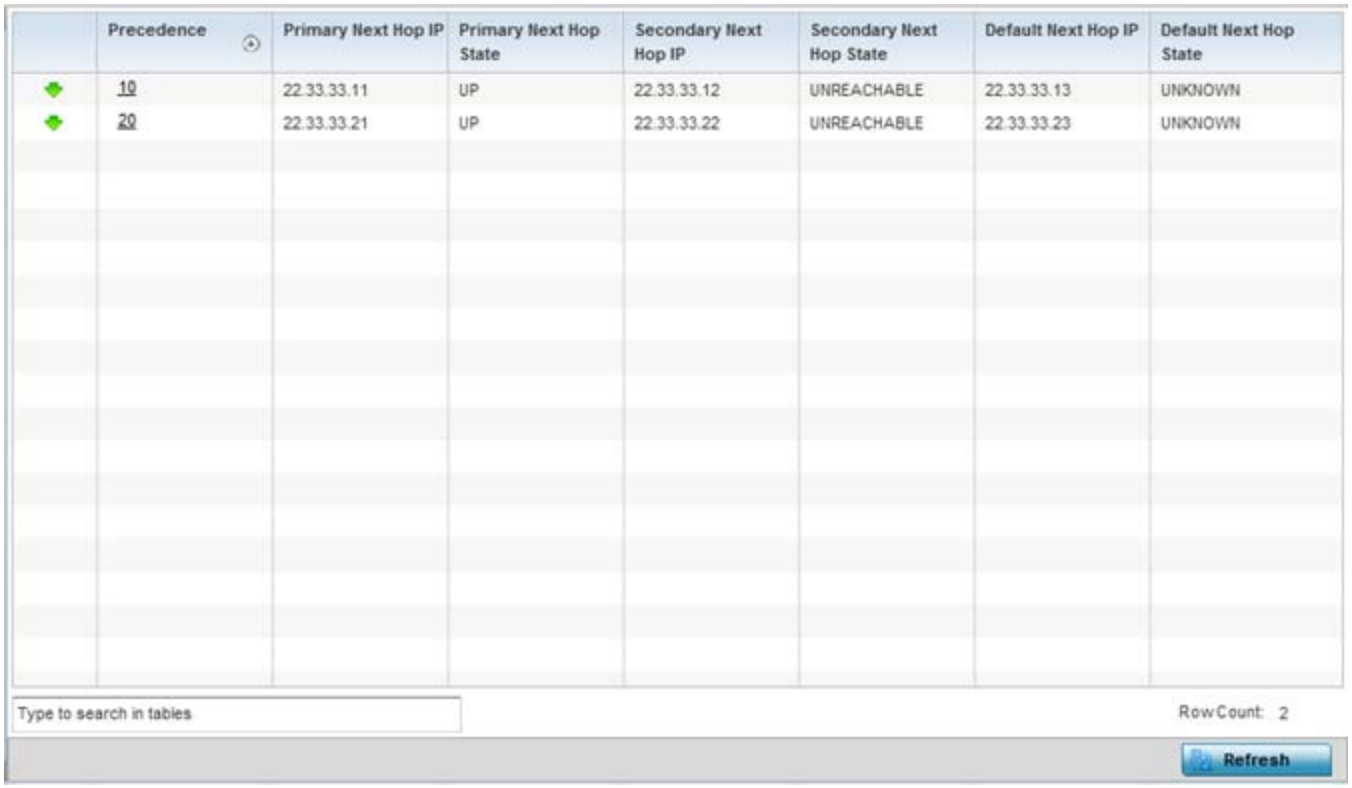


Figure 15-53 *Wireless Controller - Policy Based Routing screen*

The **Policy Based Routing** screen displays the following:

Precedence	Lists the numeric precedence (priority) assigned to each listed PBR configuration. A route-map consists of multiple entries, each carrying a precedence value. An incoming packet is matched against the route-map with the highest precedence (lowest numerical value).
Primary Next Hop IP	Lists the IP address of the virtual resource that, if available, is used with no additional route considerations.
Primary Next Hop State	Displays whether the primary hop is being applied to incoming routed packets.
Secondary Next Hop IP	If the primary hop is unavailable, a second resource is used. This column lists the address set for the alternate route in the election process.
Secondary Next Hop State	Displays whether the secondary hop is being applied to incoming routed packets.

Default Next Hop IP	If a packet subjected to PBR does not have an explicit route to the destination, the configured default next hop is used. This is either the IP address of the next hop or the outgoing interface. Only one default next hop is available. The difference between the next hop and the default next-hop is in case of former, PBR occurs first, then destination based routing. In case of the latter, the order is reverse.
Default Next Hop State	Displays whether the default hop is being applied to incoming routed packets.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.14 Radios

Controller Statistics

The radio **Status** screen provides radio association data, including radio ID, connected APs, radio type, quality index and *Signal to Noise Ratio* (SNR).

To view the radio statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Radio** from the left-hand side of the UI.

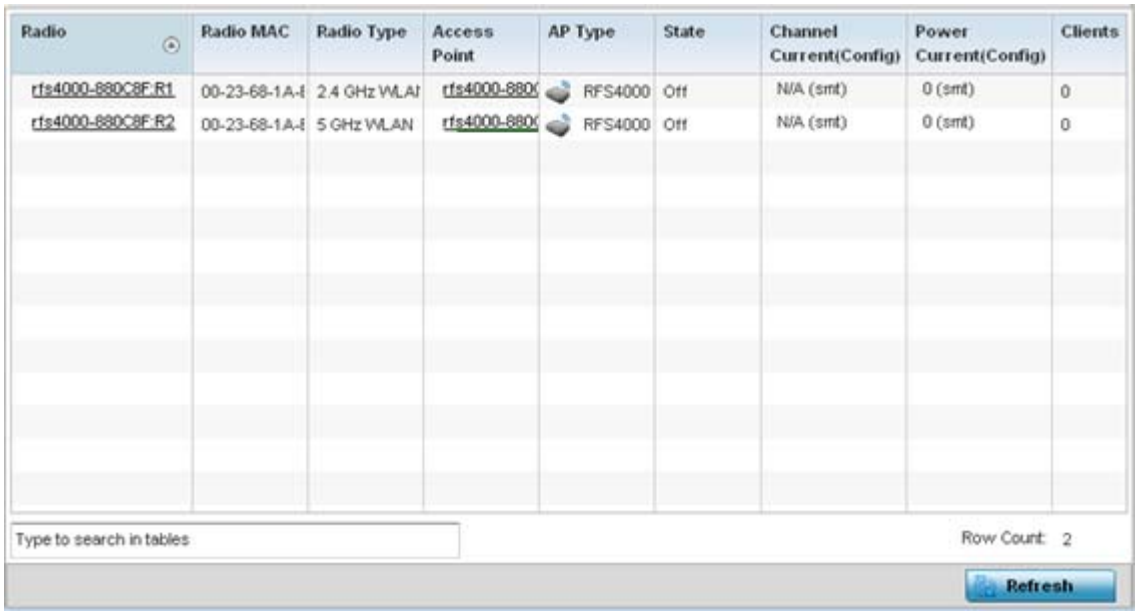


Figure 15-54 *Wireless Controller - Radio Status screen*

The **Radios Status** screen provides the following information:

Radio	Displays the model and numerical value assigned to the radio as its unique identifier. Optionally, select the listed radio (it displays as a link) to display radio configuration information in greater detail.
Radio MAC	Displays the MAC address assigned to the radio as its unique hardware identifier.

Radio Type	Defines whether the radio is operating in the 2.4 GHz or 5 GHz radio band.
Access Point	Displays the administrator assigned system name of each listed Access Point. Optionally, select the listed Access Point to display Access Point configuration information in greater detail.
AP Type	Lists the model type of the Access Point housing the listed radio.
State	Displays the current operational state (On/Off) of each radio.
Channel Current (Config)	Displays the administrator configured channel each listed radio is broadcasting on.
Power Current (Config)	Displays the administrator configured power level the radio is using for its transmissions.
Clients	Displays the number of wireless clients associated with each listed radio.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

4 Select **RF Statistics** from the expanded **Radios** menu.

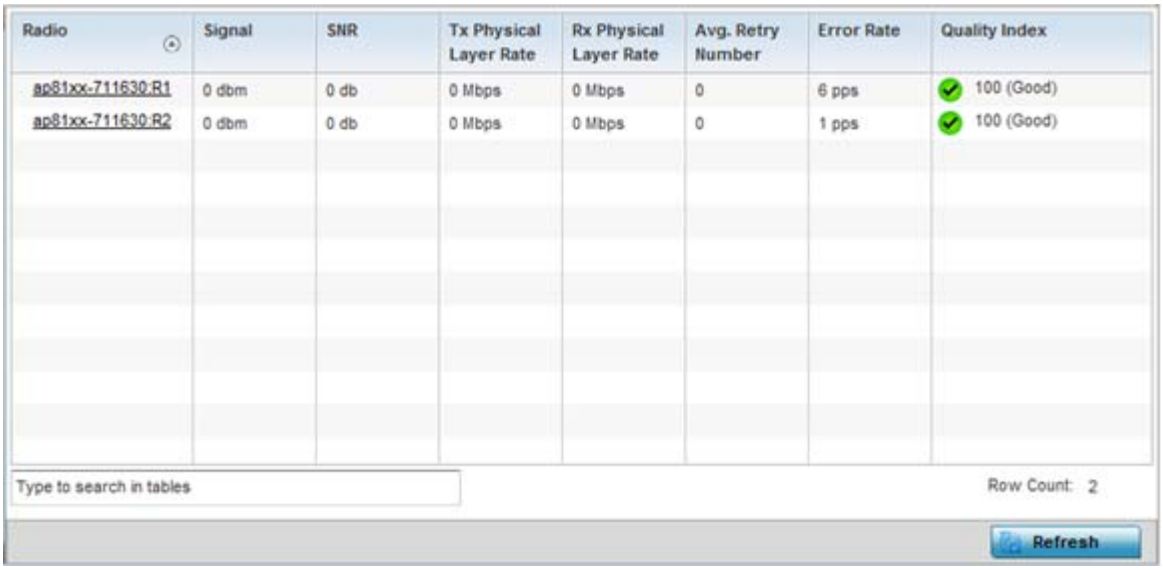


Figure 15-55 *Wireless Controller - Radio RF Statistics screen*

The **RF Statistics** screen provides the following information:

Radio	Displays the name assigned to each listed radio. Each radio name displays as a link that can be selected to display radio information in greater detail.
Signal	Displays the power of each listed radio signal in dBm.
SNR	Displays the *signal to noise ratio* (SNR) of each listed radio. SNR is a measure that compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power. A ratio higher than 1:1 indicates more signal than noise.
Tx Physical Layer Rate	Displays the data transmit rate for each radio's physical layer. The rate is displayed in Mbps.
Rx Physical Layer Rate	Displays the data receive rate for each radio's physical layer. The rate is displayed in Mbps.
Avg Retry Rate	Displays the average number of retries for each radio.

Error Rate	Displays the average number of retries per packet. A high number indicates possible network or hardware problems.
Quality Index	Displays the client's RF quality. The RF quality index is the overall effectiveness of the RF environment, as a percentage of the connect rate in both directions as well as the retry rate and the error rate. RF quality index value can be interpreted as: *0 – 20* - very poor quality *20 – 40* - poor quality *40 – 60* - average quality *60 – 100* - good quality
Refresh	Select *Refresh* to update the statistics counters to their latest values.

5 Select **Traffic Statistics** from the expanded **Radios** menu.

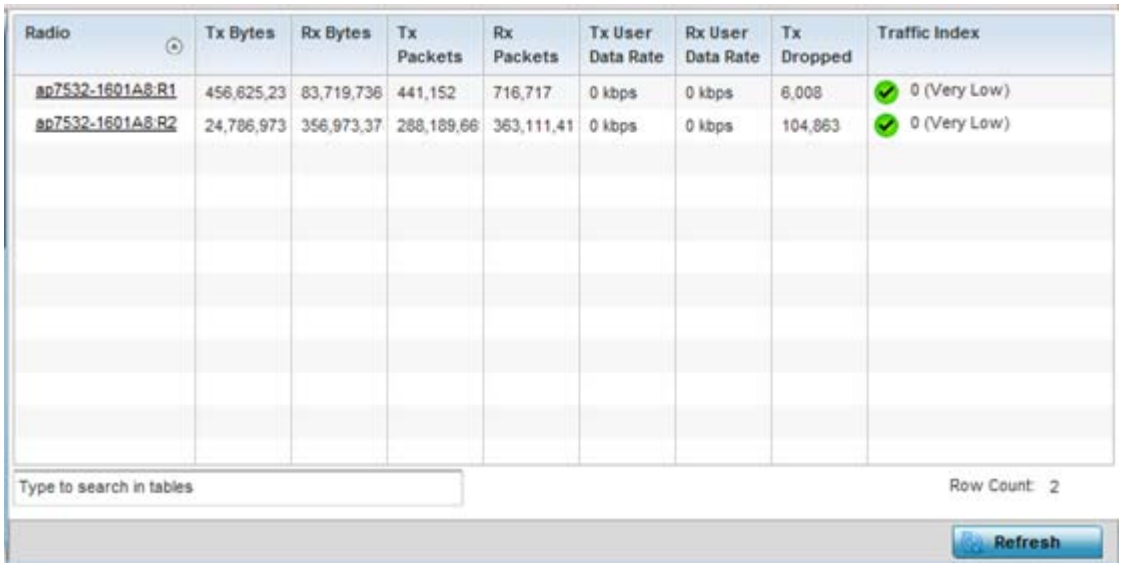


Figure 15-56 *Wireless Controller - Radio Traffic Statistics screen*

The **Traffic Statistics** screen provides the following information:

Radio	Displays the name assigned to each listed radio. Each radio name displays as a link that can be selected to display radio configuration and network address information in greater detail.
Tx Bytes	Displays the amount of transmitted data in bytes for each radio.
Rx Bytes	Displays the amount of received data in bytes for each radio.
Tx Packets	Displays the amount of transmitted data in packets for each radio.
Rx Packets	Displays the amount of received data in packets for each radio.
Tx User Data Rate	Displays the average speed in kbps of data transmitted to users for each radio.
Rx User Data Rate	Displays the average speed (in kbps of data) received from users for each radio.
Tx Dropped	Displays the number of transmissions (packets) dropped by each listed radio. An excessive number of drops and a high error rate could be an indicator to lighten the radio's current load.

Traffic Index	Displays the traffic utilization index of each listed radio, which measures how efficiently the traffic medium is used. It's defined as the percentage of current throughput relative to the maximum possible throughput. Traffic indices are: *0 – 20* (very low utilization), *20 – 40* (low utilization), *40 – 60* (moderate utilization), and *60 and above* (high utilization).
Refresh	Select *Refresh* to update the statistics counters to their latest values.

15.3.15 Mesh

Controller Statistics

The *Mesh* screen provides detailed statistics on each of Mesh capable client within the selected controller or service platform's radio coverage area.

To view Mesh statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Mesh** from the left-hand side of the UI.

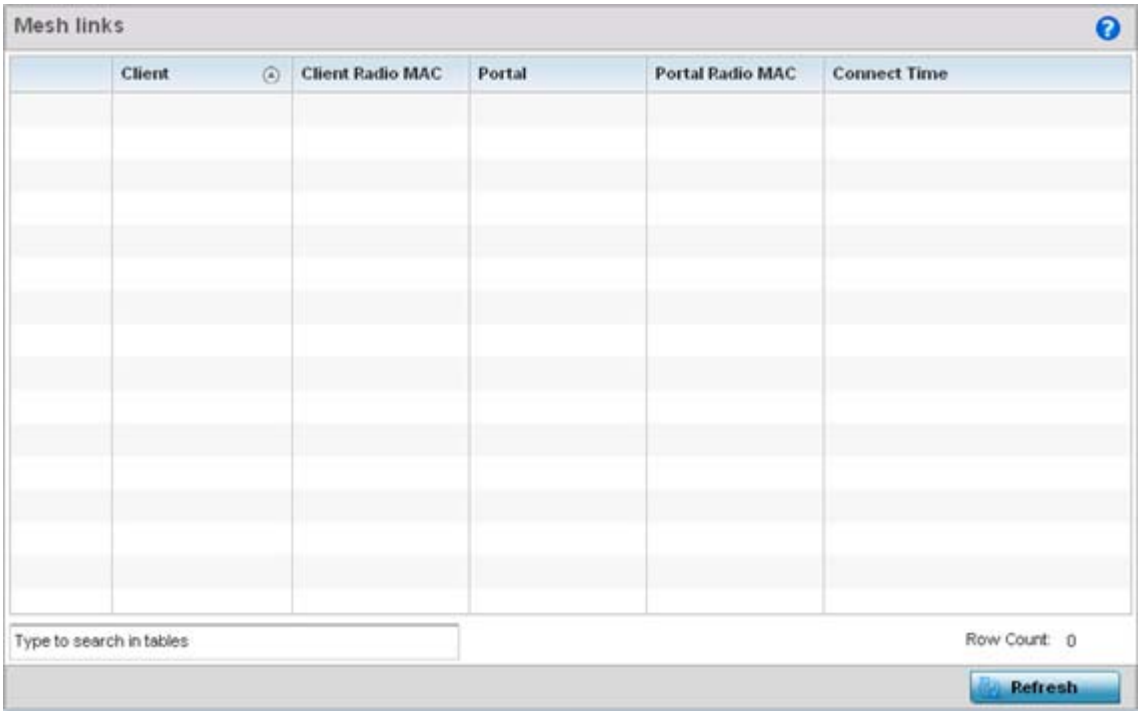


Figure 15-57 *Wireless Controller - Mesh screen*

The **Mesh** screen displays the following:

Client	Displays the name assigned to each mesh client when added to the controller or service platform managed network.
Client Radio MAC	Displays the factory encoded *Media Access Control* (MAC) address of each device within the controller or service platform managed mesh network.

Portal	Mesh portals are mesh enabled devices connected to an external network that forward traffic in and out. Mesh devices must find paths to a portal to access the Internet. When multiple portals exist, the Mesh point must select one.
Portal Radio MAC	Lists the MAC addresses of those Access Points serving as mesh portals.
Connect Time	Displays the total (elapsed) connection time for each client within the controller or service platform managed mesh network.
Refresh	Select *Refresh* to update the statistics counters to their latest value.

15.3.16 Interfaces

Controller Statistics

The *Interface* screen provides detailed statistics on each of the interfaces available on the selected controller or service platform. Use this screen to review the statistics for each interface. Interfaces vary amongst supported hardware model controllers and service platforms.

To review controller or service platform interface statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Interfaces** menu from the left-hand side of the UI.

4 Select **General**.

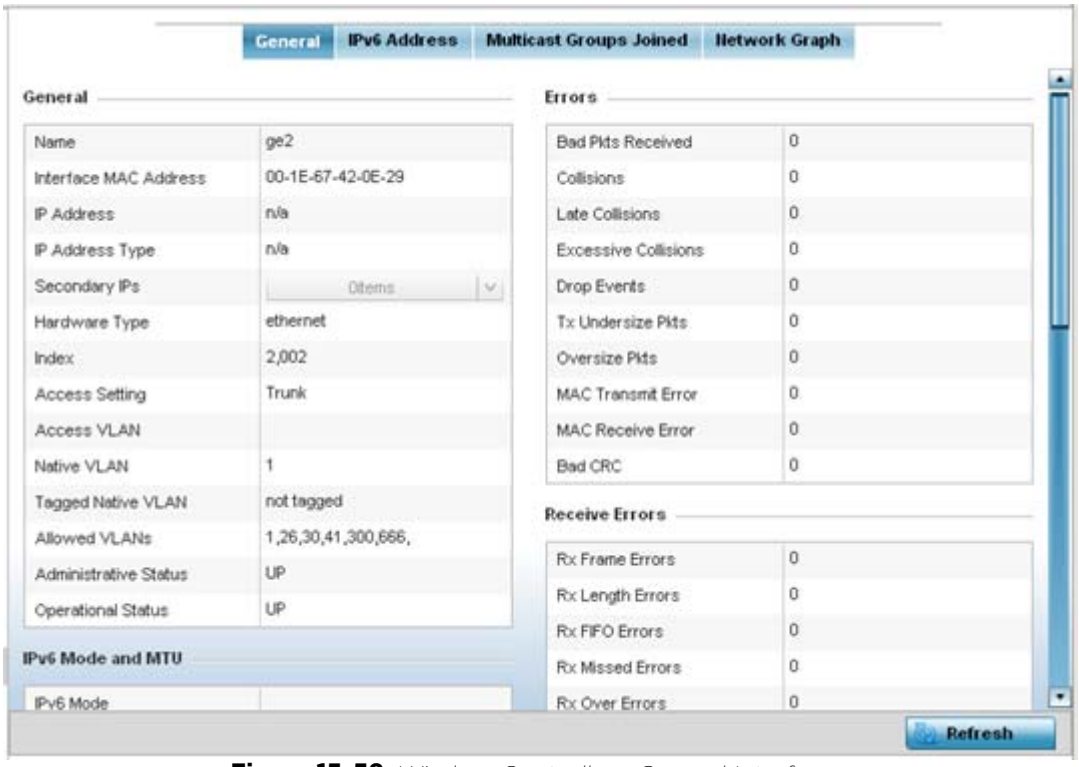


Figure 15-58 *Wireless Controller - General Interface screen*

Interface Statistics support the following:

- *General Interface Details*
- *IPv6 Address*
- *Multicast Groups Joined*
- *Network Graph*

15.3.16.1 General Interface Details

Interfaces

The *General* tab provides information on a selected controller or service platform interface such as its MAC address, type and TX/RX statistics.

The **General** table displays the following:

Name	Displays the name of the controller or service platform interface ge1, up 1etc.
Interface MAC Address	Displays the MAC address of the interface.
IP Address	IP address of the interface.
IP Address Type	Displays the IP address type, either IPv4 or IPv6.
Secondary IP	Displays a list of secondary IP resources assigned to this interface.
Hardware Type	Displays the networking technology.
Index	Displays the unique numerical identifier for the interface.
Access Setting	Displays the VLAN mode as either *Access* or *Trunk*.
Access VLAN	Displays the tag assigned to the native VLAN.
Native VLAN	The native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame. Additionally, the native VLAN is the VLAN untagged traffic is directed over when using a port in trunk mode.
Tagged Native VLAN	When a frame is tagged, the 12 bit frame VLAN ID is added to the 802.1Q header so upstream Ethernet devices know which VLAN ID the frame belongs to. The device reads the 12 bit VLAN ID and forwards the frame to the appropriate VLAN. When a frame is received with no 802.1Q header, the upstream device classifies the frame using the default or native VLAN assigned to the Trunk port. A native VLAN allows an Ethernet device to associate untagged frames to a VLAN when no 802.1Q frame is included in the frame.
Allowed VLANs	Displays the list of allowed virtual interface(s) on this interface.
Administrative Status	Displays whether the interface is currently UP or DOWN.
Operational Status	Lists whether the selected interface is currently UP (operational) or DOWN.

The **IPv6 Mode and MTU** table displays the following information:

IPv6 Mode	Lists the current IPv6 mode is utilized.
IPv6 MTU	Lists the IPv6 formatted largest packet size that can be sent over the interface.

The **Specification** table displays the following information:

Media Type	Displays the physical connection type of the interface. Medium types include: *Copper* - Used on RJ-45 Ethernet ports *Optical* - Used on fibre optic gigabit Ethernet ports
Protocol	Displays the routing protocol used by the interface.
MTU	Displays the *maximum transmission unit* (MTU) setting configured on the interface. The MTU value represents the largest packet size that can be sent over the interface. 10/100 Ethernet ports have a maximum setting of 1500.
Mode	The mode can be either: *Access* – The Ethernet interface accepts packets only from native VLANs. *Trunk* – The Ethernet interface allows packets from a list of VLANs you can add to the trunk.
Metric	Displays the metric associated with the interface's route.
Maximum Speed	Displays the maximum speed the interface uses to transmit or receive data.
Admin Speed	Displays the speed the port can transmit or receive. This value can be either *10*, *100*, *1000* or *Auto*. This value is the maximum port speed in Mbps. Auto indicates the speed is negotiated between connected devices.
Operator Speed	Displays the current speed of data transmitted and received over the interface.
Admin Duplex Setting	Displays the administrator's duplex setting.
Current Duplex Setting	Displays the interface as either *half duplex*, *full duplex* or *unknown*.

The **Traffic** table displays the following:

Good Octets Sent	Displays the number of octets (bytes) with no errors sent by the interface.
Good Octets Received	Displays the number of octets (bytes) with no errors received by the interface.
Good Packets Sent	Displays the number of good packets transmitted.
Good Packets Received	Displays the number of good packets received.
Mcast Pkts Sent	Displays the number of multicast packets sent through the interface.
Mcast Pkts Received	Displays the number of multicast packets received through the interface.
Ucast Pkts Sent	Displays the number of unicast packets sent through the interface.
Ucast Pkts Received	Displays the number of unicast packets received through the interface.
Bcast Pkts Sent	Displays the number of broadcast packets sent through the interface.
Bcast Pkts Received	Displays the number of broadcast packets received through the interface.
Packet Fragments	Displays the number of packet fragments transmitted or received through the interface.

Jabber Pkts	Displays the number of packets transmitted through the interface larger than the MTU.

The **Errors** table displays the following:

Bad Pkts Received	Displays the number of bad packets received through the interface.
Collisions	Displays the number of collisions over the selected interface.
Late Collisions	A late collision is any collision that occurs after the first 64 octets of data have been sent. Late collisions are not normal, and usually the result of out of specification cabling or a malfunctioning device.
Excessive Collisions	Displays the number of excessive collisions. Excessive collisions occur when the traffic load increases to the point a single Ethernet network cannot handle it efficiently.
Drop Events	Displays the number of dropped packets transmitted or received through the interface.
Tx Undersize Pkts	Displays the number of undersized packets transmitted through the interface.
Oversize Pkts	Displays the number of oversized packets transmitted through the interface.
MAC Transmit Error	Displays the number of failed transmits due to an internal MAC sublayer error (that's not a late collision), due to excessive collisions or a carrier sense error.
MAC Receive Error	Displays the number of received packets that failed due to an internal MAC sublayer (that's not a late collision), an excessive number of collisions or a carrier sense error.
Bad CRC	Displays the CRC error. The CRC is the 4 byte field at the end of every frame. The receiving station uses it to interpret if the frame is valid. If the CRC value computed by the interface does not match the value at the end of frame, it is considered as a bad CRC.

The **Receive Errors** table displays the following:

Rx Frame Errors	Displays the number of frame errors received at the interface. A frame error occurs when data is received, but not in an expected format.
Rx Length Errors	Displays the number of length errors received at the interface. Length errors are generated when the received frame length was either less or over the Ethernet standard.
Rx FIFO Errors	Displays the number of FIFO errors received at the interface. First-in First-out queueing is an algorithm that involves buffering and forwarding of packets in the order of arrival. FIFO entails no priority. There is only one queue, and all packets are treated equally. An increase in FIFO errors indicates a probable hardware malfunction.
Rx Missed Errors	Displays the number of missed packets. Packets are missed when the hardware received FIFO has insufficient space to store an incoming packet.
Rx Over Errors	Displays the number of overflow errors received. Overflows occur when a packet size exceeds the allocated buffer size.

The **Transmit Errors** field displays the following:

Tx Errors	Displays the number of packets with errors transmitted on the interface.
Tx Dropped	Displays the number of transmitted packets dropped from the interface.
Tx Aborted Errors	Displays the number of packets aborted on the interface because a clear-to-send request was not detected.
Tx Carrier Errors	Displays the number of carrier errors on the interface. This generally indicates bad Ethernet hardware or bad cabling.
Tx FIFO Errors	Displays the number of FIFO errors transmitted at the interface. *First-in First-Out* queueing is an algorithm that involves the buffering and forwarding of packets in the order of arrival. FIFO uses no priority. There is only one queue, and all packets are treated equally. An increase in the number of FIFO errors indicates a probable hardware malfunction.
Tx Heartbeat Errors	Displays the number of heartbeat errors. This generally indicates a software crash, or packets stuck in an endless loop.
Tx Window Errors	Displays the number of window errors transmitted. TCP uses a sliding window flow control protocol. In each TCP segment, the receiver specifies the amount of additional received data (in bytes) the receiver is willing to buffer for the connection. The sending host can send only up to that amount. If the sending host transmits more data before receiving an acknowledgment, it constitutes a window error.
Refresh	Select *Refresh* to update the statistics counters to their latest value.

15.3.16.2 IPv6 Address

Interfaces

IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

To view controller or service platform IPv6 address utilization:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Interfaces** menu from the left-hand side of the UI.

4 Select the **IPv6 Address** tab.

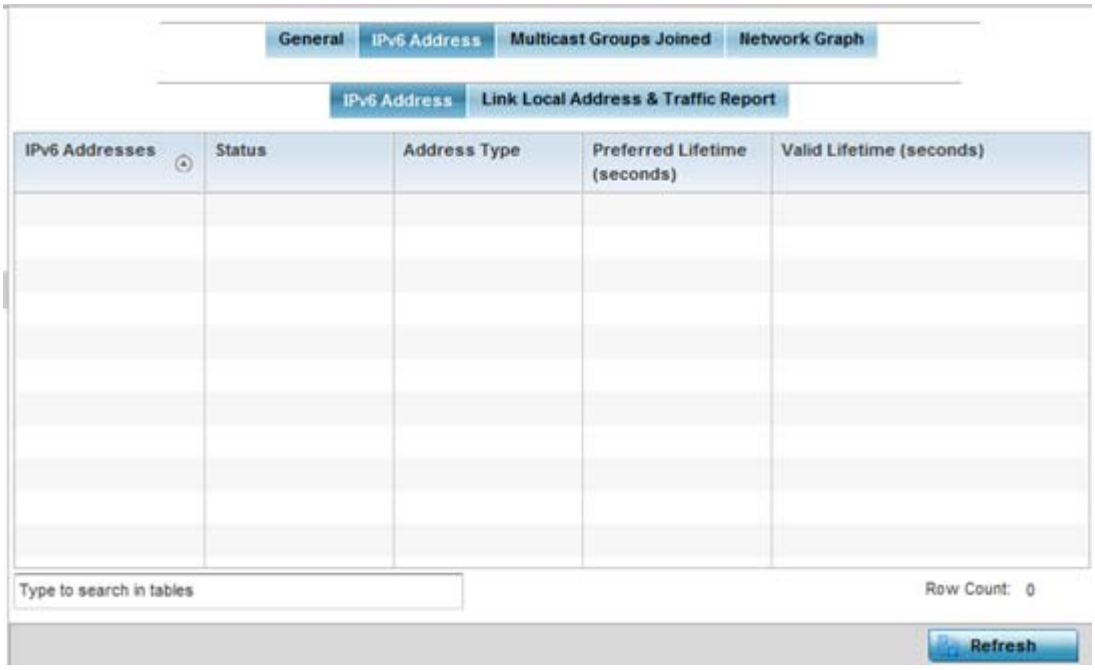


Figure 15-59 *Wireless Controller - Interface IPv6 Address screen*

5 The **IPv6 Addresses** table displays the following:

IPv6 Addresses	Lists the IPv6 formatted addresses currently utilized by the controller or service platform in the selected interface.
Status	Lists the current utilization status of each IPv6 formatted address currently in use by this controller or service platform's selected interface.
Address Type	Lists whether the address is unicast or multicast in its utilization over the selected controller or service platform interface.
Preferred Lifetime (seconds)	Lists is the time in seconds (relative to when the packet is sent) the IPv6 formatted addresses remains in a preferred state on the selected interface. The preferred lifetime must always be less than or equal to the valid lifetime.
Valid Lifetime (seconds)	Displays the time in seconds (relative to when the packet is sent) the IPv6 formatted address remains in a valid state on the selected interface. The valid lifetime must always be greater than or equal to the preferred lifetime.

6 Select the **Link Local Address & Traffic Report** tab to assess data traffic and errors discovered in transmitted and received IPv6 formatted data packets.

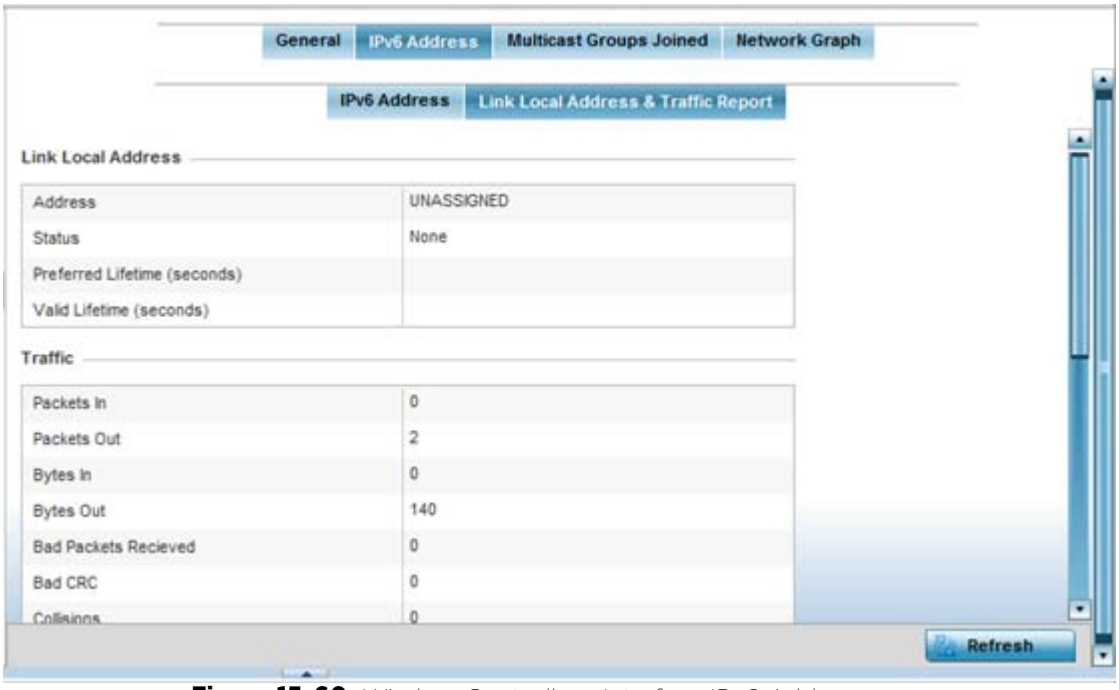


Figure 15-60 *Wireless Controller - Interface IPv6 Address screen*

7 Verify the following **Local Link Address** data for the IPv6 formatted address:

Address	Lists the IPv6 local link address. IPv6 requires a link local address assigned to every interface the IPv6 protocol is enabled on, even when one or more routable addresses are assigned.
Status	Lists the IPv6 local link address utilization status and its current availability.
Preferred Lifetime (seconds)	Lists is the time in seconds (relative to when the packet is sent) the local link addresses remains in the preferred state on the selected interface. The preferred lifetime must always be less than or equal to the valid lifetime.
Valid Lifetime (seconds)	Displays the time in seconds (relative to when the packet is sent) the local link addresses remains in the valid state on the selected interface. The valid lifetime must always be greater than or equal to the preferred lifetime.

8 Verify the following IPv6 formatted **Traffic** data:

Packets In	Lists the number of IPv6 formatted data packets received on the selected controller or service platform interface since the screen was last refreshed.
Packets Out	Lists the number of IPv6 formatted data packets transmitted on the selected controller or service platform interface since the screen was last refreshed.
Bytes In	Displays the number of octets (bytes) with no errors received by the selected interface.
Bytes Out	Displays the number of octets (bytes) with no errors sent by the selected interface.

Bad Packets Received	Displays the number of bad IPv6 formatted packets received through the interface.
Bad CRC	Displays the CRC error. The CRC is the 4 byte field at the end of every frame. The receiving station uses it to interpret if the frame is valid. If the CRC value computed by the interface does not match the value at the end of frame, it is considered as a bad CRC.
Collisions	Displays the number of collisions over the selected interface. Excessive collisions occur when the traffic load increases to the point a single Ethernet network cannot handle it efficiently. A late collision is any collision that occurs after the first 64 octets of data have been sent. Late collisions are not normal, and usually the result of out of specification cabling or a malfunctioning device.

9 Review the following **Receive Errors** for IPv6 formatted data traffic:

Receive Length Errors	Displays the number of IPv6 length errors received at the interface. Length errors are generated when the received IPv6 frame length was either less or over the Ethernet standard.
Receive Over Errors	Displays the number of IPv6 overflow errors received. Overflows occur when a packet size exceeds the allocated buffer size.
Receive Frame Errors	Displays the number of IPv6 frame errors received at the interface. A frame error occurs when data is received, but not in an expected format.
Receive FIFO Errors	Displays the number of IPv6 FIFO errors received at the interface. *First-in First-out* queueing is an algorithm that involves buffering and forwarding of packets in the order of arrival. FIFO entails no priority. There is only one queue, and all IPv6 formatted packets are treated equally. An increase in FIFO errors indicates a probable hardware malfunction.
Receive Missed Errors	Displays the number of missed IPv6 formatted packets. Packets are missed when the hardware received FIFO has insufficient space to store an incoming packet.

10 Review the following **Transmit Errors** for IPv6 formatted data traffic:

Transmit Errors	Displays the number of IPv6 formatted data packets with errors transmitted on the interface.
Transmit Aborted Errors	Displays the number of IPv6 formatted packets aborted on the interface because a clear-to-send request was not detected.
Transmit Carrier Errors	Displays the number of IPv6 formatted carrier errors on the interface. This generally indicates bad Ethernet hardware or bad cabling.
Transmit FIFO Errors	Displays the number of IPv6 formatted FIFO errors transmitted at the interface. *First-in First-Out* queueing is an algorithm that involves the buffering and forwarding of packets in the order of arrival. FIFO uses no priority. There is only one queue, and all packets are treated equally. An increase in the number of FIFO errors indicates a probable hardware malfunction.
Transmit Heartbeat Errors	Displays the number of IPv6 formatted heartbeat errors. This generally indicates a software crash, or packets stuck in an endless loop.

Transmit Window Errors	Displays the number of IPv6 formatted window errors transmitted. TCP uses a sliding window flow control protocol. In each TCP segment, the receiver specifies the amount of additional received data (in bytes) the receiver is willing to buffer for the connection. The sending host can send only up to that amount. If the sending host transmits more data before receiving an acknowledgment, it constitutes a window error.
Refresh	Select *Refresh* to update the statistics counters to their latest value.

15.3.16.3 Multicast Groups Joined

Interfaces

Multicast groups scale to a larger set of destinations by *not* requiring prior knowledge of who or how many destinations there are. Multicast devices uses their infrastructure efficiently by requiring the source to send a packet only once, even if delivered to a large number of devices. Devices replicate a packet to reach multiple receivers only when necessary.

Controllers and service platforms are free to join or leave a multicast group at any time. There are no restrictions on the location or members in a multicast group. A host may be a member of more than one multicast group at any given time and does not have to belong to a group to send messages to members of a group.

To view the controller or service platform multicast group memberships on the selected interface:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Interfaces** menu from the left-hand side of the UI.

4 Select **Multicast Groups Joined**.

Figure 15-61 *Wireless Controller - Interface Multicast Groups Joined screen*

5 The screen displays the following:

Group	Lists the name of existing multicast groups whose current members share multicast packets with one another on this selected interface as a means of collective interoperation.
Users	Lists the number of devices currently interoperating on this interface in each listed multicast group. Any single device can be a member of more then one group at a time.

6 Periodically select **Refresh** to update the screen's counters to their latest values.

15.3.16.4 Network Graph

Interfaces

The *Network Graph* tab displays statistics the controller or service platform continuously collects for its interfaces. Even when the interface statistics graph is closed, data is still collected. Display the interface statistics graph periodically for assessing the latest interface information. Up to three different stats can be selected and displayed within the graph.

To view a detailed graph for an interface, select an interface and drop it on to the graph. The graph displays Port Statistics as the Y-axis and the Polling Interval as the X-axis. Use the **Polling Interval** from the drop-down menu to define the intervals for which data is displayed on the graph.

To view the Interface Statistics graph:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Interfaces** menu from the left-hand side of the UI.

4 Select **Network Graph**. Use the **Parameters** drop-down menu to specify what's trended in the graph.

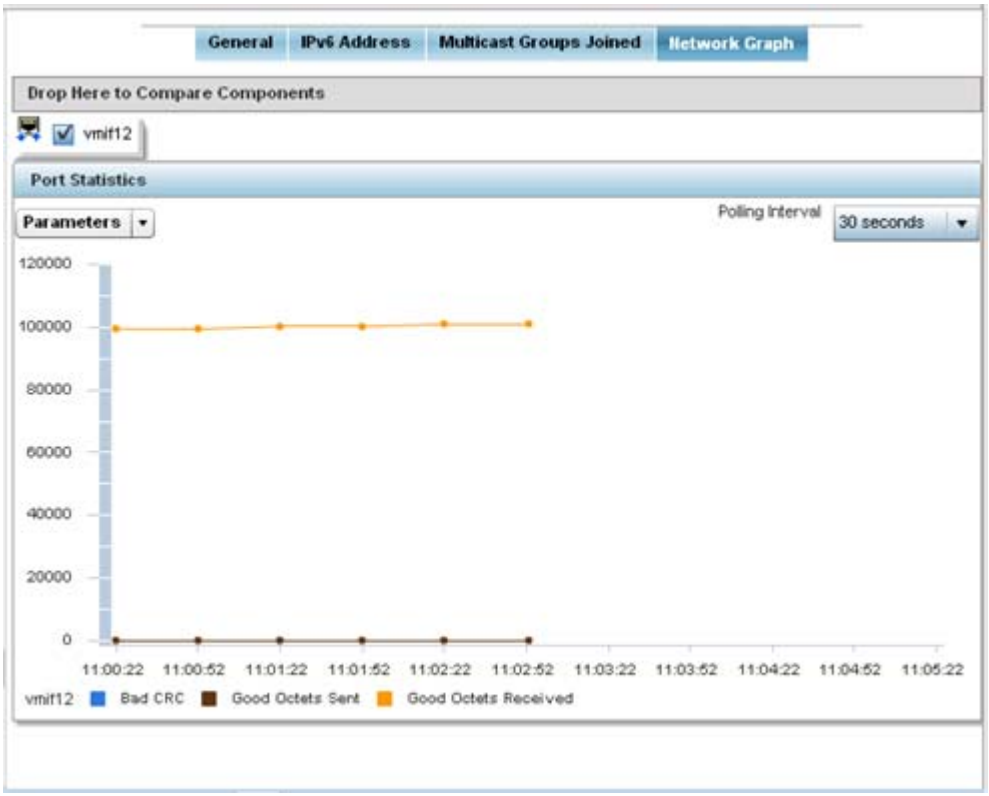


Figure 15-62 *Wireless Controller - Interface Network Graph screen*

15.3.17 Border Gateway Protocol (BGP) Statistics

Controller Statistics

Border Gateway Protocol (BGP) is an inter-ISP routing protocol which establishes routes between ISPs. ISPs use BGP to exchange routing and reachability information between *Autonomous Systems* (AS) on the Internet. BGP makes routing decisions based on paths, network policies and/or rules configured by network administrators. The primary role of a BGP system is to exchange network reachability information with other BGP peers. This information includes information on AS that the reachability information traverses. This information is sufficient to create a graph of AS connectivity from which routing decisions can be created and rules enforced.

An *Autonomous System* (AS) is a set of routers under the same administration that use *Interior Gateway Protocol* (IGP) and common metrics to define how to route packets within the AS. AS uses inter-AS routing to route packets to other ASs. For an external AS, an AS appears to have a single coherent interior routing plan and presents a consistent picture of the destinations reachable through it.

Routing information exchanged through BGP supports only destination based forwarding (it assumes a router forwards packets based on the destination address carried in the IP header of the packet).

BGP uses TCP as its transport protocol. This eliminates the need to implement explicit update fragmentation, retransmission, acknowledgement, and sequencing. BGP listens on TCP port 179. The error notification mechanism used in BGP assumes that TCP supports a *graceful* close (all outstanding data is delivered before the connection is closed).

NOTE: BGP is only supported on RFS6000, NX4500, NX6500, NX9000 and NX9500 model controllers and service platforms.

BGP statistics are available to assist an administrator in assessing the status of the service platforms's BGP feature and its neighbor BGP peers. Much of the configuration information can be filtered from the *Route Filters* screen.

To review BGP statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **BGP** from the left-hand side of the UI. The BGP **Summary** tab displays by default.

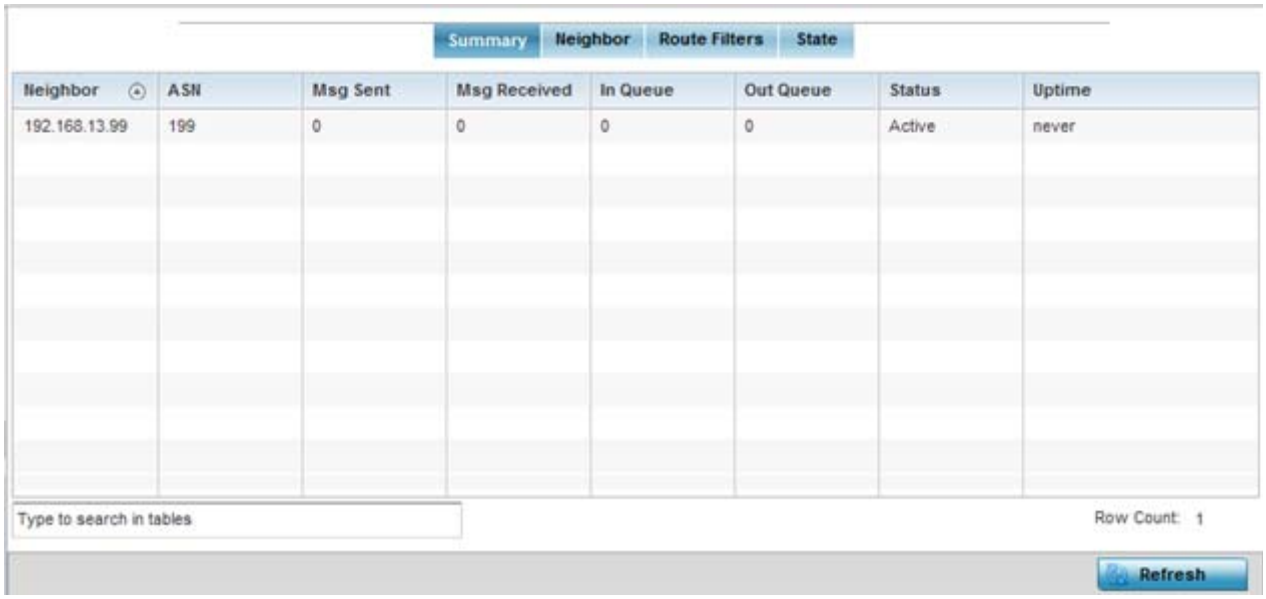


Figure 15-63 *Wireless Controller - BGP - Summary screen*

The **Summary** tab displays the following:

Neighbor	Lists the IP address of neighbor BGP supported devices.
ASN	Lists the *Autonomous System Number* (ASN) assigned to each listed neighbor BGP peer. ASN is a set of routers under the same administration that use *Interior Gateway Protocol* (IGP) and common metrics to define how to route packets
Msg Sent	Lists the number of messages sent out of this BGP peer.
Msg Received	Lists the number of messages received by this BGP peer.
In Queue	Lists the number of messages in the controller or service platform queue that have not yet been read (processed).
Out Queue	Lists the number of messages in the controller or service platform queue that have not yet been sent.
Status	Displays the status of each listed BGP neighbor as *Active* or *Disabled*.
Uptime	Displays the time duration in *HH:MM:SS* format since the connection to this neighbor BGP peer was established.

4 Periodically select **Refresh** to update the screen's counters to their latest value.

5 Select the **Neighbor** tab.

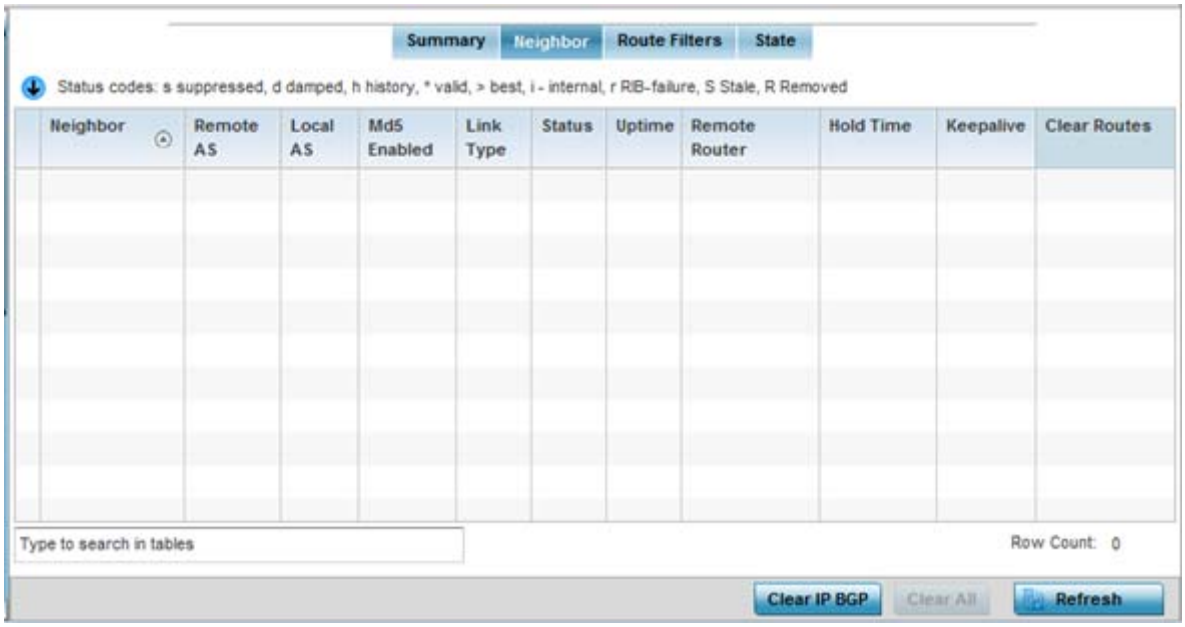


Figure 15-64 *Wireless Controller - BGP - Neighbor screen*

The **Neighbor** tab displays the following BGP neighbor information:

Neighbor	Lists the IP address of neighbor BGP supported peer controllers or service platforms. Each IP address displays as a link to display BGP supported device data in greater detail.
Remote AS	Lists the AS number configured on this BGP neighbor. An *Autonomous System* (AS) is a set of routers under the same administration that use *Interior Gateway Protocol* (IGP) and common metrics to define how to route packets within the AS.
Local AS	Lists the AS number (1 - 4,294,967,295) configured on this BGP wireless controller or service platforms.
MD5 Enabled	A green check defines MD5 authentication enabled on the listed BGP neighbor. A red X means disabled. MD5 is a message digest algorithm using a cryptographic hash producing a 128-bit (16-byte) hash value, usually expressed in text as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.
Link Type	Lists the type of BGP link. Displays *internal* if the link type is iBGP. Displays *external* if the link type is eBGP. *iBGP* exchanges routing table information between routers within an autonomous system. *eBGP* exchanges routing table information between hosts outside an autonomous system.
Status	Displays the current *Active* or *Inactive* state of each listed BGP neighbor device.
Uptime	Displays the uptime for each listed BGP neighbor.
Remote Router	Lists the IP address used by the BGP remote router resource as a network identifier.
Hold Time	Displays the duration, in seconds, for the hold (delay) of packet transmissions to each listed BGP neighbor device.
Keepalive	Displays the duration, in seconds, for the keep alive timer used to maintain the connection to each listed BGP neighbor device.

Clear Routes	Select the *Clear Retries* item (within the table) this to reset and clear all routes received from this BGP neighbor.

6 Optionally select the IP address of a listed BGP neighbor device to launch the following screen for more granular device information for the selected peer device:

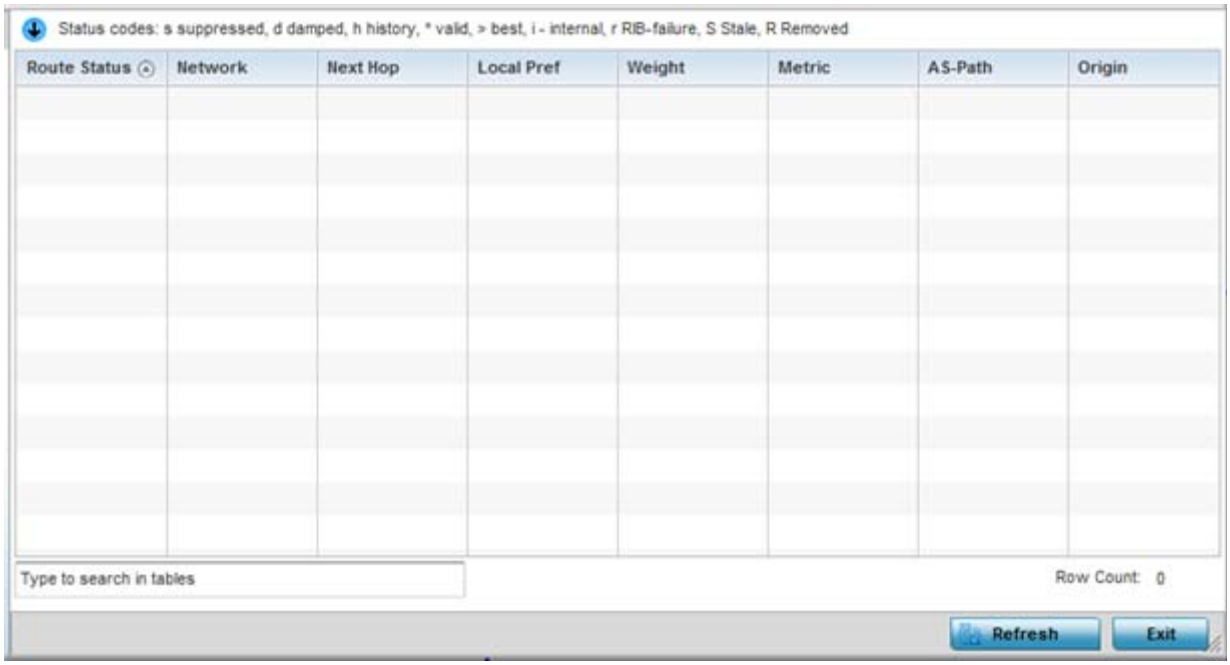


Figure 15-65 *Wireless Controller - BGP - Neighbor - Statistics screen*

The BGP neighbor **Statistics** screen displays route information for the following kinds of routes:

- *Advertised* – Displays route information for routes advertised to the selected neighbor device.
- *Received* – Displays route information for routes received from the selected neighbor device.
- *Routes* – Displays the route information for routes learned from the selected neighbor device.

7 Refer to the following for details on the displayed route. The fields are common to all the screens.

Route Status	Displays the status of this route. Route statuses include: *Suppressed* – This route has been suppressed. *Damped* – This route has been damped due to flapping. *History* - This route is kept in memory to retain flap-dampening statistics. This route is not currently announced by the peer. *Valid* – This route is a valid route. *Best* – This route is the best route of all the routes utilized. *RIB Failure* - A route with better administrative distance is already present, a memory failure exists or the number of routes in *VPN routing/forwarding* (VRF) exceeds the route-limit configured under the VRF instance. *Removed* – This route has been removed from the routes list and is no longer available to BGP supported neighbor devices.
Network	Displays network information for this route.
Next Hop	Displays the IP address of the next hop in this route.

Local Pref	Lists the IP address of this controller or service platform's preferred next hop for the route.
Weight	Displays the weight assigned to this route. Weight is used to decide the preferred route when the same route is learned from multiple neighbors. The route with the highest weight is always chosen.
Metric	Lists a measure (metric) of the quality of the path. A lower value indicates a better path.
AS-Path	Displays the AS Path information for this route.
Origin	Displays the IP address of the route's origin.

8 Select the **Refresh** button to update the information displayed in this screen to the latest values. Use the **Exit** button to exit to the **Neighbor** screen.

9 Select **Route Filters** tab.

This screen provides eight (8) different filters for viewing route statistics. Route statistics can be filtered on eight (8) different parameters.

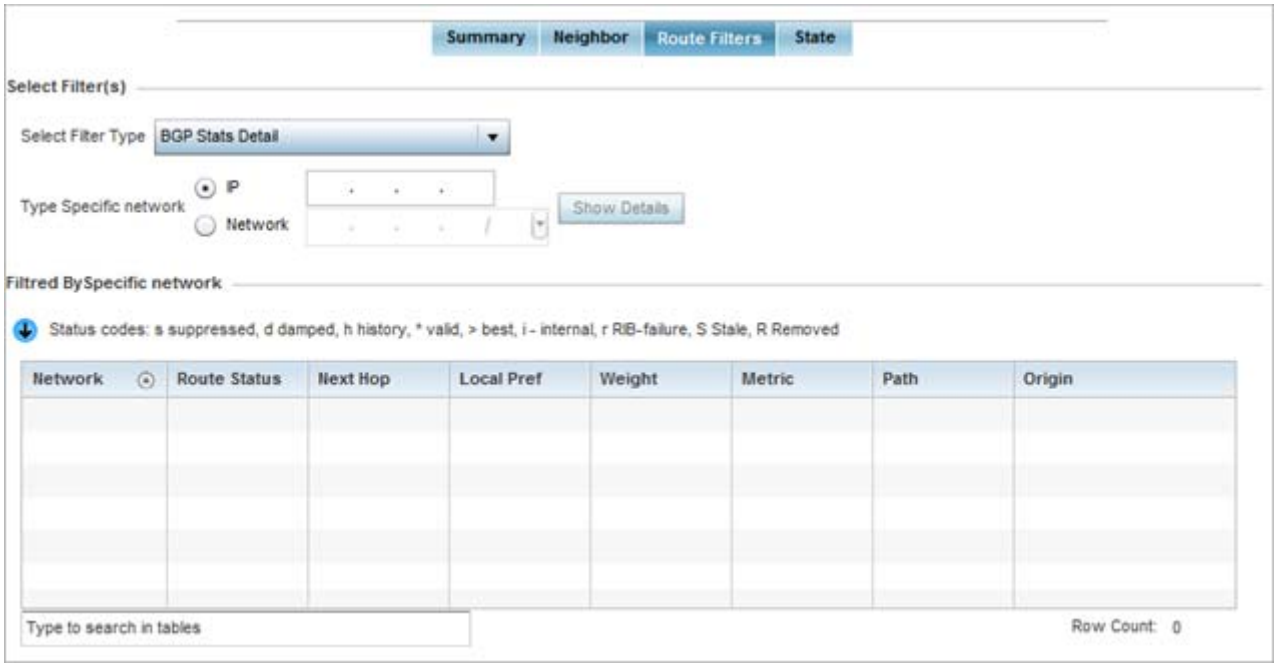


Figure 15-66 *Wireless Controller - BGP - Route Filter screen*

The Route Filters tab supports the following route filters:

- *BGP Stats Details* – Routes are filtered on BGP statistics details.
- *Community List* – Routes are filtered on the community lists included in each route.
- *Community* – Routes are filtered on the community information included in each route,
- *Expanded Community List* – Routes are filtered on the expanded community information included in each route.
- *Prefix List* – Routes are filtered on the prefix list included in each route.
- *Filter List* – Routes are filtered on the filter list included in each route.
- *Regular Expression* – Routes are filtered based on regular expressions.
- *Route Map* – Routes are filtered on the route map information included in each route.

10 Select **BGP Stats Detail** from the **Select Filter Type** list.

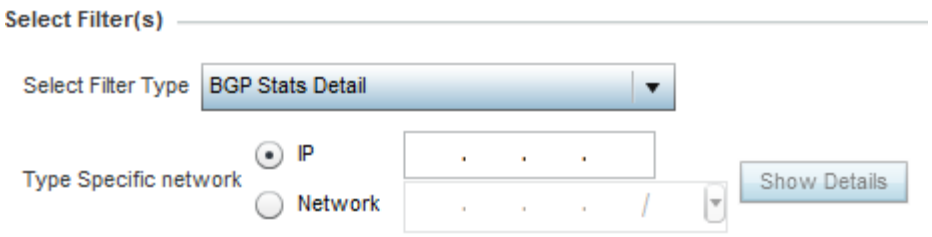


Figure 15-67 *Wireless Controller - BGP - Route Filter - BGP Stats Detail*

11 Use the **Type Specific Network** field to filter statistics based on the provided **IP** or **Network** information. Select **Show Details** to display the list of filtered routes.

Route Status	Displays the status of this route. Route status options include: *Suppressed* – This route has been suppressed. *Damped* – This route has been damped due to flapping. *History* - This route is kept in memory to retain flap-dampening statistics. This route is not currently announced by the peer. *Valid* – This route is a valid route. *Best* – This route is the best route of all routes. *RIB Failure* – A route with better administrative distance is already present, a memory failure exists or the number of routes in *VPN routing/forwarding* (VRF) exceeds the route-limit configured under the VRF instance. *Removed* – This route has been removed from the routes list.
Network	Displays network information for this route.
Next Hop	Displays the IP address of the next hop resource utilized in this route.
Local Pref	Lists the IP address of this controller or service platform's preferred next hop for this route. The local preference indicates the preferred path when there are multiple paths to the same destination. The path having the highest preference value is preferred. The preference value is sent to all routers and access servers in the local AS.
Weight	Displays the weight assigned to this route. Weight is used to decide the preferred route when the same route is learned from multiple neighbors. The route with the highest weight is always chosen.
Metric	Lists a measure (metric) of the quality of the path. A lower value indicates a better path. This value is the *Multi Exit Discriminator* (MED) evaluated by BGP during the best path selection process.
Path	Displays path information for this route.
Origin	Displays the IP address of the origin for this route.

12 Select **Community List** from the **Select Filter Type** list.

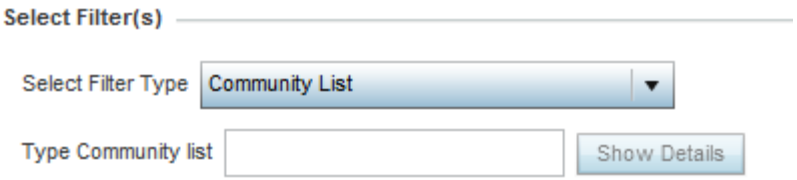


Figure 15-68 *Wireless Controller - BGP - Route Filter - Community List*

13 Use the **Type Community List** field to filter the statistics based on the community type of the route. Select **Show Details** to display the list of filtered routes.

NOTE: The following table is common to these filter types:

Community List
Community
Prefix List
Filter List
Regular Expression
Route Map

Route Status	Displays the status of this route. The route status could be one of: *Suppressed* – This route has been suppressed. *Damped* – This route has been damped due to flapping. *History* - This route is kept in memory to retain flap-dampening statistics. This route is not currently announced by the peer. *Valid* – This route is a valid route. *Best* – This route is the best route of all routes. *RIB Failure* – A route with better administrative distance is already present, a memory failure exists or the number of routes in *VPN routing/forwarding* (VRF) exceeds the route-limit configured under the VRF instance. *Removed* – This route has been removed from the routes list.
Network	Displays network information for this route.
Next Hop	Displays the IP address of the next hop in this route.
Local Pref	Lists the IP address of this controller or service platform's preferred next hop for this route. The local preference indicates the preferred path when there are multiple paths to the same destination. The path having the highest preference value is preferred. This preference value is sent to all routers and access servers in the local AS.
Weight	Displays the weight assigned to this route. Weight is used to decide the preferred route when the same route is learned from multiple neighbors. The route with the highest weight is always chosen.
Metric	Lists a measure of the quality of the path. A lower value indicates a better path. This value is the *Multi Exit Discriminator* (MED) evaluated by BGP during the best path selection process.
AS-Path	Displays AS path information for this route.
Origin	Displays the IP address of the origin for this route.

Select **Community** from the **Select Filter Type** list.

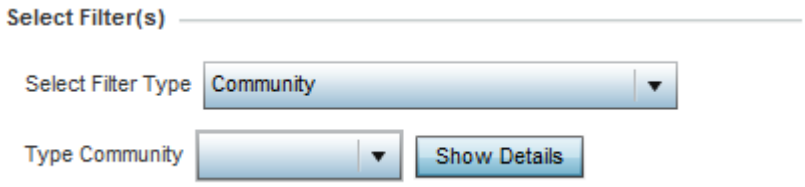


Figure 15-69 *Wireless Controller - BGP - Route Filter - Community*

14 Use the **Type Community** drop-down menu to filter the statistics based on the community of the route. Routes can be filtered on:

- *local-AS* - Displays routes that prevent the transmission of packets outside the local AS.
- *no-advertise* - Displays routes not advertised to any peer, either internal or external.
- *no-export* - Displays routes not advertised to BGP peers, keeping this route within an AS.
- *aa:nn* - Filters routes based on the AS Number specified. The first part (*aa*) represents the AS number. The second part (*nn*) represents a 2-byte number. Routes matching this number are filtered.

15 Select **Show Details** to display the list of filtered routes.

16 Select **Prefix List** from the **Select Filter Type** list.

Figure 15-70 *Wireless Controller - BGP - Route Filter - Prefix List*

17 Use the **Type Prefix list** field to filter the statistics based on the prefix of the route. Select **Show Details** to display the list of filtered routes.

18 Select **Filter List** from the **Select Filter Type** list.

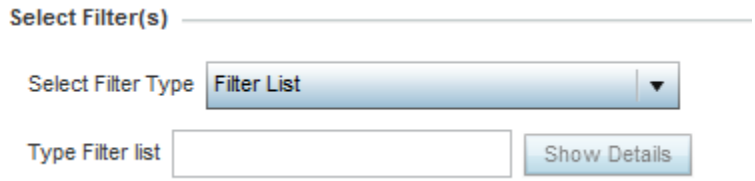


Figure 15-71 *Wireless Controller - BGP - Route Filter - Filter List*

19 Use the **Type Filter List** field to filter the statistics based on the filter list of the route. Select **Show Details** to display the list of filtered routes.

20 Select **Regular Expression** from the **Select Filter Type** list.

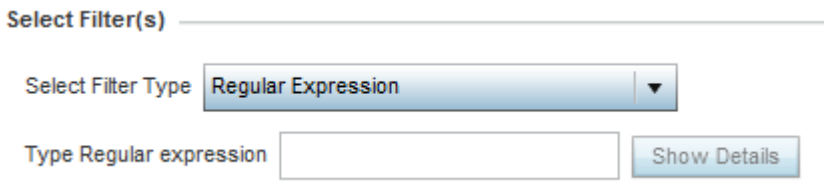


Figure 15-72 *Wireless Controller - BGP - Route Filter - Regular Expression*

21 Use the **Type Regular Expression** field to filter the routes based on regular expressions. Select **Show Details** to display the list of filtered routes.

22 Select **Route Map** from the **Select Filter Type** list.

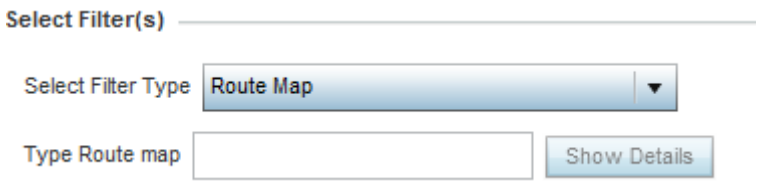


Figure 15-73 *Wireless Controller - BGP - Route Filter - Route Map*

23 Use the **Type Route Map** field to filter the routes based on route maps (enhanced packet filters). Select **Show Details** to display the list of filtered routes.

24 Select **Expanded Community List** from the **Select Filter Type** list.

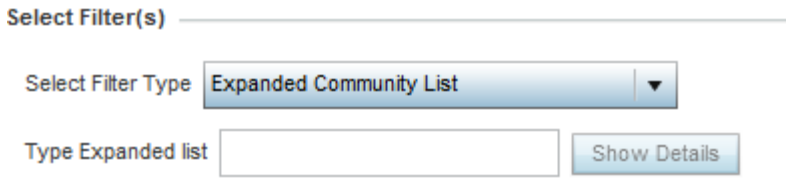


Figure 15-74 *Wireless Controller - BGP - Route Filter - Expanded Community*

25 Use the **Type Expanded list** to filter routes based on route-maps. Select **Show Details** to display a list of filtered routes.

26 Select **State** tab.

Figure 15-75 *Wireless Controller - BGP - State*

The **State** screen displays the following:

Maximum Routes Allowed	Lists the maximum number of routes allowed on the selected BGP wireless controller or service platforms.
Routes Received	Lists the number of routes received from all the BGP peers.
Current Ignore Count	Lists the number of times the BGP daemon has been put in the *Ignore* state.
Ignore Count Allowed	Lists the maximum number of times the BGP daemon can be put in an *Ignore* state before entering permanent ignore state.
Reset Time	Lists the time after which ignore state count is reset to 0 and BGP daemon continues in the state it was in previously.

Ignore Time	Lists the time duration after which BGP daemon shall exit the *Ignore* state.
Current State	Lists the current state of this BGP route utilized on the wireless controller or service platforms.

Select **Refresh** to update the statistic counters to their latest values.

15.3.18 RAID Statistics

Controller Statistics

RAID statistics are available to assist an administrator in assessing the status of the service platform's RAID array, including each physical drive. The information within the RAID statistics screen is polled by the service platform from the RAID controller hardware, then forwarded to the WiNG operating system.

NOTE: RAID controller drive arrays are available within NX7500 and NX9000 series service platforms (NX9000, NX9500 and NX9510 models) only. However, they can be administrated on behalf of a profile by a different model service platform or controller.

For information on setting the service platform drive array configuration as well as the diagnostic behavior of its member drives, refer to *RAID Operations on page 14-19*.

To view RAID statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **RAID** from the left-hand side of the UI.

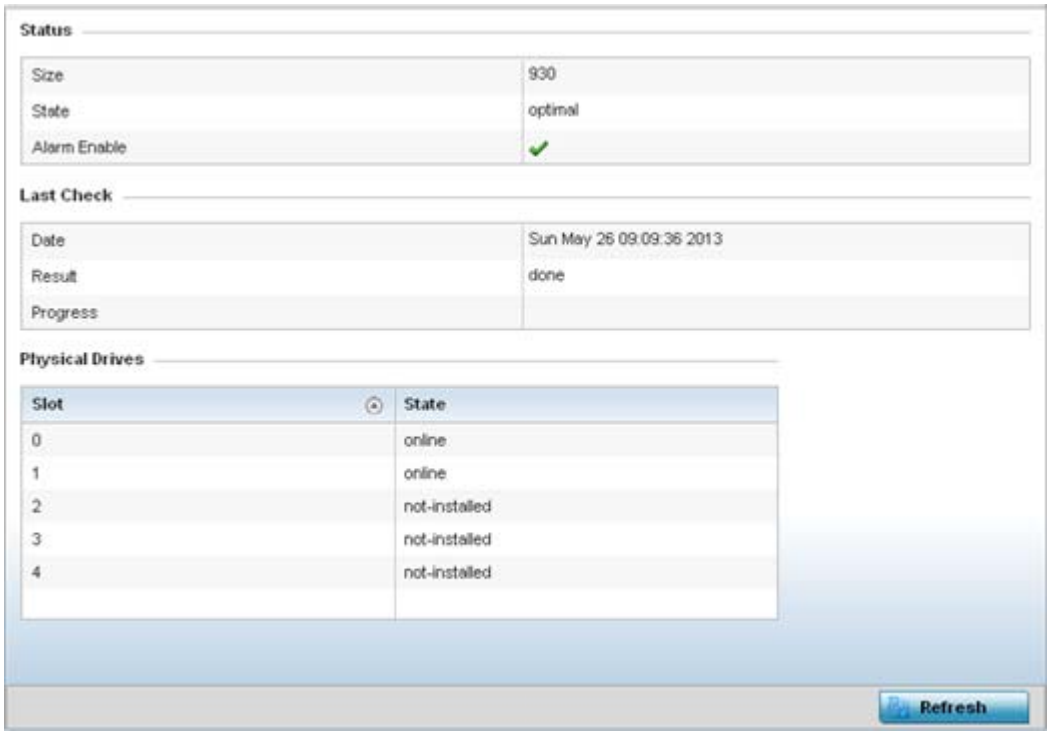


Figure 15-76 *Wireless Controller - RAID Status screen*

4 The **Status** field displays the following:

Size	Lists the size of the RAID drive array. The size is the total physical memory space available on the two physical drives comprising the active RAID controller.
State	Displays whether the drive array is currently in an *optimal* operation state or *degraded*, and in need of administration to perform diagnostics and perhaps prepare a standby drive for hot spare replacement.
Alarm Enable	Displays whether the RAID alarm has been enabled to sound the service platform's chassis alarm upon detection of a RAID controller degradation event. The RAID alarm is enabled by default. For information on enabling or disabling the service platform RAID alarm, see *General Profile Configuration on page 8-5*.

5 Refer to the **Last Check** field to assess the time, progress and results of the RAID array's most recent consistency check:

Date	Lists the date and time of the RAID controller's most recent consistency check on the integrity of the drive array.
Result	Displays *true* for a successful RAID array consistency check and *false* for a failed consistency check. A false indication would trigger the service platform's chassis alarm if RAID alarm is enabled.
Progress	Displays the progress of an in process consistency check in both percentage complete and minutes utilized (for example, 78%/116min).

6 Use the **Physical Drives** field to assess the RAID array's drive utilization and whether the drives are currently online:

Slot	Lists RAID array's drive slot utilization. Since there is only one RAID array controller reporting status to the service platform, its important to know if other drive slots house *hot spare* drives available as additional resources should one of the dedicated drives fail.
State	Displays whether a physical slot within the RAID array has a drive installed, and whether the drive is currently online.

7 Select **Refresh** at any time to update either the screen's statistic counters to their latest value.

15.3.19 Power Status

Controller Statistics

Periodically review the controller or service platform power status to assess the power budget and PoE capability (if supported).

PoE is supported on RFS4000 and RFS6000 model controllers and NX4524 and NX6524 model service platforms. Each of a NX4524 or NX6524's 24 GE ports supports 3af (15.4W) on each of its 24 ports simultaneously. NX4524 and NX6524 models support up to 30W per port, with a maximum of 360W. NX4500 and NX6500 models do not support PoE over their UP1 and UP2 ports.When enabled, the controller or service platform supports 802.3af PoE on each of its ge ports. PoE allows users to monitor port power consumption and configure power usage limits and priorities for each ge port.

To view Power Status statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Power Status** from the left-hand side of the UI.

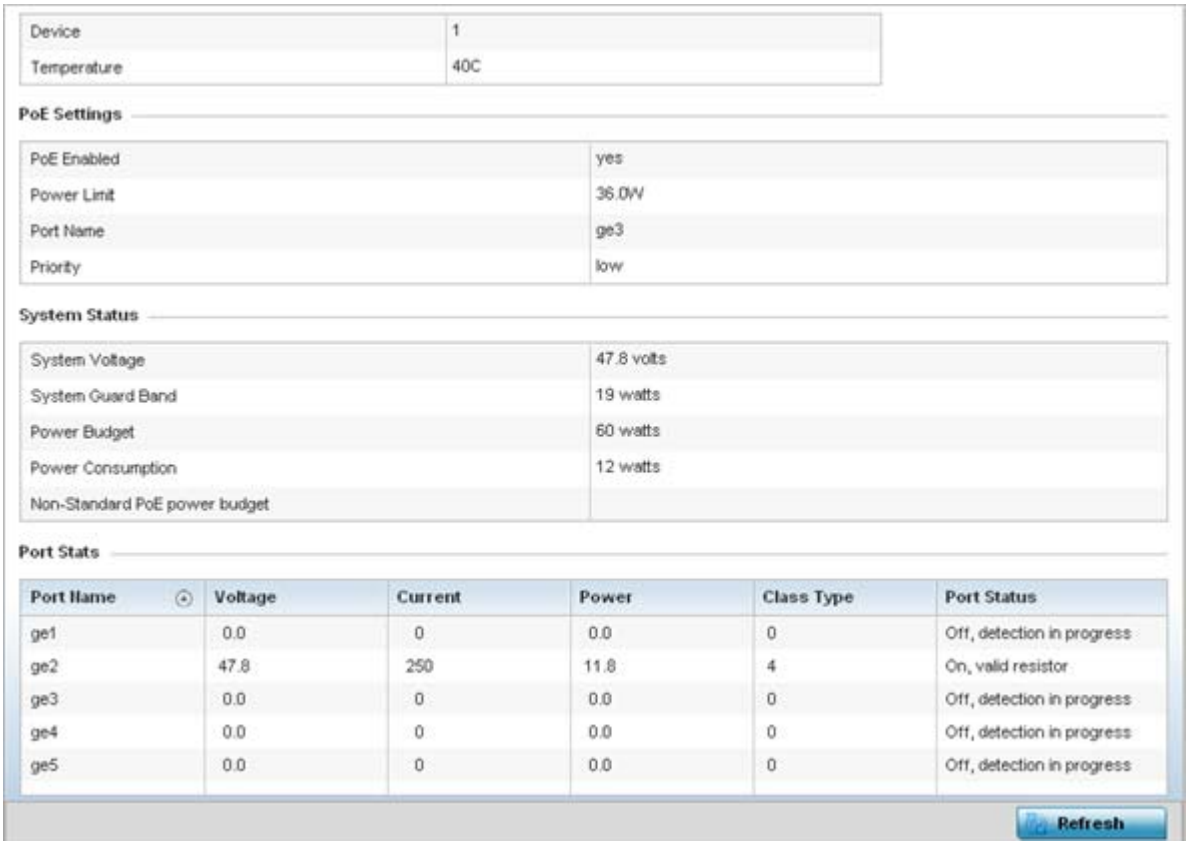


Figure 15-77 *Wireless Controller - Power Status screen*

The **Power Status** provides the following information for supported controllers or service platforms:

Device	Displays the administrator assigned device name for the controller or service platform.
Temperature	Displays the internal system temperature for the controller or service platform.
PoE Enabled	Displays whether or not *Power over Ethernet* (PoE) is enabled for the controller or service platform. When enabled, the controller or service platform supports 802.3af PoE on each of its ge ports. The PoE allows users to monitor port power consumption and configure power usage limits and priorities for each ge port.
Power Limit	Displays the total watts available for Power over Ethernet on the controller or service platform. The value should be between 0 - 40 watts.
Port Name	Displays the GE port name on the controller or service platform.
Priority	Displays the power priority for the listed port as either Critical, High or Low. This is the priority assigned to this port versus the power requirements of the other supports available on the controller or service platform.
System Voltage	Displays the total current system voltage for the controller or service platform.

System Guard Band	Displays the amount of voltage allocated to a System Guard Band. A System Guard Band is an amount of voltage allocated to prevent power loss or cycling on connected PoE devices when the power draw goes above the PoE Power Budget.
Power Budget	Displays the total amount of voltage on the controller or service platform allocated for use in Power over Ethernet.
Power Consumption	Displays the current amount of power being consumed by PoE devices on the controller or service platform.
Non-Standard PoE power budget	Displays the amount of voltage allocated to non 802.3af or 802.3at PoE devices.
Port Name	Displays the GE port name for each PoE capable port on the controller or service platform.
Voltage	Displays the voltage in use by each PoE capable port on the controller or service platform.
Current	Displays the amount of current in milliwatts being used by each PoE capable port on the controller or service platform.
Power	Displays whether or not each PoE capable port on the controller or service platform is providing power.
Class Type	Displays the PoE class type including 802.3af, 802.3at and non-standard PoE types.
Port Status	Displays the status of each PoE capable port on the controller or service platform. It will display either *Enabled* or *Disabled*.
Refresh	Select *Refresh* to update the statistics counters to their latest value.

15.3.20 PPPoE

Controller Statistics

The *PPPoE* statistics screen displays stats derived from the PPPoE capable controller or service platform's access to high-speed data and broadband networks. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables point-to-points connection to an ISP over existing Ethernet interface.

Power over Ethernet is supported on RFS4000 and RFS6000 model controllers and NX4524 and NX6524 model service platforms only. When enabled, the controller supports 802.3af PoE on each of its ge ports.

To review a selected controller or service platform's PPPoE statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **PPPoE** from the left-hand side of the UI.

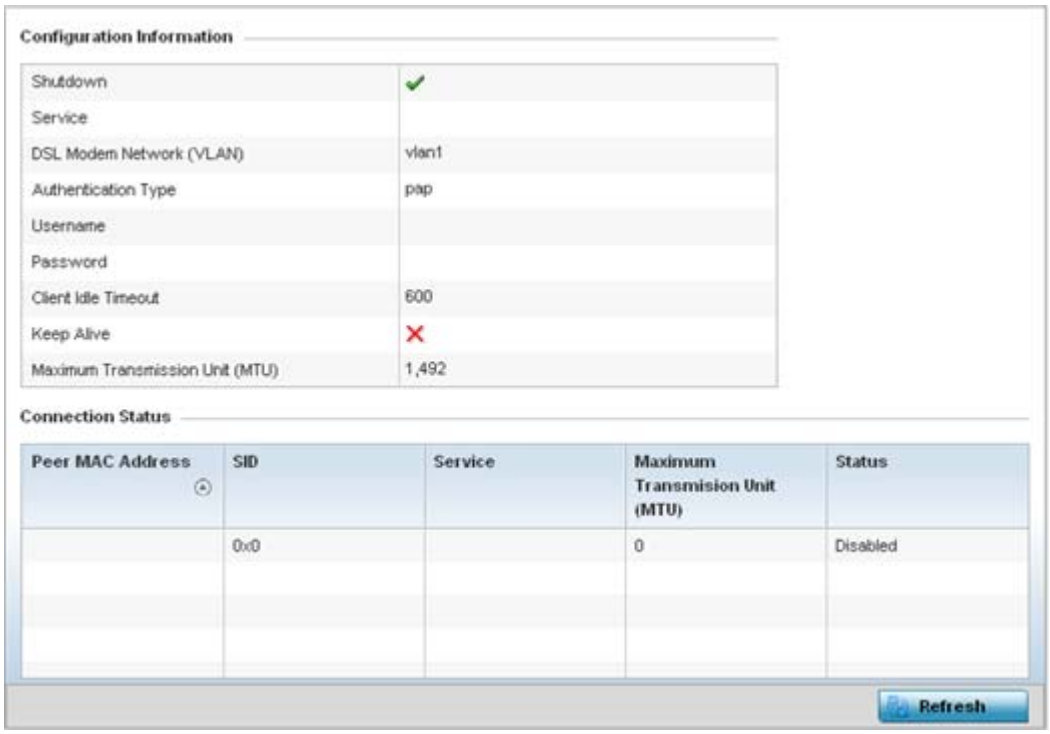


Figure 15-78 *Wireless Controller - PPPoE screen*

The **Configuration Information** field screen displays the following:

Shutdown	Displays whether a high speed client mode point-to-point connection has been enabled using the PPPoE protocol. A green checkmark defines the connection as enabled. A red X defines the connection as shutdown.
Service	Lists the 128 character maximum PPPoE client service name provided by the service provider.
DSL Modem Network (VLAN)	Displays the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to DSL modem.
Authentication Type	Lists authentication type used by the PPPoE client whose credentials must be shared by its peer. Supported authentication options include *None*, *PAP, CHAP*, *MSCHAP*, and *MSCHAP-v2*.
Username	Displays the 64 character maximum username used for authentication support by the PPPoE client.
Password	Displays the 64 character maximum password used for authentication by the PPPoE client.
Client Idle Timeout	The controller or service platform uses the listed timeout so it does not sit idle waiting for input from a PPPoE client and the server that may never come.
Keep Alive	If a keep alive is utilized (enabled displays a green checkmark, disabled a red X) the point-to-point connect to the PPPoE client is continuously maintained and not timed out.
Maximum Transmission Unit (MTU)	Displays the PPPoE client *maximum transmission unit* (MTU) from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size.

4 Refer to the **Connection Status** field.

The Connection Status table lists the MAC address, SID, Service information, MTU and status of each route destination peer. To provide this point-to-point connection, each PPPoE session learns the Ethernet address of a remote PPPoE client, and establishes a session. PPPoE uses both a discover and session phase to identify a client and establish a point-to-point connection. By using such a connection, a wireless WAN failover is available to maintain seamless network access if the Wired WAN were to fail

5 Select the **Refresh** button to update the screen's statistics counters to their latest values.

15.3.21 OSPF

Controller Statistics

Open Shortest Path First (OSPF) is a *link-state interior gateway protocol* (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

Refer to the following for detailed descriptions of the tabs available within the OSPF statistics screen:

- *OSPF Summary*
- *OSPF Neighbors*
- *OSPF Area Details*
- *OSPF Route Statistics*
- *OSPF Interface*
- *OSPF State*

15.3.21.1 OSPF Summary

OSPF

To view OSPF summary statistics:

1 Select the Statistics menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **OSPF** from the left-hand side of the UI.

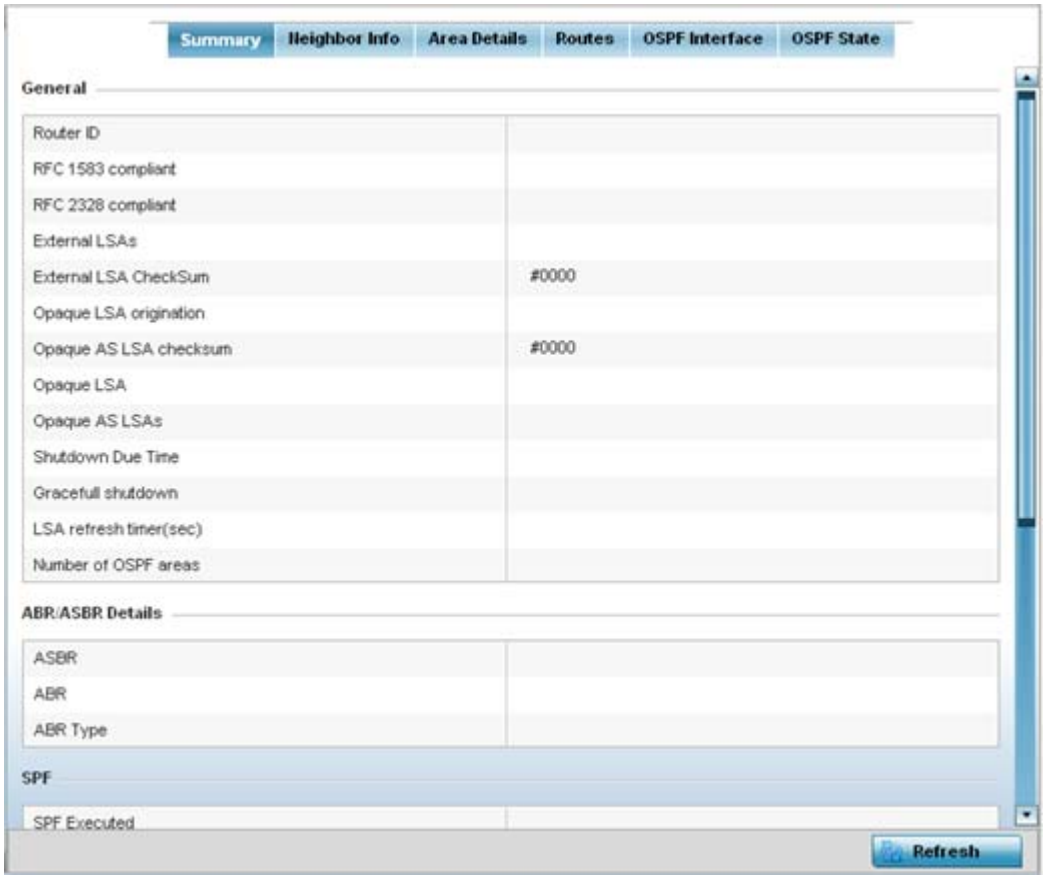


Figure 15-79 *Wireless Controller - OSPF Summary tab*

The **Summary** tab describes the following data fields:

General	The general field displays the router ID assigned for this OSPF connection, RFC compliance information and LSA data.
ABR/ASBR Details	Lists *Autonomous System Boundary Router* (ASBR) data relevant to OSPF routing, including the ASBR, ABR and ABR type. An *Area Border Router* (ABR) is a router that connects one or more areas to the main backbone network. It is considered a member of all areas it is connected to. An ABR keeps multiple copies of the link-state database in memory, one for each area to which that router is connected An ASBR is a router connected to more than one Routing protocol and exchanges routing information with routers in other protocols. ASBRs typically also run an exterior routing protocol (for example, BGP), or use static routes, or both. An ASBR is used to distribute routes received from other, external ASs throughout its own autonomous system. Routers in other areas use ABR as next hop to access external addresses. Then the ABR forwards packets to the ASBR announcing the external addresses
SPF	Refer to the SPF field to assess the status of the *shortest path forwarding* (SFF) *execution*, *last SPF execution*, *SPF delay*, *SPF due in*, *SPF hold multiplier, SPF hold time*, *SPF maximum hold time* and *SPF timer due flag*.

Stub Router	The summary screen displays information relating to stub router advertisements and shutdown and startup times. An OSPF stub router advertisement allows a new router into a network without immediately routing traffic through the new router and allows a graceful shut down or reload a router without dropping packets that are destined for other networks. This feature introduces three configuration options that allow you to configure a router that is running the OSPF protocol to advertise a maximum or infinite metric to all neighbors.

4 Select the **Refresh** button to update the statistics counters to their latest values.

15.3.21.2 OSPF Neighbors

OSPF

OSPF establishes neighbor relationships to exchange routing updates with other routers. A controller or service platform supporting OSPF sends hello packets to discover neighbors and elect a designated router. The hello packet includes link state information and list of neighbors. OSPF is savvy with layer 2 topologies. If on a point-to-point link, OSPF knows it is sufficient, and the link stays up. If on a broadcast link, the router waits for election before determining if the link is functional.

To view OSPF neighbor statistics:

1 Select the Statistics menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **OSPF** from the left-hand side of the UI.

4 Select the **Neighbor Info** tab.

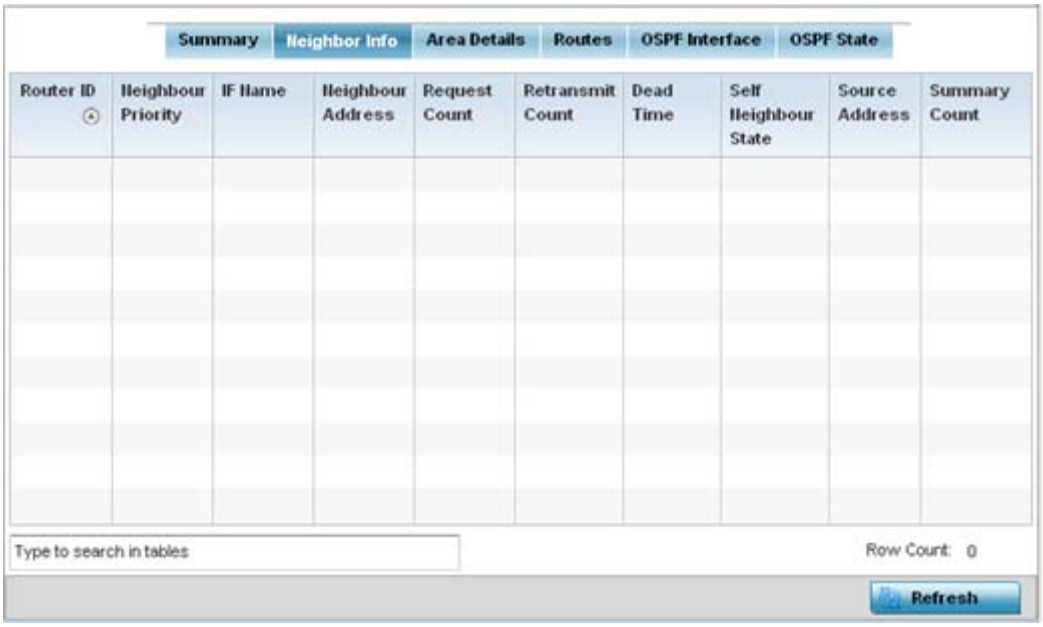


Figure 15-80 *Wireless Controller - OSPF Neighbor Info tab*

The **Neighbor Info** tab describes the following:

Router ID	Displays the router ID assigned for this OSPF connection. The router is a level three Internet Protocol packet switch. This ID must be established in every OSPF instance. If not explicitly configured, the highest logical IP address is duplicated as the router identifier. However, since the router identifier is not an IP address, it does not have to be a part of any routable subnet in the network.
Neighbor Priority	Displays each listed neighbor's priority in respect to becoming the designated router managing the OSPF connection. The designated router is the router interface elected among all routers on a particular multi-access network segment.
IF Name	Lists the name assigned to the router interface used to support connections amongst OSPF enabled neighbors.
Neighbor Address	Lists the IP address of the neighbor sharing the router interface with each listed router ID.
Request Count	Lists the connection request count (hello packets) to connect to the router interface, discover neighbors and elect a designated router.
Retransmit Count	Lists the connection retransmission count attempted in order to connect to the router interface, discover neighbors and elect a designated router. A *designated router* (DR) is the router interface elected among all routers on a particular multi-access network segment, generally assumed to be broadcast.
Dead Time	Lists the dead time between neighbors in the network topology that are currently utilizing the listed router ID.
Self Neighbor State	Displays the self-neighbor status assessment used to discover neighbors and elect a designated router.
Source Address	Displays the single source address used by all neighbor routers to obtain topology and connection status. This form of multicasting significantly reduces network load.
Summary Count	Routes that originate from other areas are called summary routes. Summary routes are not flooded in a totally stubby or NSSA totally stubby area.

5 Select the **Refresh** button to update the statistics counters to their latest values.

15.3.21.3 OSPF Area Details

OSPF

An OSPF network is subdivided into routing areas (with 32 bit area identifiers) to simplify administration and optimize traffic utilization. Areas are logical groupings of hosts and networks, including routers having interfaces connected to an included network. Each area maintains a separate link state database whose information may be summarized towards the rest of the network. An OSPF Area contains a set of routers exchanging *Link State Advertisements* (LSAs) with others in the same area. Areas limit LSAs and encourage aggregate routes. Areas are identified by 32-bit IDs, expressed either in decimal, or octet-based dot-decimal notation.

To view OSPF area statistics:

1 Select the Statistics menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **OSPF** from the left-hand side of the UI.

4 Select the **Area Details** tab.

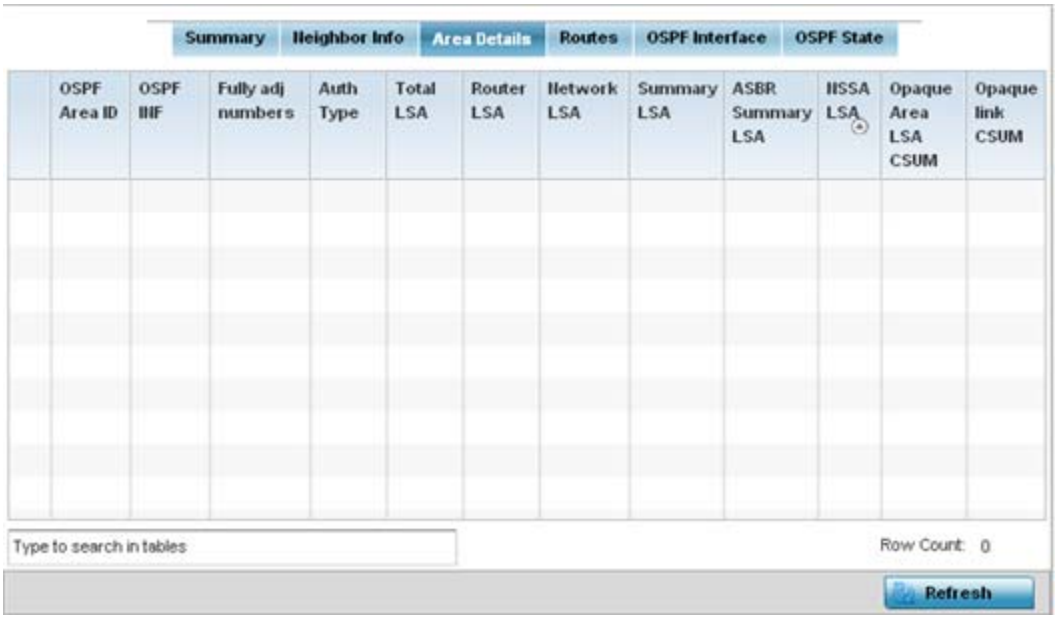


Figure 15-81 *Wireless Controller - OSPF Area Details tab*

The **Area Details** tab describes the following:

OSPF Area ID	Lists the connection request count (hello packets) to connect to the router interface, discover neighbors and elect a designated router.
OSPF INF	Lists the interface ID (virtual interface for dynamic OSPF routes) supporting each listed OSPF area ID.
Fully adj numbers	Fully adjusted numbers strip away the effects of other non OSPF and LSA factors and events, leaving only relevant OSPF area network route events counted.
Auth Type	Lists the authentication schemes used to validate the credentials of dynamic route connections and their areas.
Total LSA	Lists the *Link State Advertisements* (LSAs) of all entities using the dynamic route (in any direction) in the listed area ID.
Router LSA	Lists the Link State Advertisements of the router supporting each listed area ID. The router LSA reports active router interfaces, IP addresses, and neighbors.
Network LSA	Displays which routers are joined together by the designated router on a broadcast segment (e.g. Ethernet). Type 2 LSAs are flooded across their own area only. The link state ID of the type 2 LSA is the IP interface address of the designated route.
Summary LSA	The summary LSA is generated by ABR to leak area summary address info into another areas. ABR generates more than one summary LSA for an area if the area addresses cannot be properly aggregated by only one prefix.
ASBR Summary LSA	Originated by ABRs when an ASBR is present to let other areas know where the ASBR is. These are supported just like summary LSAs.

NSSA LSA	Routers in a *Not-so-stubby-area* (NSSA) do not receive external LSAs from Area Border Routers, but are allowed to send external routing information for redistribution. They use type 7 LSAs to tell the ABRs about these external routes, which the Area Border Router then translates to type 5 external LSAs and floods as normal to the rest of the OSPF network. Redistribution into an NSSA area creates a special type of LSA known as TYPE 7, which can exist only in an NSSA area. An NSSA ASBR generates this LSA, and an NSSA ABR router translates it into type 5 LSA which gets propagated into the OSPF domain.
Opaque Area LSA CSUM	Displays the Type-10 opaque link area checksum with the complete contents of the LSA.
Opaque link CSUM	Displays the Type-10 opaque link checksum with the complete contents of the LSA.

5 Select the **Refresh** button to update the statistics counters to their latest values.

15.3.21.4 OSPF Route Statistics

OSPF

Refer to the *Routes* tab to assess the status of OSPF *Border Routes, External Routes*, *Network Routes* and *Router Routes*.

To view OSPF route statistics:

1 Select the Statistics menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **OSPF** from the left-hand side of the UI.

4 Select the **Routes** tab. **Border Routes** display by default.

An *area border router* (ABR) connects (links) more than one area. Usually an ABR is used to connect non-backbone areas to the backbone. If OSPF virtual links are used an ABR will also be used to connect the area using the virtual link to another non-backbone area. Border routes use internal OSPF routing table entries to an ABR or *Autonomous System Boundary Router* (ASBR). Border routers maintain an LSDB for each area supported. They also participate in the backbone.

5 Refer to **External Routes** tab.

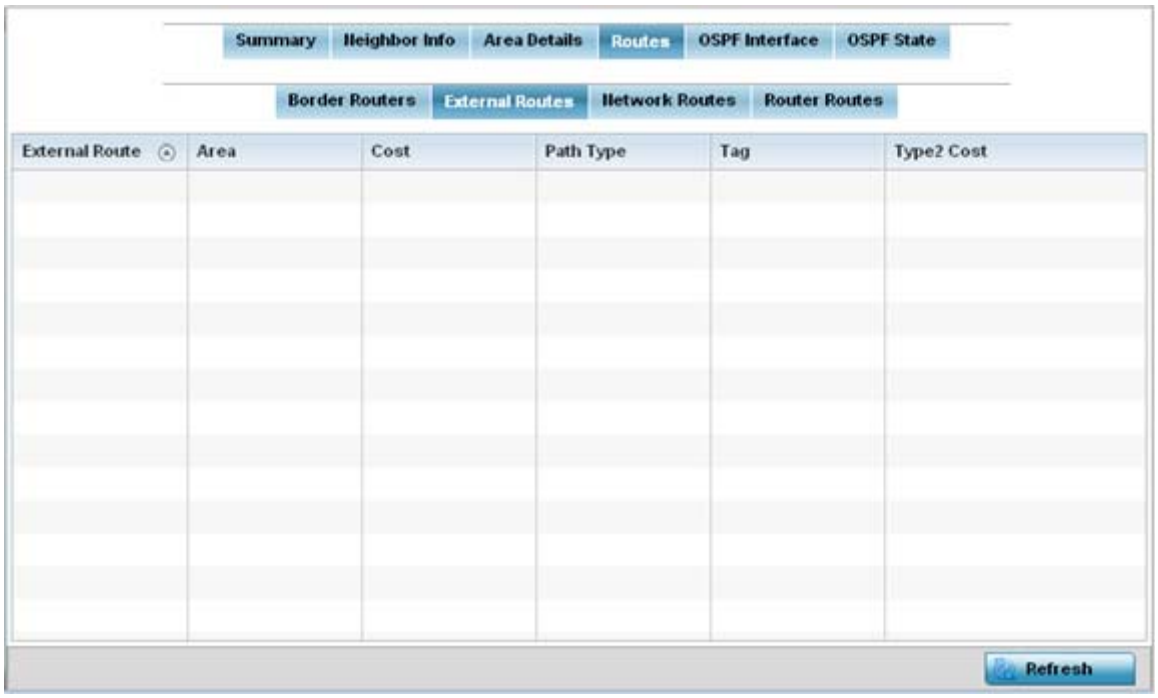


Figure 15-82 *Wireless Controller - OSPF External Routes tab*

External routes are external to area, originate from other routing protocols (or different OSPF processes) and are inserted into OSPF using redistribution. A *stub* area is configured not to carry external routes. Each external route can be tagged by the advertising router, enabling the passing of additional information between routers. Each external route can also be tagged by the advertising router, enabling the passing of additional information between routers on the boundary of the autonomous system.

The External route tab displays a list of external routes, the area impacted, cost, path type, tag and type 2 cost. Cost factors may be the distance of a router (round-trip time), network throughput of a link, or link availability and reliability, expressed as simple unit-less numbers. This provides a dynamic process of traffic load balancing between routes of equal cost.

6 Refer to the **Network Routes** tab.

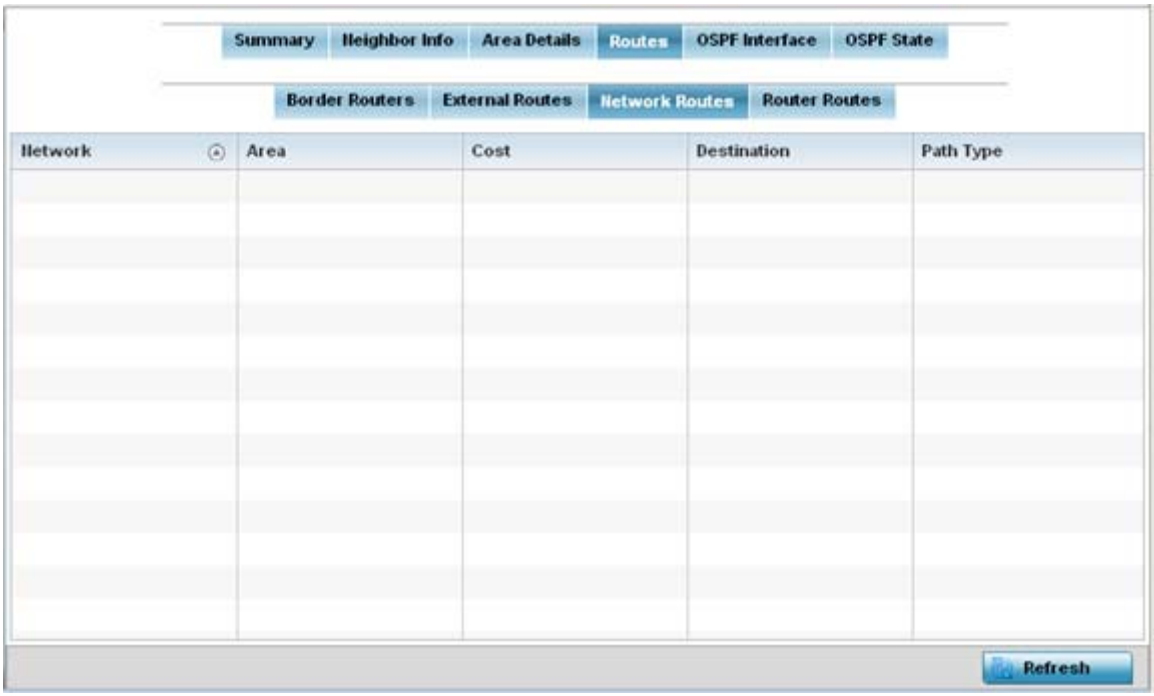


Figure 15-83 *Wireless Controller - OSPF Network Routes tab*

Network routes support more than two routers, with the capability of addressing a single physical message to all attached routers (broadcast). Neighboring routers are discovered dynamically using OSPF hello messages. This use of the hello protocol takes advantage of broadcast capability. An OSPF network route makes further use of multicast capabilities, if they exist. Each pair of routers on the network is assumed to communicate directly.

The network tab displays the network name, impacted OSPF area, cost, destination and path type.

7 Select the **Router Routes** tab.

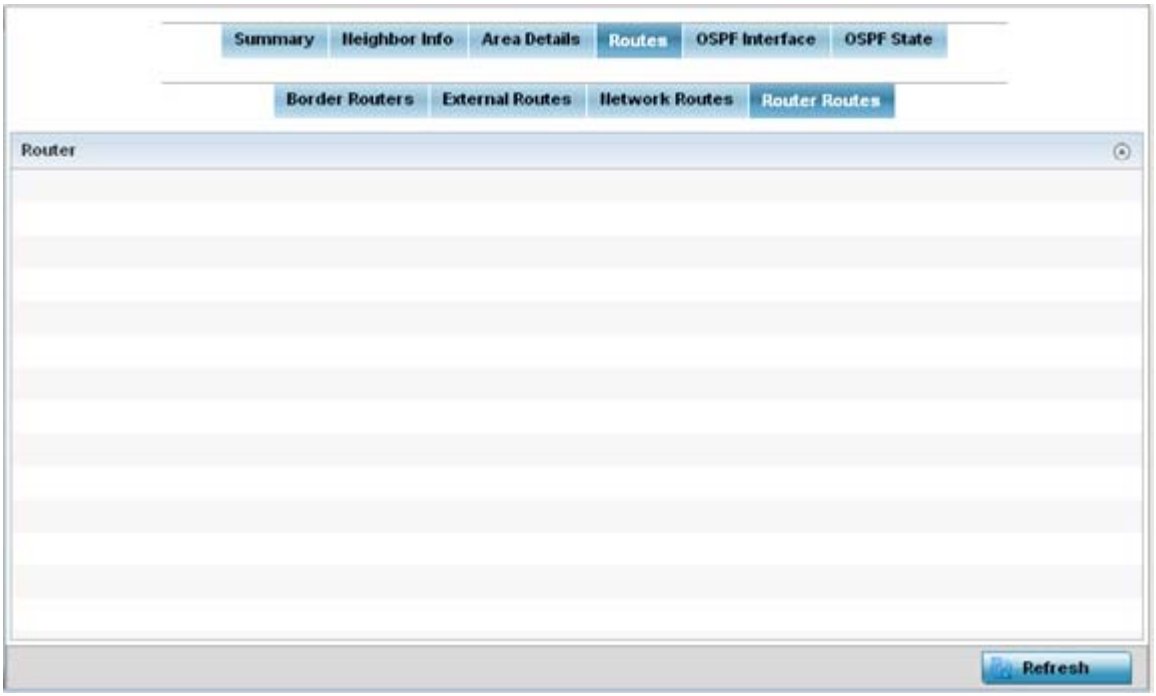


Figure 15-84 *Wireless Controller - OSPF Router Routes tab*

An internal (or *router*) route connects to one single OSPF area. All of its interfaces connect to the area in which it is located and does not connect to any other area.

8 Select the **Refresh** button (within any of the four OSPF Routes tabs) to update the statistics counters to their latest values

15.3.21.5 OSPF Interface

OSPF

An OSPF interface is the connection between a router and one of its attached networks. An interface has state information associated with it, which is obtained from the underlying lower level protocols and the routing protocol itself. A network interface has associated a single IP address and mask (unless the network is an unnumbered point-to-point network). An interface is sometimes also referred to as a link.

To view OSPF interface statistics:

1 Select the Statistics menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **OSPF** from the left-hand side of the UI.

4 Select the **OSPF Interface** tab.

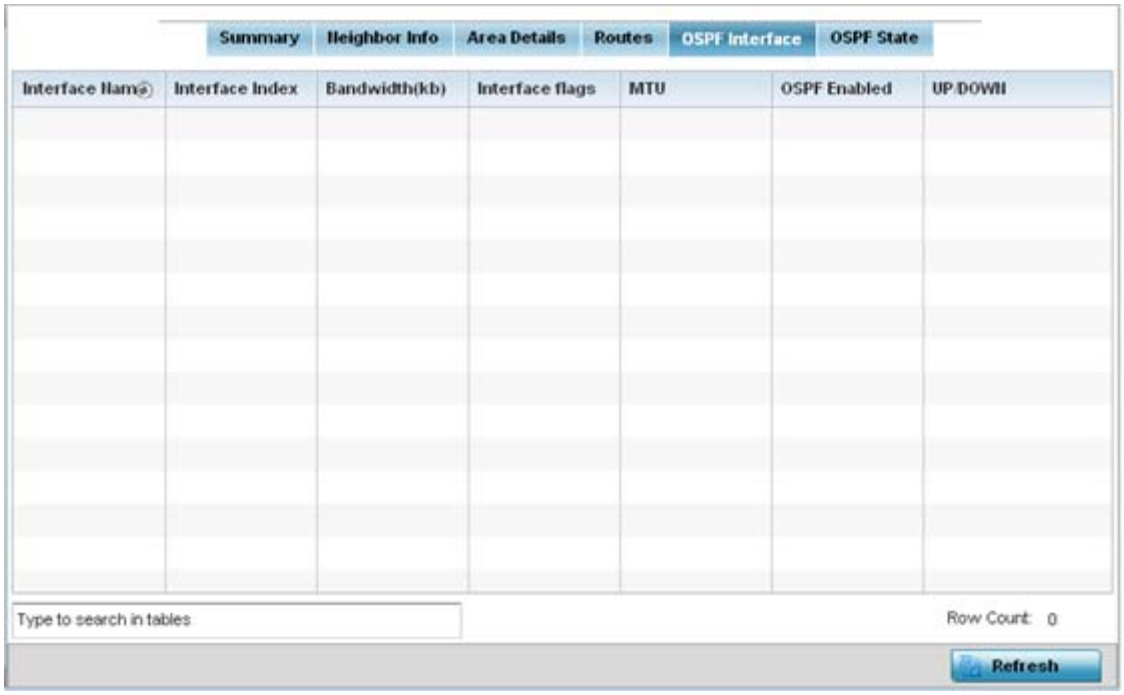


Figure 15-85 *Wireless Controller - OSPF Interface tab*

The **OSPF Interface** tab describes the following:

Interface Name	Displays the IP addresses and mask defined as the virtual interface for dynamic OSPF routes. Zero config and DHCP can be used to generate route addresses, or a primary and secondary address can be manually provided.
Interface Index	Lists the numerical index used for the OSPF interface. This interface ID is in the hello packets establishing the OSPF network connection.
Bandwidth(kb)	Lists the OSPF interface bandwidth (in Kbps) from 1 - 10,000,000.
Interface flags	Displays the flag used to determine the interface status and how to proceed.
MTU	Lists the OSPF interface *maximum transmission unit* (MTU) size. The MTU is the largest physical packet size (in bytes) a network can transmit. Any packets larger than the MTU are divided into smaller packets before being sent.
OSPF Enabled	Lists whether OSPF has been enabled for each listed interface. OSPF is disabled by default.
UP/DOWN	Displays whether the OSPF interface (the dynamic route) is currently up or down for each listed interface. An OSPF interface is the connection between a router and one of its attached networks.

5 Select the **Refresh** button to update the statistics counters to their latest values.

15.3.21.6 OSPF State

OSPF

An OSPF enabled controller or service platform sends hello packets to discover neighbors and elect a designated router for dynamic links. The hello packet includes link *state* data periodically updated on all OSPF members. The controller or service platform tracks link state information to help assess the health of the OSPF dynamic route.

To view OSPF state statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **OSPF** from the left-hand side of the UI.

4 Select the **OSPF State** tab.

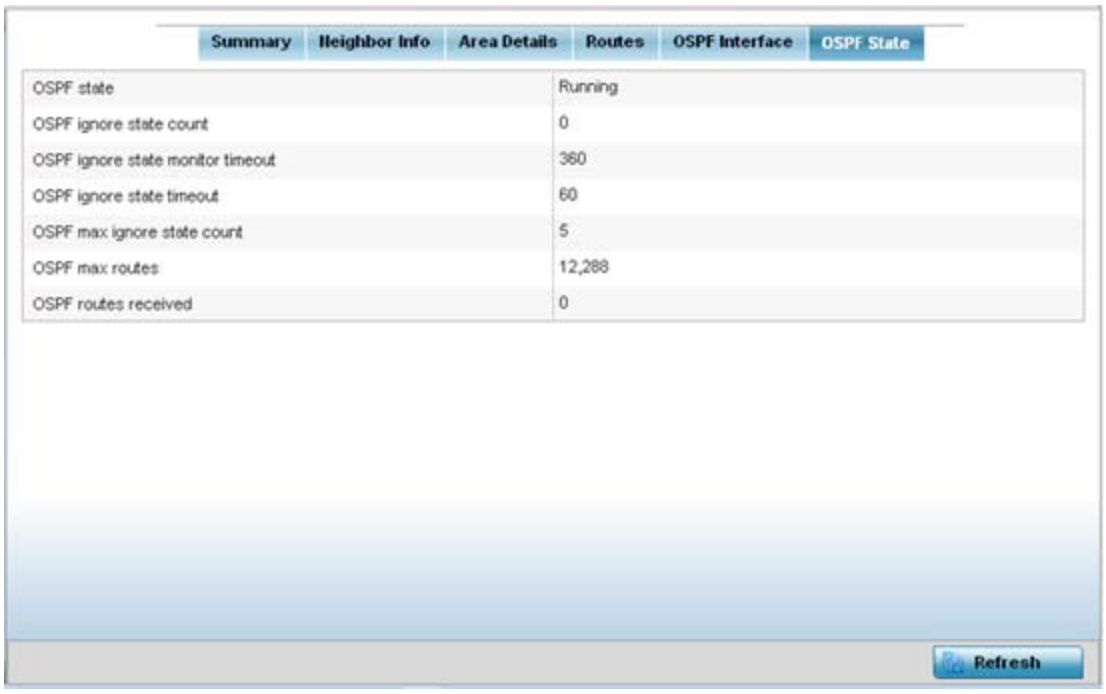


Figure 15-86 *Wireless Controller - OSPF State tab*

The **OSPF State** tab describes the following:

OSPF state	Displays the OSPF link state amongst neighbors within the OSPF topology. Link state information is maintained in a *link-state database* (LSDB) which is a tree image of the entire network topology. Identical copies of the LSDB are periodically updated through flooding on all OSPF supported nodes. Flooding is the part of the OSPF protocol that distributes and synchronizes the link-state database between OSPF routers.
OSPF ignore state count	Lists the number of times state requests have been ignored between the controller or service platform and its peers within this OSPF supported broadcast domain.
OSPF ignore state monitor timeout	Displays the timeout that, when exceeded, prohibits the controller or service platform from detecting changes to the OSPF link state.
OSPF ignore state timeout	Displays the timeout that, when exceeded, returns the controller or service platform back to state assessment amongst neighbors in the OSPF topology.
OSPF max ignore state count	Displays whether an OSPF state timeout is being ignored and not utilized in the transmission of state update requests amongst neighbors within the OSPF topology.
OSPF max routes	States the maximum number of routes negotiated amongst neighbors within the OSPF topology.

OSPF routes received	Lists the routes received and negotiated amongst neighbors within the OSPF topology.

5 Select the **Refresh** button to update the statistics counters to their latest values.

15.3.22 L2TPv3

Controller Statistics

Use L2TP V3 to create tunnels for transporting layer 2 frames. L2TP V3 enables a controller or service platform to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TP V3 tunnels can be defined between WING devices and other devices supporting the L2TP V3 protocol.

To review a selected controller or service platform's L2TPv3 statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **L2TPv3 Tunnels**.

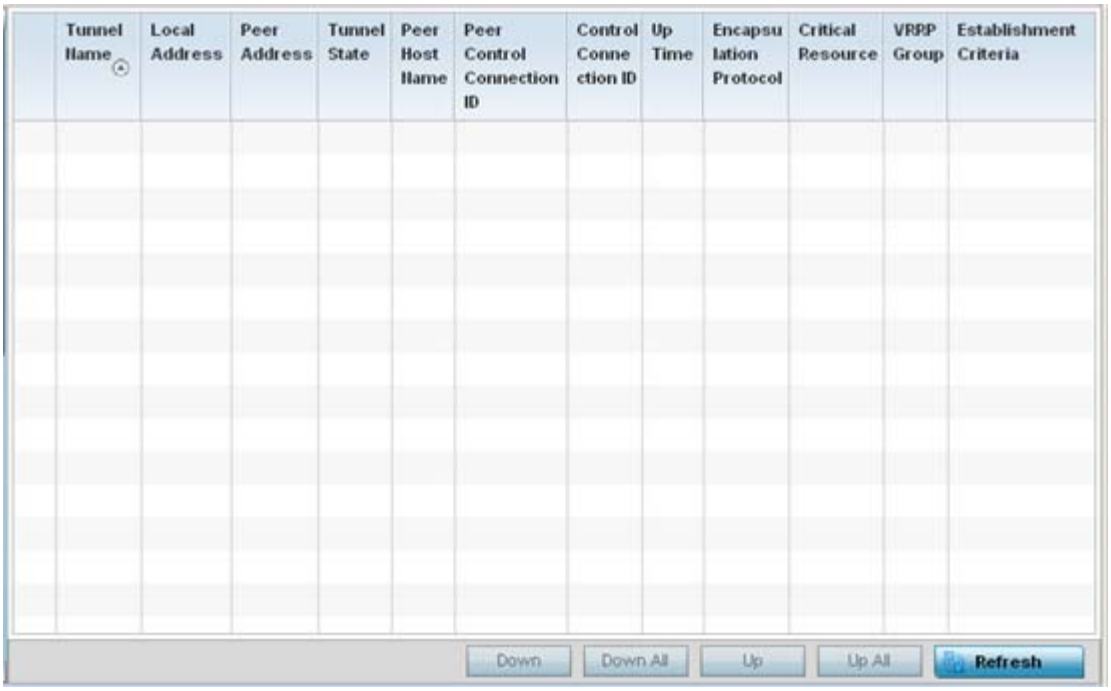


Figure 15-87 *Wireless Controller - L2TPv3 screen*

The **L2TPv3** screen displays the following:

Tunnel Name	Displays the name of each listed L2TPv3 tunnel assigned upon creation. Each listed tunnel name can be selected as a link to display session data specific to that tunnel. The Sessions screen displays cookie size information as well as psuedowire information specific to the selected tunnel. Data is also available to define whether the tunnel is a trunk session and whether tagged VLANs are used. The number of transmitted, received and dropped packets also display to provide a throughput assessment of the tunnel connection. Each listed session name can also be selected as a link to display VLAN information specific to that session. The VLAN Details screen lists those VLANs used an interface in L2TP tunnel establishment.
Local Address	Lists the IP address assigned as the local tunnel end point address, not the tunnel interface's IP address. This IP is used as the tunnel source IP address. If a local address is not specified, the source IP address is chosen automatically based on the tunnel peer IP address.
Peer Address	Lists the IP address of the L2TP tunnel peer establishing the tunnel connection.
Tunnel State	States whether the tunnel is Idle (not utilized by peers) or is currently active.
Peer Host Name	Lists the assigned peer hostname used as matching criteria in the tunnel establishment process.
Peer Control Connection ID	Displays the numeric identifier for the tunnel session. This is the peer pseudowire ID for the session. This source and destination IDs are exchanged in session establishment messages with the L2TP peer.
Control Connection ID	Displays the router ID(s) sent in tunnel establishment messages with a potential peer device.
Up Time	Lists the amount of time the L2TP connection has remained established amongst peers sharing the L2TPv3 tunnel connection. The Up Time is displayed in a *Days*: *Hours*: *Minutes*: *Seconds*: format. If D:0 H:0 M:0 S:0 is displayed, the tunnel connection is not currently established.
Encapsulation Protocol	Displays either *IP* or *UDP* as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes. Tunneling is also called encapsulation. Tunneling works by encapsulating a network protocol within packets carried by the second network.
Critical Resource	Displays monitored critical resources. Critical resources are device IP addresses or interface destinations interopreted as critical to the health of the network. Critical resources allow for the continuous monitoring of these defined addresses. A critical resource, if not available, can result in the network suffering performance degradation. A critical resource can be a gateway, AAA server, WAN interface or any hardware or service on which the stability of the network depends.
VRRP Group	Lists a VRRP group ID (if utilized). A VRRP group is only enabled when the establishment criteria is set to vrrp-master. A VRRP master responds to ARP requests, forwards packets with a destination link MAC layer address equal to the virtual router MAC layer address, rejects packets addressed to the IP associated with the virtual router and accepts packets addressed to the IP associated with the virtual router.

Establishment Criteria	Displays the tunnel establishment criteria for this tunnel. Tunnel establishment involves exchanging 3 message types (SCCRQ, SCCRP and SCCN) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest value.

15.3.23 VRRP

Controller Statistics

The *VRRP* statistics screen displays *Virtual Router Redundancy Protocol* (VRRP) configuration statistics supporting router redundancy in a wireless network requiring high availability.

To review a selected controller or service platform's VRRP statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **VRRP**.

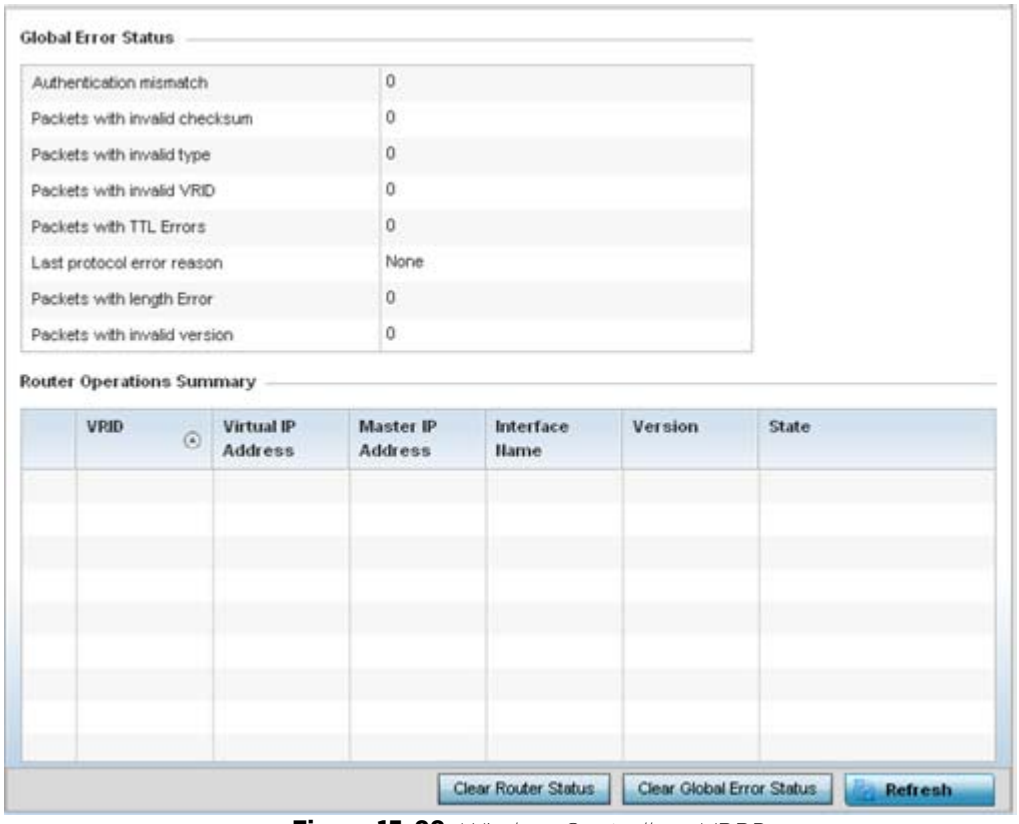


Figure 15-88 *Wireless Controller - VRRP screen*

4 Refer to the **Global Error Status** field to review the various sources of packet errors logged during the implementation of the virtual route.

Errors include the mismatch of authentication credentials, invalid packet checksums, invalid packet types, invalid virtual route IDs, TTL errors, packet length errors and invalid (non matching) VRRP versions.

5 Refer to the **Router Operations Summary** for the following status:

VRID	Lists a numerical index (1 - 254) used to differentiate VRRP configurations. The index is assigned when a VRRP configuration is initially defined. This ID identifies the virtual router a packet is reporting status for. The ID displays as a link that can optionally selected to list the ID's VRRP information in greater detail.
Virtual IP Address	Lists the virtual interface IP address used as the redundant gateway address for the virtual route.
Master IP Address	Displays the IP address of the elected VRRP master. A VRRP master (once elected) responds to ARP requests, forwards packets with a destination link layer MAC address equal to the virtual router MAC address, rejects packets addressed to the IP address associated with the virtual router and accepts packets addressed to the IP address associated with the virtual router.
Interface Name	Displays the interfaces selected to supply VRRP redundancy failover support.
Version	Display VRRP version 3 (RFC 5798) or 2 (RFC 3768) as selected to set the router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP.
State	Displays the current state of each listed virtual router ID.
Clear Router Status	Select the *Clear Router Status* button to clear the Router Operations Summary table values to zero and begin new data collections.
Clear Global Error Status	Select the *Clear Global Error Status* button to clear the Global Error Status table values to zero and begin new data collections.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

6 Optionally select a **VRID** to list the ID's VRRP information in greater detail.

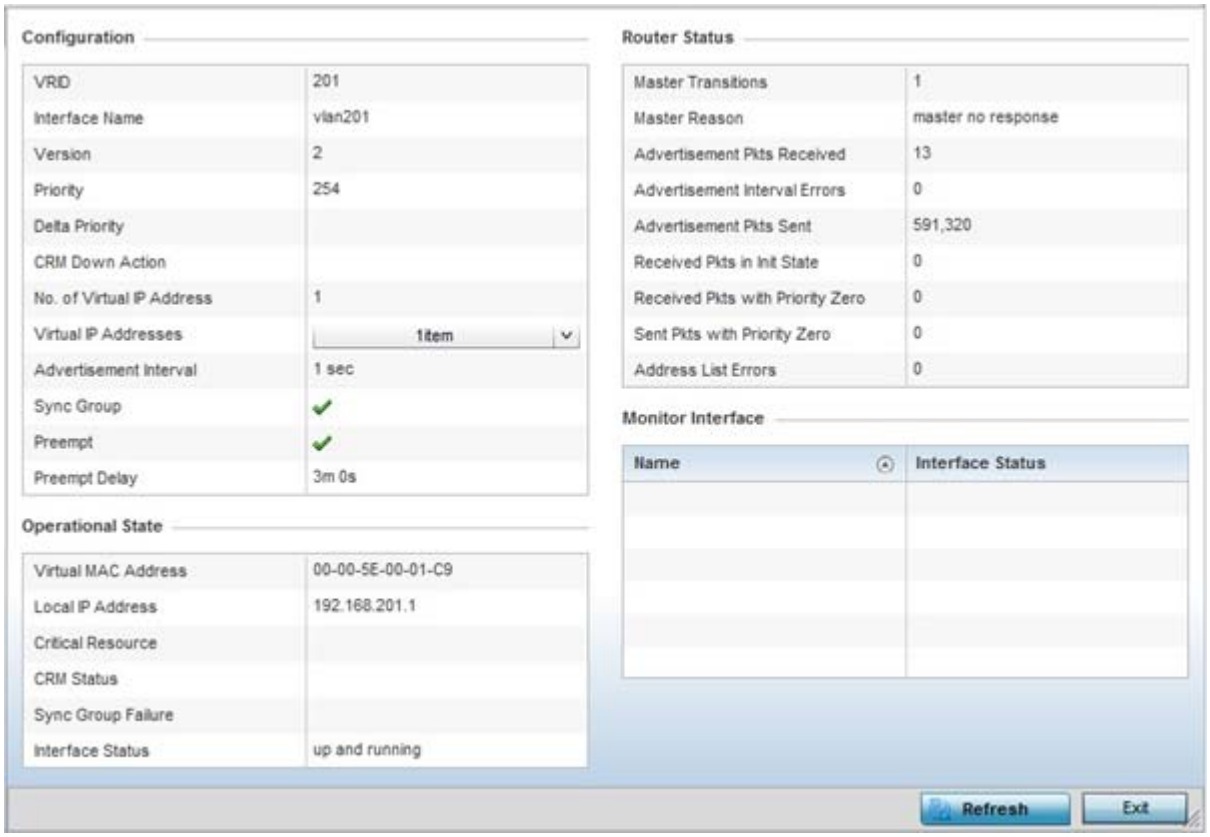


Figure 15-89 *Wireless Controller - VRRP VRID Detail screen*

7 The **Configuration** field lists the following for the selected VRID:

VRID	Lists this selected ID's assigned ID. The index is assigned when a VRRP configuration is initially defined. This ID identifies the virtual router a packet is reporting status for.
Interface	Displays the interfaces selected to supply VRRP redundancy failover support.
Version	Displays the VRRP version scheme used with the configuration. VRRP version 3 (RFC 5798) and 2 (RFC 3768) are selectable to set the router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP. For more information on the VRRP protocol specifications (available publicly) refer to *http://www.ietf.org/rfc/rfc3768.txt* (version 2) and *http://www.ietf.org/rfc/rfc5798.txt* (version 3).
Priority	Lists the ID's numerical value (from 1 - 254) used for the virtual router master election process. The higher the numerical value, the higher the priority in the election process.
Delta Priority	Displays the configured priority (by the set value) when the monitored interface is down. When critical resource monitoring, the configured value is incremented by the value defined.
CRM Down Action	Lists the critical resource down action applied to this listed VRID.
No. of Virtual IP Address	Lists the number of virtual interface IP address used as the redundant gateway address for the virtual route.
Virtual IP Addresses	Lists the virtual interface IP address set as the redundant gateway address for the virtual route.

Advertisement Interval	Lists the interval for unsolicited router assignments.The advertisement interval is the minimum interval between sending router updates. Sending too many updates creates flapping of routes leading to possible disruption.
Sync Group	Lists whether a VRRP sync group is assigned to this VRRP ID's group of virtual IP addresses. This triggers VRRP failover if an advertisement is not received from the virtual masters that are part of this VRRP sync group.
Preempt	Lists whether preempt is enabled for the selected ID. Preempt ensures a high priority backup router is available to preempt a lower priority backup router resource. The default setting is enabled. When selected, the preempt delay option becomes enabled to set the actual delay interval for pre-emption. This setting determines if a node with a higher priority can take over all the Virtual IPs from the nodes with a lower priority.
Preempt Delay	If preempt is enabled, this item lists the delay interval (in seconds) for pre-emption.

8 The **Operational State** field lists the following for the selected VRID:

Virtual MAC Address	Lists the alpha numeric virtual MAC address utilized by the selected VRID.
Local IP Address	This address represents an alternative to an interface IP address. The last byte of the address (XX) is the VRID, which is different for each virtual router in the network
Critical Resource	Displays the critical resource currently utilized by the selected VRID.
CRM Status	Lists operational network status of the critical resource used by this VRID.
Sync Group Failure	Lists any sync failures detected with the sync group of virtual IP addresses.
Interface Status	Lists the operational network status of the interfaces selected to supply VRRP redundancy failover support.

9 The **Router Status** field lists the following router performance and error data:

Master Transitions	Lists the number of transitions to master router designation that have occurred with this VRID's router.
Master Reason	Displays an event message in respect the dedicated VRRP router's availability.
Advertisement Pkts Received	Lists the number of router advertisements received by this selected VRID. Router advertisements are periodically sent to hosts or sent in response to solicitation requests. Router advertisements contain prefixes used for link determination, address configuration and maximum hop limits.
Advertisement Interval Errors	Lists this VRID's number of advertisement prefix errors for link determination, address configuration and maximum hop limits.
Advertisement Pkts Sent	Lists the number of router advertisements sent by this selected VRID. Router advertisements are periodically sent to hosts or sent in response to solicitation requests. Router advertisements contain prefixes used for link determination, address configuration and maximum hop limits.
Received Pkts in Init State	Lists the number of packets received by the selected VRID when a router receives a hello packet but the local router ID is not listed in the received neighbor field. This means bidirectional communication is not been established.

Received Pkts with Priority Zero	Lists this VRID's number of received packets with a value of zero.
Sent Pkts with Priority Zero	Lists this VRID's number of sent packets with a value of zero.
Address List Errors	Lists the number of router event errors detected where an address that could not be resolved and bidirectional communication could not be established.

10 Refer to the **Monitor Interface** field to assess the names of this VRID's interface utilization and their respective statuses.

15.3.24 Critical Resources

Controller Statistics

The Critical Resources statistics screen displays a list of device IP addresses on the network (gateways, routers etc.). These defined IP addresses are critical to the health of the controller or service platform managed network. These device addresses are pinged regularly by the Access Point. If there is a connectivity issue, an event is generated stating a critical resource is unavailable.

To view controller or service platform Critical Resource statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Critical Resource** from the left-hand side of the UI.

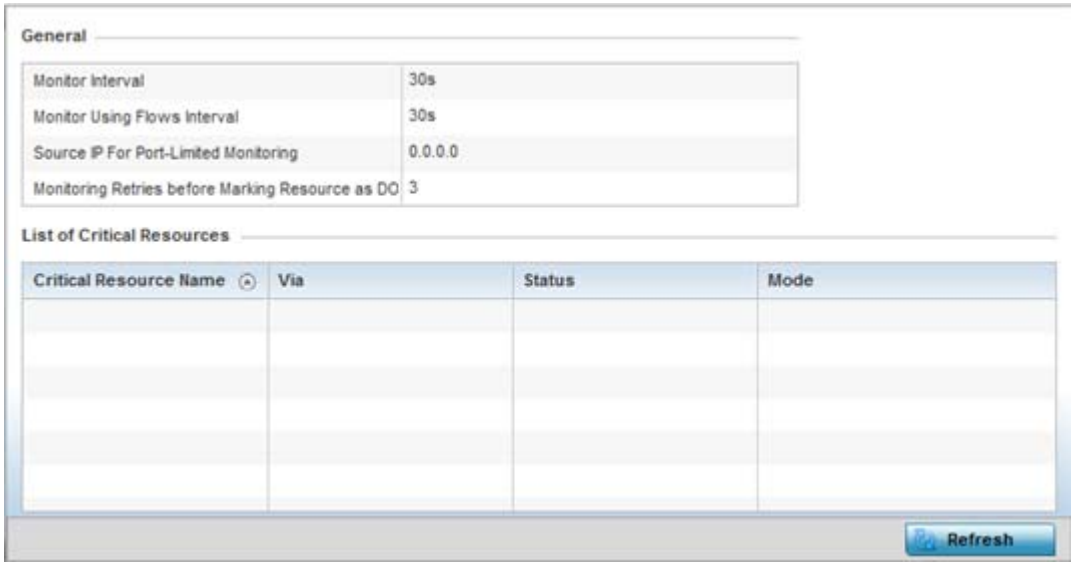


Figure 15-90 *Wireless Controller - Critical Resource screen*

4 Refer to the **General** field to assess the **Monitor Interval** and **Monitor Using Flows Interval** used to poll for updates from the critical resource IP listed for **Source IP For Port-Limited Monitoring**. **Monitoring Retries before Marking Resource as DOWN** are the number of retry connection attempts permitted before this listed resource is defined as down (offline).

5 Refer to the following **List of Critical Resources**:

Critical Resource Name	Lists the name of the resource being monitored by the controller or service platform.
Via	Lists the VLAN used by the critical resource as a virtual interface. the VLAN displays as a link than can be selected to list configuration and network address information in greater detail.
Status	Defines the operational state of each listed critical resource VLAN interface (Up or Down).
Error Reason	Provides an error status as to why the critical resource is not available over its designated VLAN.
Mode	Defines the operational state of each listed critical resource (up or down).
Refresh	Select *Refresh* to update the statistics counters to their latest values.

15.3.25 LDAP Agent Status

Controller Statistics

When LDAP has been specified as an external resource (as opposed to local RADIUS resources) to validate PEAP-MS-CHAP v2 authentication requests, user credentials and password information needs to be made available locally to successfully connect to the external LDAP server. Up to two LDAP Agents (primary and secondary external resources) can be defined as external resources for PEAP-MS-CHAP v2 authentication requests. For more information on setting LDAP agents as part of the RADIUS server policy, see *Configuring RADIUS Server Policies on page 11-57*.

To view controller or service platform LDAP agent statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **LDAP Agent Status** from the left-hand side of the UI.

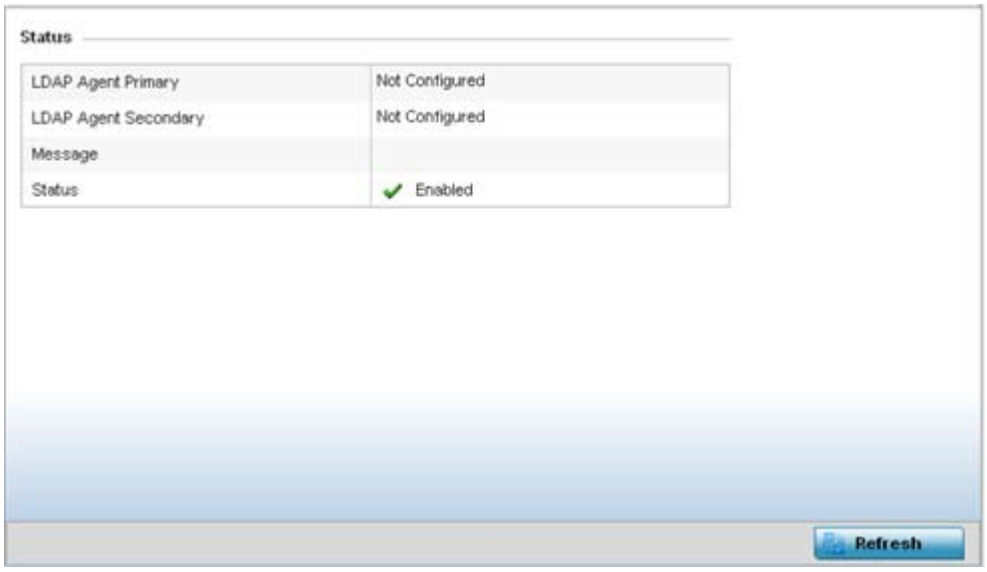


Figure 15-91 *Wireless Controller - LDAP Agent Status screen*

The LDAP Agent Status screen displays the following:

LDAP Agent Primary	Lists the primary IP address of a remote LDAP server resource used by the controller or service platform to validate PEAP-MS-CHAP v2 authentication requests. When a RADIUS server policy's data source is set to LDAP, this is the first resource for authentication requests.
LDAP Agent Secondary	Lists the secondary IP address of a remote LDAP server resource used by the controller or service platform to validate PEAP-MS-CHAP v2 authentication requests. When a RADIUS server policy's data source is set to LDAP, this is the second resource for authentication requests.
Message	Displays any system message generated in the controller or service platform's connection with the primary or secondary LDAP agent. If there's a problem with the username and password used to connection to the LDAP agent it would be listed here.
Status	Displays whether the controller or service platform has successfully joined the remote LDAP server domain designated to externally validate PEAP-MS-CHAP v2 authentication requests.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

15.3.26 Mint Links

Controller Statistics

Wireless controllers and Access Points use the MiNT protocol as the primary means of device discovery and communication for Access point adoption and management. MiNT provides a mechanism to discover neighbor devices in the network, and exchange packets between devices regardless of how these devices are connected (L2 or L3).

MiNT provides the means to secure communications at the transport layer. Using MiNT, a device can be configured to only communicate with other authorized (MiNT enabled) devices of the same model. MiNT links can be established over a VLAN (Among Access Points on a VLAN) or IP (remote access point to controller).

MiNT Links are automatically created between controllers and Access Points during adoption using MLCP (*MiNT Link Creation Protocol*). They can also be manually created between a controller and Access Point (or) between Access Points. MiNT links are manually created between controllers while configuring a cluster.

Level 2 (or) remote MiNT links are controller aware links, and requires IP network for communication. This level 2 MiNT links at access points are intended for remote Adaptive AP deployment and management from NOC. With Level2 MiNT links, access points are only aware of the controllers and not about other Access points. Level 2 MiNT links also provide partitioning, between Access Points deployed at various remote sites.

To view controller or service platform Mint link statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Mint Links** from the left-hand side of the UI.

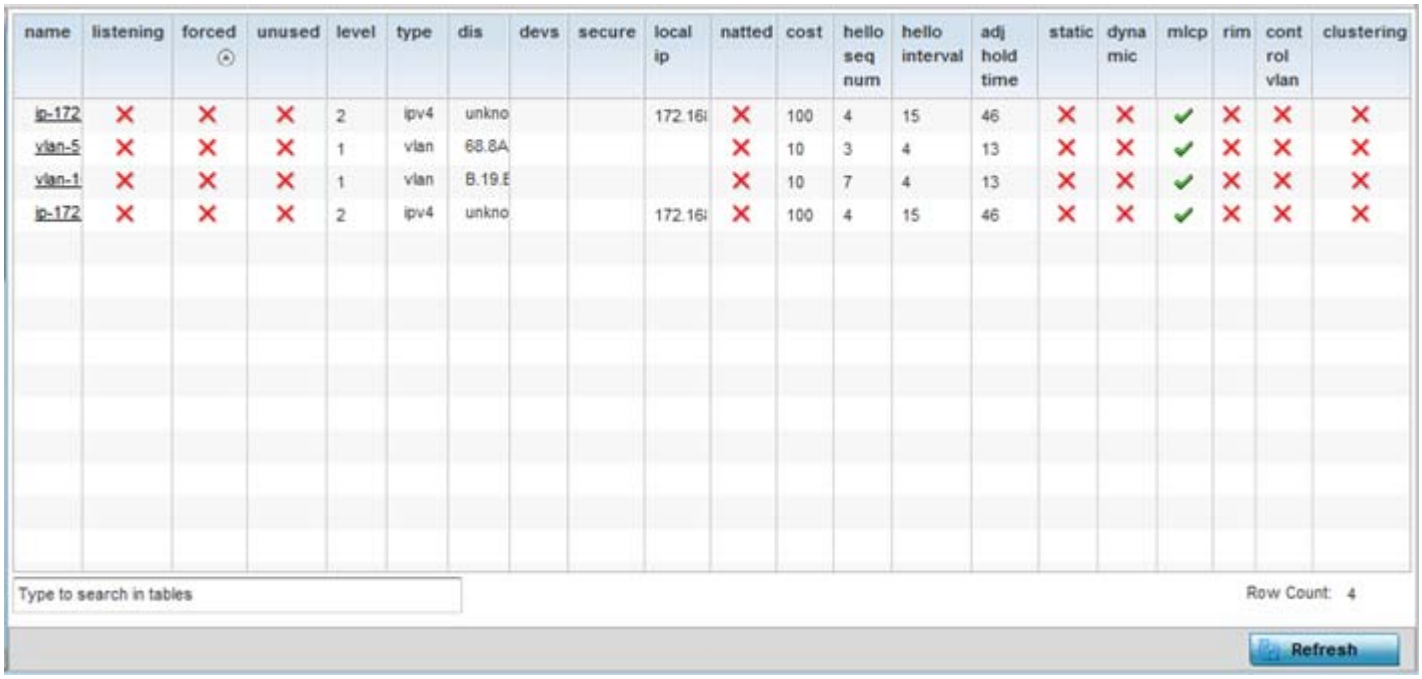


Figure 15-92 *Wireless Controller - Mint Links screen*

The Mint Links screen lists the *name* of the impacted VLAN or link in the form of a link that can be selected to display more granular information about that VLAN. A green check mark or a red X defines whether the listed VLAN is *listening* to traffic, *forced* to stay up or *unused* with the Mint link. The *level* column specifies whether the listed Mint link is traditional switching link (level 2) or a routing link (level 3). The *type* column defines whether the listed Mint link is a VLAN or an IPv4 or IPv6 type network address. The *dis* column lists how each link was discovered.

Refer to the *secure* column to assess whether the listed links are isolated between peers. The *local ip* column lists the IP address assigned as the link's end point address, not the interface's IP address. The *natted* column lists whether the link is NAT enabled or disabled for modifying network address information in IP packet headers in transit. The *cost* defines the cost for a packet to travel from its originating port to its end point destination.

The *hello seq number* and *hello interval* define the interval between hello keep alive messages between link end points. While the *adj hold time* sets the time after the last hello packet when the connected between end points is defined as lost.

The *static* and *dynamic* link columns state whether each listed link is static route using a manually configured route entry, or a dynamic route characterized by its destination The *rim* column defines whether the listed link is managed remotely. The *control vlan* column states whether the listed link has enabled as a control VLAN. Lastly, the *clustering* column states whether listed link members discover and establish connections to other peers and provide self-healing in the event of cluster member failure.

4 Periodically select **Refresh** to update the screen's data counters to their latest values.

5 If needed, select a Mint link from the *name* column to display more granular information for that link.

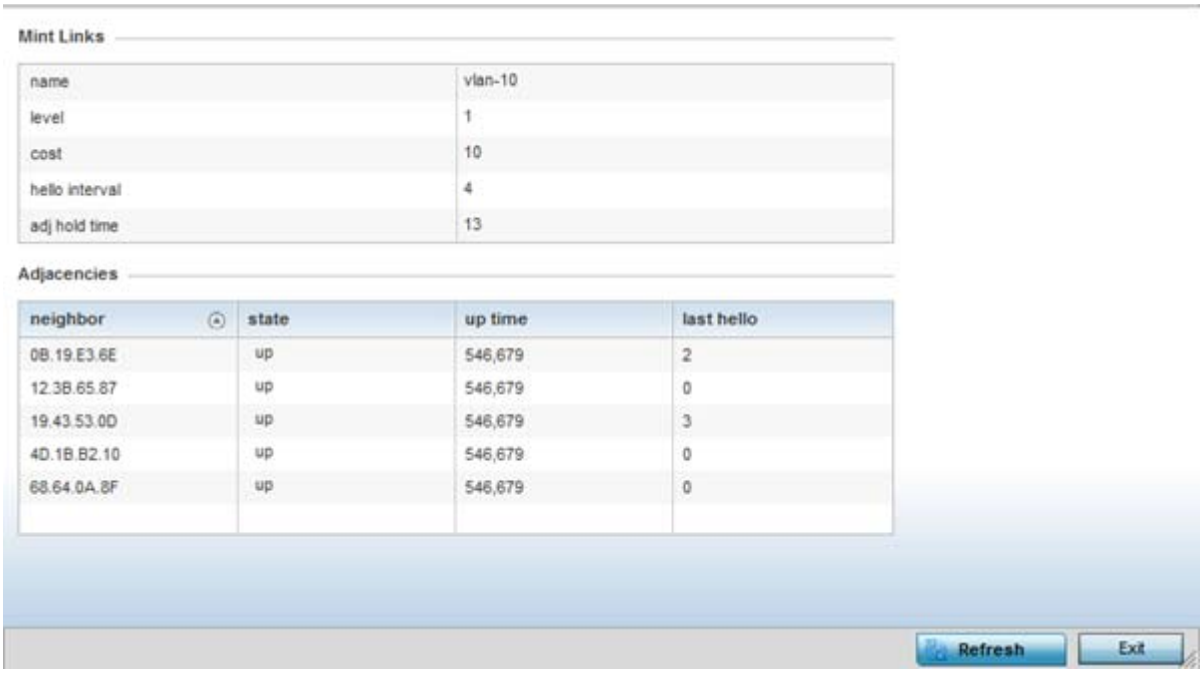


Figure 15-93 *Wireless Controller - Mint Link Details screen*

The first table lists the Mint link's name and *level* specifying whether the Mint link is traditional switching link (level 2) or a routing link (level 3). The *cost* defines the cost for a packet to travel from its originating port to its end point destination. The *hello interval* lists the time between hello keep alive messages between link end points. The *adj hold time* sets the time after the last hello packet when the connected between end points is defined as lost.

The *Adjacencies* table lists *neighbor* devices by their hardware identifiers and operational *state* to help determine their availability as Mint link end points and peers. The *up time* lists the selected link's detection on the network and the last hello lists when the *last hello* message was exchanged.

6 Periodically select *Refresh* to update the statistics counters to their latest values.

15.3.27 Guest Users

Controller Statistics

A *captive portal* is an access policy for providing guests temporary and restrictive access to the wireless network. A captive portal configuration provides secure authenticated access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Captive portals can have their access durations set by an administrator to either provide temporary access to the controller or service platform managed network or provide access without limitations.

For information on setting captive portal duration and authentication settings, refer to *Configuring Captive Portal Policies on page 11-1*.

To view the controller or service platform guest user utilization:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Guest Users** from the left-hand side of the UI.

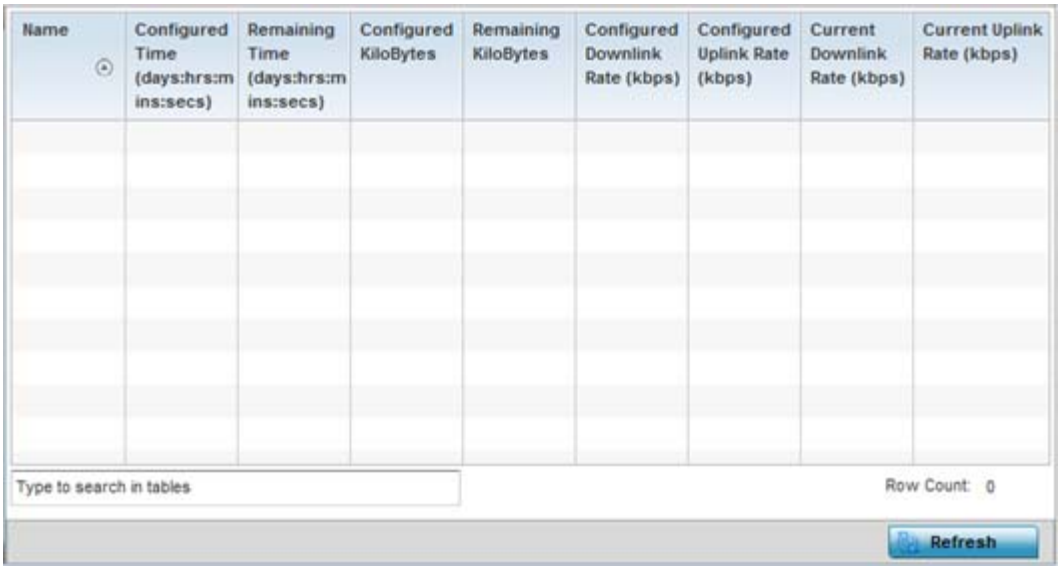


Figure 15-94 *Wireless Controller – Guest Users screen*

The **Guest Users** screen describes the following:

Name	Lists the administrator assigned name of the client utilizing the controller or service platform for guest access to the wireless network.
Configured Time (days:hrs:mins:secs)	Displays the restricted permissions each listed client was initially configured for their captive portal guest user session with this managing controller or service platform.
Remaining Time (days:hrs:mins:secs)	Displays the time each listed client has remaining in their captive portal guest user session with this managing controller or service platform.
Configured Kilobytes	Lists the maximum configured bandwidth consumable by the listed guest user (in kilobytes).
Remaining Kilobytes	Lists the remaining bandwidth available to the listed guest user (in kilobytes). This is the difference between the configured (maximum) bandwidth and the users's current utilization.
Configured Downlink Rate (kbps)	Specifies the download speed configured for the listed guest user. When bandwidth is available, the user can download data at the specified rate (in kilobytes per second). If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to the defined reduced downlink rate. For more information, refer to *Defining User Pools on page 11-53*.
Configured Uplink Rate (kbps)	Specifies the upload speed dedicated to the listed guest user. When bandwidth is available, the user is able to upload data at the specified rate (in kilobytes per second). If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to the reduced uplink rate. For more information, refer to *Defining User Pools on page 11-53*.
Current Downlink Rate (Kbps)	Lists the listed guest user's current downlink rate in kbps. Use this information to assess whether this user's configured downlink rate is adequate for their session requirements and whether their reduced downlink rate need adjustment if the configured downlink rate is exceeded. For more information, refer to *Defining User Pools on page 11-53*.

Current Uplink Rate (Kbps)	Lists the listed guest user's current uplink rate in kbps. Use this information to assess whether this user's configured uplink rate is adequate for their session requirements and whether their reduced uplink rate need adjustment if the configured uplink rate is exceeded. For more information, refer to *Defining User Pools on page 11-53*.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest value.

15.3.28 GRE Tunnels

Controller Statistics

Generic Routing Encapsulation (GRE) is one of the available tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.

Use the GRE Tunnel screen to view information on the traffic flow in a GRE tunnel.

To view the GRE Tunnel statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **GRE Tunnels** from the left-hand side of the UI.

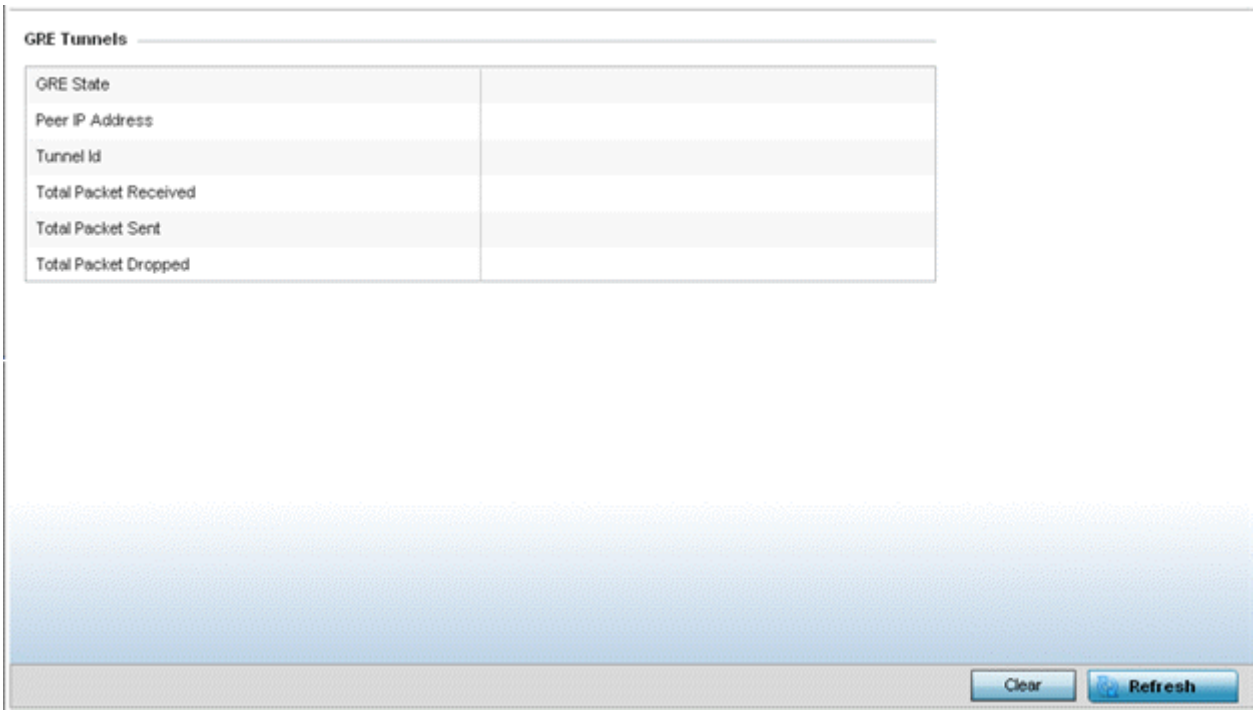


Figure 15-95 *Wireless Controller – GRE Tunnel screen*

The **GRE Tunnels** screen describes the following:

GRE State	Displays the current operational state of the GRE tunnel.

Peer IP Address	Displays the IP address of the peer device on the remote end of the GRE tunnel.
Tunnel Id	Displays the session ID of an established GRE tunnel. This ID is only viable while the tunnel is operational and does not carry to subsequent sessions.
Total Packets Received	Displays the total number of packets received from a peer at the remote end of the GRE tunnel.
Total Packets Sent	Displays the total number of packets sent from this controller or service platform to a peer at the remote end of the GRE tunnel.
Total Packets Dropped	Lists the number of packets dropped from tunneled exchanges between this controller or service platform and a peer at the remote end of the VPN tunnel
Clear	Select Clear to revert the screen counters to zero and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest value.

15.3.29 Dot1x

Controller Statistics

Dot1x (or 802.1x) is an IEEE standard for network authentication. Devices supporting Dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a Dot1x network, a device automatically connects and authenticates without needing to manually login.

To view the Dot1x statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select the Wireless Controller node from the left navigation pane.

3 Select **Dot1x** from the left-hand side of the UI.

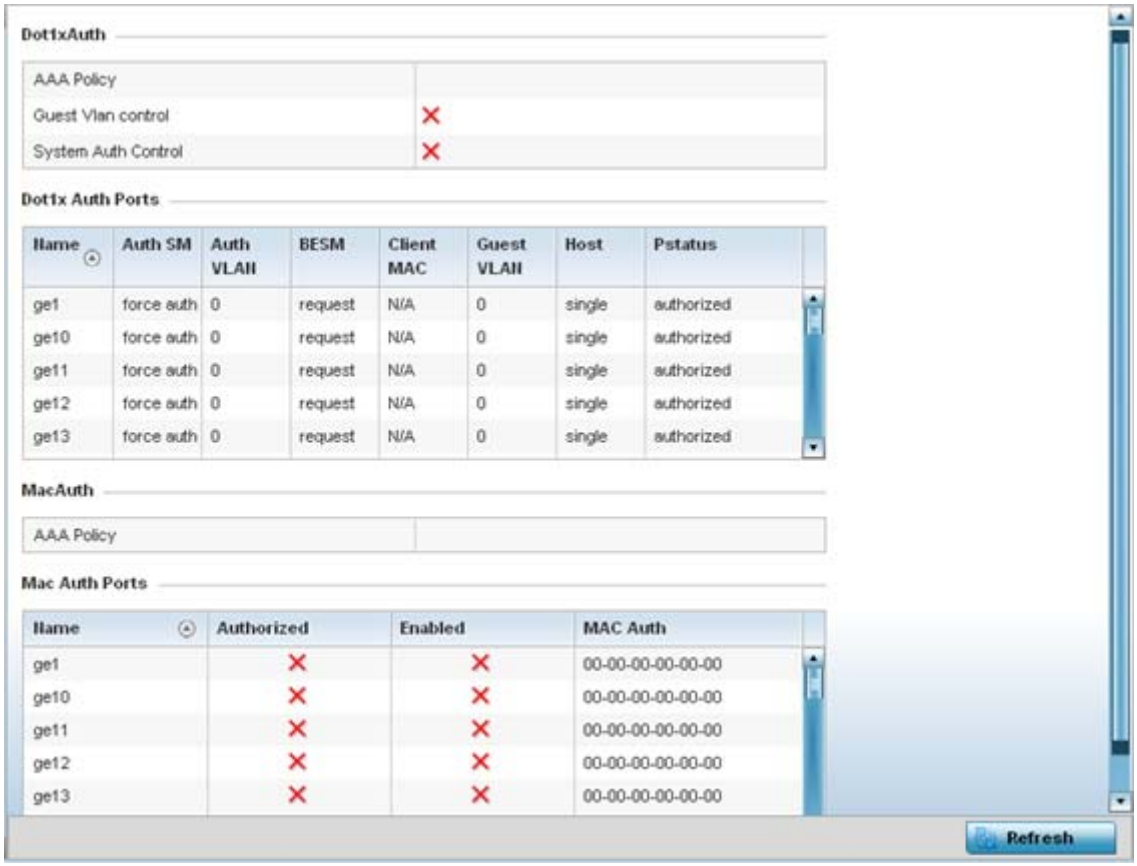


Figure 15-96 *Wireless Controller – Dot1x screen*

4 Refer to the following **Dot1xAuth** statistics:

AAA Policy	Lists the AAA policy currently being utilized for authenticating user requests.
Guest Vlan Control	Lists whether guest VLAN control has been allowed (or enabled). This is the VLAN traffic is bridged on if the port is unauthorized and guest VLAN globally enabled. A green checkmark designates guest VLAN control as enabled. A red X defines guest VLAN control as disabled.
System Auth Control	Lists whether Dot1x authorization is globally enabled for the controller or service platform. A green checkmark designates Dot1x authorization globally enabled. A red X defines Dot1x as globally disabled.

5 Review the following **Dot1x Auth Ports** utilization information:

Name	Lists the controller or service platform ge ports subject to automatic connection and authentication using Dot1x.
Auth SM	Lists whether Dot1x authentication is forced over the listed port.
Auth VLAN	Lists the numeric VLAN ID used as a virtual interface for authentication requests over the listed port.
BESM	Lists whether an authentication request is pending on the listed port.
Client MAC	Lists the MAC address of requesting clients seeking authentication over the listed port.

Guest VLAN	Lists the guest VLAN utilized for the listed port. This is the VLAN traffic is bridged on if the port is unauthorized and guest VLAN globally enabled.
Host	Lists whether the host is a single entity or not.
Pstatus	Lists whether the listed port has been authorized for Dot1x network authentication.

6 Refer to the **MacAuth** table to assess the AAA policy applied to MAC authorization requests.

7 Review the following **MAC Auth Ports** utilization information:

Name	Lists the controller or service platform ge ports subject to automatic connection and MAC authentication using Dot1x.
Authorized	Lists whether MAC authorization using Dot1x has been authorized (permitted) on the listed ge port. A green checkmark designates Dot1x authorization as permitted. A red X defines authorization as disabled.
Enabled	Lists whether MAC authorization using Dot1x has been enabled on the listed ge port. A green checkmark designates Dot1x authorization as allowed. A red X defines authorization as disabled.
MAC Auth	Lists the port's factory encoded MAC address.

8 Select the **Refresh** button to update the screen's statistics counters to their latest value.

15.3.30 Network

Controller Statistics

Use the *Network* screen to view information for ARP, DHCP, Routing, MLD and Bridging. Each of these screens provides enough data to troubleshoot issues related to the following:

- *ARP Entries*
- *Route Entries*
- *Default Routes*
- *Bridge*
- *IGMP*
- *MLD*
- *LACP*
- *Traffic Shaping*
- *DHCP Options*
- *Cisco Discovery Protocol*
- *Link Layer Discovery Protocol*
- *IPv6 Neighbor Discovery*
- *MSTP*

15.3.30.1 ARP Entries

Network

The *Address Resolution Protocol* (ARP) is a networking protocol for determining a network host's hardware address when its IP address or network layer address is known.

To view the ARP entries on the network statistics screen:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Networks** menu from the left-hand side of the UI.

4 Select **ARP**.

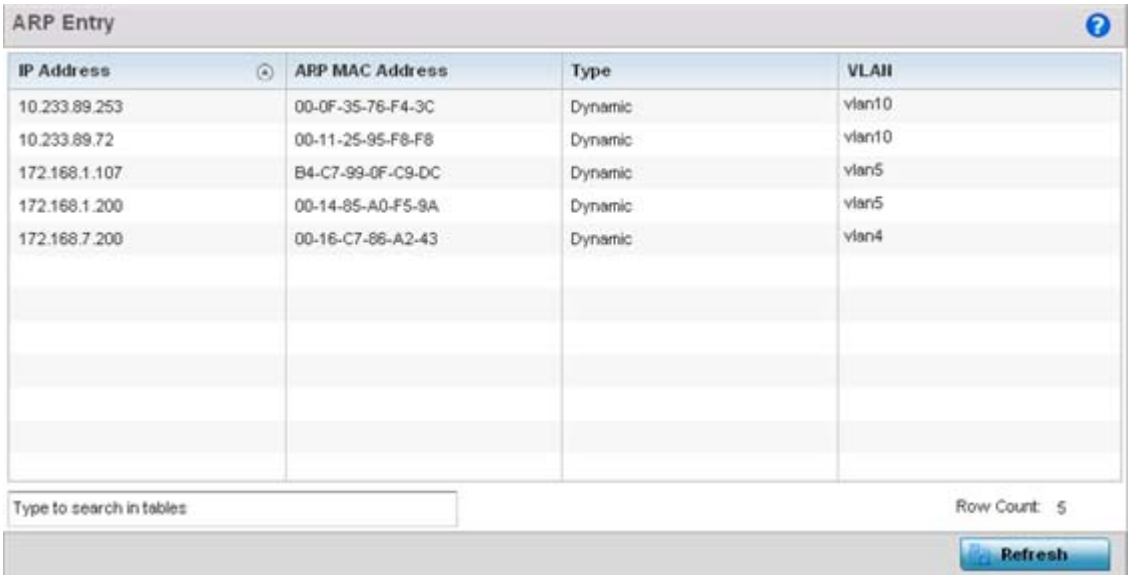


Figure 15-97 *Wireless Controller - Network ARP screen*

The **ARP Entries** screen displays the following:

IP Address	Displays the IP address of the client being resolved on behalf of the controller or service platform.
ARP MAC Address	Displays the MAC address of the device where an IP address is being resolved.
Type	Defines whether the entry was added statically or created dynamically in respect to network traffic. Entries are typically static.
VLAN	Displays the name of the virtual interface where the IP address was found.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.30.2 Route Entries

Network

The *Route Entries* screen displays data for routing packets to a defined destination. When an existing destination subnet does not meet the needs of the network, add a new destination subnet, subnet mask and gateway as needed for either IPv4 or IPv6 formatted data packets.

IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity.

IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for devices on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

To view the route entries:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **Route Entries**. The **IPv4 Route Entries** tab displays by default.

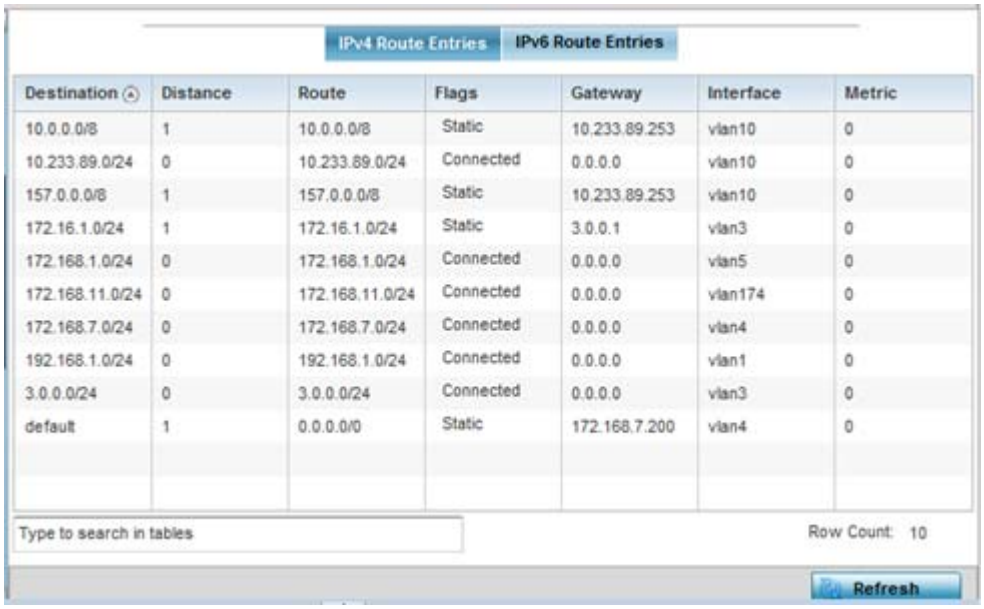


Figure 15-98 *Wireless Controller - IPv4 Route Entries screen*

The **IPv4 Route Entries** screen provides the following information:

Destination	Displays the IPv4 formatted address of the destination route address.
Distance	Lists the hop distance to a desired route. Devices regularly send neighbors their own assessment of the total cost to get to all known destinations. A neighboring device examines the information and compares it to their own routing data. Any improvement on what's already known is inserted in that device's own routing tables. Over time, each networked device discovers the optimal next hop for each destination.
Route	Lists the IPv4 formatted IP address used for routing packets to a defined destination.
Flags	The flag signifies the condition of the *direct* or *indirect* route.
Gateway	Displays the gateway IP address used to route packets to the destination subnet.
Interface	Displays the name of the controller interface or VLAN utilized by the destination subnet.

Metric	Lists the metric (or cost) of the route to select (or predict) the best route. The metric is computed using a routing algorithm, and covers information bandwidth, network delay, hop count, path cost, load, MTU, reliability, and communication cost.
Refresh	Select *Refresh* to update the display to the latest values.

5 Select the **IPv6 Route Entries** tab to review route data for IPv6 formatted traffic.

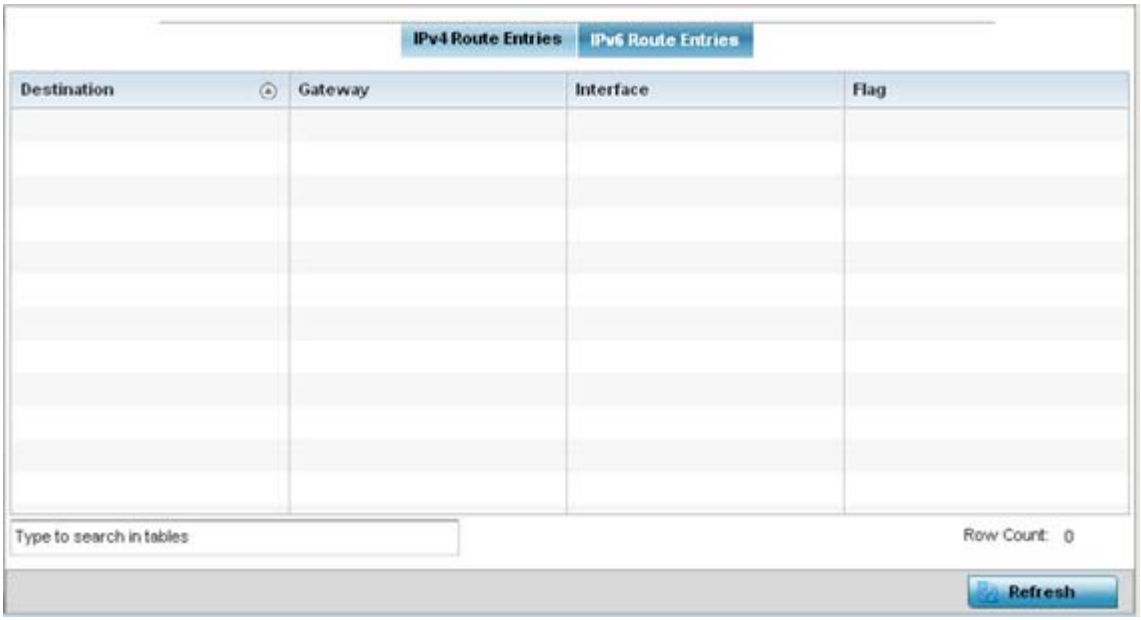


Figure 15-99 *Wireless Controller - IPv6Route Entries screen*

The **IPv6 Route Entries** screen provides the following information:

Destination	Displays the IPv6 formatted address of the destination route address. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Gateway	Displays the gateway IP address used to route packets to the destination subnet.
Interface	Displays the name of the controller interface or VLAN utilized by the destination subnet.
Flag	The flag signifies the condition of the *direct* or *indirect* route.
Refresh	Select *Refresh* to update the display to the latest values.

15.3.30.3 Default Routes

Network

In an IPv6 supported environment unicast routing is always enabled. A controller or service platform routes IPv6 formatted traffic between interfaces as long as the interfaces are enabled for IPv6 and ACLs allow IPv6 formatted traffic. However, an administrator can add a default routes as needed.

Static routes are manually configured. They work fine in simple networks. However, static routes with topology changes require an administrator to manually configure and modify the corresponding route revisions. Default routes are useful, as they forward packets that match no specific routes in the routing table.

To view controller or service platform default routes:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **Default Routes**. The **IPv4 Default Routes** tab displays by default.

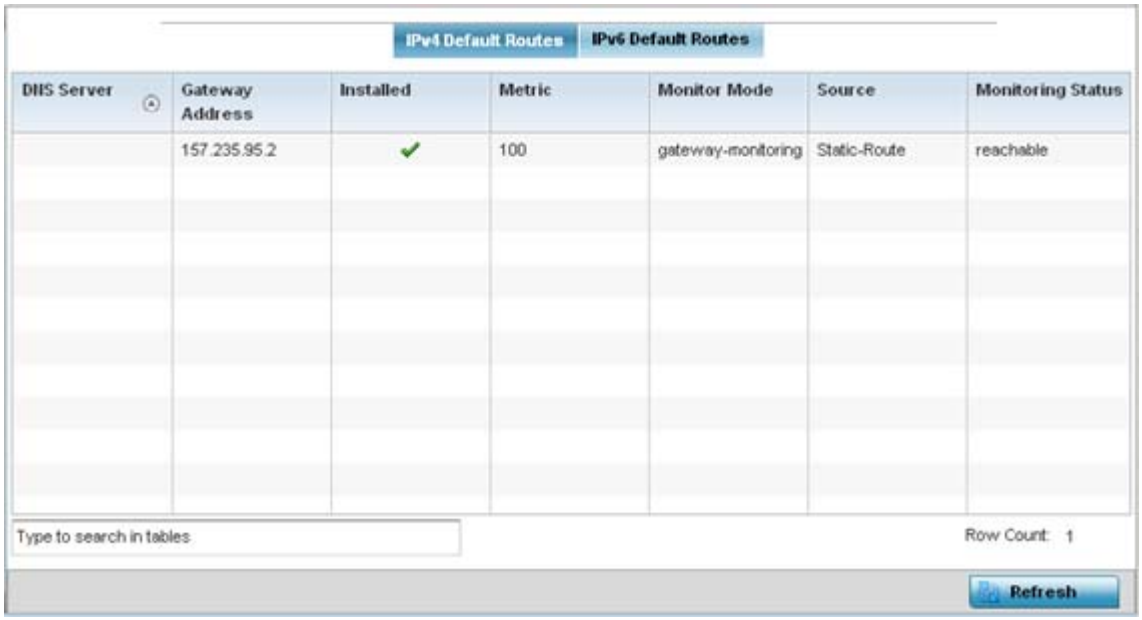


Figure 15-100 *Wireless Controller - IPv4 Default Routes screen*

The **IPv4 Default Routes** screen provides the following information:

DNS Server	Lists the address of the DNS server providing IPv4 formatted address assignments on behalf of the controller or service platform.
Gateway Address	Lists the IP address of the gateway resource used with the listed route.
Installed	A green checkmark defines the listed route as currently installed on the controller or service platform. A red X defines the route as not currently installed and utilized.
Metric	The metric (or cost) could be the distance of a router (round-trip time), link throughput or link availability.
Monitor Mode	Displays where in the network the route is monitored for utilization status.
Source	Lists whether the route is *static* or an administrator defined *default* route. Static routes are manually configured. Static routes work adequately in simple networks. However, static routes with topology changes require an administrator to manually configure and modify the corresponding route revisions. Default routes are useful, as they forward packets that match no specific routes in the routing table.
Monitoring Status	Lists whether the defined IPv4 route is currently reachable on the controller or service platform managed network. If not, perhaps a topology change has occurred to a static route requiring a default route be utilized.
Refresh	Select *Refresh* to update the display to the latest values.

5 Select the **IPv6 Default Routes** tab to review default route availabilities for IPv6 formatted traffic.

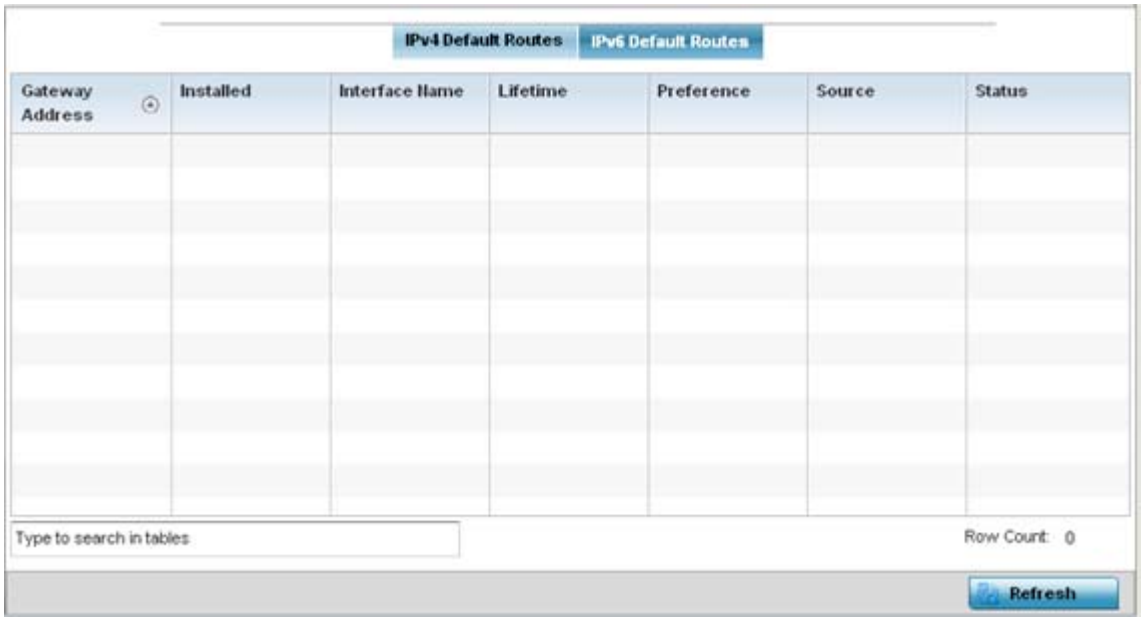


Figure 15-101 *Wireless Controller - IPv6 Default Routes screen*

The **IPv6 Default Routes** screen provides the following information:

Gateway Address	Lists the IP address of the gateway resource used with the listed route.
Installed	A green checkmark defines the listed IPv6 default route as currently installed on the controller or service platform. A red X defines the route as not currently installed and utilized.
Interface Name	Displays the interface on which the IPv6 default route is being utilized.
Lifetime	Lists the lifetime representing the valid usability of the default IPv6 route.
Preference	Displays the administrator defined IPv6 preferred route for IPv6 traffic.
Source	Lists whether the route is *static* or an administrator defined *default* route. Static routes are manually configured. Static routes work adequately in simple networks. However, static routes with topology changes require an administrator to manually configure and modify the corresponding route revisions. Default routes are useful, as they forward packets that match no specific routes in the routing table.
Status	Lists whether the defined IPv6 route is currently reachable on the controller or service platform managed network. If not, perhaps a topology change has occurred to a static route requiring a default route be utilized.
Refresh	Select *Refresh* to update the display to the latest values.

15.3.30.4 Bridge

Network

Bridging is a forwarding technique making no assumption about where a particular network address is located. It depends on flooding and the examination of source addresses in received packet headers to locate unknown devices. Once a device is located, its location is stored in a table to avoid broadcasting to that device again.

Bridging is limited by its dependency on flooding, and is used in local area networks only. A bridge and a controller or service platform are very similar, since a controller or service platform is a bridge with a number of ports.

To view network bridge information:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **Bridge**.

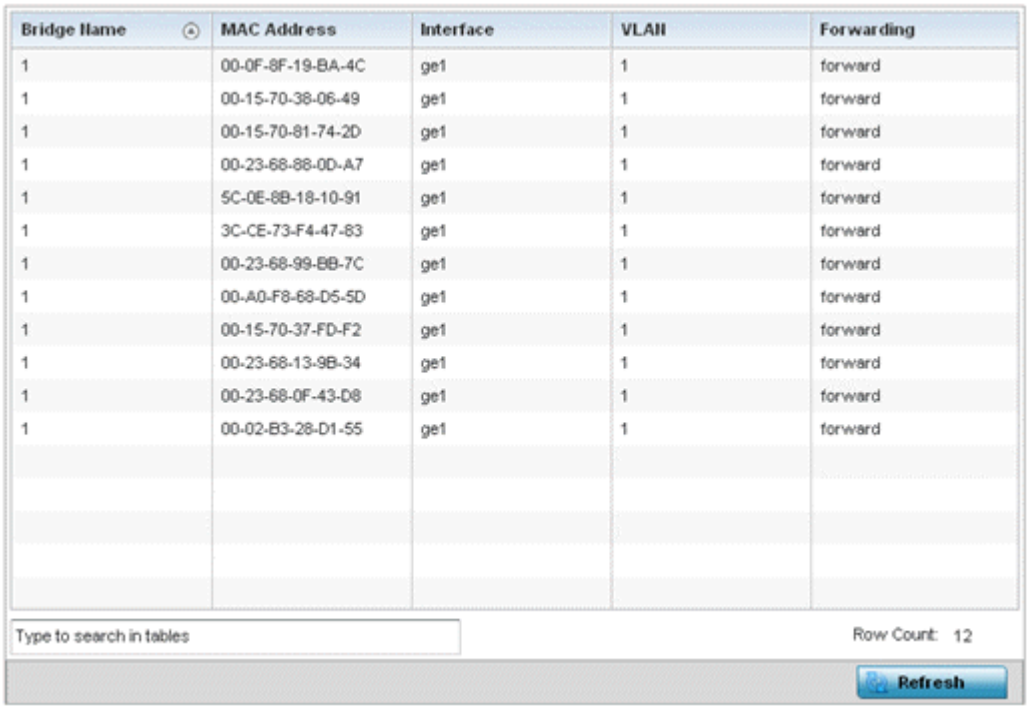


Figure 15-102 *Wireless Controller - Network Bridge screen*

The **Bridge** screen displays the following:

Bridge Name	Displays the numeric ID of the network bridge.
MAC Address	Displays the MAC address of each listed bridge.
Interface	Displays the controller or service platform physical port interface the bridge uses to transfer packets. Interface availability is slightly different amongst supported controller and service platform models.
VLAN	Displays the VLAN the bridge is using as a virtual interface within the controller or service platform managed network.
Forwarding	Displays whether the bridge is forwarding packets.
Refresh	Select *Refresh* to update the statistics counters to the latest values.

15.3.30.5 IGMP

Network

Internet Group Management Protocol (IGMP) is a protocol used for managing members of IP multicast groups. The Access Point listens to IGMP network traffic and forwards the IGMP multicast packets to radios on which the

interested hosts are connected. On the wired side of the network, the Access Point floods all the wired interfaces. This feature reduces unnecessary flooding of multicast traffic in the network.

To view network IGMP configuration options:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **IGMP**.

Figure 15-103 *Wireless Controller - Network IGMP screen*

The **Group** field describes the following:

VLAN	Displays the group VLAN where the multicast transmission is conducted.
Group Address	Displays the Multicast Group ID supporting the statistics displayed. This group ID is the multicast address hosts are listening to.
Port Members	Displays the ports on which multicast clients have been discovered. For example, ge1, radio1, etc. Ports can vary somewhat amongst supported controller and service platform models.
Version	Displays each listed group IGMP version compatibility as either version 1, 2 or 3.

The **Multicast Router (MRouter)** field describes the following:

VLAN	Displays the group VLAN where the multicast transmission is conducted.
Learn Mode	Displays the learning mode used by the router as either *Static* or *PIM-DVMRP.*
Port Members	Displays the physical ports on which multicast clients have been discovered by the multicast router. For example, ge1, radio1, etc. Ports can vary somewhat amongst supported controller and service platform models.

MiNT IDs	Lists MiNT IDs for each listed VLAN. MiNT provides the means to secure Access Point profile communications at the transport layer. Using MiNT, an Access Point can be configured to only communicate with other authorized (MiNT enabled) Access Points of the same model.
Query Interval	Lists the IGMP query interval implemented when the querier functionality is enabled. The default value is 60 seconds.
Version	Lists the multicast router IGMP version compatibility as either version 1, 2 or 3. The default setting is 3.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.30.6 MLD

Network

Multicast Listener Discovery (MLD) snooping enables a controller, service platform or Access Point to examine MLD packets and make forwarding decisions based on content. MLD is used by IPv6 devices to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups.

MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or Access Point VLANs. When enabled, MLD messages are examined between hosts and multicast routers and to discern which hosts are receiving multicast group traffic. The controller, service platform or Access Point then forwards multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces.

To view network MLD configuration options:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **MLD**.

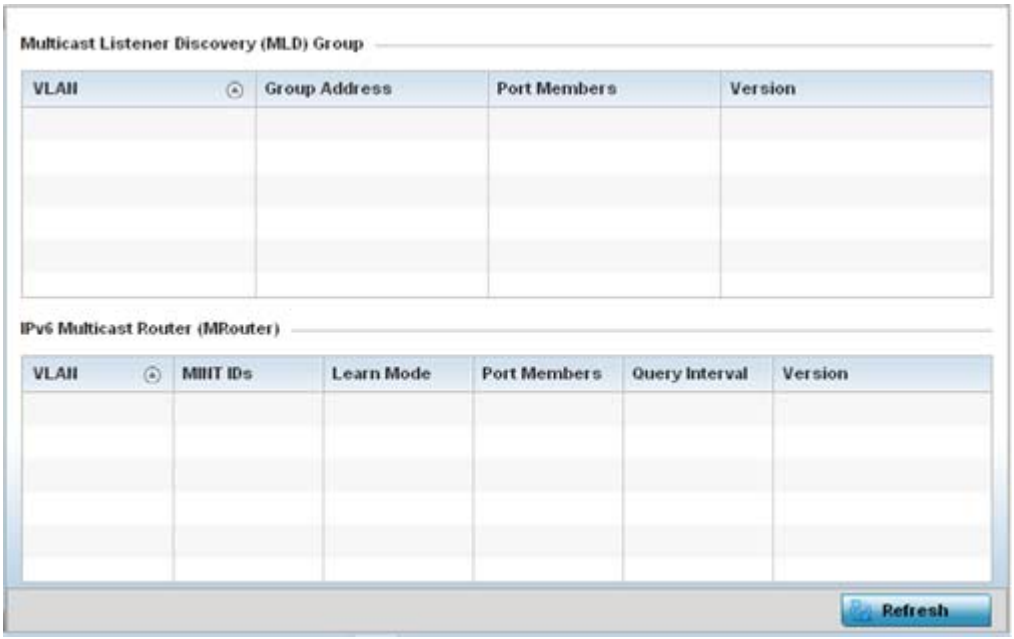


Figure 15-104 *Wireless Controller - Network MLD screen*

The **Multicast Listener Discovery (MLD) Group** field describes the following:

VLAN	Displays the group VLAN where the MLD groups multicast transmission is conducted.
Group Address	Displays the Multicast Group ID supporting the statistics displayed. This group ID is the multicast address hosts are listening to.
Port Members	Displays the ports on which MLD multicast clients have been discovered. For example, ge1, radio1, etc. Ports can vary somewhat amongst supported controller and service platform models.
Version	Displays each listed group's version compatibility as either version 1, 2 or 3.

The **IPv6 Multicast Router (MRouter)** field describes the following:

VLAN	Displays the group VLAN where the multicast transmission is conducted.
MiNT IDs	Lists MiNT IDs for each listed VLAN. MiNT provides the means to secure communications at the transport layer. Using MiNT, a controller or service platform can be configured to only communicate with other authorized (MiNT enabled) devices.
Learn Mode	Displays the learning mode used by the router as either *Static* or *PIM-DVMRP*.
Port Members	Displays the physical ports on which multicast clients have been discovered by the multicast router. For example, ge1, radio1, etc. Ports can vary somewhat amongst supported controller and service platform models.
Query Interval	Lists the query interval implemented when the querier functionality is enabled. The default value is 60 seconds.
Version	Lists the multicast router version compatibility as either version 1, 2 or 3. The default setting is 3.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.30.7 LACP

Network

Link Aggregation Control Protocol (LACP) is used to dynamically determine if link aggregation is possible and then to automatically configure the aggregation. LACP is a part of the IEEE 802.1ad standard and allows the switch to dynamically reconfigure the link aggregation groups (LAGs). A LAG is enabled only if the LACP determines that the remote device is also using LACP and is able to join the LAG.

To view network LACP statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **LACP**. The **System and Aggregator Statistics** tab displays by default.

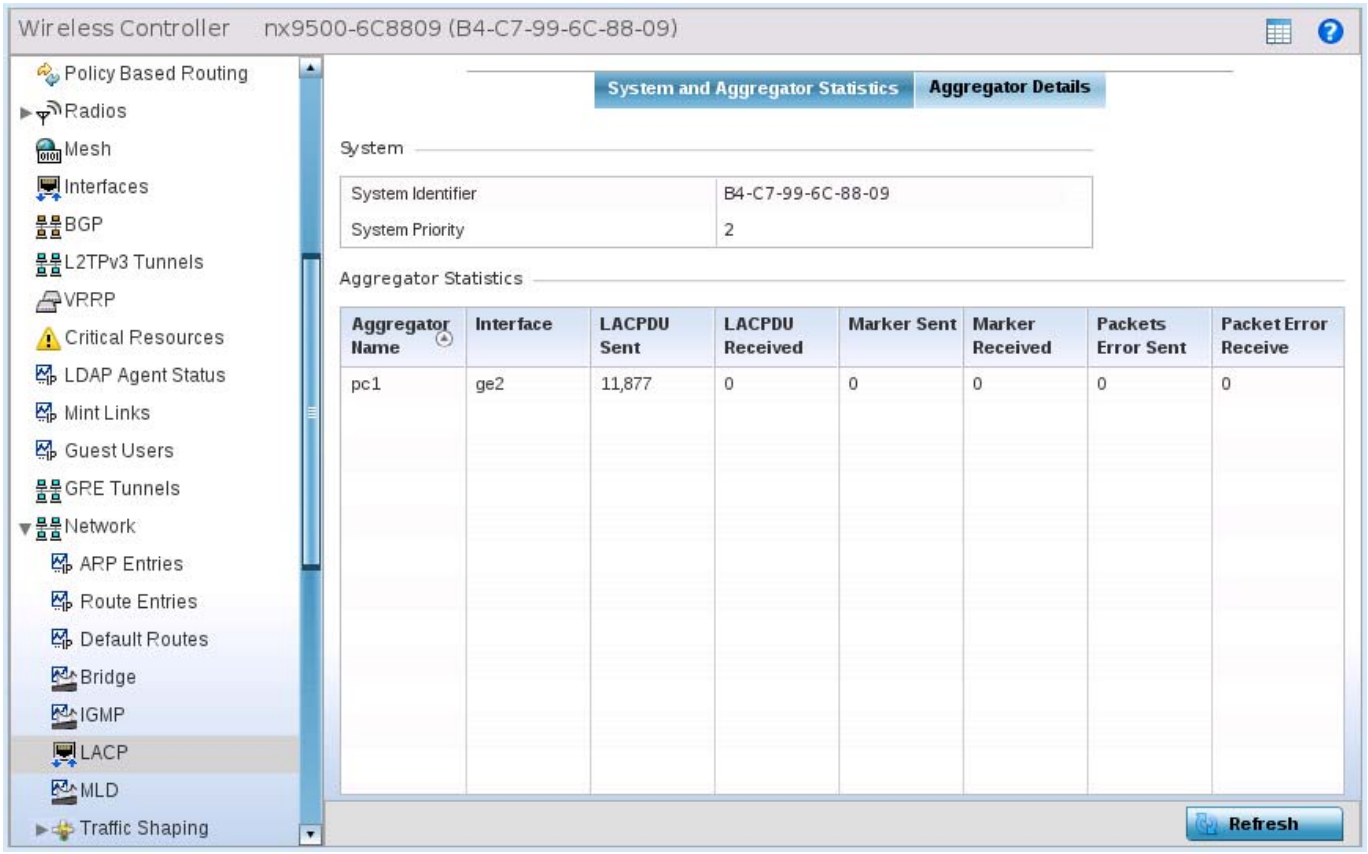


Figure 15-105 *Wireless Controller - Network LACP - System And Aggregator Statistics screen*

The **System** field describes the following:

System Identifier	Displays the MAC address of the device.
System Priority	Displays the system's LACP priority value.

The **Aggregator Statistics** field describes the following:

Aggregator Name	Displays the name of the port channel configured on this device.

Interface	Displays the name of the interface for which these statistics are being displayed.
LACPDU Sent	Displays the number of Link Aggregation Control Protocol Data Units (LACPDUs) sent from this device.
LACPDU Received	Displays the number of LACPDUs received by this device.
Marker Sent	Displays the number of marker packets sent. Marker packets are sent to the remote device to ensure that all frames transmitted through the link have been received.
Marker Received	Displays the number of marker packet responses received from the remote device.
Packets Error Sent	Displays the total number packets transmitted with error
Packets Error Received	Displays the total number packets received with error

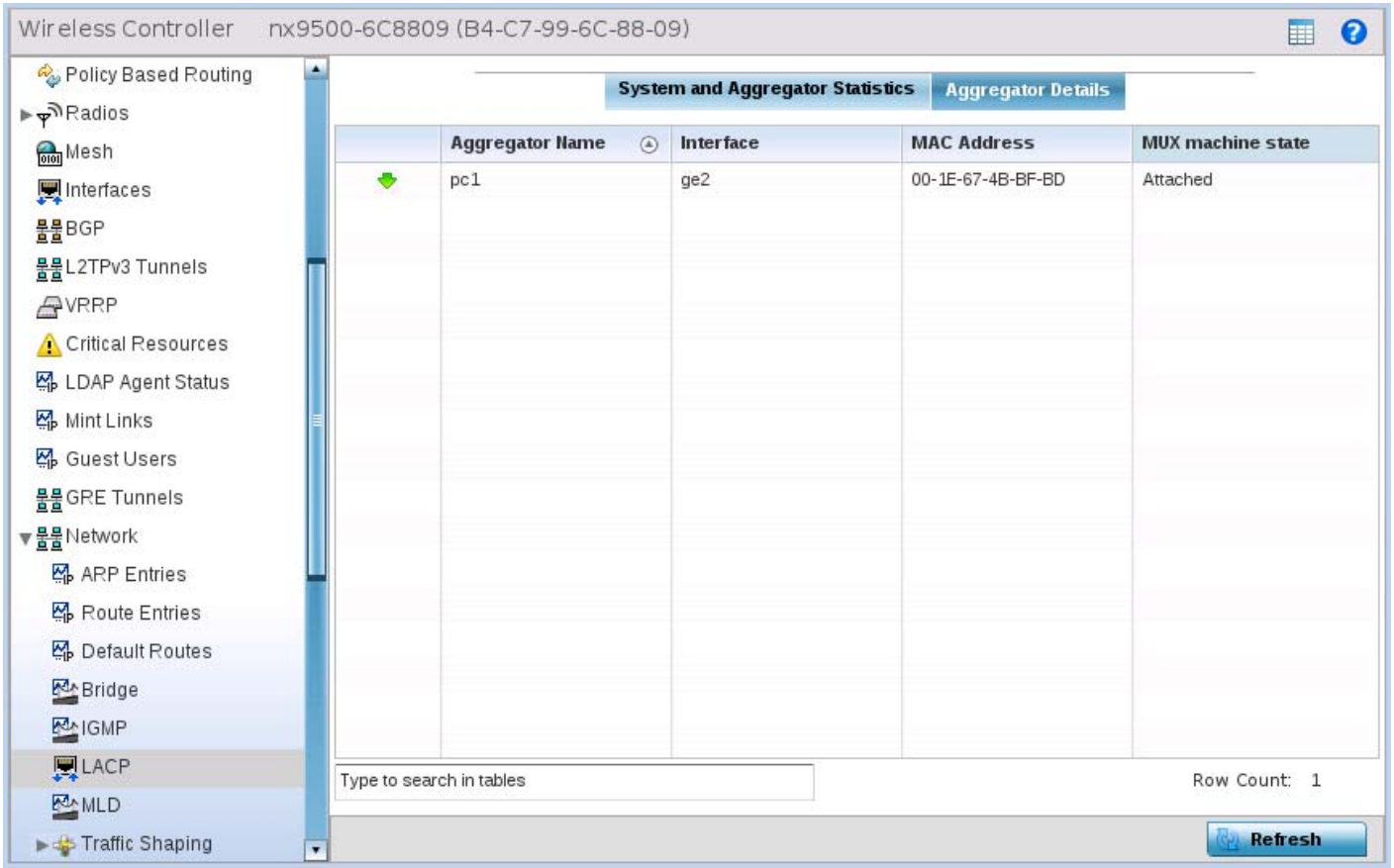


Figure 15-106 *Wireless Controller - Network LACP screen - Aggregator Details tab*

5 Select the **Aggregator Details** tab. This field describes the following:

Aggregator Name	Displays the name of the link aggregator (LAG).
Interface	Displays the name of the interface that is a member of the LAG.
MAC Address	Displays the MAC address of the physical interface.

MUX machine state	Displays the state of the multiplexer state machine for the aggregation port. The values are: • attached – Displays the state as attached, when the multiplexer state machine is initiating the process of attaching the port to the selected aggregator. • detached – Displays the state as detached, when the multiplexer state machine is initiating the process of detaching the port from the aggregator. • collecting/distributing – Displays the state as collecting/distributing. Collecting and distributing states are merged together to form a combined state (coupled control). Because independent control is not possible, the coupled control state machine does not wait for the partner to signal that collection has started before enabling both collection and distribution.

15.3.30.8 Traffic Shaping

Network

Traffic shaping regulates network data transfers to ensure a specific performance level. Traffic shaping delays the flow of packets defined as less important than prioritized traffic streams. Traffic shaping enables traffic control out an interface to match its flow to the speed of a remote target's interface and ensure traffic conforms applied policies. Traffic can be shaped to meet downstream requirements and eliminate network congestion when data rates are in conflict.

Apply traffic shaping to specific applications to apply application categories. When application and ACL rules are conflicting, an application takes precedence over an application category, then ACLs.

To view network the controller or service platform's traffic shaping configuration:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **Traffic Shaping**. The Status screen displays by default, and lists the controller or service platform's traffic shaping status.

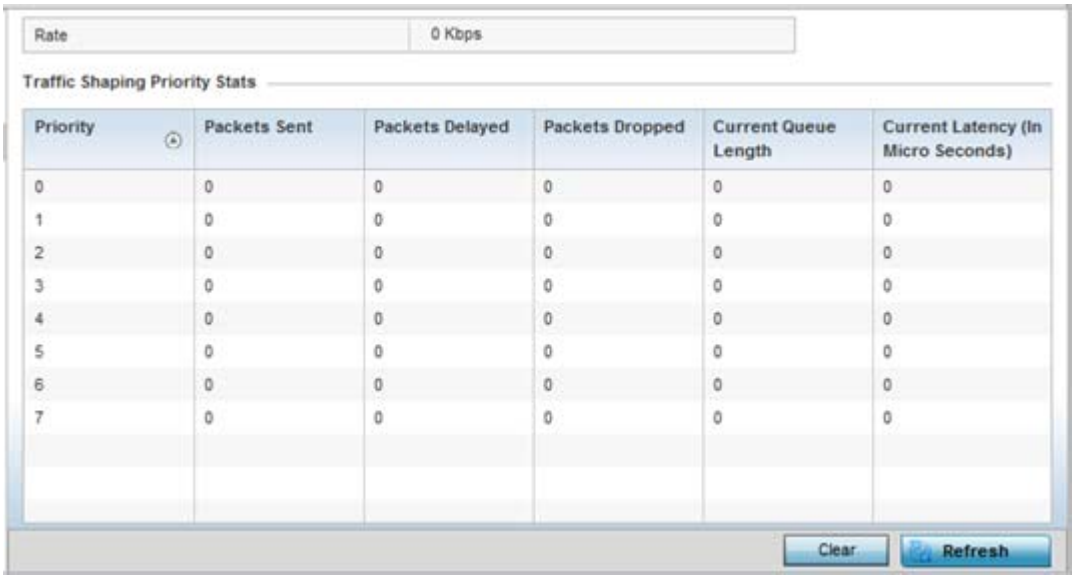


Figure 15-107 *Wireless Controller - Network Traffic Shaping screen*

5 Select **Statistics**.

6 Refer to the following **Traffic Shaping** statistics:

Rate	The rate configuration controls the maximum traffic rate sent or received on an interface. Consider this form of rate limiting on interfaces at the edge of a network to limit traffic into or out of the network. Traffic within the set limit is sent and traffic exceeding the set limit is dropped or sent with a different priority.
Priority	Lists the traffic shaper queue priority. There are 8 queues (0 - 7), and traffic is queued in each based on incoming packets 802.1p markings.
Packets Sent	Provides a baseline of the total number of packets sent to assess packet delays and drops as a result of the filter rules applied in the traffic shaping configuration.
Packets Delayed	Lists the packets defined as less important than prioritized traffic streams and delayed as a result of traffic shaping filter rules applied.
Packets Dropped	Lists the packets defined as less important than prioritized traffic streams, delayed and eventually dropped as a result of traffic shaping filter rules applied.
Current Length	Lists the packet length of the data traffic *shaped* to meet downstream requirements.
Current Latency	Traffic shaping latency is the time limit after which packets start dropping as a result of the traffic prioritization filter rules applied.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.30.9 DHCP Options

Network

Controllers and service platforms contain an internal *Dynamic Host Configuration Protocol* (DHCP) server. The DHCP server can provide the dynamic assignment of IP addresses automatically from existing address pools. This

is a protocol that includes IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters include IP address, gateway and network mask.

To view network DHCP options:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **DHCP Options**.

Figure 15-108 *Wireless Controller - Network DHCP Options screen*

The **DHCP Options** screen describes the following:

Server Information	Lists server information specific to each DHCP server resource available to requesting clients for the dynamic assignment of IP addresses.
Image File	Displays the image file name. BOOTP or the bootstrap protocol can be used to boot diskless clients. An image file is sent from the boot server. The file contains the operating system image. DHCP servers can be configured to support BOOTP.
Configuration	Displays the name of the configuration file on the DHCP server.
Legacy Adoption	Displays legacy (historical) device adoption information.
Adoption	Displays pending (current) adoption information.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.30.10 Cisco Discovery Protocol

Network

The *Cisco Discovery Protocol* (CDP) is a proprietary Data Link Layer network protocol implemented in Cisco networking equipment and used to share information about network devices.

To view a controller or service platform's CDP Statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **Cisco Discovery Protocol**.

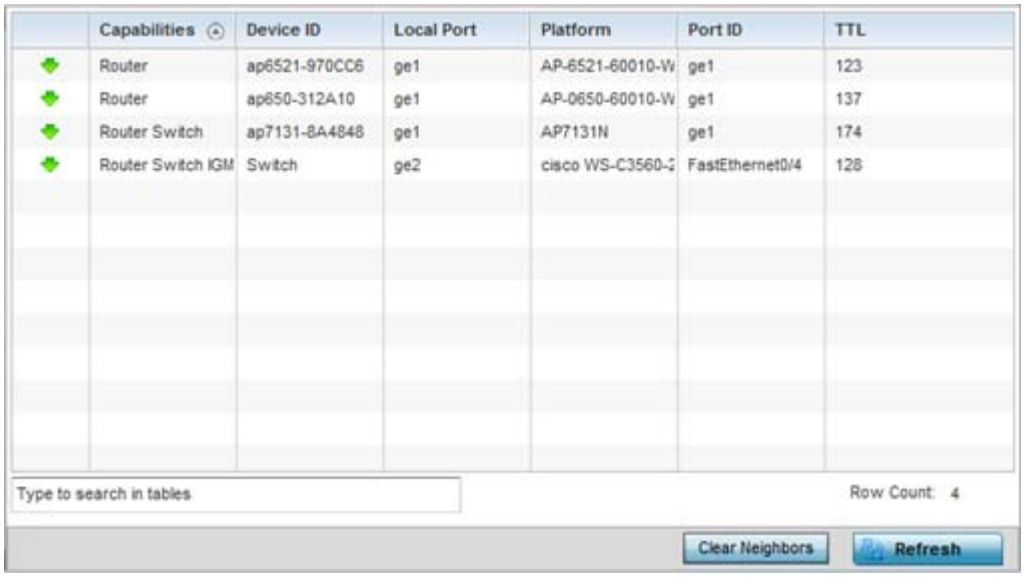


Figure 15-109 *Wireless Controller - Network CDP screen*

The **Cisco Discovery Protocol** screen displays the following:

Capabilities	Displays the capabilities code for Cisco neighbors.
Device ID	Displays the configured device ID or name for each device in the table.
Local Port	Displays the local port name for each CDP capable device.
Platform	Displays the model number of the CDP capable device.
Port ID	Displays the identifier for the local port.
TTL	Displays the *time to live* (TTL) for each CDP connection.
Clear Neighbors	Click *Clear Neighbors* to remove all known CDP neighbors from the table.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.30.11 Link Layer Discovery Protocol

Network

The *Link Layer Discovery Protocol* (LLDP) or IEEE 802.1AB is a vendor-neutral data link layer protocol used by network devices for advertising of (announcing) their identity, capabilities, and interconnections on a IEEE 802 LAN network. The protocol is formally referred to by the IEEE as *Station and Media Access Control Connectivity Discovery*.

To view a controller or service platform's Link Layer Discovery Protocol statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **Link Layer Discovery Protocol**.

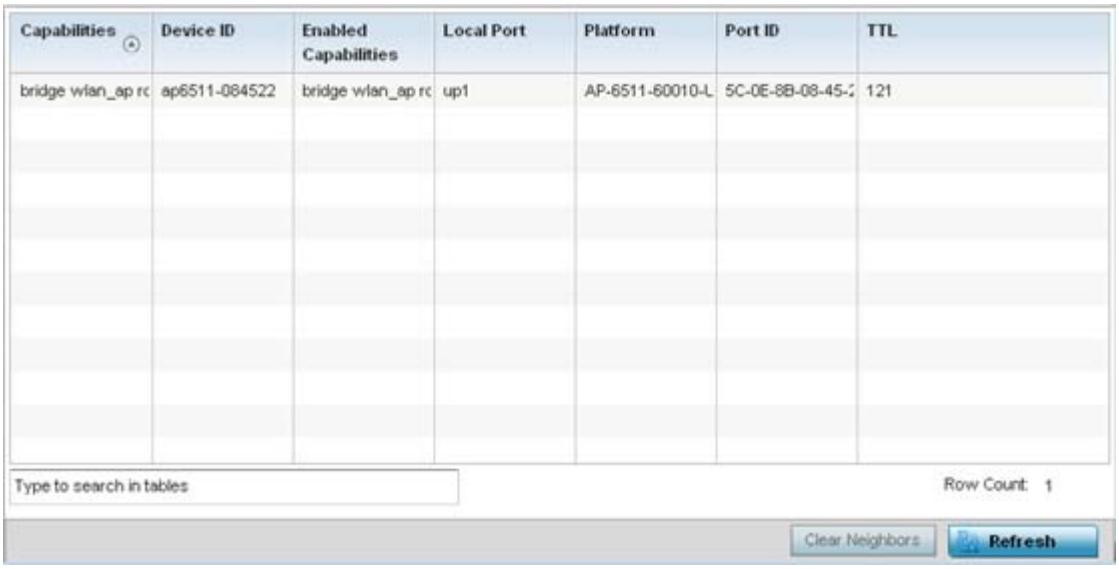


Figure 15-110 *Wireless Controller - Network LLDP screen*

The **Link Layer Discovery Protocol** screen displays the following:

Capabilities	Displays the Access Point capabilities code.
Device ID	Displays the configured device ID or name for each device in the table.
Enabled Capabilities	Displays which LLDP capabilities are currently utilized by the listed device.
Local Port	Displays the physical local port name for each LLDP capable device.
Platform	Displays the model number of the LLDP capable device and its firmware load.
Port ID	Displays the identifier for the local port.
TTL	Displays the *time to live* (TTL) for each LLDP connection.
Clear Neighbors	Click *Clear Neighbors* to remove all known LLDP neighbors from the table.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.30.12 IPv6 Neighbor Discovery

Network

IPv6 neighbor discovery uses ICMP messages and solicited multicast addresses to find the link layer address of a neighbor on the same local network, verify the neighbor's reachability and track neighboring devices.

Upon receiving a neighbor solicitation message, the destination replies with *neighbor advertisement* (NA). The source address in the advertisement is the IPv6 address of the device sending the message. The destination address in the advertisement message is the IPv6 address of the device sending the neighbor solicitation. The data portion of the NA includes the link layer address of the node sending the neighbor advertisement.

Neighbor solicitation messages also verify the availability of a neighbor once its the link layer address is identified. When a node wants to verify the reachability of a neighbor, the destination address in a neighbor solicitation message is the unicast address of the neighbor.

A neighbor is interpreted as reachable when an acknowledgment is returned indicating packets have been received and processed. If packets are reaching the device, they're also reaching the next hop neighbor, providing a confirmation the next hop is reachable.

To view a controller or service platform's IPv6 neighbor statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **IPv6 Neighbor Discovery**.

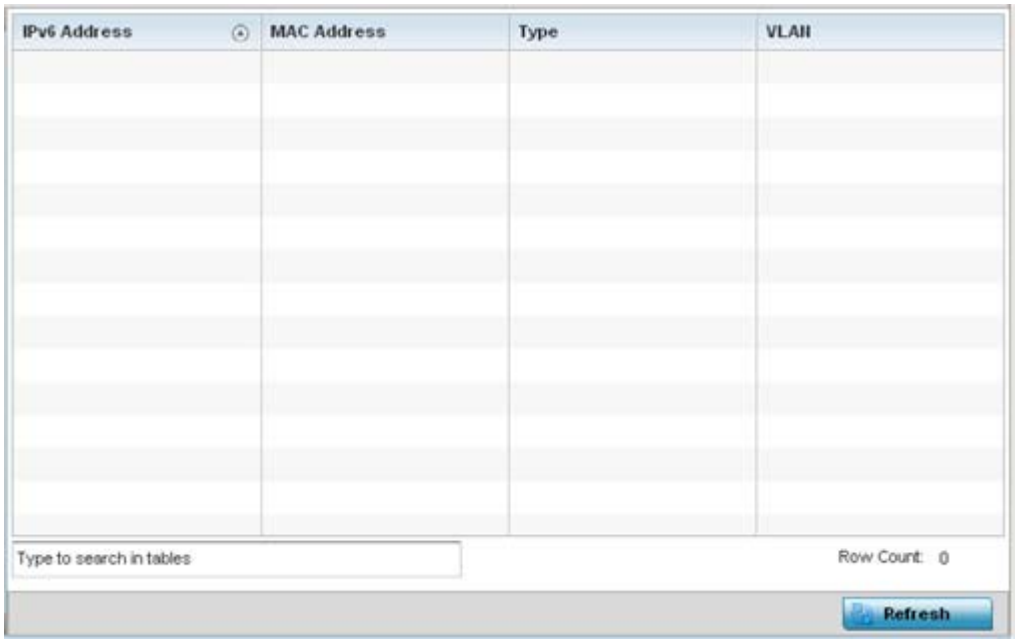


Figure 15-111 *Wireless Controller - Network IPv6 Neighbor screen*

The **IPv6 Neighbor** screen displays the following:

IPv6 Address	Lists an IPv6 IP address for neighbor discovery. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via CMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
MAC Address	Lists the factory encoded hardware MAC address of the neighbor device using an IPv6 formatted IP address as its network identifier.
Type	Displays the device type for the neighbor solicitation. Neighbor solicitations request the link layer address of a target node while providing the sender's own link layer address to the target. Neighbor solicitations are multicast when the node needs to resolve an address and unicast when the node seeks to verify the reachability of a neighbor. Options include *Host, Router* and *DHCP Server.*
VLAN	Lists the virtual interface (from 1 - 4094) used for the required neighbor advertisements and solicitation messages used for neighbor discovery.

Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.30.13 MSTP

Network

The *Multiple Spanning Tree Protocol* (MSTP) provides an extension to RSTP to optimize the usefulness of VLANs. MSTP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.

If there's just one VLAN in the Access Point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it's possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

MSTP includes all of its spanning tree information in a single *Bridge Protocol Data Unit* (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. MSTP encodes additional region information after the standard RSTP BPDU as well as a number of MSTI messages. Each MSTI messages conveys spanning tree information for each instance. Each instance can be assigned a number of configured VLANs. The frames assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, the Access Point encodes an MD5 digest of their VLAN to an instance table in the MSTP BPDU. This digest is used by other MSTP supported devices to determine if the neighboring device is in the same MST region as itself.

To view a controller or service platform's MSTP statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **MSTP.**

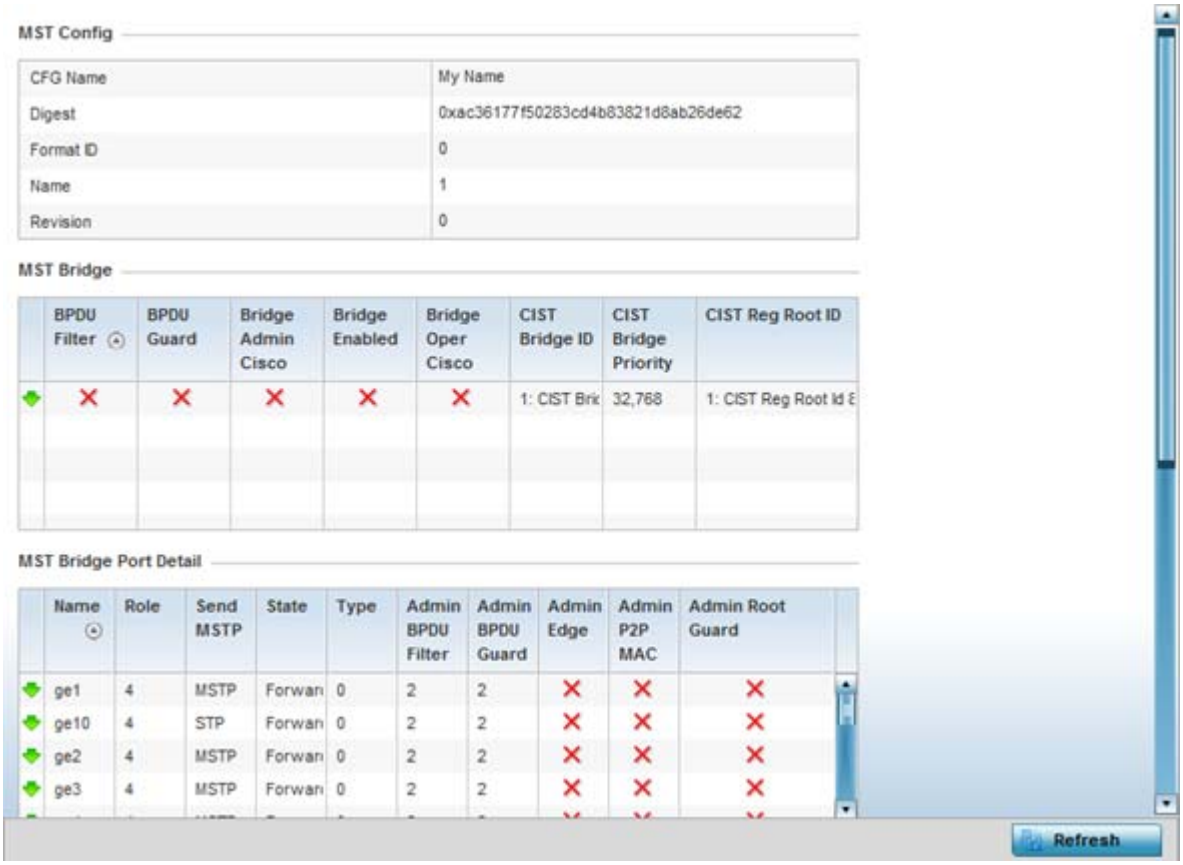


Figure 15-112 *Wireless Controller - Network MSTP screen*

The **MST Config** field displays the name assigned to the MSTP configuration, its digest, format ID, name and revision.

The **MST Bridge** field lists the filters and guards that have been enabled and whether Cisco interoperability if enabled.

The **MST Bridge Port Detail** field lists specific controller or service platform port status and their current state.

15.3.31 DHCPv6 Relay & Client

Controller Statistics

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. DHCPv6 relay agents receive messages from clients and forward them a DHCPv6 server. The server sends responses back to the relay agent and the relay agent sends the responses to the client on the local link.

To assess the DHCPv6 relay configuration:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **DHCP Relay & Client** from the left-hand side of the UI.

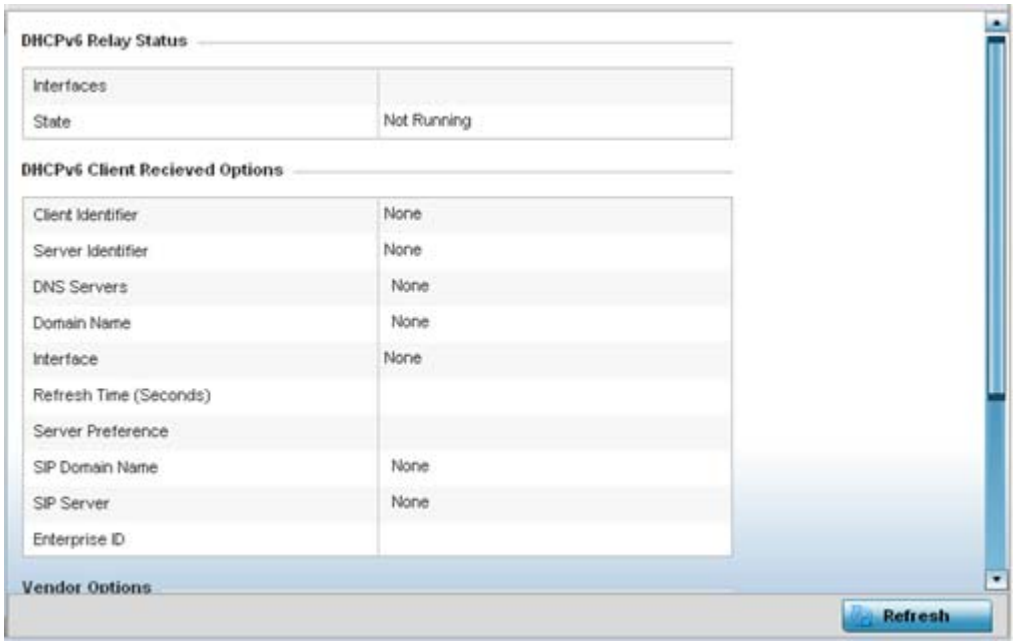


Figure 15-113 *Wireless Controller - DHCPv6 Relay and Client screen*

4 The **DHCPv6 Relay Status** tables defines the following:

Interfaces	Displays the controller or service platform interface used for DHCPv6 relay.
State	Displays the current operational state of the DHCPv6 server to assess its availability as a viable IPv6 provisioning resource.

5 The **DHCPv6 Client Received Options** tables defines the following:

Client Identifier	Lists whether the reporting client is using a *hardware address* or *client identifier* as its identifier type within requests to the DHCPv6 server.
Server Identifier	Displays the server identifier supporting client DHCPv6 relay message reception.
DNS Servers	Lists the DNS server resources supporting relay messages received from clients.
Domain Name	Lists the domain to which the remote server resource belongs.
Interface	Displays the interfaces dedicated to client DHCPv6 relay message reception.
Refresh Time (Seconds)	Lists the time (in seconds) since the data populating the DHCPv6 client received options table has been refreshed.
Server Preference	Lists the preferred DHCPv6 server resource supporting relay messages received from clients.
SIP Domain Name	Lists the SIP domain name supporting DHCPv6 client telephone extensions or voice over IP systems.
SIP Server	Displays the SIP server name supporting DHCPv6 telephone extensions or voice over IP systems.
Enterprise ID	Lists the enterprise ID associated with DHCPv6 received client options.

6 Refer to the **Vendor Options** table for the following:

Code	Lists the relevant numeric DHCP vendor code.
Data	Lists the supporting data relevant to the listed DHCP vendor code.

7 Select the **Refresh** button to update the screen's statistics counters to their latest values.

15.3.32 DHCP Server

Controller Statistics

Controllers and service platforms contain an internal *Dynamic Host Configuration Protocol* (DHCP) server. DHCP can provide IP addresses automatically. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters (IP address, network mask gateway etc.) from a DHCP server to a host.

To review DHCP server statistics, refer to the following:

- *Viewing General DHCP Information*
- *Viewing DHCP Binding Information*
- *Viewing DHCP Server Networks Information*

15.3.32.1 Viewing General DHCP Information

DHCP Server

To view *General* DHCP status and binding information for both DHCPv4 and DHCPv6:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller from the left navigation pane.

3 Expand the **DHCP Server** menu from the left-hand side of the UI.

4 Select **General.**

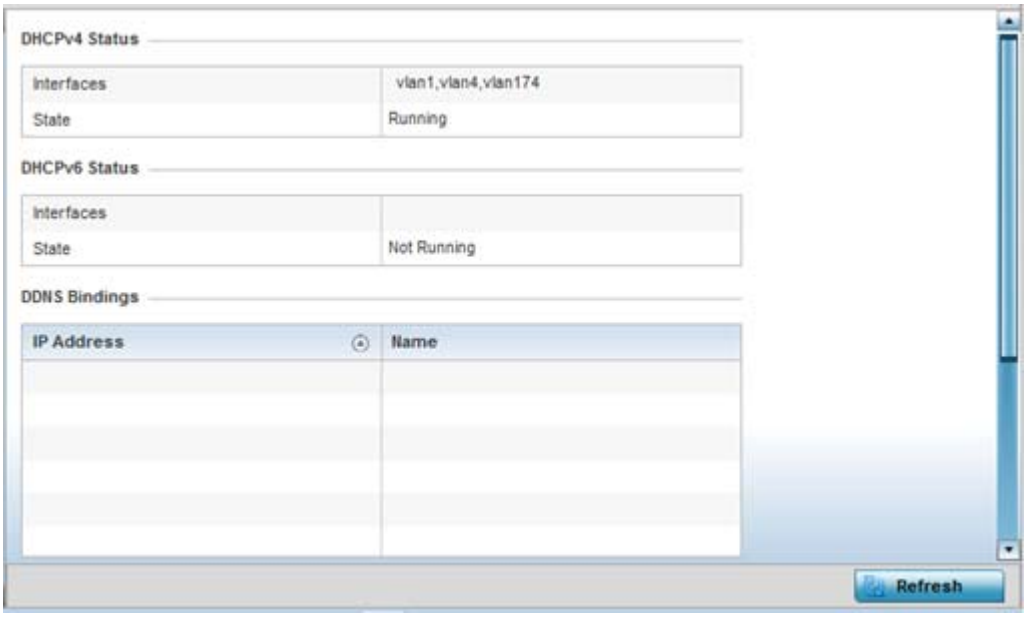


Figure 15-114 *Wireless Controller - DHCP Server General screen*

5 The **DHCPv4 Status** and **DHCPv6 Status** tables defines the following:

Interfaces	Displays the controller or service platform interface used with the DHCPv4 or DHCPv6 resource for IP address provisioning.
State	Displays the current operational state of the DHCPv4 or DHCPv6 server to assess its availability as a viable IP provisioning resource.

6 The **DDNS Bindings** table displays the following:

IP Address	Displays the IP address assigned to the requesting client.
Name	Displays the domain name mapping corresponding to the listed IP address.

7 The **DHCP Manual Bindings** table displays the following:

IP Address	Displays the IP address for clients requesting DHCP provisioning resources.
Client Id	Displays the client's ID used to differentiate requesting clients.

8 Select the **Refresh** button to update the screen's statistics counters to their latest values.

15.3.32.2 Viewing DHCP Binding Information

DHCP Server

The *DHCP Binding* screen displays DHCP binding information such as expiry time, client IP addresses and their MAC address.

Controllers and service platforms build and maintain a DHCP snooping table (DHCP binding database). A controller or service platform uses the snooping table to identify and filter untrusted messages. The DHCP binding database keeps track of DHCP addresses assigned to ports, as well as filtering DHCP messages from untrusted ports. Incoming packets received on untrusted ports, are dropped if the source MAC address does not match the MAC in the binding table.

To view the DHCP binding information:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **DHCP Server** menu from the left-hand side of the UI.

4 Select **Bindings.**

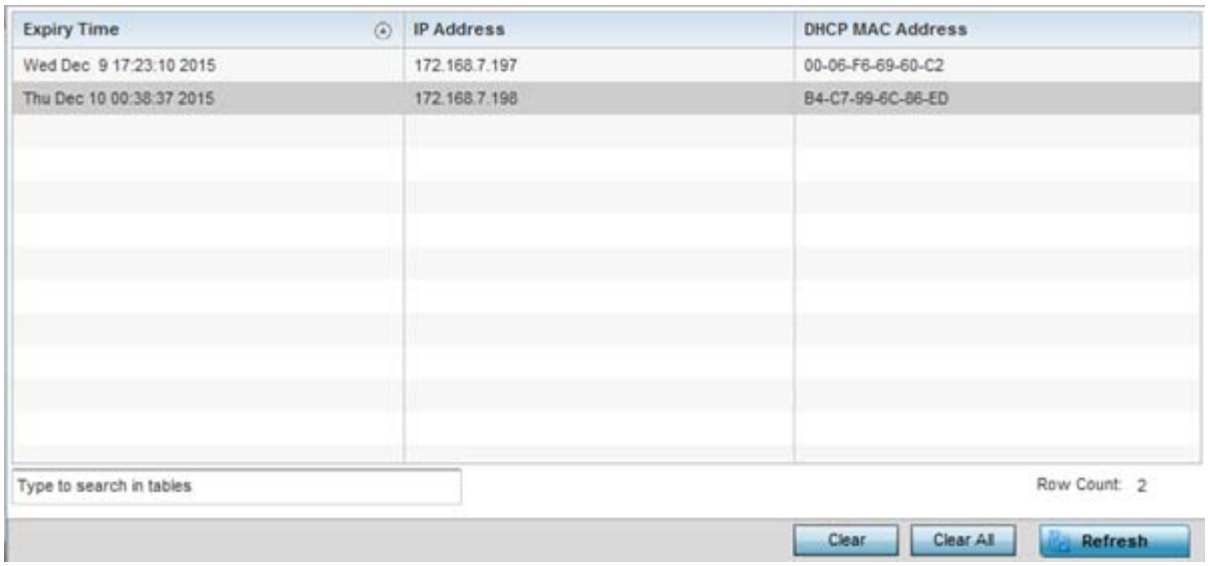


Figure 15-115 *Wireless Controller - DHCP Server Bindings screen*

The **Bindings** screen displays the following:

Expiry Time	Displays the expiration of the lease used by the client for controller or service platform DHCP resources.
IP Address	Displays the IP address of each listed client requesting DHCP services.
DHCP MAC Address	Displays the MAC address of each listed client requesting DHCP services.
Clear	Select a table entry and select *Clear* to remove the client from the list of devices requesting DHCP services from the controller or service platform.
Clear All	Select *Clear All* to remove all listed clients from the list of requesting clients.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.32.3 Viewing DHCP Server Networks Information

DHCP Server

The DHCP server maintains a pool of IP addresses and client configuration parameters (default gateway, domain name, name servers etc). On receiving a valid client request, the server assigns the requestor an IP address, a lease (the validity of time), and other IP configuration parameters.

The *Networks* screen provides network pool information such as the subnet for the addresses you want to use from the pool, the pool name, the used addresses and the total number of addresses.

To view the **DHCP Server Networks** information:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **DHCP Server** menu from the left-hand side of the UI.

4 Select **Networks.**

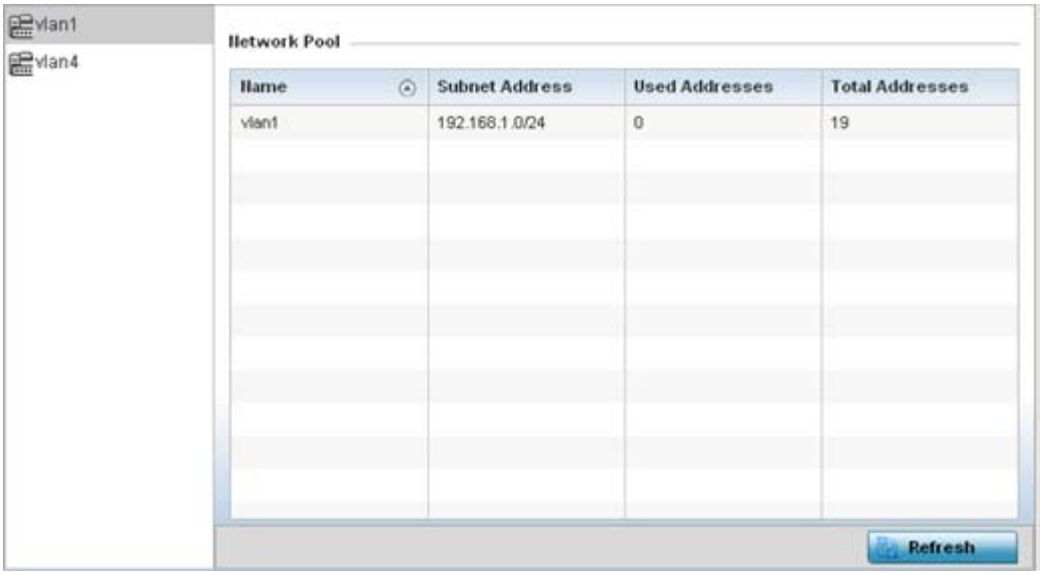


Figure 15-116 *Wireless Controller - DHCP Server Networks screen*

The **Networks** screen displays the following:

Name	Displays the name of the virtual network (VLAN) from which IP addresses can be issued to DHCP client requests on the listed controller or service platform interface.
Subnet Address	Displays the subnet for the IP addresses used from the network pool.
Used Addresses	Displays the number of host IP addresses allocated by the DHCP server.
Total Addresses	Displays the total number of IP addresses available in the network pool for requesting clients.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.33 Firewall

Controller Statistics

A firewall is designed to block unauthorized access while permitting authorized communications. It's a device or a set of devices configured to permit or deny computer applications based on a set of rules. For more information, refer to the following:

- *Viewing Packet Flow Statistics*
- *Viewing Denial of Service Statistics*
- *IP Firewall Rules*
- *IPv6 Firewall Rules*
- *MAC Firewall Rules*
- *NAT Translations*
- *Viewing DHCP Snooping Statistics*
- *IPv6 Neighbor Snooping*

15.3.33.1 Viewing Packet Flow Statistics

Firewall

The *Packet Flows* screen displays data traffic packet flow utilization. The chart lists the different protocol flows supported, and displays a proportional view of the flows in respect to their percentage of data traffic utilized. The *Total Active Flows* field displays the total number of flows supported by the controller or service platform.

To view the packet flow statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Firewall** menu from the left-hand side of the UI.

4 Select **Packets Flows.**

Select **Clear All** to revert the statistics counters to zero and begin a new data collection, or select **Refresh** to update the display to the latest values.

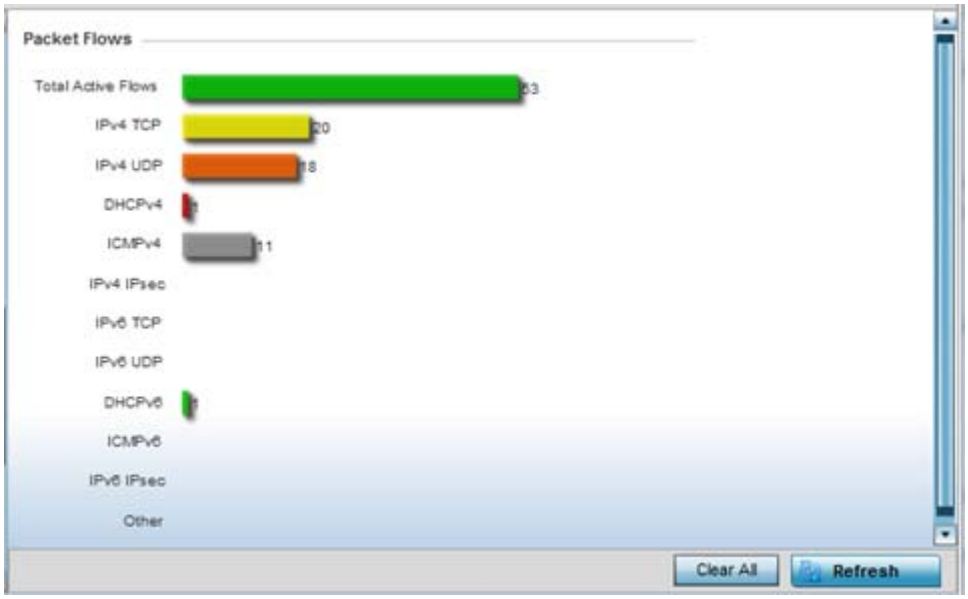


Figure 15-117 *Firewall Packet Flows*

15.3.33.2 Viewing Denial of Service Statistics

Firewall

A *denial-of-service attack* (DoS attack), or distributed denial-of-service attack, is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out a DoS attack may vary, it generally consists of a concerted effort to prevent an Internet site or service from functioning efficiently.

One common attack involves saturating the target's (victim's) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service.

The *Denial of Service* screen displays attack type, number of occurrences, and time of last occurrence.

To view the denial of service statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Firewall** menu from the left-hand side of the UI.

4 Select **Denial of Service.**

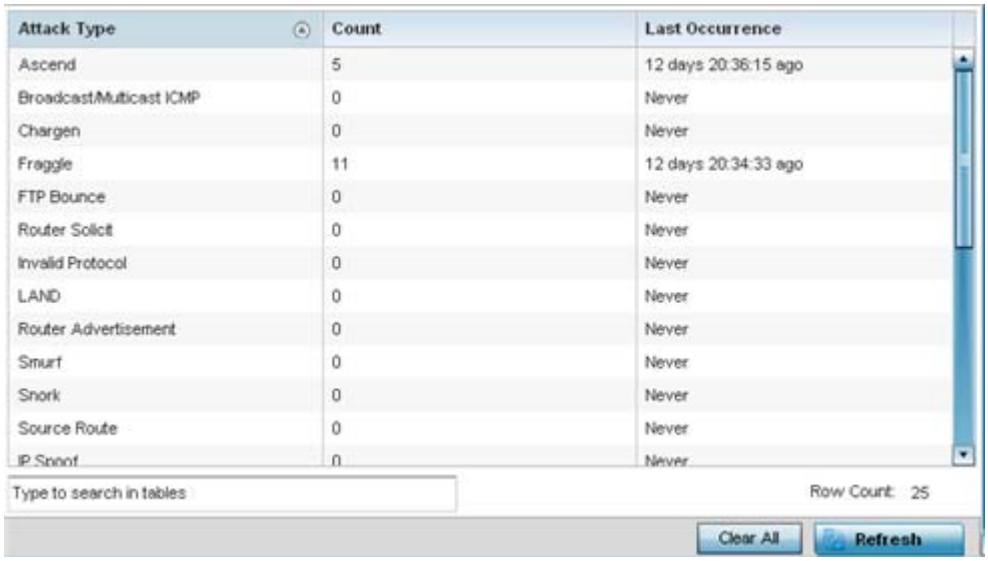


Figure 15-118 *Wireless Controller - Firewall DoS screen*

The **Denial of Service** screen displays the following:

Attack Type	Displays the DoS attack type. The controller or service platform supports enabling or disabling 24 different DoS attack filters.
Count	Displays the number of times each DoS attack was observed by the controller or service platform's firewall.
Last Occurrence	Displays the amount of time since the DoS attack has been observed by the controller or service platform's firewall.
Clear All	Select *Clear All* to revert the statistics counters to zero and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.33.3 IP Firewall Rules

Firewall

Create firewall rules to let any computer send IPv4 traffic to, or receive traffic from, programs, system services, computers or users. Firewall rules can be created to provide one of the three actions listed below that match the rule's criteria:

- *Allow a connection*
- *Allow a connection only if it is secured through the use of Internet Protocol security*
- *Block a connection*

Rules can be created for either inbound or outbound traffic.

To view existing IPv4 firewall rules:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Firewall** menu from the left-hand side of the UI.

4 Select **IP Firewall Rules.**

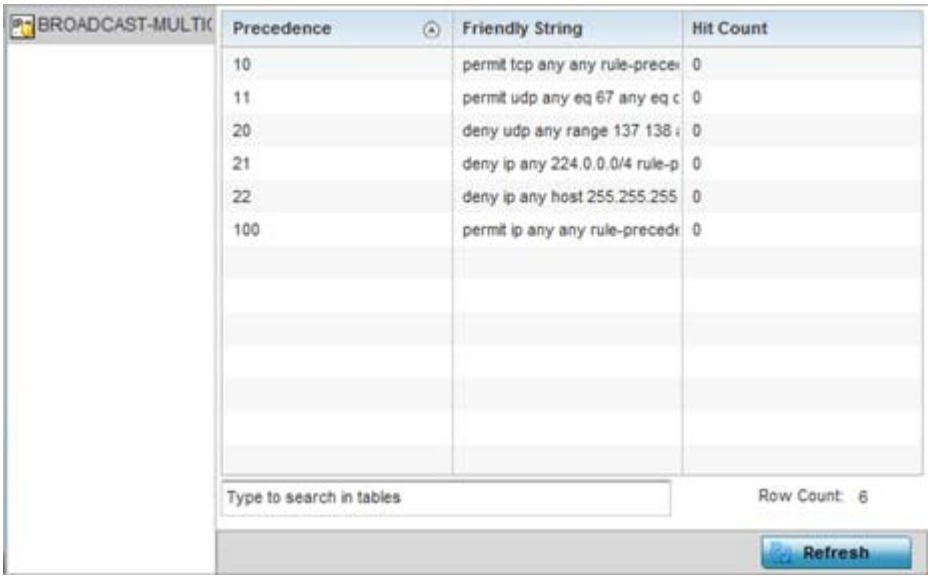


Figure 15-119 *Wireless Controller - Firewall IP Firewall Rules screen*

The **IP Firewall Rules** screen displays the following:

Precedence	Displays the precedence (priority) applied to packets. Every rule has a unique precedence value between 1 - 5000. You cannot add two rules with the same precedence value.
Friendly String	This is a string that provides more information as to the contents of the rule. This is for information purposes only.
Hit Count	Displays the number of times each IP ACL has been triggered.
Hardware Hit Count	On NX4500 and NX6500 series service platforms, intra-vlan packets are switched locally (on the service platform), preventing ACL or stateful firewall inspection. However, a unique ACL is available on NX4500 and NX6500 service platform GE ports providing a stateless firewall using IP based ACLs. The *Hardware Hit Count* constitutes the number of times one of the service platform's 1024 IP hardware rules has been triggered on one of its GE ports. NX4500 and NX6500 models have 2 GE ports, and NX4524 and NX6524 models have 24 GE ports.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.33.4 IPv6 Firewall Rules

Firewall

IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. These hosts require firewall packet protection unique to IPv6 traffic, as IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the *neighbor discovery* (ND) protocol via ICMPv6 router discovery

messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet layer configuration parameters.

- *Allow an IPv6 formatted connection*
- *Allow a connection only if it is secured through the use of IPv6 security*
- *Block a connection and exchange of IPv6 formatted packets*

To view existing IPv6 firewall rules:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Firewall** menu from the left-hand side of the UI.

4 Select **IPv6 Firewall Rules.**

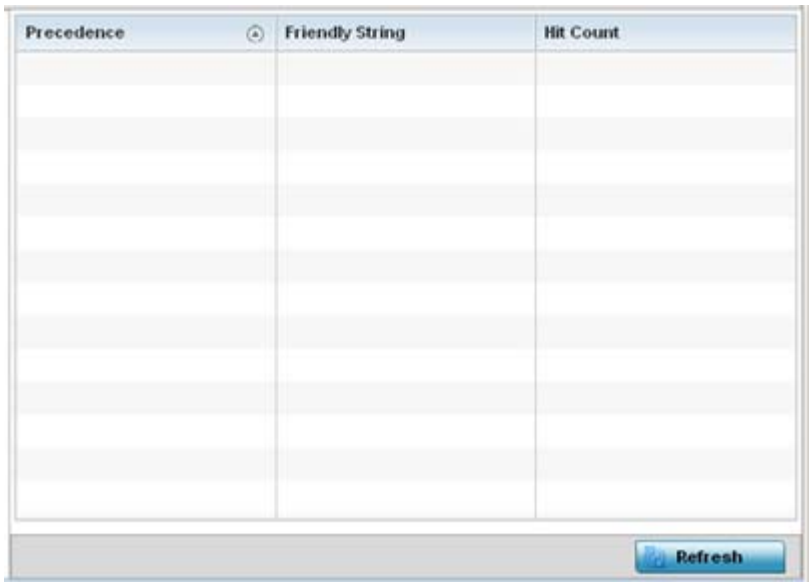


Figure 15-120 *Wireless Controller - Firewall IPv6 Firewall Rules screen*

The **IPv6 Firewall Rules** screen displays the following:

Precedence	Displays the precedence (priority) applied to IPV6 formatted packets. Unlike IPv4, IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. Every rule has a unique precedence value between 1 - 5000. You cannot add two rules with the same precedence value.
Friendly String	This is a string that provides more information as to the contents of the IPv6 specific IP rule. This is for information purposes only.
Hit Count	Displays the number of times each IPv6 ACL has been triggered.

Hardware Hit Count	On NX4500 and NX6500 series service platforms, intra-vlan packets are switched locally (on the service platform), preventing ACL or stateful firewall inspection. However, a unique ACL is available on NX4500 and NX6500 service platform GE ports providing a stateless firewall using IP based ACLs. The *Hardware Hit Count* constitutes the number of times one of the service platform's 1024 IP hardware rules has been triggered on one of its GE ports. NX4500 and NX6500 models have 2 GE ports, and NX4524 and NX6524 models have 24 GE ports.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.33.5 MAC Firewall Rules

Firewall

The ability to allow or deny client access by MAC address ensures malicious or unwanted users are unable to bypass security filters. Firewall rules can use one of the three following actions based on a rule criteria:

- *Allow a connection*
- *Allow a connection only if it is secured through the MAC firewall security*
- *Block a connection*

To view MAC firewall rules:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Firewall** menu from the left-hand side of the UI.

4 Select **MAC Firewall Rules.**

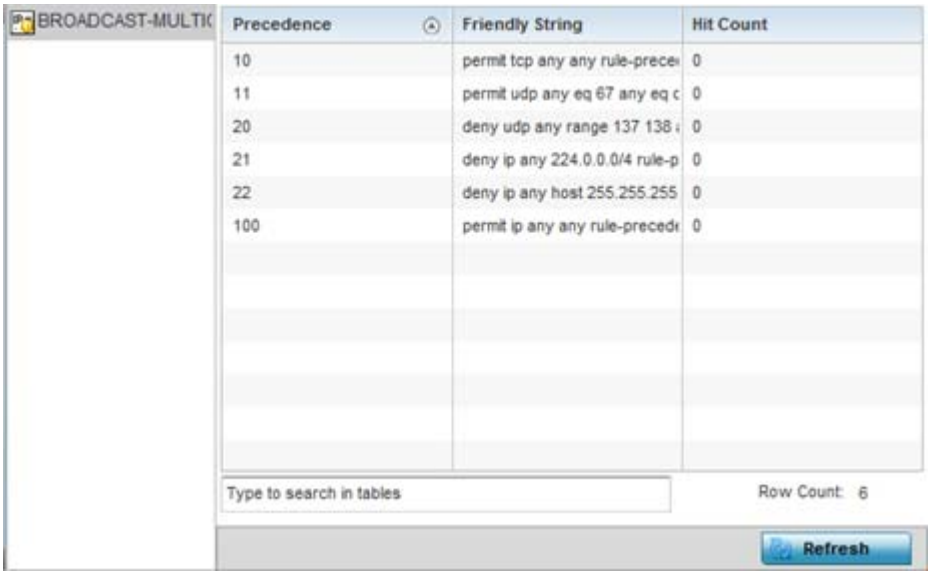


Figure 15-121 *Wireless Controller - Firewall MAC Firewall Rules screen*

The **MAC Firewall Rules** screen displays the following:

Precedence	Displays the precedence (priority) applied to packets. The rules within an *Access Control Entries* (ACL) list are based on their precedence values. Every rule has a unique precedence value between 1 and 5000. You cannot add two rules with the same precedence value.
Friendly String	This string provides more information as to the contents of the rule. This is for information purposes only.
Hit Count	Displays the number of times each WLAN ACL has been triggered.
Hardware Hit Count	On NX4500 and NX6500 series service platforms, intra-vlan packets are switched locally (on the service platform), preventing ACL or stateful firewall inspection. However, a unique ACL is available on NX4500 and NX6500 service platform GE ports providing a stateless firewall using MAC based ACLs. The *Hardware Hit Count* constitutes the number of times one of the service platform's 1024 MAC hardware rules has been triggered on one of its GE ports. NX4500 and NX6500 models have 2 GE ports, and NX4524 and NX6524 models have 24 GE ports.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.33.6 NAT Translations

Firewall

Network Address Translation (NAT) is a technique to modify network address information within IP packet headers in transit. This enables mapping one IP address to another to protect wireless controller managed network address credentials. With typical deployments, NAT is used as an IP masquerading technique to hide private IP addresses behind a single, public facing, IP address.

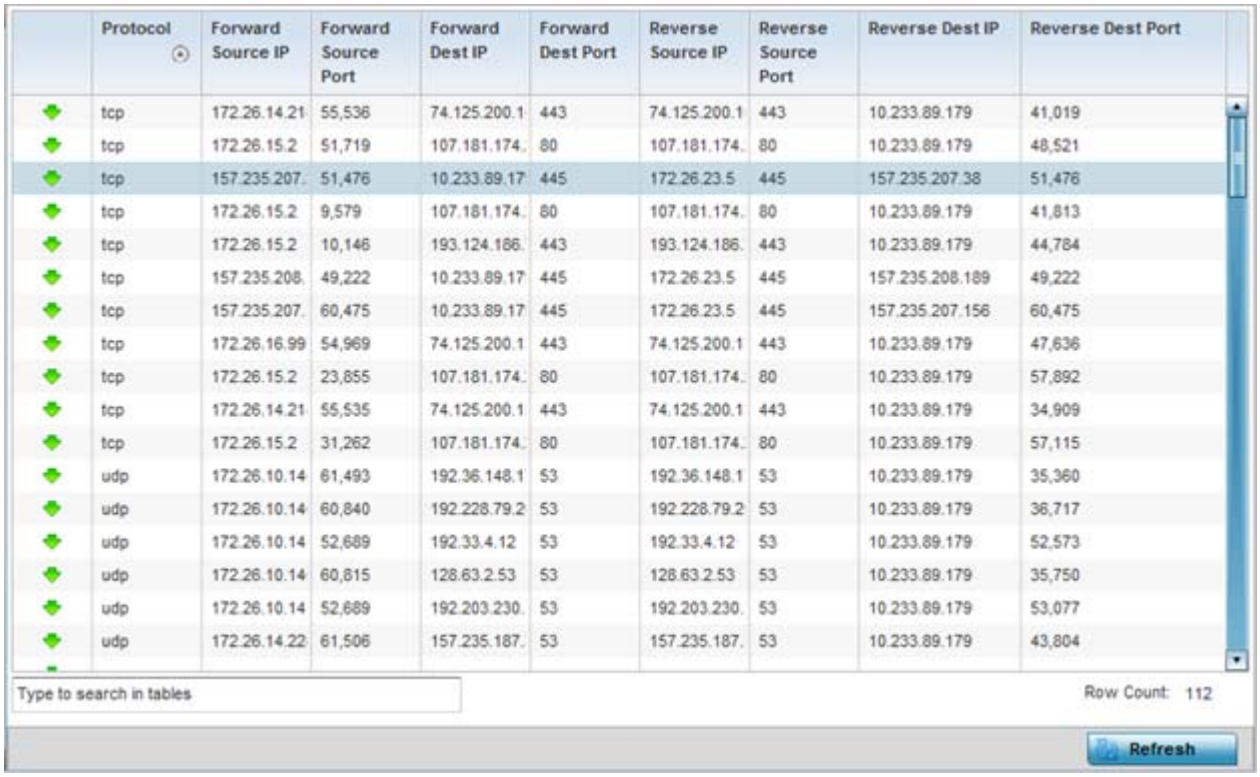
NAT can provide a profile outbound Internet access to wired and wireless hosts connected to either an Access Point or a wireless controller. Many-to-one NAT is the most common NAT technique for outbound Internet access. Many-to-one NAT allows an Access Point or wireless controller to translate one or more internal private IP addresses to a single, public facing, IP address assigned to a 10/100/1000 Ethernet port or 3G card.

To assess the controller or service platform's NAT configuration and statistics.

1 Select the Statistics menu from the Web UI.

2 Select an Access Point node from the left navigation pane.
Expand the Firewall menu from the left-hand side of the UI.

3 Select **NAT Translations.**



Protocol	Forward Source IP	Forward Source Port	Forward Dest IP	Forward Dest Port	Reverse Source IP	Reverse Source Port	Reverse Dest IP	Reverse Dest Port
tcp	172.26.14.21	55,536	74.125.200.1	443	74.125.200.1	443	10.233.89.179	41,019
tcp	172.26.15.2	51,719	107.181.174.	80	107.181.174.	80	10.233.89.179	48,521
tcp	157.235.207.	51,476	10.233.89.17	445	172.26.23.5	445	157.235.207.38	51,476
tcp	172.26.15.2	9,579	107.181.174.	80	107.181.174.	80	10.233.89.179	41,813
tcp	172.26.15.2	10,146	193.124.186.	443	193.124.186.	443	10.233.89.179	44,784
tcp	157.235.208.	49,222	10.233.89.17	445	172.26.23.5	445	157.235.208.189	49,222
tcp	157.235.207.	60,475	10.233.89.17	445	172.26.23.5	445	157.235.207.156	60,475
tcp	172.26.16.99	54,969	74.125.200.1	443	74.125.200.1	443	10.233.89.179	47,636
tcp	172.26.15.2	23,855	107.181.174.	80	107.181.174.	80	10.233.89.179	57,892
tcp	172.26.14.21	55,535	74.125.200.1	443	74.125.200.1	443	10.233.89.179	34,909
tcp	172.26.15.2	31,262	107.181.174.	80	107.181.174.	80	10.233.89.179	57,115
udp	172.26.10.14	61,493	192.36.148.1	53	192.36.148.1	53	10.233.89.179	35,360
udp	172.26.10.14	60,840	192.228.79.2	53	192.228.79.2	53	10.233.89.179	36,717
udp	172.26.10.14	52,689	192.33.4.12	53	192.33.4.12	53	10.233.89.179	52,573
udp	172.26.10.14	60,815	128.63.2.53	53	128.63.2.53	53	10.233.89.179	35,750
udp	172.26.10.14	52,689	192.203.230.	53	192.203.230.	53	10.233.89.179	53,077
udp	172.26.14.22	61,506	157.235.187.	53	157.235.187.	53	10.233.89.179	43,804

Figure 15-122 *Wireless Controller - Firewall NAT Translation screen*

4 The **NAT Translations** screen displays the following:

Protocol	Displays the translation protocol as either *TCP, UDP* or *ICMP.*
Forward Source IP	Displays the internal network IP address for forward facing NAT translations.
Forward Source Port	Displays the internal network (virtual) port for forward facing NAT translations.
Forward Dest IP	Displays the external network destination IP address for forward facing NAT translations.
Forward Dest Port	Displays the external network destination port for forward facing NAT translations.
Reverse Source IP	Displays the internal network IP address for reverse facing NAT translations.
Reverse Source Port	Displays the internal network port for reverse facing NAT translations.
Reverse Dest IP	Displays the external network destination IP address for reverse facing NAT translations.
Reverse Dest Port	Displays the external network destination port for reverse facing NAT translations.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.33.7 Viewing DHCP Snooping Statistics

Firewall

When DHCP servers are allocating IP addresses to the clients, DHCP snooping can strengthen the security on the LAN allowing only clients with specific IP/MAC addresses.

To view the DHCP snooping statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Firewall** menu from the left-hand side of the UI.

4 Select **DHCP Snooping.**

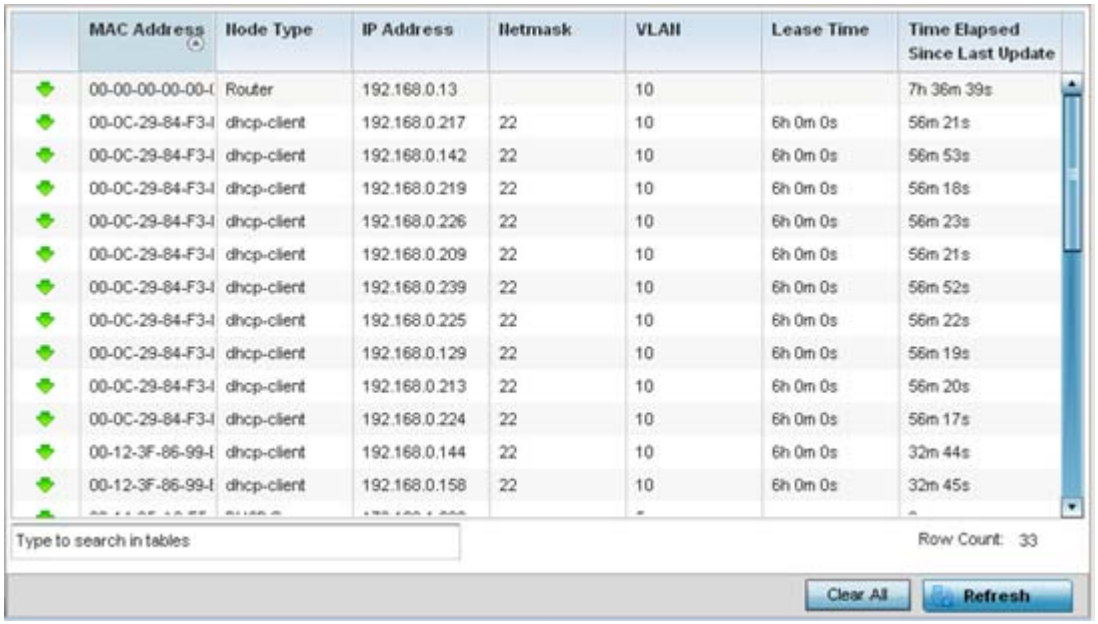


Figure 15-123 *Wireless Controller - Firewall DHCP Snooping screen*

The **DHCP Snooping** screen displays the following:

MAC Address	Displays the MAC address of the client.
Node Type	Displays the NetBios node with an IP pool from which IP addresses can be issued to client requests on this interface.
IP Address	Displays the IP address used for DHCP discovery and requests between the DHCP server and DHCP clients.
Netmask	Displays the subnet mask used for DHCP discovery and requests between the DHCP server and DHCP clients.
VLAN	Displays the controller or service platform virtual interface ID used for a new DHCP configuration.

Lease Time	When a DHCP server allocates an address for a DHCP client, the client is assigned a lease (which expires after a designated interval defined by the administrator). The lease is the time an IP address is reserved for re-connection after its last use. Using short leases, DHCP can dynamically reconfigure networks in which there are more computers than available IP addresses. This is useful, for example, in education and customer environments where client users change frequently. Use longer leases if there are fewer users.
Time Elapsed Since Last Update	Displays the amount of time elapsed since the DHCP server was last updated.
Clear All	Select *Clear All* to revert the counters to zero and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's counters to their latest values.

15.3.33.8 IPv6 Neighbor Snooping

Firewall

IPv6 snooping bundles layer 2 IPv6 hop security features, such as IPv6 *neighbor discovery* (ND) inspection, IPv6 address gleaning and IPv6 device tracking. When IPv6 ND is configured on a device, packet capture instructions redirect the ND protocol and DHCP for IPv6 traffic up to the controller for inspection.

A database of connected IPv6 neighbors is created from the IPv6 neighbor snoop. The database is used by IPv6 to validate the link layer address, IPv6 address and prefix binding of the neighbors to prevent spoofing and potential redirect attacks.

To review IPv6 neighbor snooping statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Expand the **Firewall** menu from the left-hand side of the UI.

4 Select **IPv6 Neighbor Snooping.**

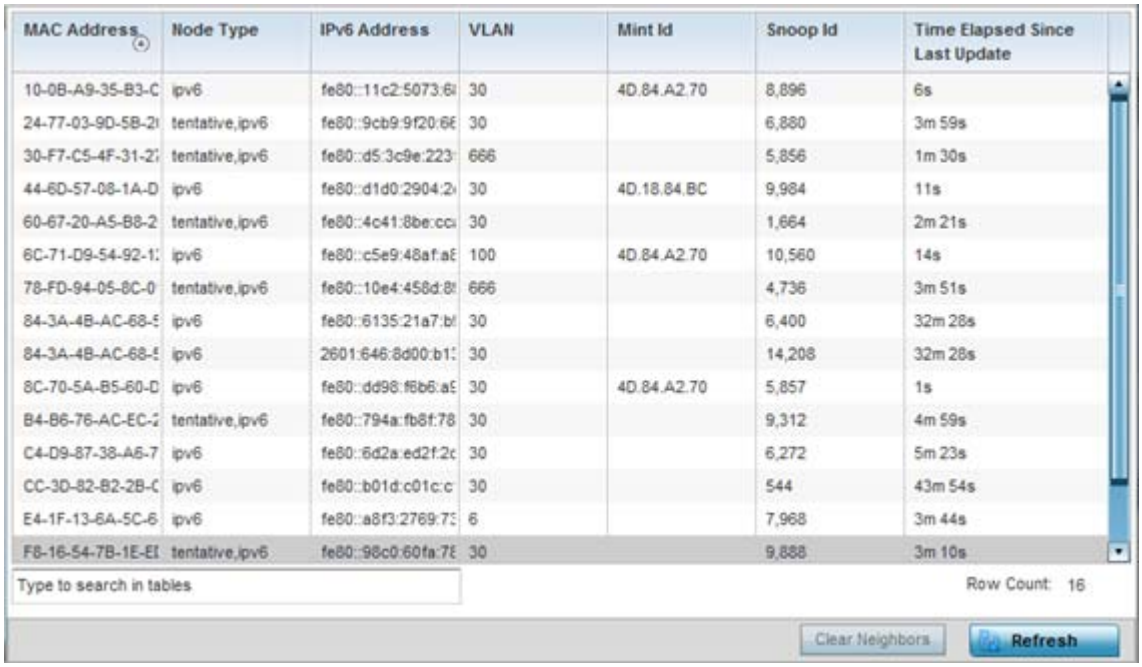


Figure 15-124 *Wireless Controller - Firewall IPv6 Neighbor Snooping screen*

The **IPv6 Neighbor Snooping** screen displays the following:

MAC Address	Displays the hardware encoded MAC address of an IPv6 client reporting to the controller or service platform.
Node Type	Displays the NetBios node type from an IPv6 address pool from which IP addresses can be issued to requesting clients.
IPv6 Address	Displays the IPv6 address used for DHCPv6 discovery and requests between the DHCPv6 server and DHCP clients.
VLAN	Displays the controller or service platform virtual interface ID used for a new DHCPv6 configuration.
Mint Id	Lists MiNT IDs for each listed VLAN. MiNT provides the means to secure communications at the transport layer. Using MiNT, a device can be configured to only communicate with other authorized (MiNT enabled) devices of the same model.
Snoop Id	Lists a numeric snooping ID associated with each packet inspection snooping session conducted by the controller or service platform.
Time Elapsed Since Last Update	Displays the amount of time elapsed since the DHCPv6 server was last updated.
Clear Neighbors	Select *Clear Neighbors* to revert the counters to zero and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's counters to their latest values.

15.3.34 VPN

Controller Statistics

IPSec VPN provides a secure tunnel between two networked peer controllers or service platforms. Administrators can define which packets are sent within the tunnel, and how they are protected. When a tunnelled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination.

Tunnels are sets of *security associations* (SA) between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunnelled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

Crypto maps combine the elements comprising IPSec SAs. Crypto maps also include *transform sets*. A transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic. One crypto map is utilized for each IPsec peer, however for remote VPN deployments one crypto map is used for all the remote IPsec peers.

Internet Key Exchange (IKE) protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs, and enables secure communications without time consuming manual pre-configuration.

VPN statistics are partitioned into the following:

- *IKESA*
- *IPSec*

15.3.34.1 IKESA

VPN

The *IKESA* screen allows for the review of individual peer security association statistics.

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **VPN** and expand the menu to reveal its sub menu items.

4 Select **IKESA**.

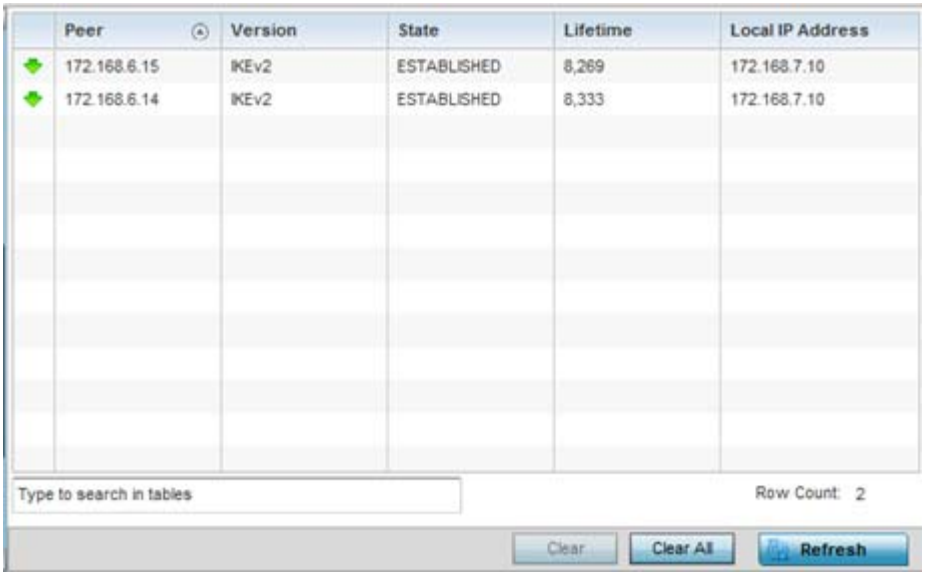


Figure 15-125 *Wireless Controller - VPN IKESA screen*

Review the following VPN peer security association statistics:

Peer	Lists IDs for peers sharing *security associations* (SA) for tunnel interoperability. When a peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its destination.
Version	Displays each peer's IKE version used for auto IPSec secure authentication with the IPSec gateway and other controllers or service platforms.
State	Lists the online or offline state of each listed peer's SA.
Lifetime	Displays the lifetime for the duration of each listed peer IPSec VPN security association. Once the set value is exceeded, the association is timed out.
Local IP Address	Displays each listed peer's local tunnel end point IP address. This address represents an alternative to an interface IP address.
Clear/Clear All	Select Clear to remove a selected peer. Select the *Clear All* button to clear each peer of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.34.2 IPSec

VPN

Use the *IPSec* VPN screen to assess tunnel status between networked peers.

To view IPSec VPN status for tunnelled peers:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **VPN** and expand the menu to reveal its sub menu items.

4 Select **IPSec**.

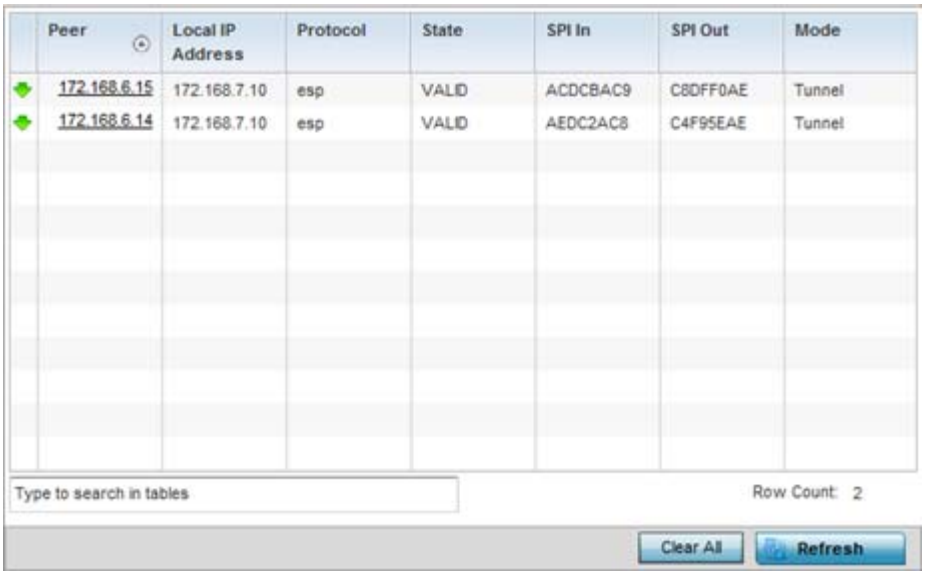


Figure 15-126 *Wireless Controller - VPN IPSec screen*

Review the following VPN peer security association statistics:

Peer	Lists IP addresses for peers sharing *security associations* (SA) for tunnel interoperability. When a peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its destination.
Local IP Address	Displays each listed peer's local tunnel end point IP address. This address represents an alternative to an interface IP address.
Protocol	Lists the security protocol used with the VPN IPSec tunnel connection. SAs are unidirectional, existing in each direction and established per security protocol. Options include ESP and AH.
State	Lists the state of each listed peer's security association.
SPI In	Lists *stateful packet inspection* (SPI) status for incoming IPSec tunnel packets. SPI tracks each connection traversing the IPSec VPN tunnel and ensures they are valid.
SPI Out	Lists SPI status for outgoing IPSec tunnel packets. SPI tracks each connection traversing the IPSec VPN tunnel and ensures they are valid.
Mode	Displays the IKE mode. IPSEC has two modes in IKEv1 for key exchanges. Aggressive mode requires 3 messages be exchanged between the IPSEC peers to setup the SA, Main requires 6 messages

Clear All	Select the *Clear All* button to clear each peer of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.35 Viewing Certificate Statistics

Controller Statistics

The *Secure Socket Layer* (SSL) protocol is used to ensure secure transactions between Web servers and browsers. This protocol uses a third-party, a certificate authority, to identify one end or both ends of the transactions. A browser checks the certificate issued by the server before establishing a connection.

For more information, see:

- *Viewing Trustpoints Statistics*
- *Viewing the RSA Key Details*

15.3.35.1 Viewing Trustpoints Statistics

Viewing Certificate Statistics

Each certificate is digitally signed by a trustpoint. The trustpoint signing the certificate can be a certificate authority, corporate or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters and an association with an enrolled identity certificate.

To view controller or service platform trustpoint statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Certificate** and expand the menu to reveal its sub menu items.

4 Select **Trustpoint**.

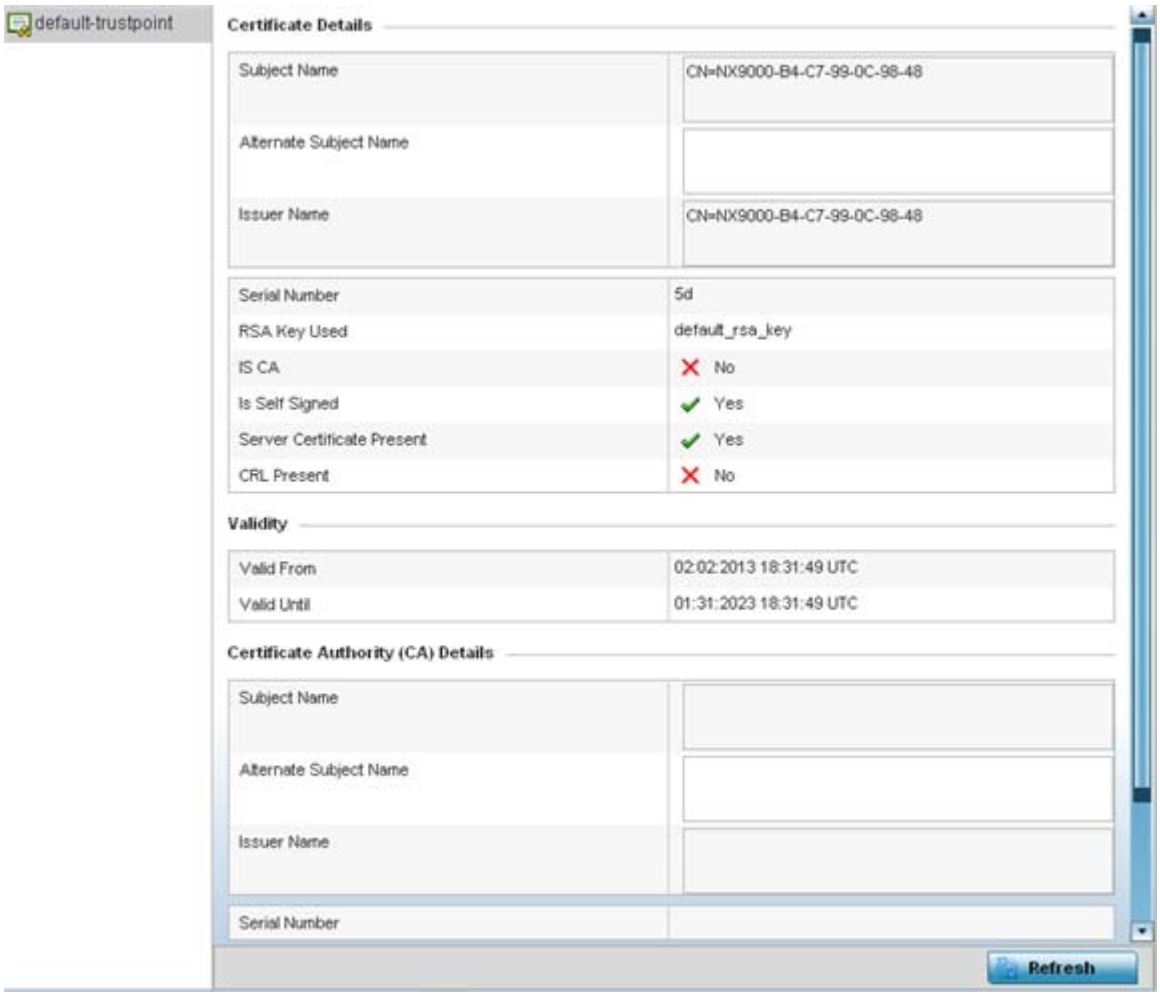


Figure 15-127 *Wireless Controller - Certificates Trustpoint screen*

The **Certificate Details** field displays the following:

Subject Name	Describes the entity to which the certificate is issued.
Alternate Subject Name	Lists alternate subject information about the certificate as provided to the certificate authority.
Issuer Name	Displays the name of the organization issuing the certificate.
Serial Number	Lists the unique serial number of the certificate.
RSA Key Used	Displays the name of the key pair generated separated, or automatically when selecting a certificate.
IS CA	Indicates whether this certificate is an authority certificate (Yes/No).
Is Self Signed	Displays whether the certificate is self-signed (Yes/No).
Server Certification Present	Displays whether a server certification is present or not (Yes/No).
CRL Present	Displays whether a *Certificate Revocation List* (CRL) is present (Yes/No). A CRL contains a list of subscribers paired with digital certificate status. The list displays revoked certificates along with the reasons for revocation. The date of issuance and the entities that issued the certificate are also included.

The **Validity** field displays the following:

Valid From	Displays the certificate's issue date stating the beginning of the certificate's validity.
Valid Until	Displays the certificate's expiration date.

The **Certificate Authority (CA) Details** field displays the following:

Subject Name	Displays information about the entity to which the certificate is issued.
Alternate Subject Name	This section provides alternate information about the certificate as provided to the certificate authority. This field is used to provide more information that supports information provided in the *Subject Name* field.
Issuer Name	Displays the organization issuing the certificate.
Serial Number	Lists the unique serial number of each certificate issued.

The **Certificate Authority Validity** field displays the following:

Validity From	Displays the date when the validity of a CA begins.
Validity Until	Displays the date when the validity of a CA expires.

5 Select the **Refresh** button to update the screen's statistics counters to their latest values.

15.3.35.2 Viewing the RSA Key Details

- *Viewing Certificate Statistics*

Rivest, Shamir, and Adleman (RSA) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing as well as encryption.

The RSA Keys screen displays a list of RSA keys installed in the selected Access Point. RSA Keys are generally used for establishing a SSH session, and are a part of the certificate set used by RADIUS, VPN and HTTPS.

To view the RSA Key details:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Certificate** and expand the menu to reveal its sub menu items.

4 Select **RSA Keys**.

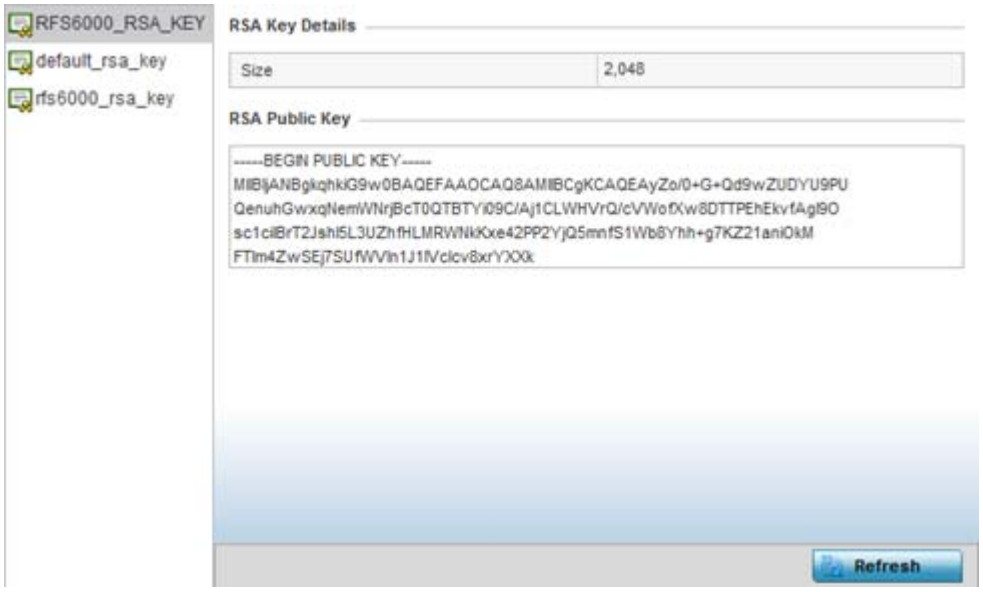


Figure 15-128 *Wireless Controller - Certificates RSA Keys screen*

The **RSA Key Details** field describes the size (in bits) of the desired key. If not specified, a default key size of 1024 is used.

The **RSA Public Key** field describes the public key's character set used for encrypting messages. This key is known to everyone.

5 Select the **Refresh** button to update the screen's statistics counters to their latest values.

15.3.36 WIPS Statistics

Controller Statistics

Wireless Intrusion Protection System (WIPS) detects the presence of unauthorized Access Points. Unauthorized attempts to access the WLAN is generally accompanied by intruding clients finding network vulnerabilities. Basic forms of this behavior can be monitored and reported without a dedicated WIPS deployment. When the parameters exceed a configurable threshold, the controller or service platform generates a SNMP trap and reports the result via the management interfaces. Basic WIPS functionality does not require monitoring APs and does not perform off-channel scanning.

For more information, see:

- *Viewing the Client Blacklist*
- *Viewing WIPS Event Statistics*

15.3.36.1 Viewing the Client Blacklist

WIPS Statistics

This *Client Blacklist* displays blacklisted clients detected using WIPS. Blacklisted clients are not allowed to associate to connected devices within the controller or service platform managed network.

To view the client blacklist screen:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **WIPS** and expand the menu to reveal its sub menu items.

4 Select **Client Blacklist**.

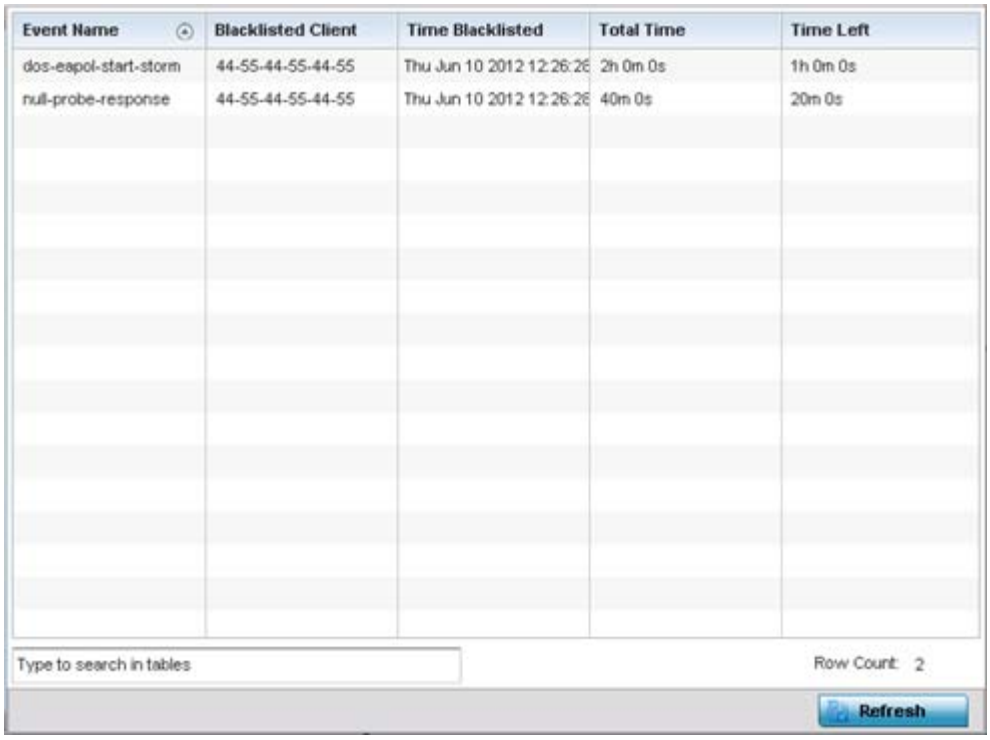


Figure 15-129 *Wireless Controller - WIPS Client Blacklist screen*

The **Client Blacklist** screen displays the following:

Event Name	Displays the name of the detected wireless intrusion resulting in a blacklisting of the client from controller or service platform resources.
Blacklisted Client	Displays the MAC address of the intruding client device pending exclusion from the controller or service platform managed network.
Time Blacklisted	Displays the time this client was blacklisted.
Total Time	Displays the duration the unauthorized device remained in the WLAN.
Time Left	Displays the duration after which the blacklisted client is removed from the blacklist.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.36.2 Viewing WIPS Event Statistics

The *WIPS Events* screen displays event information for rogue Access Point intrusions within the controller or service platform managed network.

To view WIPS event statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **WIPS** and expand the menu to reveal its sub menu items.

4 Select **WIPS Events**

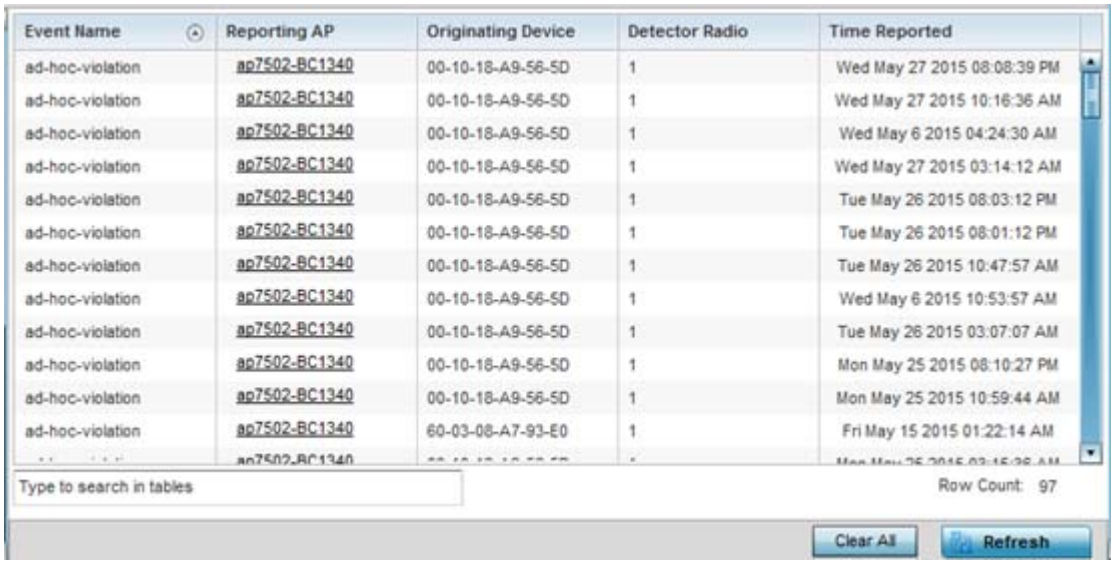


Figure 15-130 *Wireless Controller - WIPS Events screen*

The **WIPS Events** screen displays the following:

Event Name	Displays the name of the detected intrusion event.
Reporting AP	Displays the hostname of the AP reporting each intrusion. The Access Point displays as a link that can be selected to provide configuration and network address information in greater detail.
Originating Device	Displays the MAC address of the intruder AP.
Detector Radio	Displays which AP radio is making the intrusion detection.
Time Reported	Displays the time when the intruding AP was detected.
Clear All	Select *Clear All* to reset the statistics counters to zero and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.37 Sensor Server

Controller Statistics

Sensor servers allow the monitor and download of data from multiple sensors and remote locations using Ethernet, TCP/IP or serial communication. Repeaters are available to extend the transmission range and combine sensors with various frequencies on the same receiver.

To view the Sensor Server statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Sensor Servers** from the left-hand side of the controller or service platform UI.

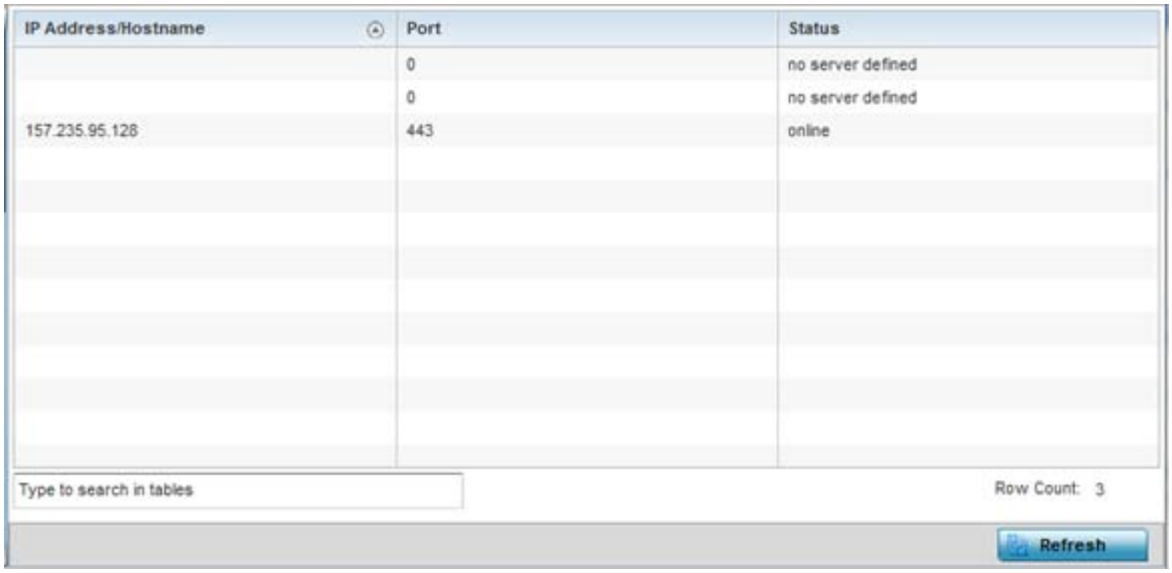


Figure 15-131 *Wireless Controller - Sensor Server screen*

The **Sensor Servers** screen displays the following:

IP Address/ Hostname	Displays a list of sensor server IP addresses. These are sensor resources available to the controller or service platform.
Port	Displays the port on which this server is listening.
Status	Displays whether the server is *connected* or *not connected*.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.38 Bonjour Services

Controller Statistics

Bonjour is Apple's zero-configuration networking (Zeroconf) implementation. Zeroconf is a group of technologies including service discovery, address assignment and hostname resolution. Bonjour locates the devices (printers, computers etc.) and services these computers provide over a local network.

Bonjour provides a method to discover services on a LAN. Bonjour allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.

To view the Bonjour service statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Bonjour Services** from the left-hand side of the controller or service platform UI.

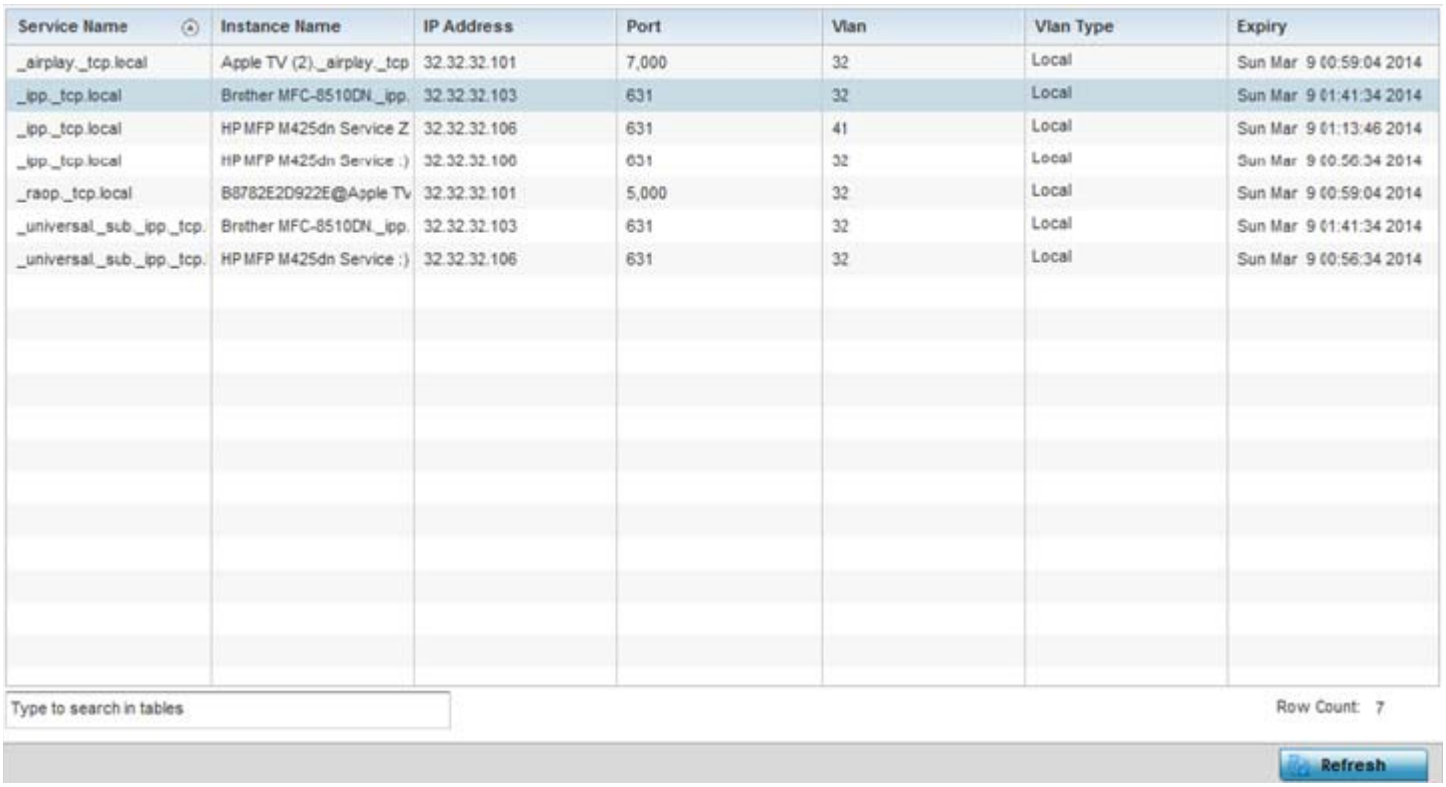


Figure 15-132 *Wireless Controller - Bonjour Services screen*

Refer to the following Bonjour service utilization stats:

Service Name	Lists the services discoverable by the Bonjour gateway. Services can either be *pre-defined* Apple services (scanner, printer etc.) or an *alias* not available on the predefined list.
Instance Name	Lists the name of each Bonjour service instance (session) utilized by the controller or service platform.
IP Address	Lists the network IP address utilized by the listed Bonjour service providing resources to the controller or service platform.
Port	Displays the port used to secure a connection with the listed Bonjour service.
Vlan	Lists the VLAN(s) on which a listed Bonjour service is routable.
Vlan Type	Lists the VLAN type as either a *local* bridging mode or a shared *tunnel*.
Expiry	Lists the expiration date of the listed Bonjour service, and its availability to discover resources on the LAN.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.39 Captive Portal Statistics

Controller Statistics

A captive portal redirects an HTTP client to a Web page (usually for authentication purposes) before authenticating for Internet access. A captive portal turns a Web browser into an authenticator. This is done by

intercepting packets (regardless of the address or port) until the user opens a browser and attempts to access the Internet. At that time, the browser is redirected to a Web page requiring authentication.

To view the controller or service platform captive portal statistics:

1 Select the **Statistics** tab from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Captive Portal** from the left-hand side of the controller or service platform UI.

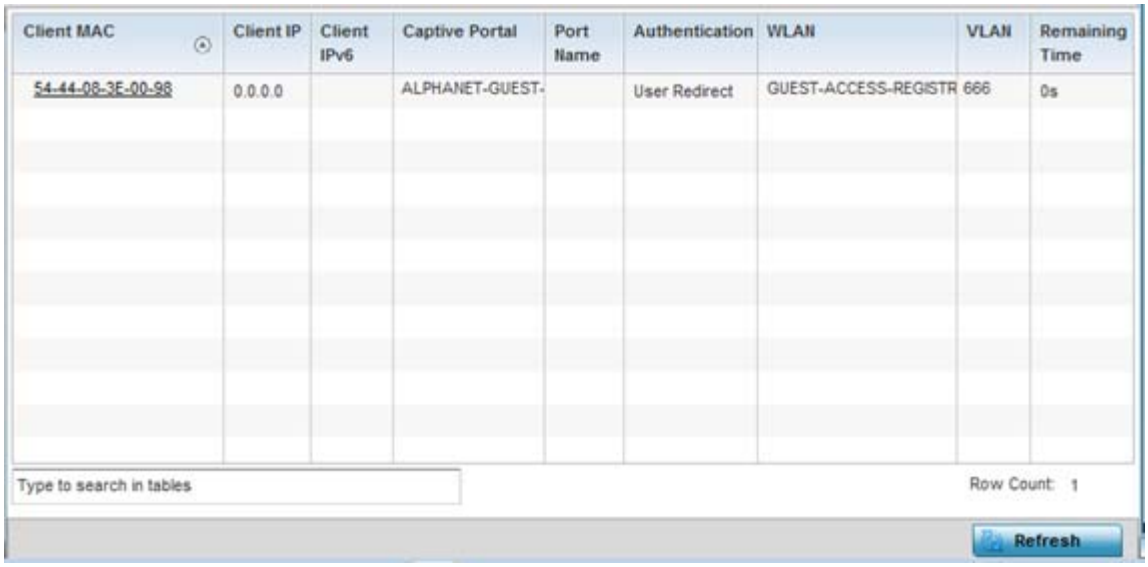


Figure 15-133 *Wireless Controller - Captive Portal screen*

The **Captive Portal** screen displays the following:

Client MAC	Displays the requesting client's MAC address. The MAC displays as a link that can be selected to display client configuration and network address information in greater detail.
Client IP	Displays the requesting client's IPv4 formatted IP address.
Client IPv6	Displays the requesting client's IPv6 formatted IP address.
Captive Portal	Displays the captive portal name that each listed client is utilizing for guest access to controller resources.
Port Name	Lists the controller or service platform port name supporting the captive portal connection with the listed client MAC address.
Authentication	Displays the authentication status of the requesting client.
WLAN	Displays the name of the WLAN the client belongs to.
VLAN	Displays the name of the requesting client's VLAN interface.
Remaining Time	Displays the time after which the client is disconnected from the captive portal managed Internet.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.40 Network Time

Controller Statistics

Network Time Protocol (NTP) is central to networks that rely on their controller or service platform to supply system time. Without NTP, system time is unpredictable, which can result in data loss, failed processes and compromised security. With network speed, memory, and capability increasing at an exponential rate, the accuracy, precision, and synchronization of network time is essential in a controller or service platform managed network. The controller or service platform can use a dedicated server to supply system time. The controller or service platform can also use several forms of NTP messaging to sync system time with authenticated network traffic.

15.3.40.1 Viewing NTP Status

Network Time

The *NTP Status* screen displays performance (status) information relative to the NTP association status. Verify the NTP status to assess the controller or service platform's current NTP resource.

To view the NTP status of a managed network:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Network Time**.

4 Select **NTP Status**.

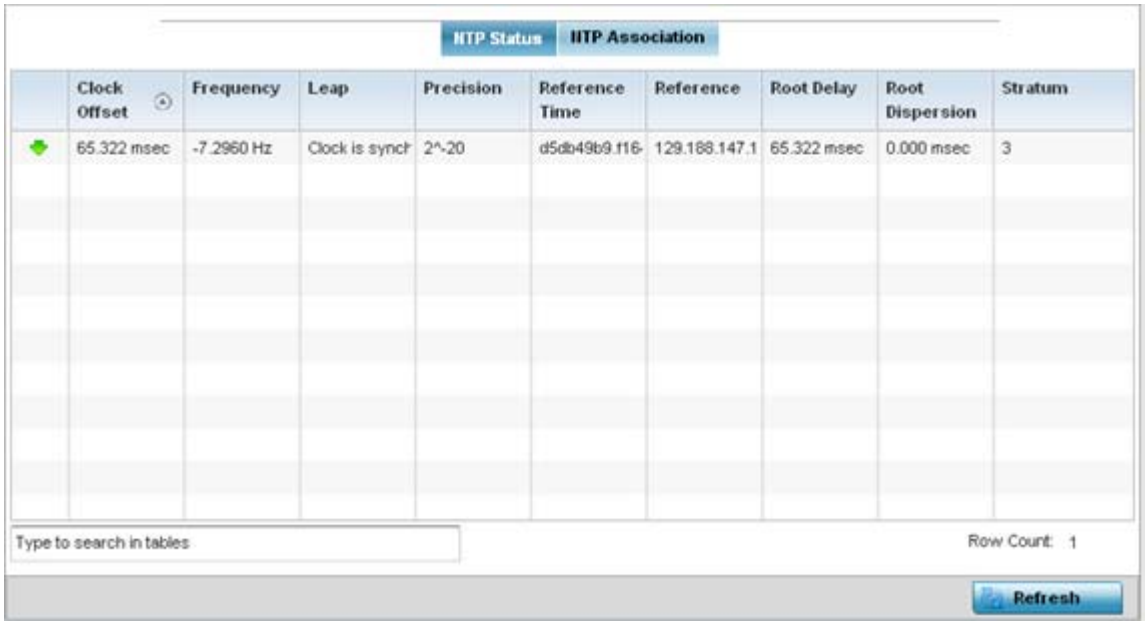


Figure 15-134 *Wireless Controller - NTP Status screen*

Refer to the **NTP Status** table to review the accuracy and performance of the controller or service platform's synchronization with an NTP server.

Clock Offset	Displays the time differential between the controller or service platform time and the NTP resource.

Frequency	An SNTP server clock's skew (difference) for the controller or service platform and the dedicated NTP resource.
Leap	Indicates if a second is added or subtracted to SNTP packet transmissions, or if transmissions are synchronized.
Precision	Displays the precision of the controller's time clock (in Hz). The values that normally appear in this field range from -6 for mains-frequency clocks to -20 for microsecond clocks.
Reference Time	Displays the time stamp the local clock was last set or corrected.
Reference	Displays the address of the time source the controller or service platform is synchronized to.
Root Delay	The total round-trip delay in seconds. This variable can take on both positive and negative values, depending on relative time and frequency offsets. The values that normally appear in this field range from negative values (a few milliseconds) to positive values (several hundred milliseconds).
Root Dispersion	The difference between the time on the root NTP server and it's reference clock. The reference clock is the clock used by the NTP server to set its own clock.
Stratum	Displays how many hops the controller or service platform is from its current NTP resource.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.3.40.2 Viewing NTP Associations

Network Time

The interaction between the controller or service platform and an SNTP server constitutes an association. SNTP associations can be either peer associations (the controller or service platform synchronizes to another system or allows another system to synchronize to it), or a server associations (only the controller or service platform synchronizes to the SNTP resource, not the other way around).

To view the NTP associations:

1 Select the **Statistics** menu from the Web UI.

2 Select a Wireless Controller node from the left navigation pane.

3 Select **Network Time**.

4 Select **NTP Associations**.

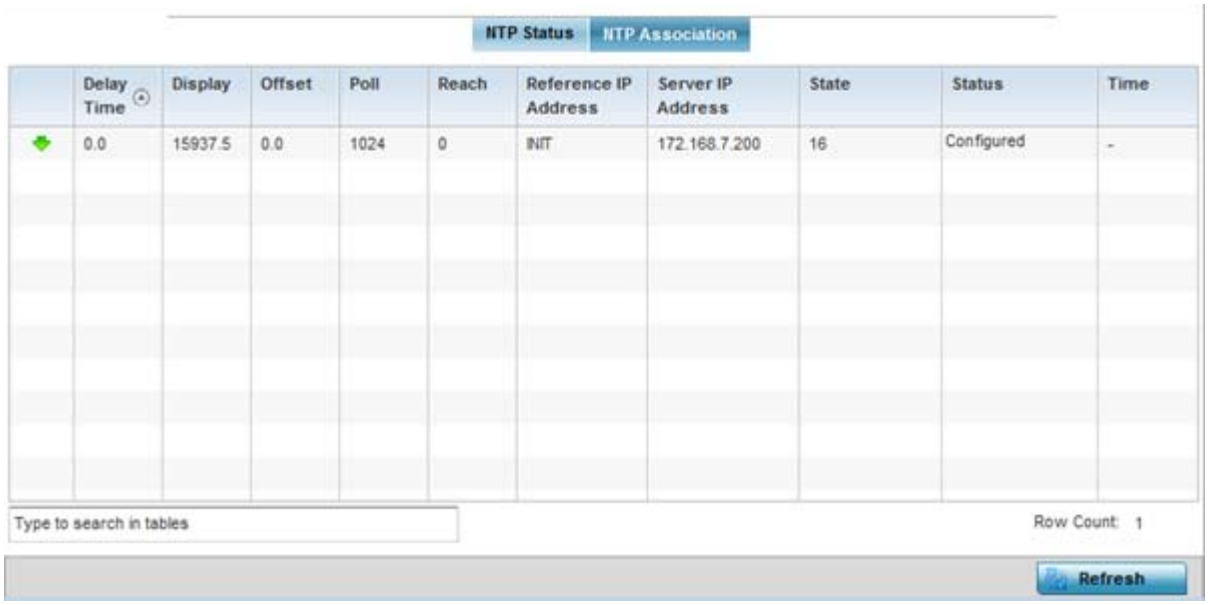


Figure 15-135 *Wireless Controller - NTP Association screen*

The **NTP Associations** screen provides the controller or service platform's current NTP associations:

Delay Time	Displays the round-trip delay (in seconds) for SNTP broadcasts between the SNTP server and the controller or service platform.
Display	Displays the time difference between the peer NTP server and the onboard wireless controller clock.
Offset	Displays the calculated offset between the controller or service platform and the SNTP server. The controller or service platform adjusts its clock to match the server's time. The offset gravitates towards zero overtime, but never completely reduces its offset to zero.
Poll	Displays the maximum interval between successive messages (in seconds) to the nearest power of two.
Reach	Displays the status of the last eight SNTP messages. If an SNTP packet is lost, the lost packet is tracked over the next eight SNTP messages.
Reference IP Address	Displays the address of the time source the controller or service platform is synchronized to.
Server IP Address	Displays the numerical IP address of the SNTP resource (server) providing SNTP updates to the controller.
State	Displays the NTP association status code.
Status	Displays the NTP peer's current status.
Time	Displays the timestamp of the last NTP packet received from the NTP peer.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4 Access Point Statistics

Statistics

The Access Point statistics screens displays controller or service platform connected Access Point *performance, health, version, client support, radio, mesh, interface, DHCP, firewall, WIPS, sensor, captive portal, NTP* and *load* information. Access point statistics consists of the following:

- *Health*
- *Device*
- *Web-Filtering*
- *Application Visibility (AVC)*
- *Device Upgrade*
- *Adoption*
- *AP Detection*
- *Guest User*
- *Wireless LANs*
- *Policy Based Routing*
- *Radios*
- *Mesh*
- *Interfaces*
- *RTLS*
- *PPPoE*
- *Bluetooth*
- *OSPF*
- *L2TPv3 Tunnels*
- *VRRP*
- *Critical Resources*
- *LDAP Agent Status*
- *Mint Links*
- *Guest Users*
- *GRE Tunnels*
- *Dot1x*
- *Network*
- *DHCPv6 Relay & Client*
- *DHCP Server*
- *Firewall*
- *VPN*
- *Certificates*
- *WIPS*
- *Sensor Servers*
- *Bonjour Services*
- *Captive Portal*
- *Network Time*
- *Load Balancing*
- *Environmental Sensors (AP8132 Models Only)*

15.4.1 Health

Access Point Statistics

The *Health* screen displays a selected Access Point's hardware version and software version. Use this information to fine tune the performance of an Access Point. This screen should also be the starting point for troubleshooting an Access Point since it's designed to present a high level display of Access Point performance efficiency.

To view the Access Point health:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Health**.

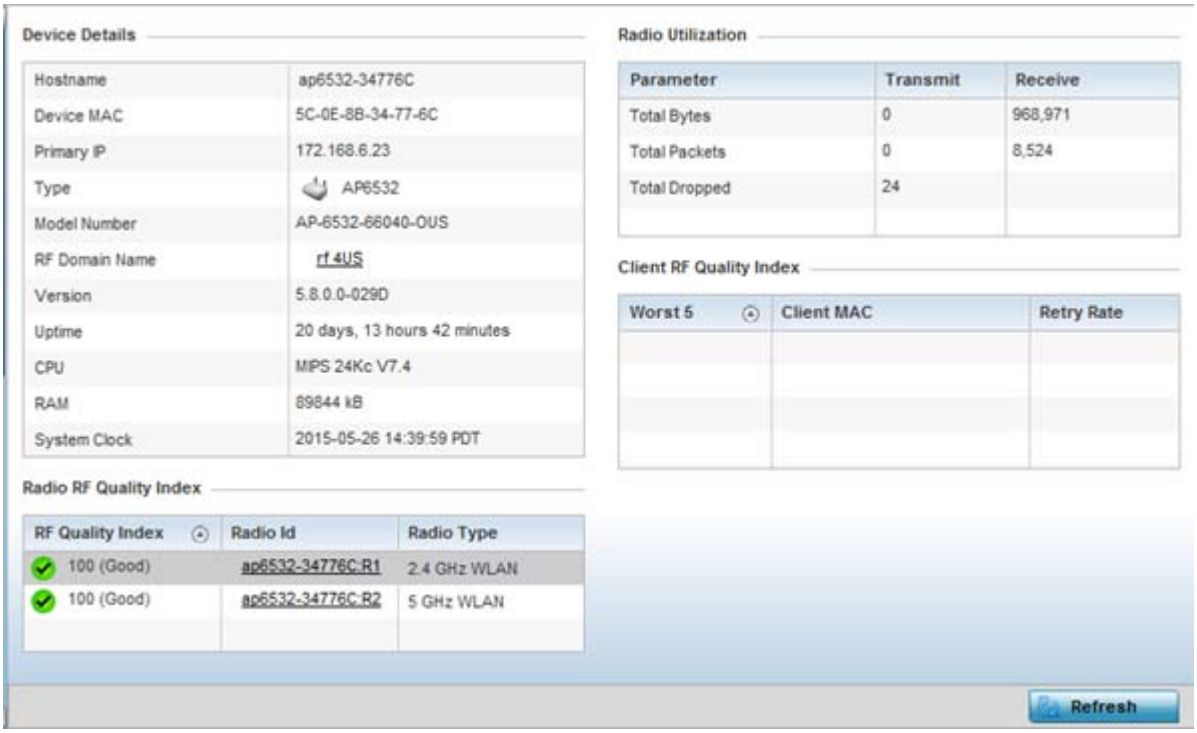


Figure 15-136 *Access Point - Health screen*

The **Device Details** field displays the following information:

Hostname	Displays the AP's unique name as assigned within the controller or service platform managed network. A hostname is assigned to a device connected to a computer network.
Device MAC	Displays the MAC address of the AP. This is factory assigned and cannot be changed.
Primary AP	Displays the IP address of assigned to this device either through DHCP or through static IP assignment.
Type	Displays the Access Point's model type.
Model Number	Displays the Access Point's model number to help further differentiate the Access Point from others of the same model series and defined country of operation.

RF Domain Name	Displays the Access Point's RF Domain membership. Unlike a controller or service platform, an Access Point can only belong to one RF Domain based on its model. The domain name appears as a link that can be selected to show RF Domain utilization in greater detail.
Version	Displays the Access Point's current firmware version. Use this information to assess whether an upgrade is required for better compatibility.
Uptime	Displays the cumulative time since the Access Point was last rebooted or lost power.
CPU	Displays the processor core.
RAM	Displays the free memory available with the RAM.
System Clock	Displays the system clock information.

The **Radio RF Quality Index** field displays the following:

RF Quality Index	Displays Access Point radios and their quality indices. RF quality index indicates the overall RF performance. The RF quality indices are: *0 – 50* (poor) *50 – 75* (medium) *75 – 100* (good)
Radio Id	Displays a radio's hardware encoded MAC address The ID appears as a link that can be selected to show radio utilization in greater detail.
Radio Type	Identifies whether the radio is a 2.4 or 5 GHz.

The **Radio Utilization Index** field displays the following:

Total Bytes	Displays the total bytes of data transmitted and received by the Access Point since the screen was last refreshed.
Total Packets	Lists the total number of data packets transmitted and received by the Access Point since the screen was last refreshed.
Total Dropped	List the number of dropped data packets by an Access Point radio since the screen was last refreshed.

The **Client RF Quality Index** field displays the following:

Worst 5	Displays clients having lowest RF quality within the network.
Client MAC	Displays the MAC addresses of the clients with the lowest RF indices.
Retry Rate	Displays the average number of retries per packet. A high number indicates possible network or hardware problems.

4 Select the **Refresh** button as needed to update the screen's statistics counters to their latest values.

15.4.2 Device

Access Point Statistics

The *Device* screen displays basic information about the selected Access Point. Use this screen to gather version information, such as the installed firmware image version, the boot image and upgrade status.

To view the device statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Device**.

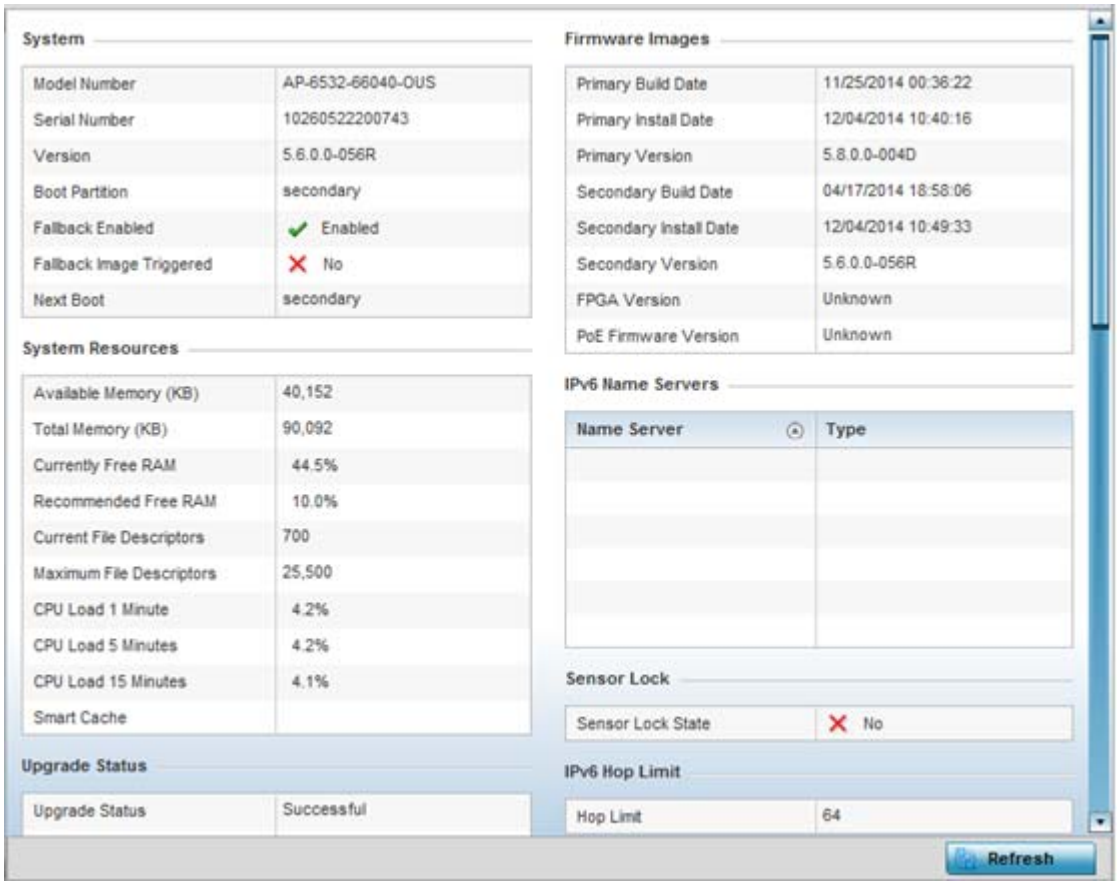


Figure 15-137 *Access Point - Device screen*

The **System** field displays the following:

Model Number	Displays the model of the selected Access Point to help distinguish its exact SKU and country of operation.
Serial Number	Displays the numeric serial number set for the Access Point.
Version	Displays the software (firmware) version on the Access Point.
Boot Partition	Displays the boot partition type.
Fallback Enabled	Displays whether this option is enabled. This method enables a user to store a known legacy version and a new version in device memory. The user can test the new software, and use an automatic fallback, which loads the old version on the Access Point if the new version fails.
Fallback Image Triggered	Displays whether the fallback image was triggered. The fallback image is an old version of a known and operational software stored in device memory. This allows a user to test a new version of software. If the new version fails, the user can use the old version of the software.

Next Boot	Designates this version as the version used the next time the AP is booted.

The **System Resources** field displays the following:

Available Memory (MB)	Displays the available memory (in MB) available on the Access Point.
Total Memory (MB)	Displays the Access Point's total memory.
Currently Free RAM	Displays the Access Point's free RAM space. If its very low, free up some space by closing some processes.
Recommended Free RAM	Displays the recommended RAM required for routine operation.
Current File Descriptors	Displays the Access Point's current file description.
Maximum File Descriptors	Displays the Access Point's maximum file description.
CPU Load 1 Minute	Lists this Access Point's CPU utilization over a 1 minute span.
CPU Load 5 Minutes	Lists this Access Point's CPU utilization over a 5 minute span.
CPU Load 15 Minutes	Lists this Access Point's CPU utilization over a 15 minute span.

The **Upgrade Status** field displays the following:

Upgrade Status	Displays the status of the last firmware upgrade performed by this controller or service platform.
Upgrade Status Time	Lists a time stamp defining the occurrence of the most recent upgrade operation.

The **Fan Speed** field displays the following:

Number	Displays the number of fans supported on the this Access Point.
Speed (Hz)	Displays the fan speed in Hz.

The **Temperature** field displays the following:

Number	Displays the number of temperature elements used by the Access Point.
Temperature	Displays the current temperature (in Celsius) to assess a potential Access Point overheat condition.

The **Kernal Buffers** field displays the following:

Buffer Size	Lists the sequential buffer size.
Current Buffers	Displays the current buffers available to the selected Access Point.
Maximum Buffers	Lists the maximum buffers available to the selected Access Point.

The IP Domain field displays the following:

Number	Displays the number of fans supported on the this Access Point.

Speed (Hz)	Displays the fan speed in Hz.

The **IP Name Servers** field displays the following:

Name Server	Displays the names of the servers designated to provide DNS resources to this Access Point.
Type	Displays the type of server for each server listed.

The **Firmware Images** field displays the following:

Primary Build Date	Displays the build date when this Access Point firmware version was created.
Primary Install Date	Displays the date this version was installed.
Primary Version	Displays the primary version string.
Secondary Build Date	Displays the build date when this version was created.
Secondary Install Date	Displays the date this secondary version was installed.
Secondary Version	Displays the secondary version string.
FPGA Version	Displays whether a FPGA supported firmware load is being utilized.
PoE Firmware Version	Displays whether a PoE supported firmware load is being utilized.

The **IPv6 Name Servers** field displays the following:

Name Server	List the IPv6 name server hosting a network service for providing responses to queries against a directory. The IPv6 name server maps a human recognizable identifier to a system's internal identifier. This service is performed by the server in response to a network service protocol request.
Type	Lists the type of IPv6 name server mapping a human readable identifier to system identifier.

The **Sensor Lock** field displays the following:

Sensor Lock	Displays whether a lock has been applied to Access Point sensor capabilities.

The **Power Management** field displays the following:

Power Management Mode	Displays the power mode currently invoked by the selected Access Point.
Power Management Status	Lists the power status of the Access Point.
Ethernet Power Status	Displays the Access Point's Ethernet power status.
Radio Power Status	Displays the power status of the Access Point's radios.

The **IPv6v Hop Limit** table displays the following:

Hop Limit	Lists the maximum number of times IPv6 traffic can hop. The IPv6 header contains a hop limit field that controls the number of hops a datagram can be sent before being discarded (similar to the TTL field in an IPv4 header).

The **IPv6 Delegated Prefixes** table displays the following:

IPv6 Delegated Prefix	In IPv6, prefix delegation is used to assign a network address prefix, configuring the controller or service platform with the prefix.
Prefix Name	Lists the name assigned to the IPv6 delegated prefix.
DHCPv6 Client State	Displays the current DHCPv6 client state as impacted by the IPv6 delegated prefix.
Interface Name	Lists the interface over which IPv6 prefix delegation occurs.
T1 timer (seconds)	Lists the amount of time in seconds before the DHCP T1 (delay before renew) timer expires.
T2 timer (seconds)	Lists the amount of time in seconds before the DHCP T2 (delay before rebind) timer expires.
Last Refreshed (seconds)	Lists the time, in seconds, since IPv6 prefix delegation has been updated.
Preferred Lifetime (seconds)	Lists is the time in seconds (relative to when the packet is sent) the IPv6 formatted addresses remains in a preferred state on the selected interface. The preferred lifetime must always be less than or equal to the valid lifetime.
Valid Lifetime (seconds)	Displays the time in seconds (relative to when the packet is sent) the IPv6 formatted address remains in a valid state on the selected interface. The valid lifetime must always be greater than or equal to the preferred lifetime.

4 Select **Refresh** to update the statistics counters to their latest values.

15.4.3 Web-Filtering

Access Point Statistics

The *Web-Filtering* screen displays information on Web requests for content and whether the requests were blocked or approved based on URL filter settings defined for the selected Access Point. A URL filter is comprised of several filter rules. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.

To view this Access Point's Web filter statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Web-Filtering**.

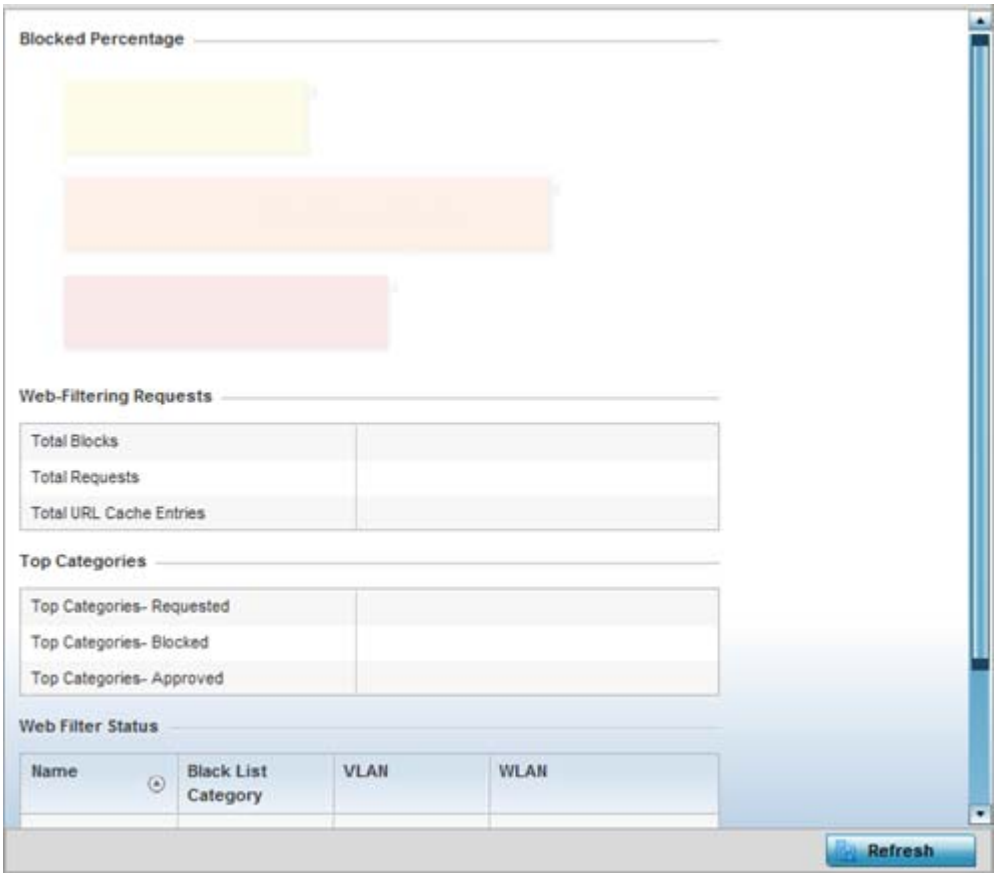


Figure 15-138 *Access Point - Web Filtering screen*

The **Web-Filtering Requests** field displays the following information:

Total Blocks	Lists the number of Web request hits against content blocked in the URL blacklist.
Total Requests	Lists the total number of requests for URL content cached locally on this Access Point.
Total URL Cache Entries	Displays the number of chached URL data entries made on this Access Point on the request of requesting clients requiring URL data managed by the Access Point and their respective whitelist or blacklist.

The **Top Categories** field helps administrators assess the content most requested, blocked or approved based on the defined whitelist and blacklist permissions:

Top Categories - Requested	Lists those Web content categories most requested by clients managed by this Access Point. Use this information to assess whether the permissions defined in the blacklist and whitelist optimally support these client requests for cached Web content.

Top Categories - Blocked	Lists those Web content categories blocked most often for requesting clients managed by this Access Point. Use this information to periodically assess whether the permissions defined in the blacklist and whitelist still restrict the desired cached Web content from requesting clients. Remember, a whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.
Top Categories - Approved	Lists those Web content categories approved most often on behalf of requesting clients managed by this Access Point. Periodically review this information to assess whether this cached and available Web content still adhere's to your organization's standards for client access.

The **Web Filter Status** field displays the following information:

Name	Displays the name of the filter whose URL rule set has been invoked.
Blacklist Category	Lists the blacklist category whose URL filter rule set has caused data to be filtered to a requesting client. Periodically assess whether these rules are still relevant to the data requirements of requesting clients.
VLAN	Lists the impacted Access Point VLAN whose Web data traffic has been filtered based on the restrictions in the listed blacklist category.
WLAN	Lists the impacted Access Point WLAN whose Web data traffic has been filtered based on the restrictions in the listed blacklist category. Periodically assess whether clients are segregated to the correct WLAN based on their cached Web data requirements and impending filter rules.

4 Periodically select **Refresh** to update this screen to its latest values.

15.4.4 Application Visibility (AVC)

Access Point Statistics

Access Points can inspect every byte of each application header packet allowed to pass to their connected clients. When an application is recognized and classified by the WiNG application recognition engine, administrator defined actions can be applied to that specific application. For information on categorizing, filtering and logging the application data allowed to proliferate the WiNG network, refer to *Application on page 7-58* and *Application on page 7-58*.

To view Access Point application utilization statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Application Visibility (AVC).**

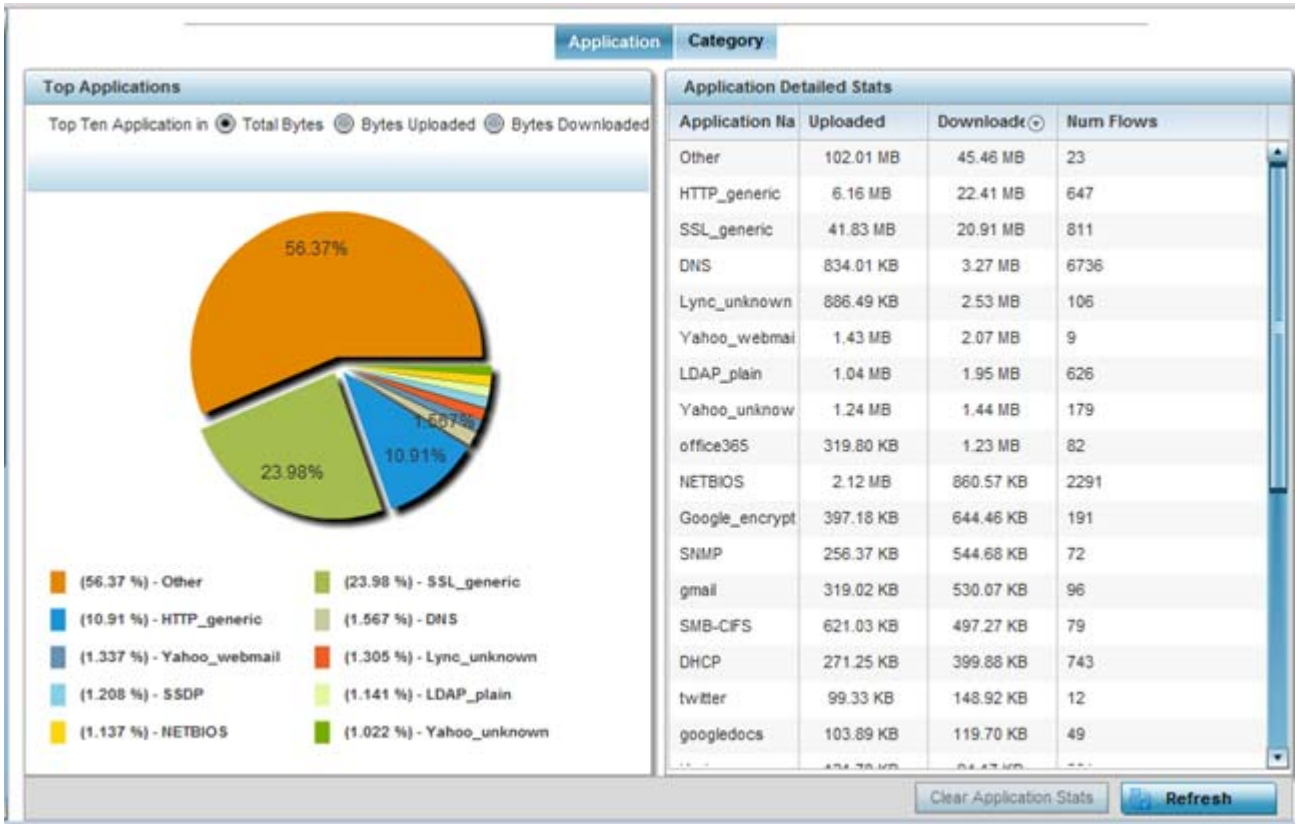


Figure 15-139 *Access Point - Application Visibility*

4 Refer to the **Top Applications** graph to assess the most prolific, and allowed, application data passing through the Access Point.

Total Bytes	Displays the top ten utilized applications in respect to total data bytes passing through the Access Point. These are only the administrator *allowed* applications approved for proliferation within the Access Point managed network.
Bytes Uploaded	Displays the top ten applications in respect to total data bytes uploaded through the Access Point managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).
Bytes Downloaded	Displays the top ten applications in respect to total data bytes downloaded from the Access Point managed network. If this application data is not aligned with application utilization expectations, consider allowing or denying additional applications and categories or adjusting their precedence (priority).

5 Refer to the **Application Detailed Stats** table to assess specific application data utilization:

Application Name	Lists the allowed application name whose data (bytes) are passing through the Access Point managed network.
Uploaded	Displays the number of uploaded application data (in bytes) passing the through the Access Point managed network.

Downloaded	Displays the number of downloaded application data (in bytes) passing the through the Access Point managed network.
Num Flows	Lists the total number of application data flows passing through the Access Point for each listed application. An application flow can consist of packets in a specific connection or media stream. Application packets with the same source address/port and destination address/port are considered one flow.
Clear Application Stats	Select this option to clear the application assessment data counters and begin a new assessment.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

6 Select the **Category** tab.

Categories are existing WiNG or user defined application groups (video, streaming, mobile, audio etc.) that assist administrators in filtering (allowing or denying) application data. For information on categorizing application data, refer to *Application Policy on page 7-54* and *Application on page 7-58*.

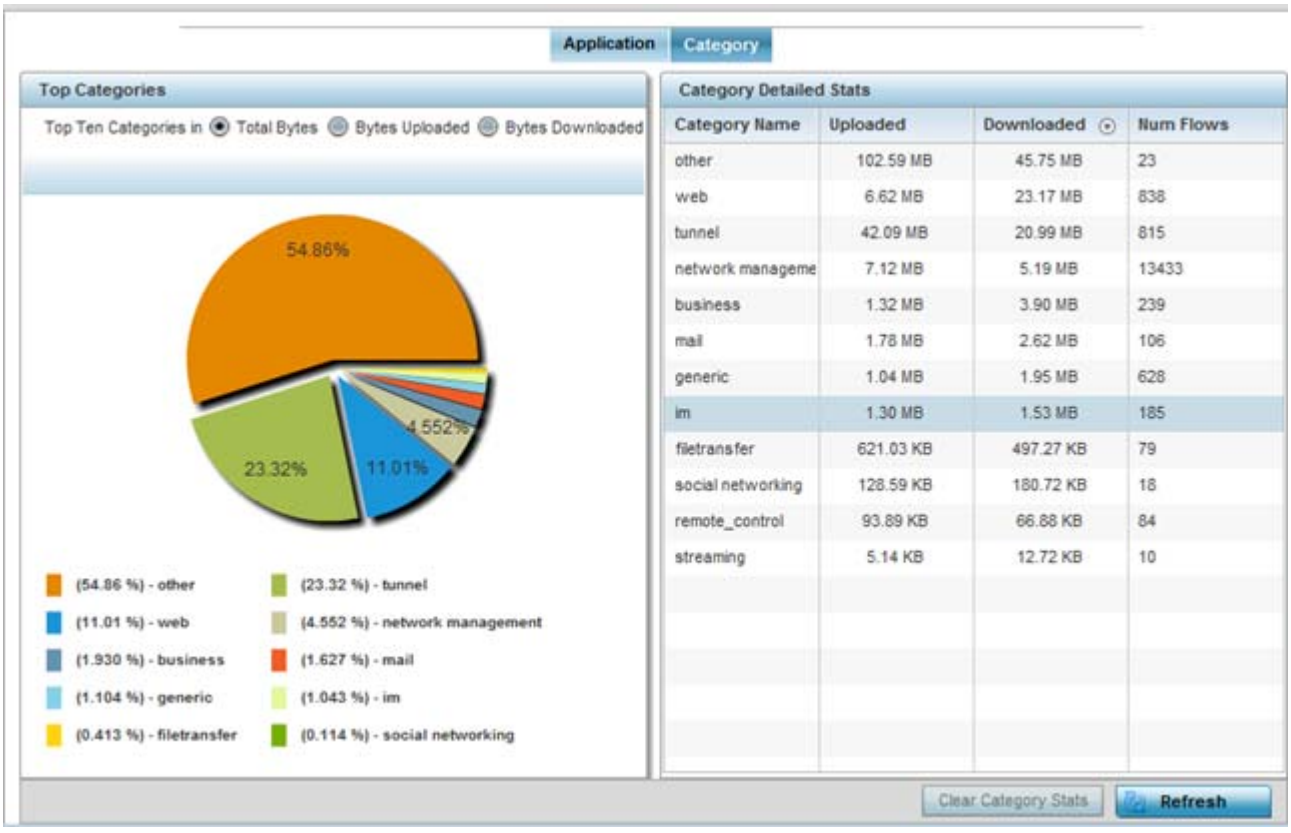


Figure 15-140 *Access Point - Application Category Visibility*

7 Refer to the **Top Categories** graph to assess the most prolific, and allowed, application data categories utilized by the Access Point.

Total Bytes	Displays the top ten application categories in respect to total data bytes passing through the Access Point managed network. These are only the administrator *allowed* application categories approved for proliferation within the Access Point managed network.

Bytes Uploaded	Displays the top ten application categories in respect to total data bytes uploaded through the controller or service platform managed network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories or adjusting their precedence (priority).
Bytes Downloaded	Displays the top ten application categories in respect to total data bytes downloaded from the Access Point managed network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories and categories or adjusting their precedence (priority).

8 Refer to the **Category Detailed Stats** table to assess specific application category data utilization:

Category Name	Lists the allowed category whose application data (in bytes) is passing through the Access Point managed network.
Uploaded	Displays the number of uploaded application category data (in bytes) passing the through the Access Point managed network.
Downloaded	Displays the number of downloaded application category data (in bytes) passing the through the Access Point managed network.
Num Flows	Lists the total number of application category data flows passing through Access Point connected clients. A category flow can consist of packets in a specific connection or media stream. Packets with the same source address/port and destination address/port are considered one flow.
Clear Application Stats	Select this option to clear the application category assessment data counters and begin a new assessment.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.4.5 Device Upgrade

Access Point Statistics

The *Device Upgrade* screen displays information about devices receiving updates and the devices used to provision them. Use this screen to gather version data, install firmware images, boot an image and upgrade status.

To view the device upgrade statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Device Upgrade**.

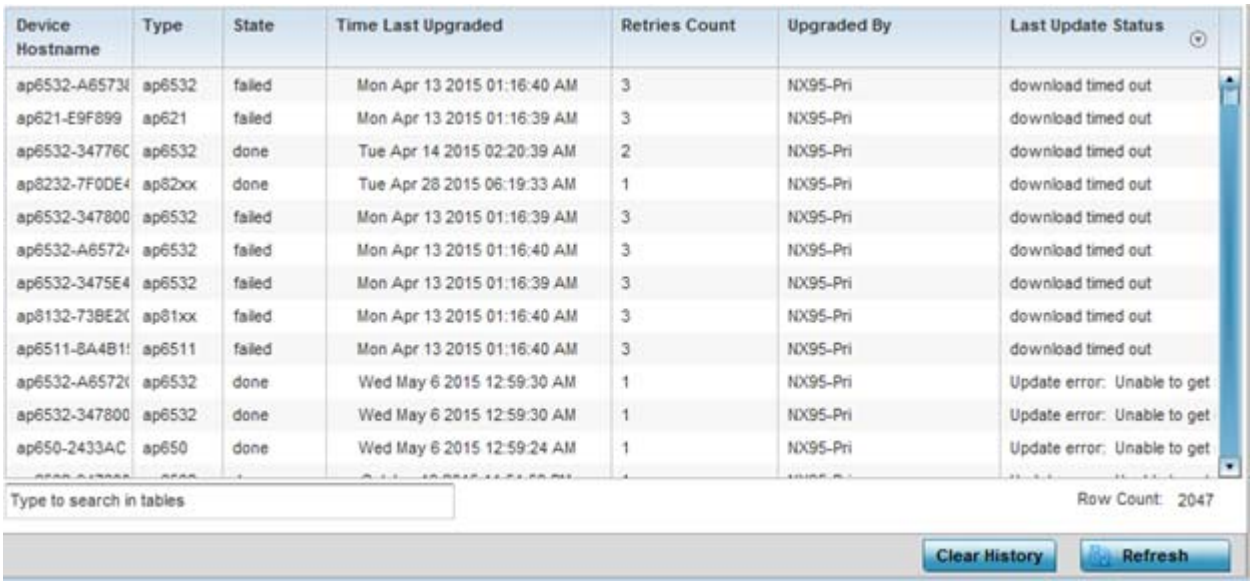


Figure 15-141 *Access Point - Device Upgrade screen*

The **Upgrade** screen displays the following information:

Device Hostname	Displays the administrator assigned hostname of the Access Point receiving the update.
Type	Displays the Access Point model type of the device receiving a firmware update from the provisioning Access Point.
State	Displays the current state of the Access Point upgrade (*done*, *failed* etc.).
Time Last Upgraded	Displays the date and time of the last successful Access Point firmware upgrade operation.
Retries Count	Displays the number of retries made in an Access Point firmware update operation.
Upgraded By	Displays the MAC address of the Access Point that performed the upgrade operation.
Last Update Status	Displays the status of the last upgrade operation (*Start Upgrade, Update Error* etc.).
Clear History	Select the *Clear History* button to clear the screen of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.6 Adoption

Access Point Statistics

Access point adoption stats are available for both currently adopted and Access Points pending adoption. Historical data can be also be fetched for adopted Access Points.

For more information, refer to the following:

- *Adopted APs*
- *AP Adoption History*
- *AP Self Adoption History*
- *Pending Adoptions*

15.4.6.1 Adopted APs

Adoption

The *Adopted APs* screen lists Access Points adopted by the selected Access Point, their RF Domain memberships and network service information.

To view adopted Access Point statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand the **Adoption** menu item.

4 Select **Adopted APs**.

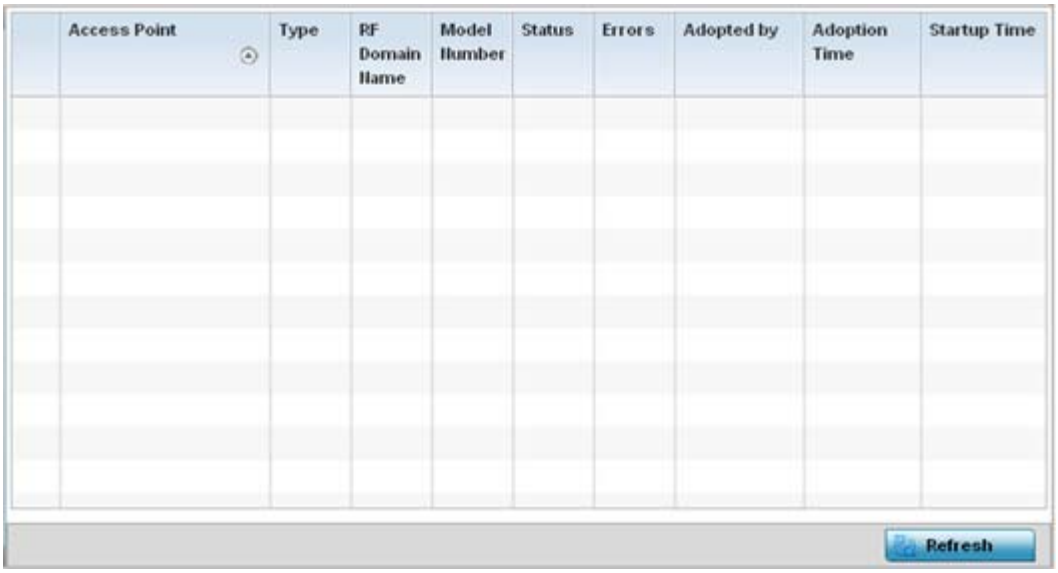


Figure 15-142 *Access Point - Adopted APs screen*

The **Adopted APs** screen displays the following:

Access Point	Displays the name assigned to the adopted Access Point as part of its device configuration.
Type	Lists the each listed Access Point type adopted by this Access Point.

RF Domain Name	Displays each Access Point's RF Domain membership. An Access Point can only share RF Domain membership with other Access Points of the same model.
Model Number	Displays each listed Access Point's numeric model (AP6532, AP6511 etc.).
Status	Displays each listed Access Point's configuration status to help determine its service role.
Errors	Lists any configuration errors that may be hindering a clean adoption.
Adopted By	Lists the adopting Access Point.
Adoption time	Displays each listed Access Point's time of adoption.
Startup Time	Displays each listed Access Point's in service time since last offline.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.6.2 AP Adoption History

Adoption

The *AP Adoption History* screen displays a list of peer Access Points and their adoption event status.

To review a selected Access Point's adoption history:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand the a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand the **Adoption** menu item.

4 Select **AP Adoption History**.

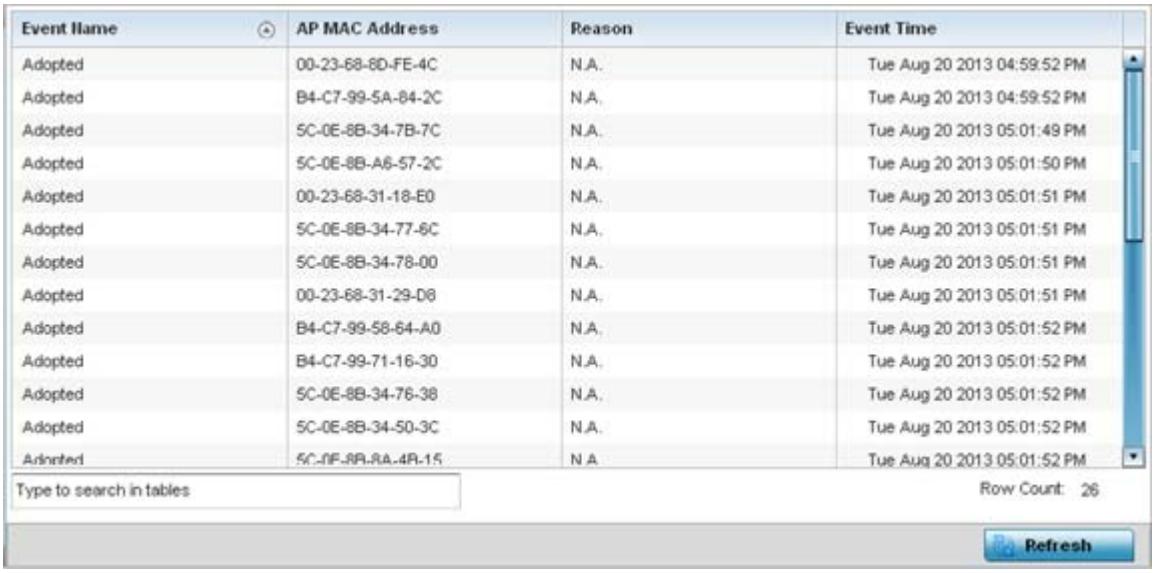


Figure 15-143 *Access Point - AP Adoption History screen*

The **Adopted Devices** screen describes the following historical data for adopted Access Points:

Event Name	Displays the adoption status of each listed Access Point as either *adopted* or *un-adopted*.
AP MAC Address	Displays the MAC address of each Access Point this Access Point has attempted to adopt.
Reason	Displays the reason code for each event listed.
Event Time	Displays day, date and time for each Access Point adoption attempt.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.6.3 AP Self Adoption History

Adoption

The *AP Self Adoption History* displays an event history of peer Access Points that have adopted to the selected Access Point.

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand the a RF Domain, select a controller, and select one of its connected Access Points.

3 Expand the **Adoption** menu item.

4 Select **AP Self Adoption History**.

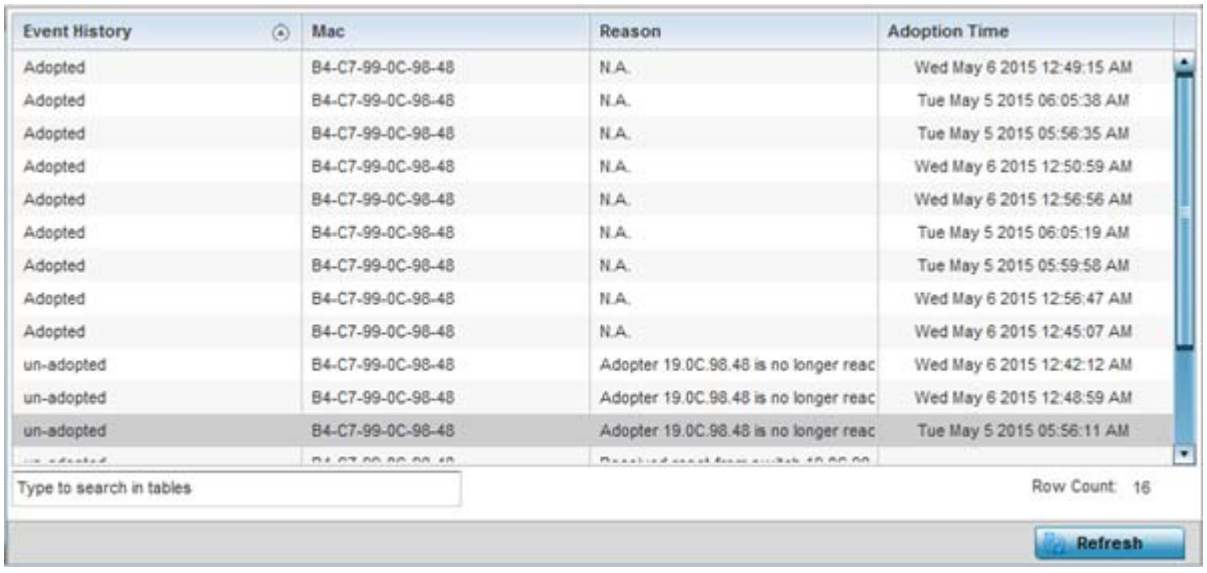


Figure 15-144 *Access Point - AP Self Adoption History screen*

The **AP Self Adoption History** screen describes the following historical data for adopted Access Points:

Event History	Displays the self adoption status of each AP as either *Adopted* or *un-adopted*.
MAC	Displays the hardware encoded *Media Access Control* (MAC) of the auto adopted Access Point.
Reason	Displays the adoption reason code for an Access Point's auto adoption.

Adoption Time	Displays a timestamp for the Access Point's auto-adoption by the controller or service platform.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.6.4 Pending Adoptions

Adoption

The *Pending Adoptions* screen displays a list of devices yet to be adopted to this peer Access Point, or Access Points in the process of adoption.

To view pending Access Point statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand the a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand the **Adoption** menu item.

4 Select **Pending Adoptions**.

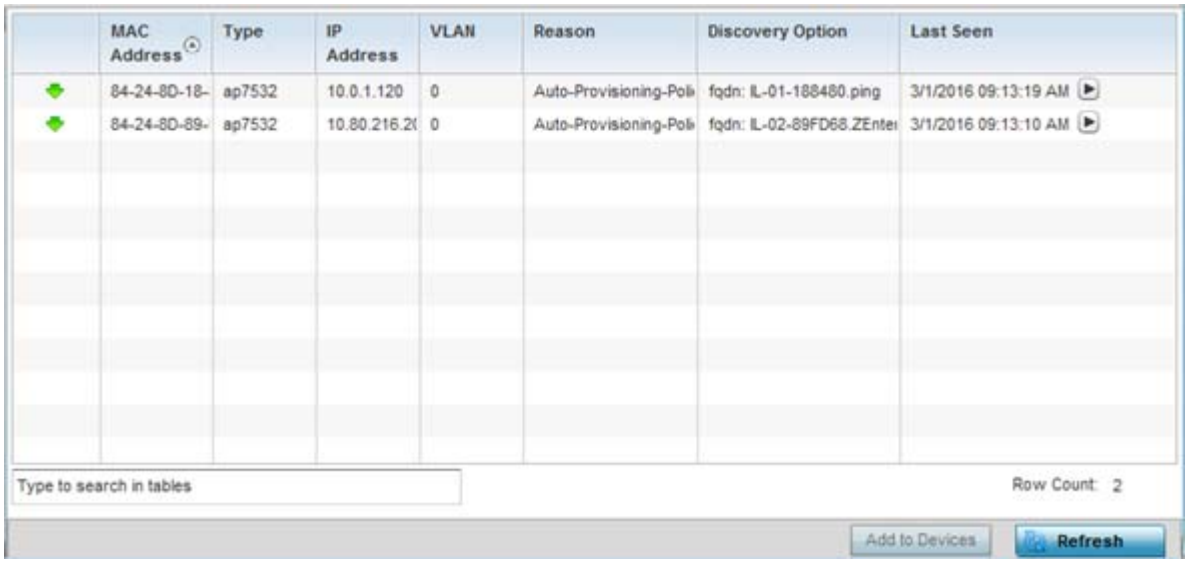


Figure 15-145 *Access Point - Pending Adoptions screen*

The **Pending Adoptions** screen provides the following:

MAC Address	Displays the MAC address of the device pending adoption.
Type	Displays the Access Point's model type.
IP Address	Displays the current network IP Address of the device pending adoption.
VLAN	Displays the current VLAN used as a virtual interface by device pending adoption.
Reason	Displays the status as to why the device is still pending adoption and has not yet successfully connected to this Access Point.
Discovery Option	Displays the discovery option code for each AP listed pending adoption.

Last Seen	Displays the date and time stamp of the last time the device was seen. Click the arrow next to the date and time to toggle between standard time and UTC.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.7 AP Detection

Access Point Statistics

The *AP Detection* screen displays potentially hostile Access Points, their SSIDs, reporting AP, and so on. Continuously revalidating the credentials of detected devices reduces the possibility of an Access Point hacking into the network.

To view the AP detection statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **AP Detection**.

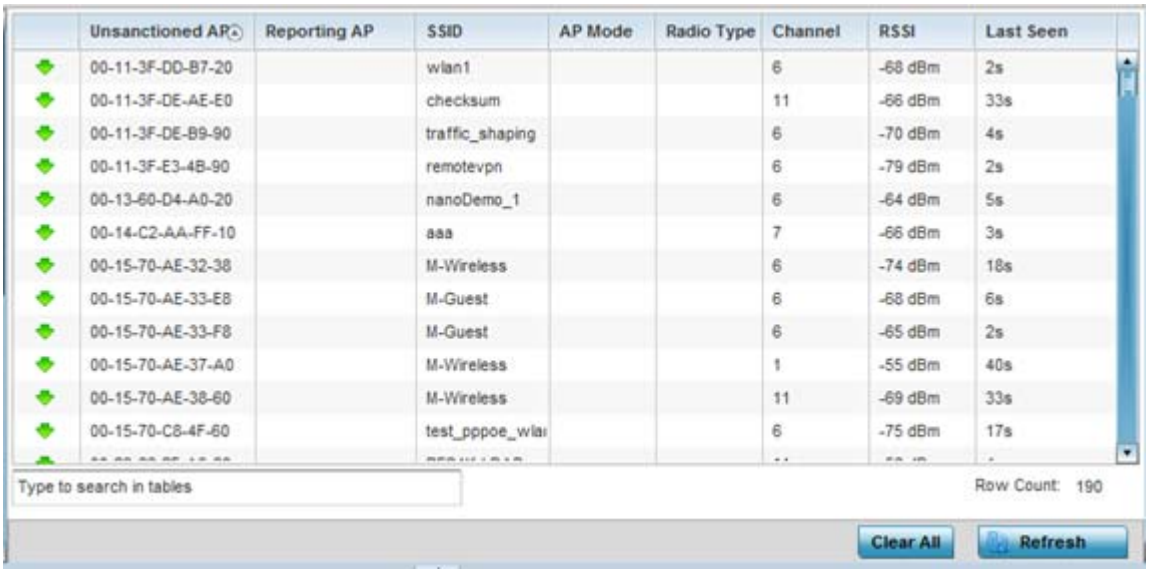


Figure 15-146 *Access Point - AP Detection*

The **AP Detection** screen displays the following:

Unsanctioned AP	Displays the MAC address of a detected Access Point that is yet to be authorized for interoperability within the Access Point managed network.
Reporting AP	Displays the hardware encoded MAC address of the radio used by the detecting Access Point. Select an Access Point to display configuration and network address information in greater detail.
SSID	Displays the WLAN SSID the unsanctioned Access Point was detected on.
AP Mode	Displays the operating mode of the unsanctioned Access Point.
Radio Type	Displays the type of the radio on the unsanctioned Access Point. The radio can be 802.11b, 802.11bg, 802.1bgn, 802.11a or 802.11an.

Channel	Displays the channel the unsanctioned Access Point is currently transmitting on.
RSSI	Lists a *relative signal strength indication* (RSSI) for a detected (and perhaps unsanctioned) Access Point.
Last Seen	Displays the time (in seconds) the unsanctioned Access Point was last seen on the network.
Clear All	Select the *Clear All* button to clear the screen of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.8 Guest User

Access Point Statistics

The *Guest User* screen displays credential information for wireless clients associated with an Access Point. Use this information to assess if configuration changes are required to improve network performance.

To view guest user statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Guest User**.

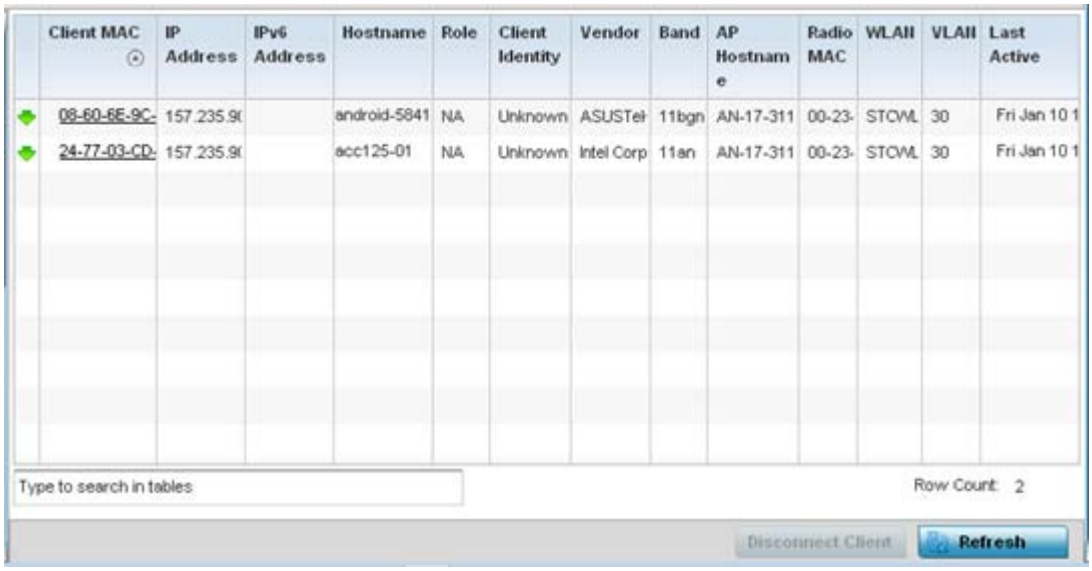


Figure 15-147 *Access Point - Guest User screen*

The **Guest User** screen displays the following client information:

Client MAC	Displays the hardcoded MAC address assigned to the guest client at the factory. The address displays as a link that can be selected to display configuration and network address information in greater detail.

IP Address	Displays the unique IP address of the guest client. Use this address as necessary throughout the applet for filtering and device intrusion recognition and approval.
IPv6 Address	Displays the current IPv6 formatted IP address a listed guest client is using as a network identifier. IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
Hostname	Displays the hostname (MAC addresses) of connected guest clients. The hostname displays as a link that can be selected to display configuration and network address information in greater detail.
Role	Lists the guest client's defined role within the Access Point managed network.
Client Identity	Displays the unique identity of the listed guest client as it appears to its adopting Access Point.
Vendor	Displays the name of the client vendor (manufacturer).
Band	Displays the 802.11 radio band on which the listed guest client operates.
AP Hostname	Displays the administrator assigned hostname of the Access Point to which this Access Point is adopted.
Radio MAC	Displays the MAC address of the radio which the wireless client is using.
WLAN	Displays the name of the WLAN the Access Point's using with each listed guest client. Use this information to determine if the client's WLAN assignment best suits its intended deployment in respect to the WLAN's QoS objective.
VLAN	Displays the VLAN ID each listed guest client is currently mapped to as a virtual interface for Access Point interoperability.
Last Active	Displays the time when this guest client was last seen (or detected) by a device within the Access Point managed network.
Disconnect Client	Select a specific client MAC address and select the *Disconnect Client* button to terminate this client's connection to its Access Point.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.9 Wireless LANs

Access Point Statistics

The *Wireless LANs* screen displays an overview of Access Point WLAN utilization. This screen displays Access Point WLAN assignment, SSIDs, traffic utilization, number of radios the Access Point is utilizing on the WLAN and transmit and receive statistics.

To review a selected Access Point's WLAN statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Wireless LANs**.

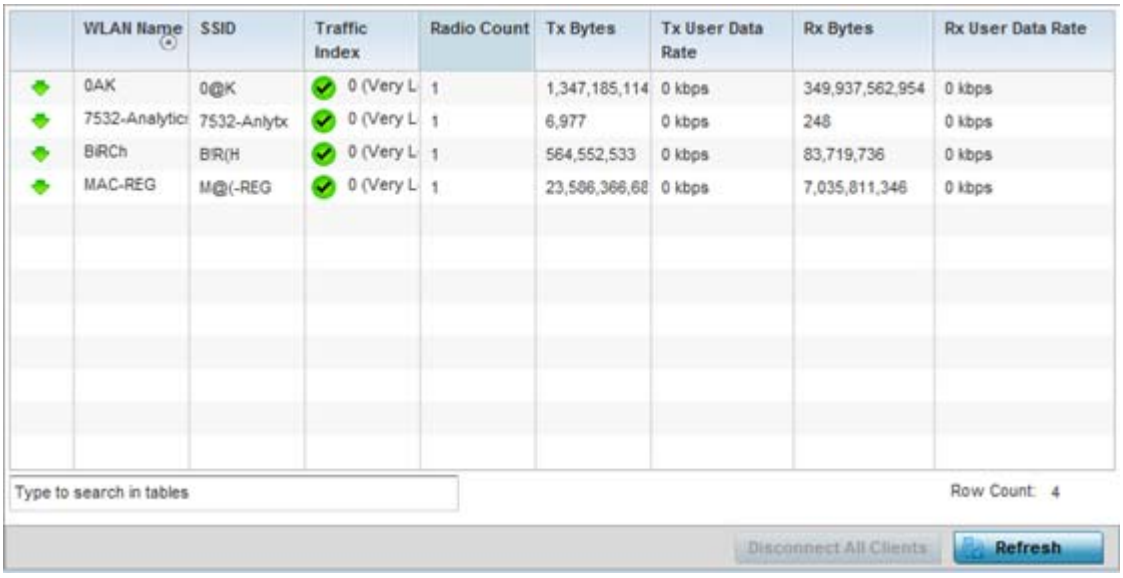


Figure 15-148 *Access Point - Wireless LANs screen*

The **Wireless LANs** screen displays the following:

WLAN Name	Displays the name of the WLAN the Access Point is currently using for client transmissions.
SSID	Displays each listed WLAN's *Service Set ID* (SSID) used as the WLAN's network identifier.
Traffic Index	Displays the traffic utilization index, which measures how efficiently the WLAN's traffic medium is used. It's defined as the percentage of current throughput relative to maximum possible throughput. Traffic indices are: *0 – 20* (very low utilization) *20 – 40* (low utilization) *40 – 60* (moderate utilization) *60 and above* (high utilization)
Radio Count	Displays the cumulative number of peer Access Point radios deployed within each listed WLAN.
Tx Bytes	Displays the average number of transmitted bytes sent on each listed WLAN.
Tx User Data Rate	Displays the transmitted user data rate in kbps for each listed WLAN.
Rx Bytes	Displays the average number of packets in bytes received on each listed WLAN.
Rx User Data Rate	Displays the received user data rate on each listed WLAN.
Disconnect All Clients	Select an WLAN then *Disassociate All Clients* to terminate the client connections within that WLAN.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.10 Policy Based Routing

Access Point Statistics

The *Policy Based Routing* statistics screen displays statistics for selective path packet redirection. PBR can optionally mark traffic for preferential services (QoS). PBR is applied to incoming routed packets, and a route-map is created containing a set of filters and associated actions. Based on the actions defined in the route-map, packets are forwarded to the next relevant hop. Route-maps are configurable under a global policy called *routing-policy*, and applied to profiles and devices.

To review Access Point PBR statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Policy Based Routing**.

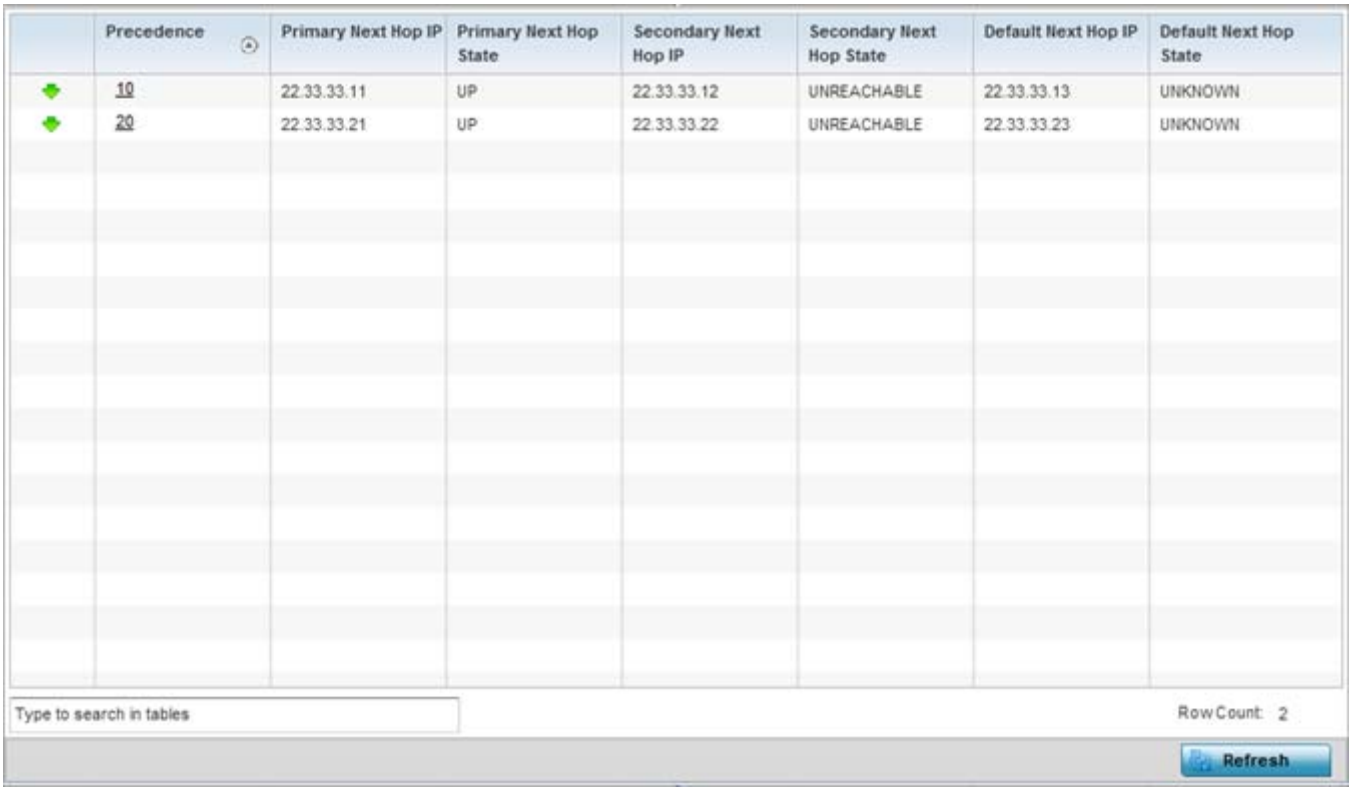


Figure 15-149 *Access Point - Policy Based Routing screen*

The **Policy Based Routing** screen displays the following:

Precedence	Lists the numeric precedence (priority) assigned to each listed PBR configuration. A route-map consists of multiple entries, each carrying a precedence value. An incoming packet is matched against the route-map with the highest precedence (lowest numerical value).
Primary Next Hop IP	Lists the IP address of the virtual resource that, if available, is used with no additional route considerations.
Primary Next Hop State	Displays whether the primary hop is applied to incoming routed packets (UP/ UNREACHABLE).

Secondary Next Hop IP	If the primary hop is unavailable, a second resource is used. This column lists the address set for the alternate route in the election process.
Secondary Next Hop State	Displays whether the secondary hop is applied to incoming routed packets (UP/UNREACHABLE).
Default Next Hop IP	If a packet subjected to PBR does not have an explicit route to the destination, the configured default next hop is used. This is either the IP address of the next hop or the outgoing interface. Only one default next hop is available. The difference between the next hop and the default next-hop is in case of former, PBR occurs first, then destination based routing. In case of the latter, the order is reverse.
Default Next Hop State	Displays whether the default hop is being applied to incoming routed packets.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.11 Radios

Access Point Statistics

The *Radio* statistics screens display information on Access Point radios. The actual number of radios depend on the Access Point model and type. This screen displays information on a per radio basis. Use this information to refine and optimize the performance of each radio and therefore improve network performance.

The Access Point's radio statistics screens provide details about associated radios. It provides radio ID, radio type, RF quality index etc. Use this information to assess the overall health of radio transmissions and Access Point placement.

Each of these screens provide enough statistics to troubleshoot issues related to the following three areas:

- *Status*
- *RF Statistics*
- *Traffic Statistics*

Individual Access Point radios display as selectable links within each of the three Access Point radio screens. To review a radio's configuration in greater detail, select the link within the Radio column of either the *Status*, *RF Statistics* or *Traffic Statistics* screens.

Additionally, navigate the *Traffic*, *WMM TSPEC*, *Wireless LANs* and *Graph* options available on the upper, left-hand side, of the screen to review radio traffic utilization, WMM QoS settings, WLAN advertisement and radio graph information in greater detail. This information can help determine whether the radio is properly configured in respect to its intended deployment objective.

15.4.11.1 Status

Use the *Status* screen to review Access Point radio stats in detail. Use the screen to assess radio type, operational state, operating channel and current power to assess whether the radio is optimally configured.

To view Access Point radio statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand the **Radios** menu item.

4 Select **Status**.

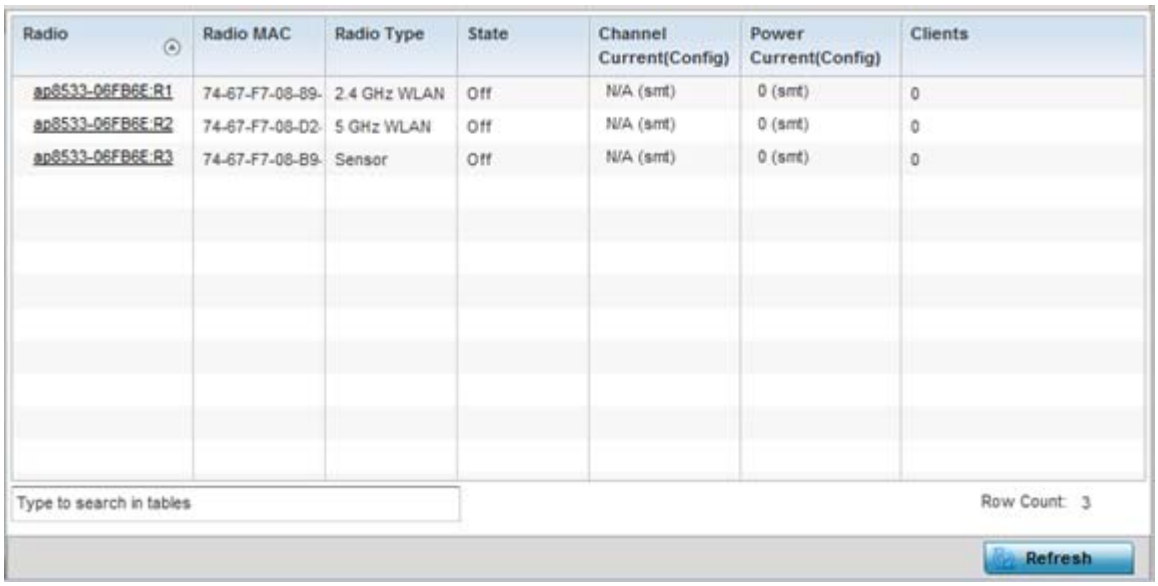


Figure 15-150 *Access Point - Radio Status screen*

The radio **Status** screen provides the following information:

Radio	Displays the name assigned to the radio as its unique identifier. The name displays in the form of a link that can be selected to launch a detailed screen containing radio throughout data.
Radio MAC	Displays the factory encoded hardware MAC address assigned to the radio.
Radio Type	Displays the radio as supporting the 2.4 or 5 GHZ radio band or functioning as a sensor device.
State	Lists a radio's On/Off operational designation.
Channel Current (Config)	Displays the configured channel each listed radio is set to transmit and receive on.
Power Current (Config)	Displays the configured power each listed radio is using to transmit and receive.
Clients	Displays the number of connected clients currently utilizing the listed Access Point radio.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.11.2 RF Statistics

Use the *RF Statistics* screen to review Access Point radio transmit and receive statistics, error rate and RF quality.

To view Access Point radio RF statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand the **Radios** menu item.

4 Select **RF Statistics**.

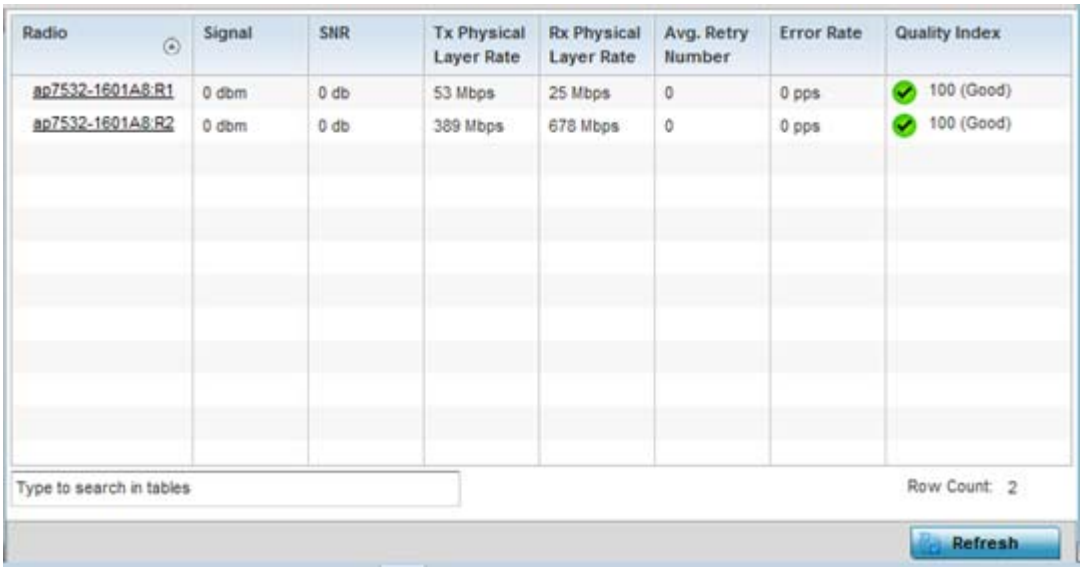


Figure 15-151 *Access Point - Radio RF Statistics screen*

The **RF Statistics** screen lists the following:

Radio	Displays the name assigned to the radio as its unique identifier. The name displays in the form of a link that can be selected to launch a detailed screen containing radio throughout data.
Signal	Displays the radio's current power level in - dBm.
SNR	Displays the signal to noise ratio of the radio's associated wireless clients.
Tx Physical Layer Rate	Displays the data transmit rate for the radio's physical layer. The rate is displayed in Mbps.
Rx Physical Layer Rate	Displays the data receive rate for the radio's physical layer. The rate is displayed in Mbps.
Avg Retry Number	Displays the average number of retries per packet. A high number indicates possible network or hardware problems. Assess the error rate in respect to potentially high signal and SNR values to determine whether the error rate coincides with a noisy signal.
Error Rate	Displays the total number of received packets which contained errors for the listed radio.

Quality Index	Displays the traffic utilization index of the radio. This is expressed as an integer value. 0 – 20 indicates very low utilization, and 60 and above indicate high utilization.
Quality Index	Displays an integer that indicates overall RF performance. The RF quality indices are: *0 – 50* (poor) *50 – 75* (medium) *75 – 100* (good)
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.11.3 Traffic Statistics

Refer to the *Traffic Statistics* screen to review Access Point radio transmit and receive statistics, data rate, and packets dropped during both transmit and receive operations.

To view the Access Point radio traffic statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand **Radios**.

4 Select **Traffic Statistics**.

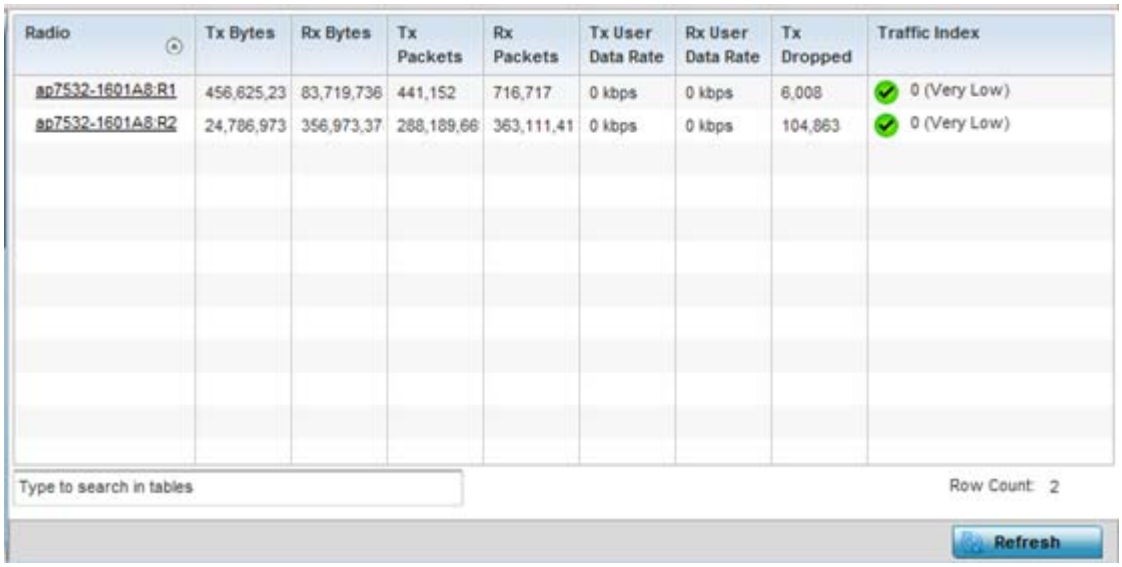


Figure 15-152 *Access Point - Radio Traffic Statistics screen*

The **Traffic Statistics** screen displays the following:

Radio	Displays the name assigned to the radio as its unique identifier. The name displays in the form of a link that can be selected to launch a detailed screen containing radio throughout data.

Tx Bytes	Displays the total number of bytes transmitted by each listed radio. This includes all user data as well as any management overhead data.
Rx Bytes	Displays the total number of bytes received by each listed radio. This includes all user data as well as any management overhead data.
Tx Packets	Displays the total number of packets transmitted by each listed radio. This includes all user data as well as any management overhead packets.
Rx Packets	Displays the total number of packets received by each listed radio. This includes all user data as well as any management overhead packets.
Tx User Data Rate	Displays the rate (in kbps) user data is transmitted by each listed radio. This rate only applies to user data and does not include management overhead.
Rx User Data Rate	Displays the rate (in kbps) user data is received by the radio. This rate only applies to user data and does not include management overhead.
Tx Dropped	Displays the total number of transmitted packets dropped by each listed radio. This includes all user data as well as management overhead packets that were dropped.
Traffic Index	This area displays the traffic index, which measures how efficiently the traffic medium is utilized. It's defined as the percentage of current throughput relative to the maximum possible throughput.The indices include: *0 – 20* (Very low utilization) *20 – 40* (Low utilization) *40 – 60* (Moderate utilization) *60 and above* (High utilization)
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.12 Mesh

Access Point Statistics

The *Mesh* screen provides detailed statistics on each Mesh capable client available within the selected Access Point's radio coverage area.

To view the Mesh statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Mesh**.

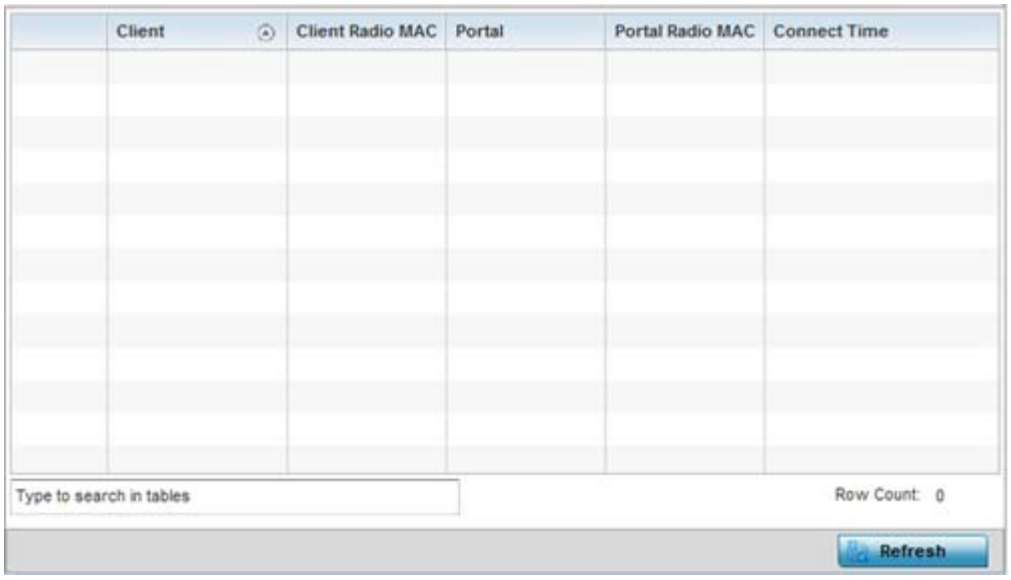


Figure 15-153 *Access Point - Mesh screen*

The **Mesh** screen describes the following:

Client	Displays the system assigned name of each member of the mesh network.
Client Radio MAC	Displays the MAC address of each client radio in the mesh network.
Portal	Mesh points connected to an external network and forward traffic in and out are Mesh Portals. Mesh points must find paths to a Portal to access the Internet. When multiple Portals exist, the Mesh point must select one.
Portal Radio MAC	Lists the MAC addresses of those Access Points serving as mesh portals.
Connect Time	Displays the elapsed connection time for each listed client in the mesh network.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.13 Interfaces

Access Point Statistics

The *Interface* screen provides detailed statistics on each of the interfaces available on the selected Access Point. Use this screen to review the statistics for each interface. Interfaces vary amongst supported Access Point models.

To review Access Point interface statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Interfaces**.

The **General** tab displays by default.

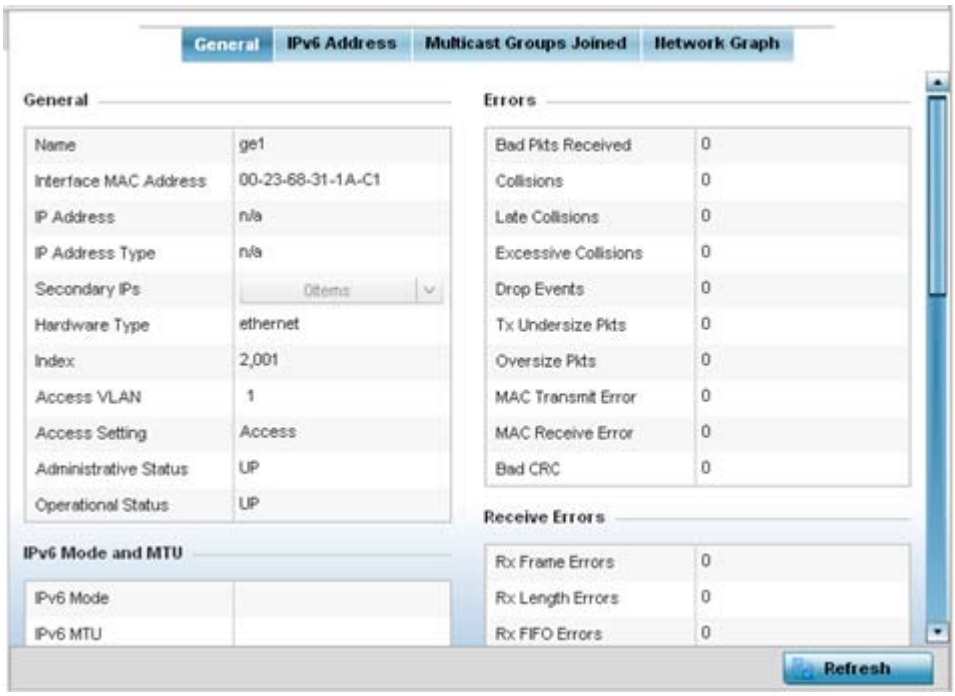


Figure 15-154 *Access Point- General Interface screen*

Interface Statistics support the following:

- *General Interface Details*
- *IPv6 Address*
- *Multicast Groups Joined*
- *Network Graph*

15.4.13.1 General Interface Details

Interfaces

The *General* tab provides information on a selected Access Point interface such as its MAC address, type and TX/RX statistics.

The **General** table displays the following:

Name	Displays the name of the Access Point interface ge1, vlan1 etc.
Interface MAC Address	Displays the MAC address of the interface.
IP Address	IP address of the interface.
IP Address Type	Displays the IP address type, either IPv4 or IPv6.
Secondary IP	Displays a list of secondary IP resources assigned to this interface.
Hardware Type	Displays the networking technology.
Index	Displays the unique numerical identifier for the interface.
Access VLAN	Displays the tag assigned to the native VLAN.
Access Setting	Displays the VLAN mode as either *Access* or *Trunk*.
Administrative Status	Displays whether the interface is currently UP or DOWN.
Operational Status	Lists whether the selected interface is currently UP (operational) or DOWN.

The **IPv6 Mode and MTU** table displays the following:

IPv6 Mode	Lists the current IPv6 mode utilized.
IPv6 MTU	Lists the IPv6 formatted largest packet size that can be sent over the interface.

The **Specification** table displays the following information:

Media Type	Displays the physical connection type of the interface. Medium types include: *Copper* - Used on RJ-45 Ethernet ports *Optical* - Used on fibre optic gigabit Ethernet ports
Protocol	Displays the routing protocol used by the interface.
MTU	Displays the *maximum transmission unit* (MTU) setting configured on the interface. The MTU value represents the largest packet size that can be sent over a link. 10/100 Ethernet ports have a maximum setting of 1500.
Mode	Lists whether traffic on the listed port is Layer 2 or Layer 3.
Metric	Displays the metric associated with the interface's route.
Maximum Speed	Displays the maximum speed the interface uses to transmit or receive data.
Admin Speed	Displays the speed the port can transmit or receive. This value can be either *10*, *100*, *1000* or *Auto*. This value is the maximum port speed in Mbps. Auto indicates the speed is negotiated between connected devices.
Operator Speed	Displays the current speed of data transmitted and received over the interface.
Admin Duplex Setting	Displays the administrator's duplex setting.
Current Duplex Setting	Displays the interface as either *half duplex*, *full duplex* or *unknown*.

The **Traffic** table displays the following:

Good Octets Sent	Displays the number of octets (bytes) with no errors sent by the interface.
Good Octets Received	Displays the number of octets (bytes) with no errors received by the interface.
Good Packets Sent	Displays the number of good packets transmitted.
Good Packets Received	Displays the number of good packets received.
Mcast Pkts Sent	Displays the number of multicast packets sent through the interface.
Mcast Pkts Received	Displays the number of multicast packets received through the interface.
Ucast Pkts Sent	Displays the number of unicast packets sent through the interface.
Ucast Pkts Received	Displays the number of unicast packets received through the interface.
Bcast Pkts Sent	Displays the number of broadcast packets sent through the interface.
Bcast Pkts Received	Displays the number of broadcast packets received through the interface.

Packet Fragments	Displays the number of packet fragments transmitted or received through the interface.
Jabber Pkts	Displays the number of packets transmitted through the interface larger than the MTU.

The **Errors** table displays the following:

Bad Pkts Received	Displays the number of bad packets received through the interface.
Collisions	Displays the number of collisions over the selected interface.
Late Collisions	A late collision is any collision that occurs after the first 64 octets of data have been sent. Late collisions are not normal, and usually the result of out of specification cabling or a malfunctioning device.
Excessive Collisions	Displays the number of excessive collisions. Excessive collisions occur when the traffic load increases to the point a single Ethernet network cannot handle it efficiently.
Drop Events	Displays the number of dropped packets transmitted or received through the interface.
Tx Undersize Pkts	Displays the number of undersized packets transmitted through the interface.
Oversize Pkts	Displays the number of oversized packets transmitted through the interface.
MAC Transmit Error	Displays the number of failed transmits due to an internal MAC sublayer error (that's not a late collision), due to excessive collisions or a carrier sense error.
MAC Receive Error	Displays the number of received packets that failed due to an internal MAC sublayer (that's not a late collision), an excessive number of collisions or a carrier sense error.
Bad CRC	Displays the CRC error. The CRC is the 4 byte field at the end of every frame. The receiving station uses it to interpret if the frame is valid. If the CRC value computed by the interface does not match the value at the end of frame, it is considered as a bad CRC.

The **Receive Errors** table displays the following:

Rx Frame Errors	Displays the number of frame errors received at the interface. A frame error occurs when data is received, but not in an expected format.
Rx Length Errors	Displays the number of length errors received at the interface. Length errors are generated when the received frame length was either less or over the Ethernet standard.
Rx FIFO Errors	Displays the number of FIFO errors received at the interface. First-in First-out queueing is an algorithm that involves buffering and forwarding of packets in the order of arrival. FIFO entails no priority. There is only one queue, and all packets are treated equally. An increase in FIFO errors indicates a probable hardware malfunction.
Rx Missed Errors	Displays the number of missed packets. Packets are missed when the hardware received FIFO has insufficient space to store an incoming packet.
Rx Over Errors	Displays the number of overflow errors received. Overflows occur when a packet size exceeds the allocated buffer size.

The **Transmit Errors** field displays the following:

Tx Errors	Displays the number of packets with errors transmitted on the interface.
Tx Dropped	Displays the number of transmitted packets dropped from the interface.
Tx Aborted Errors	Displays the number of packets aborted on the interface because a clear-to-send request was not detected.
Tx Carrier Errors	Displays the number of carrier errors on the interface. This generally indicates bad Ethernet hardware or bad cabling.
Tx FIFO Errors	Displays the number of FIFO errors transmitted at the interface. *First-in First-Out* queueing is an algorithm that involves the buffering and forwarding of packets in the order of arrival. FIFO uses no priority. There is only one queue, and all packets are treated equally. An increase in the number of FIFO errors indicates a probable hardware malfunction.
Tx Heartbeat Errors	Displays the number of heartbeat errors. This generally indicates a software crash, or packets stuck in an endless loop.
Tx Window Errors	Displays the number of window errors transmitted. TCP uses a sliding window flow control protocol. In each TCP segment, the receiver specifies the amount of additional received data (in bytes) the receiver is willing to buffer for the connection. The sending host can send only up to that amount. If the sending host transmits more data before receiving an acknowledgment, it constitutes a window error.

4 Select the **Refresh** button to update the screen's statistics counters to their latest values.

15.4.13.2 IPv6 Address

Interfaces

IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

To view IPv6 address utilization:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand the **Interfaces** menu from the left-hand side of the UI.

4 Select **IPv6 Address**.

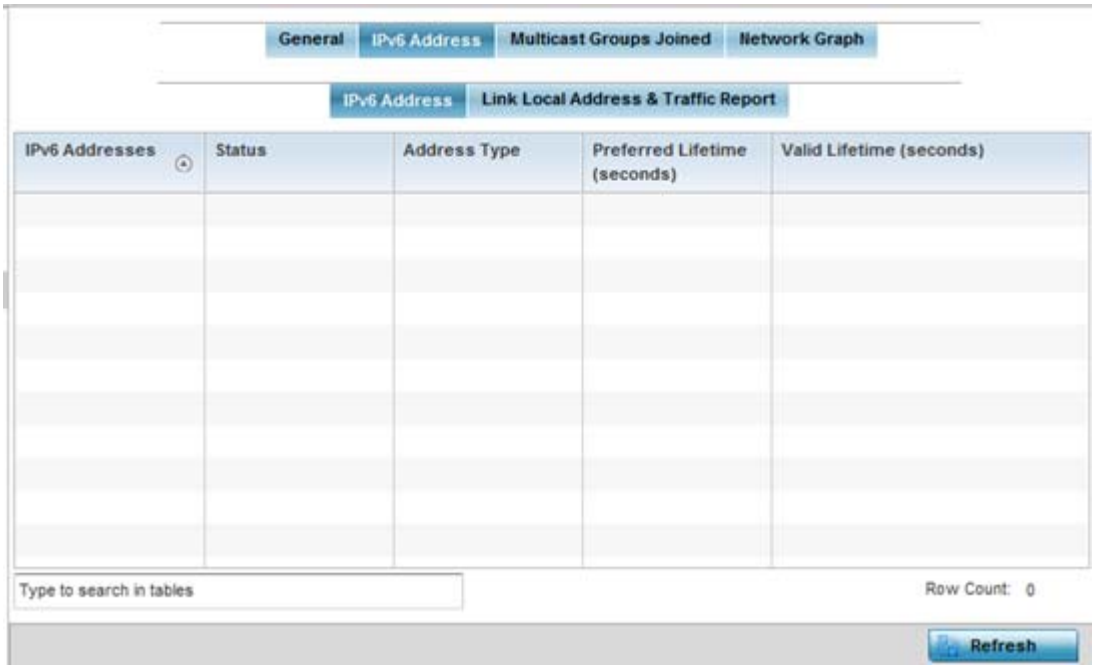


Figure 15-155 *Access Point - Interface IPv6 Address screen*

5 The **IPv6 Addresses** table displays the following:

IPv6 Addresses	Lists the IPv6 formatted addresses currently utilized by the Access Point on the selected interface.
Status	Lists the current utilization status of each IPv6 formatted address currently in use by this controller or Access Point's selected interface.
Address Type	Lists whether the address is unicast or multicast in its utilization over the selected Access Point interface.
Preferred Lifetime (seconds)	Lists is the time in seconds (relative to when the packet is sent) the IPv6 formatted addresses remains in a preferred state on the selected interface. The preferred lifetime must always be less than or equal to the valid lifetime
Valid Lifetime (seconds)	Displays the time in seconds (relative to when the packet is sent) the IPv6 formatted address remains in a valid state on the selected interface. The valid lifetime must always be greater than or equal to the preferred lifetime.

6 Select the **Link Local Address & Traffic Report** tab to assess data traffic and errors discovered in transmitted and received IPv6 formatted data packets.

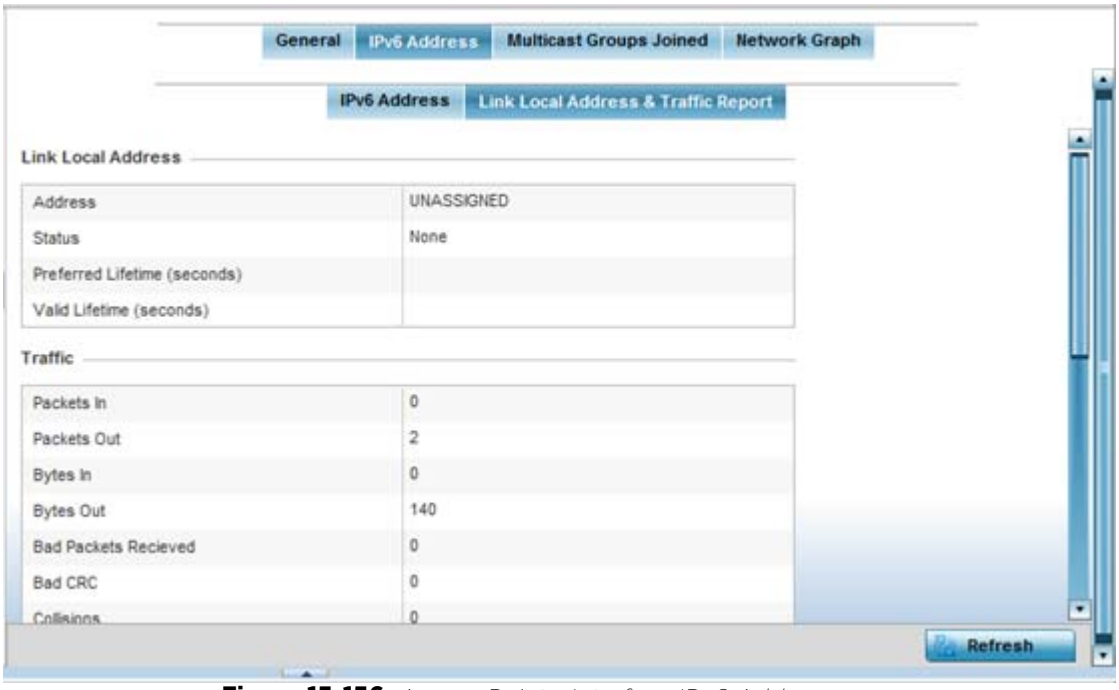


Figure 15-156 *Access Point - Interface IPv6 Address screen*

7 Verify the following **Local Link Address** data for the IPv6 formatted address:

Address	Lists the IPv6 local link address. IPv6 requires a link local address assigned to every interface the IPv6 protocol is enabled on, even when one or more routable addresses are assigned.
Status	Lists the IPv6 local link address utilization status and its current availability.
Preferred Lifetime (seconds)	Lists is the time in seconds (relative to when the packet is sent) the local link addresses remains in the preferred state on the selected interface. The preferred lifetime must always be less than or equal to the valid lifetime.
Valid Lifetime (seconds)	Displays the time in seconds (relative to when the packet is sent) the local link addresses remains in the valid state on the selected interface. The valid lifetime must always be greater than or equal to the preferred lifetime.

8 Verify the following IPv6 formatted **Traffic** data:

Packets In	Lists the number of IPv6 formatted data packets received on the selected Access Point interface since the screen was last refreshed.
Packets Out	Lists the number of IPv6 formatted data packets transmitted on the selected Access Point interface since the screen was last refreshed.
Refresh	Periodically select *Refresh* to update the screen's counters to their latest values.

9 Review the following **Receive Errors** for IPv6 formatted data traffic:

Receive Length Errors	Displays the number of IPv6 length errors received at the interface. Length errors are generated when the received IPv6 frame length was either less or over the Ethernet standard.

Receive Over Errors	Displays the number of IPv6 overflow errors received. Overflows occur when a packet size exceeds the allocated buffer size.
Receive Frame Errors	Displays the number of IPv6 frame errors received at the interface. A frame error occurs when data is received, but not in an expected format.
Receive FIFO Errors	Displays the number of IPv6 FIFO errors received at the interface. *First-in First-out* queueing is an algorithm that involves buffering and forwarding of packets in the order of arrival. FIFO entails no priority. There is only one queue, and all IPv6 formatted packets are treated equally. An increase in FIFO errors indicates a probable hardware malfunction.
Receive Missed Errors	Displays the number of missed IPv6 formatted packets. Packets are missed when the hardware received FIFO has insufficient space to store an incoming packet.

10 Review the following **Transmit Errors** for IPv6 formatted data traffic:

Transmit Errors	Displays the number of IPv6 formatted data packets with errors transmitted on the interface.
Transmit Aborted Errors	Displays the number of IPv6 formatted packets aborted on the interface because a clear-to-send request was not detected.
Transmit Carrier Errors	Displays the number of IPv6 formatted carrier errors on the interface. This generally indicates bad Ethernet hardware or bad cabling.
Transmit FIFO Errors	Displays the number of IPv6 formatted FIFO errors transmitted at the interface. *First-in First-Out* queueing is an algorithm that involves the buffering and forwarding of packets in the order of arrival. FIFO uses no priority. There is only one queue, and all packets are treated equally. An increase in the number of FIFO errors indicates a probable hardware malfunction.
Transmit Heartbeat Errors	Displays the number of IPv6 formatted heartbeat errors. This generally indicates a software crash, or packets stuck in an endless loop.
Transmit Window Errors	Displays the number of IPv6 formatted window errors transmitted. TCP uses a sliding window flow control protocol. In each TCP segment, the receiver specifies the amount of additional received data (in bytes) the receiver is willing to buffer for the connection. The sending host can send only up to that amount. If the sending host transmits more data before receiving an acknowledgment, it constitutes a window error.
Refresh	Select *Refresh* to update the statistics counters to their latest value.

15.4.13.3 Multicast Groups Joined

Interfaces

Multicast groups scale to a larger set of destinations by *not* requiring prior knowledge of who or how many destinations there are. Multicast devices uses their infrastructure efficiently by requiring the source to send a packet only once, even if delivered to a large number of devices. Devices replicate a packet to reach multiple receivers only when necessary.

Access Points are free to join or leave a multicast group at any time. There are no restrictions on the location or members in a multicast group. A host may be a member of more than one multicast group at any given time and does not have to belong to a group to send messages to members of a group.

To view the Access Point's multicast group memberships on the selected interface:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Interfaces**.

4 Select **Multicast Groups Joined.**

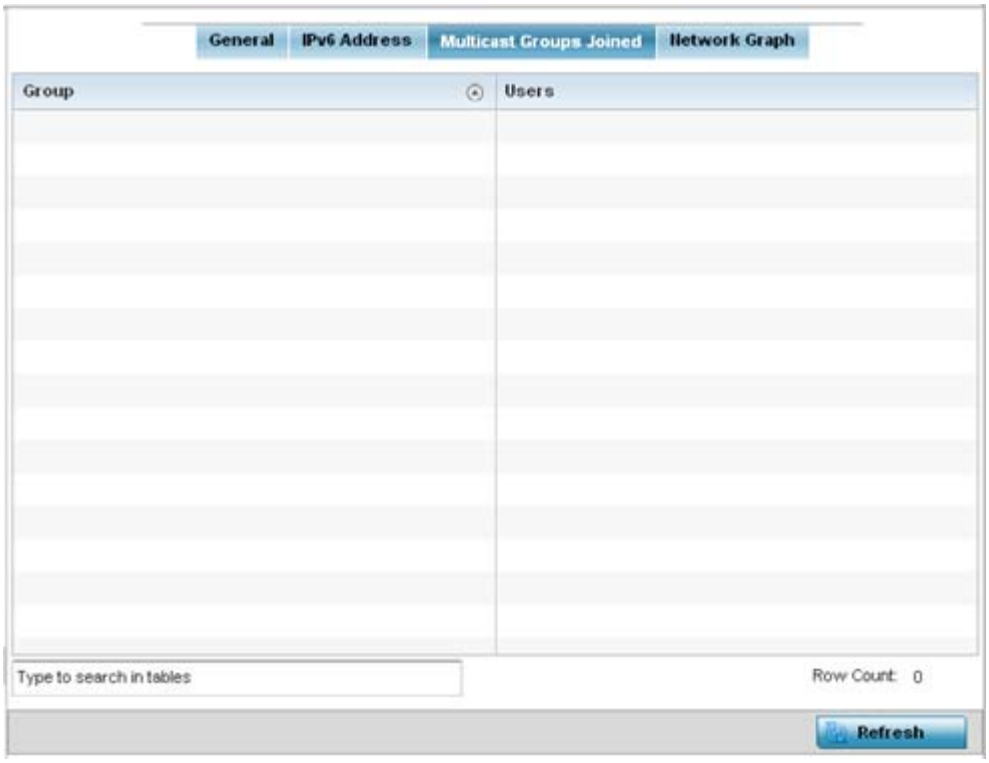


Figure 15-157 *Access Point - Interface Multicast Groups Joined screen*

5 The screen displays the following:

Group	Lists the name of existing multicast groups whose current members share multicast packets with one another on this selected interface as a means of collective interoperation.
Users	Lists the number of devices currently interoperating on this interface in each listed multicast group. Any single device can be a member of more then one group at a time.

6 Periodically select **Refresh** to update the screen's counters to their latest values.

15.4.13.4 Network Graph

Interfaces

The *Network Graph* displays statistics the Access Point continuously collects for its interfaces. Even when the interface statistics graph is closed, data is still collected. Display the interface statistics graph periodically for assessing the latest interface information. Up to three different stats can be selected and displayed within the graph.

To view a detailed graph for an interface, select an interface and drop it on to the graph. The graph displays Port Statistics as the Y-axis and the Polling Interval as the X-axis. Use the **Polling Interval** from the drop-down menu to define the intervals data is displayed on the graph.

To view the Interface Statistics graph:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Interfaces**.

4 Select **Network Graph**. Use the **Parameters** drop-down menu to specify interface values to trend.

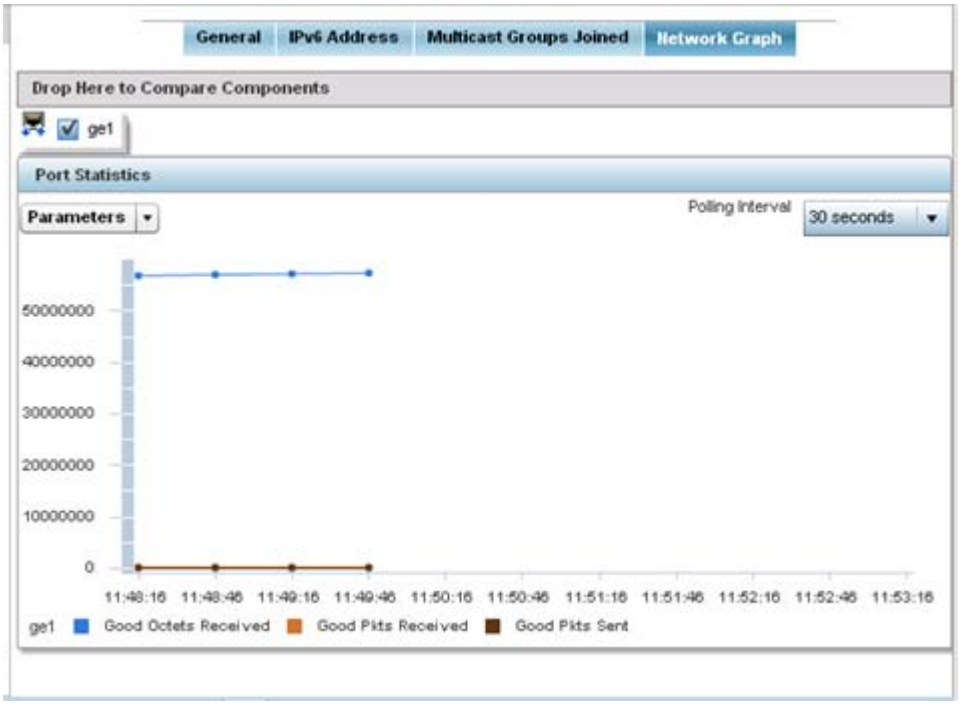


Figure 15-158 *Access Point- Interface Network Graph screen*

15.4.14 RTLS

Access Point Statistics

The *real time locationing system* (RTLS) enables accurate location determination and presence detection capabilities for Wi-Fi-based devices, Wi-Fi-based active RFID tags and passive RFID tags. While the operating system does not support locationing locally, it does report the locationing statistics of both Aeroscout and Ekahau tags.

To review a selected Access Point's RTLS statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **RTLS**.

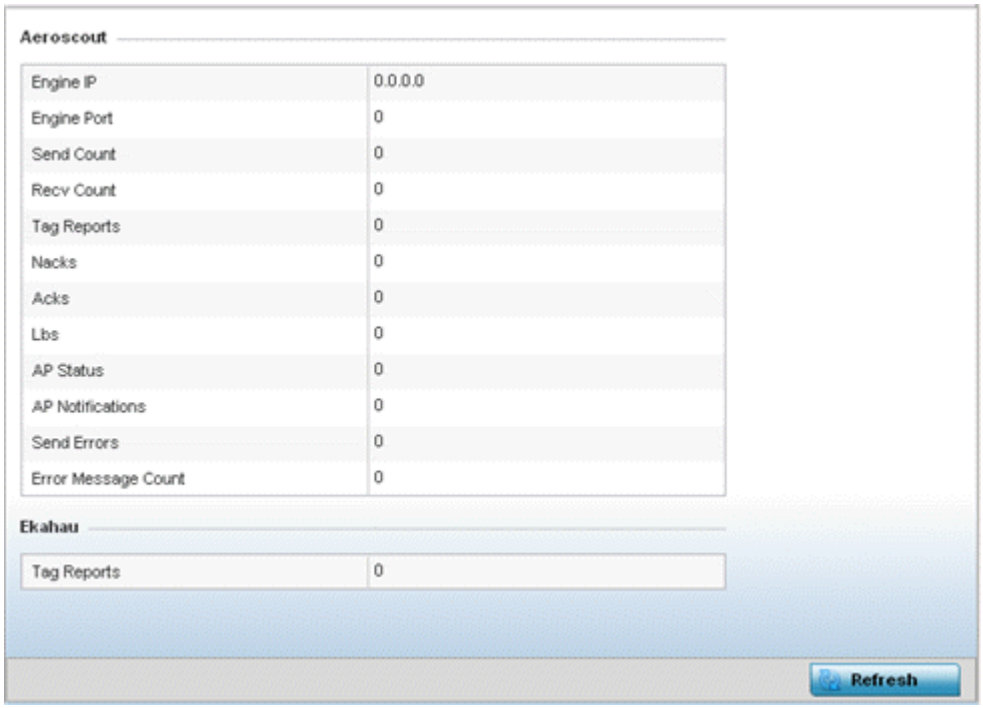


Figure 15-159 *Access Point - RTLS screen*

The Access Point **RTLS** screen displays the following for Aeroscout tags:

Engine IP	Lists the IP address of the Aeroscout locationing engine.
Engine Port	Displays the port number of the Aeroscout engine.
Send Count	Lists the number location determination packets sent by the locationing engine.
Recv Count	Lists the number location determination packets received by the locationing engine.
Tag Reports	Displays the number of tag reports received from locationing equipped radio devices supporting RTLS.
Nacks	Displays the number of *Nack* (no acknowledgement) frames received from RTLS supported radio devices providing locationing services.

Acks	Displays the number of *Ack* (acknowledgment) frames received from RTLS supported radio devices providing locationing services.
Lbs	Displays the number of *location based service* (LBS) frames received from RTLS supported radio devices providing locationing services.
AP Status	Provides the status of peer APs providing locationing assistance.
AP Notifications	Displays a count of the number of notifications sent to Access Points that may be available to provide RTLS support.
Send Errors	Lists the number of send errors received by the RTLS initiating Access Point.
Error Message Count	Displays a cumulative count of error messages received from RTLS enabled Access Point radios.

The Access Point **RTLS** screen displays the following for Ekahau tags:

Tag Reports	Displays the number of tag reports received from locationing equipped radio devices supporting RTLS.

4 Select the **Refresh** button to update the screen's statistics counters to their latest values.

15.4.15 PPPoE

Access Point Statistics

The *PPPoE* statistics screen displays stats derived from the AP's access to high-speed data and broadband networks. PPPoE uses standard encryption, authentication, and compression methods as specified by the PPPoE protocol. PPPoE enables Access Points to establish a point-to-point connection to an ISP over existing Ethernet interface.

To review a selected Access Point's PPPoE statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **PPPoE**.

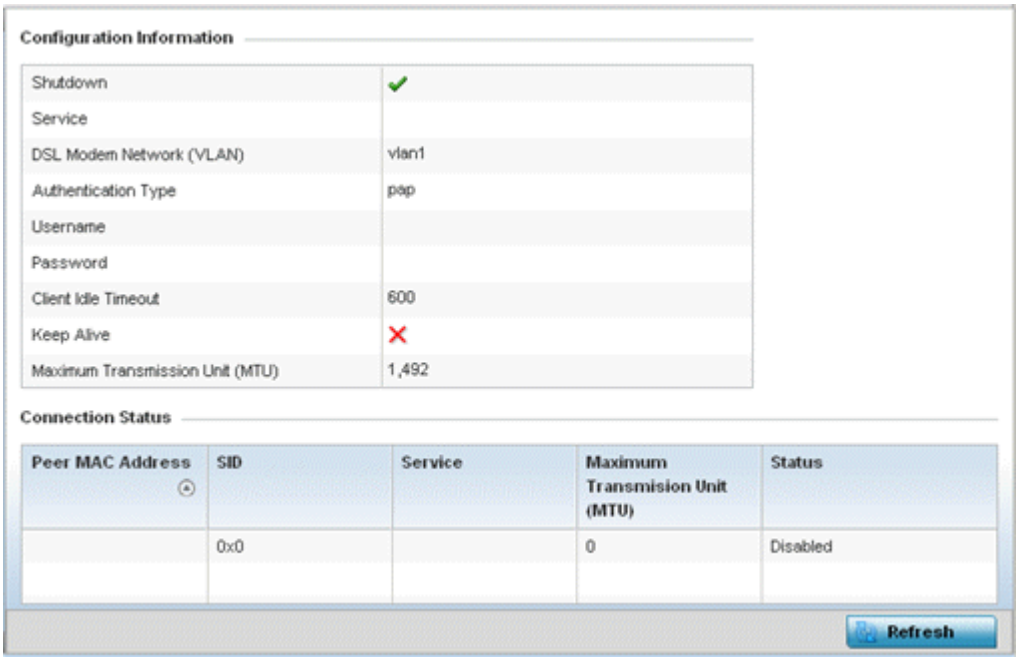


Figure 15-160 *Access Point - PPPoE screen*

The **Configuration Information** field screen displays the following:

Shutdown	Displays whether a high speed client mode point-to-point connection has been enabled using the PPPoE protocol.
Service	Lists the 128 character maximum PPPoE client service name provided by the service provider.
DSL Modem Network (VLAN)	Displays the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to DSL modem.
Authentication Type	Lists authentication type used by the PPPoE client whose credentials must be shared by its peer Access Point. Supported authentication options include *None*, *PAP, CHAP*, *MSCHAP*, and *MSCHAP-v2*.
Username	Displays the 64 character maximum username used for authentication support by the PPPoE client.
Password	Displays the 64 character maximum password used for authentication by the PPPoE client.
Client Idle Timeout	The Access Point uses the listed timeout so it does not sit idle waiting for input from the PPPoE client and the server, that may never come.
Keep Alive	If a keep alive is utilized, the point-to-point connect to the PPPoE client is continuously maintained and not timed out.
Maximum Transmission Unit (MTU)	Displays the PPPoE client *maximum transmission unit* (MTU) from 500 - 1,492. The MTU is the largest physical packet size in bytes a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. A PPPoE client should be able to maintain its point-to-point connection for this defined MTU size.

4 Refer to the **Connection Status** field.

The Connection Status table lists the MAC address, SID, Service information, MTU and status of each route destination peer. To provide this point-to-point connection, each PPPoE session learns the Ethernet address of

a remote PPPoE client, and establishes a session. PPPoE uses both a discover and session phase to identify a client and establish a point-to-point connection. By using such a connection, a Wireless WAN failover is available to maintain seamless network access if the Access Point's Wired WAN were to fail.

5 Select the **Refresh** button to update the screen's statistics counters to their latest values.

15.4.16 Bluetooth

Access Point Statistics

AP-8432 and AP-8533 model Access Points utilize a built in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network. AP-8432 and AP-8533 models support both Bluetooth *classic* and Bluetooth *low energy* technology. These platforms can use their Bluetooth classic enabled radio to sense other Bluetooth enabled devices and report device data (MAC address, RSSI and device calls) to an ADSP server for intrusion detection. If the device presence varies in an unexpected manner, ADSP can raise an alarm.

AP-8432 and AP-8533 model Access Points support Bluetooth beaconing to emit either iBeacon or Eddystone-URL beacons. The Access Point's Bluetooth radio sends non-connectable, undirected *low-energy* (LE) advertisement packets on a periodic basis. These advertisement packets are short, and sent on Bluetooth advertising channels that conform to already-established iBeacon and Eddystone-URL standards.

To view Bluetooth radio statistics for an Access Point:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Point

3 Select **Bluetooth**.

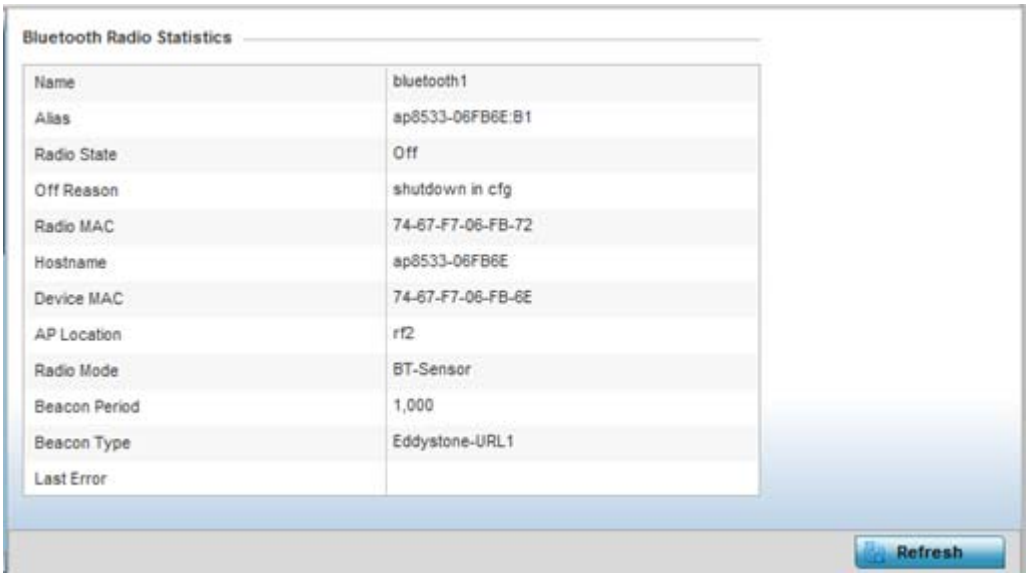


Figure 15-161 *Access Point - Bluetooth screen*

The Access Point's **Bluetooth** screen displays the following:

Name	Lists the name of the Access Point's Bluetooth radio.

Alias	If an alias has been defined for the Access Point its listed here. The alias value is expressed in the form of <hostname>: B<Bluetooth_radio_number>. If the administrator has defined a hostname for the Access Point, it's used in place of the Access Point's default hostname.
Radio State	Displays the current operational state (On/Off) of the Bluetooth radio.
Off Reason	If the Bluetooth radio is offline, this field states the reason.
Radio MAC	Lists the Bluetooth radio's factory encoded MAC address serving as this device's hardware identifier on the network.
Hostname	Lists the hostname set for the Access Point as its network identifier.
Device MAC	Lists the Access Point's factory encoded MAC address serving as this device's hardware identifier on the network.
AP Location	Lists the Access Point's administrator assigned deployment location.
Radio Mode	Lists an Access Point's Bluetooth radio functional mode as either *bt-sensor* or *le-beacon*.
Beacon Period	Lists the Bluetooth radio's beacon transmission period from 100 -10,000 milliseconds.
Beacon Type	Lists the type of beacon currently configured.
Last Error	Lists descriptive text on any error that's preventing the Bluetooth radio from operating.
Refresh	Select *Refresh* to update the screen's statistics counters to their latest values.

15.4.17 OSPF

Access Point Statistics

Open Shortest Path First (OSPF) is a *link-state interior gateway protocol* (IGP). OSPF routes IP packets within a single routing domain (autonomous system), like an enterprise LAN. OSPF gathers link state information from neighbor routers and constructs a network topology. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

Refer to the following for detailed descriptions of the tabs available within the OSPF statistics screen:

- *OSPF Summary*
- *OSPF Neighbors*
- *OSPF Area Details*
- *OSPF Route Statistics*
- *OSPF Route Statistics*
- *OSPF State*

15.4.17.1 OSPF Summary

OSPF

To view OSPF summary statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen), expand the default node and select an Access Point for statistical observation.

3 Select **OSPF**. The *Summary* tab displays by default.

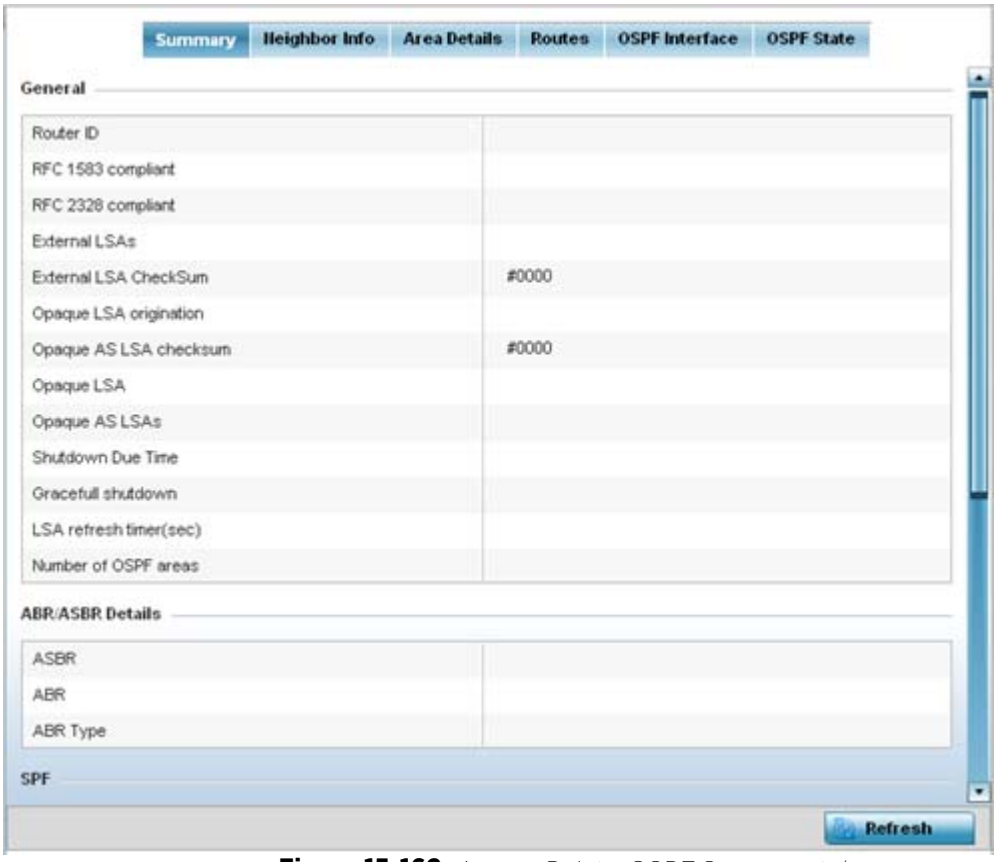


Figure 15-162 *Access Point - OSPF Summary tab*

The **Summary** tab describes the following information fields:

General	The general field displays the router ID assigned for this OSPF connection, RFC compliance information and LSA data.

ABR/ASBR Details	Lists *Autonomous System Boundary Router* (ASBR) data relevant to OSPF routing, including the ASBR, ABR and ABR type. An *Area Border Router* (ABR) is a router that connects one or more areas to the main backbone network. It is considered a member of all areas it is connected to. An ABR keeps multiple copies of the link-state database in memory, one for each area to which that router is connected An ASBR is a router connected to more than one Routing protocol and exchanges routing information with routers in other protocols. ASBRs typically also run an exterior routing protocol (for example, BGP), or use static routes, or both. An ASBR is used to distribute routes received from other, external ASs throughout its own autonomous system. Routers in other areas use ABR as next hop to access external addresses. Then the ABR forwards packets to the ASBR announcing the external addresses.
SPF	Refer to the SPF field to assess the status of the *shortest path forwarding* (SFF) *execution*, *last SPF execution*, *SPF delay*, *SPF due in*, *SPF hold multiplier, SPF hold time*, *SPF maximum hold time* and *SPF timer due flag*.
Stub Router	The summary screen displays information relating to stub router advertisements and shutdown and startup times. An OSPF stub router advertisement allows a new router into a network without immediately routing traffic through the new router and allows a graceful shut down or reload a router without dropping packets that are destined for other networks. This feature introduces three configuration options that allow you to configure a router that is running the OSPF protocol to advertise a maximum or infinite metric to all neighbors.

4 Select the **Refresh** button to update the statistics counters to their latest values.

15.4.17.2 OSPF Neighbors

▸ *OSPF*

OSPF establishes neighbor relationships to exchange routing updates with other routers. An Access Point supporting OSPF sends hello packets to discover neighbors and elect a designated router. The hello packet includes link state information and list of neighbors. OSPF is savvy with layer 2 topologies. If on a point-to-point link, OSPF knows it is sufficient, and the link stays up. If on a broadcast link, the router waits for election before determining if the link is functional.

To view OSPF neighbor statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen), expand the default node and select an Access Point for statistical observation.

3 Select **OSPF**.

4 Select the **Neighbor Info** tab.

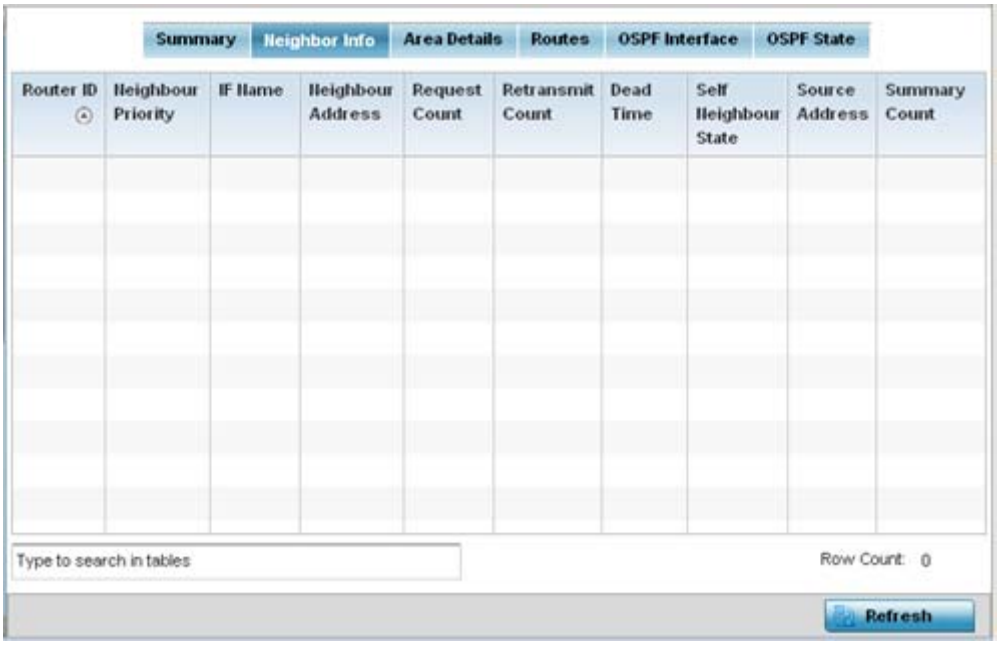


Figure 15-163 *Access Point - OSPF Neighbor Info tab*

The **Neighbor Info** tab describes the following:

Router ID	Displays the router ID assigned for this OSPF connection. The router is a level three Internet Protocol packet switch. This ID must be established in every OSPF instance. If not explicitly configured, the highest logical IP address is duplicated as the router identifier. However, since the router identifier is not an IP address, it does not have to be a part of any routable subnet in the network.
Neighbor Priority	Displays each listed neighbor's priority in respect to becoming the designated router managing the OSPF connection. The designated router is the router interface elected among all routers on a particular multi-access network segment.
IF Name	Lists the name assigned to the router interface used to support connections amongst OSPF enabled neighbors.
Neighbor Address	Lists the IP address of the neighbor sharing the router interface with each listed router ID.
Request Count	Lists the connection request count (hello packets) to connect to the router interface, discover neighbors and elect a designated router.
Retransmit Count	Lists the connection retransmission count attempted in order to connect to the router interface, discover neighbors and elect a designated router. A *designated router* (DR) is the router interface elected among all routers on a particular multi-access network segment, generally assumed to be broadcast.
Dead Time	Lists the dead time between neighbors in the network topology that are currently utilizing the listed router ID.
Self Neighbor State	Displays the self-neighbor status assessment used to discover neighbors and elect a designated router.
Source Address	Displays the single source address used by all neighbor routers to obtain topology and connection status. This form of multicasting significantly reduces network load.

Summary Count	Routes that originate from other areas are called summary routes. Summary routes are not flooded in a totally stubby or NSSA totally stubby area.

5 Select the **Refresh** button to update the statistics counters to their latest values.

15.4.17.3 OSPF Area Details

OSPF

An OSPF network is subdivided into routing areas (with 32 bit area identifiers) to simplify administration and optimize traffic utilization. Areas are logical groupings of hosts and networks, including routers having interfaces connected to an included network. Each area maintains a separate link state database whose information may be summarized towards the rest of the network. An OSPF Area contains a set of routers exchanging *Link State Advertisements* (LSAs) with others in the same area. Areas limit LSAs and encourage aggregate routes. Areas are identified by 32-bit IDs, expressed either in decimal, or octet-based dot-decimal notation.

To view OSPF area statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen), expand the default node and select an Access Point for statistical observation.

3 Select **OSPF**.

4 Select the **Area Details** tab.

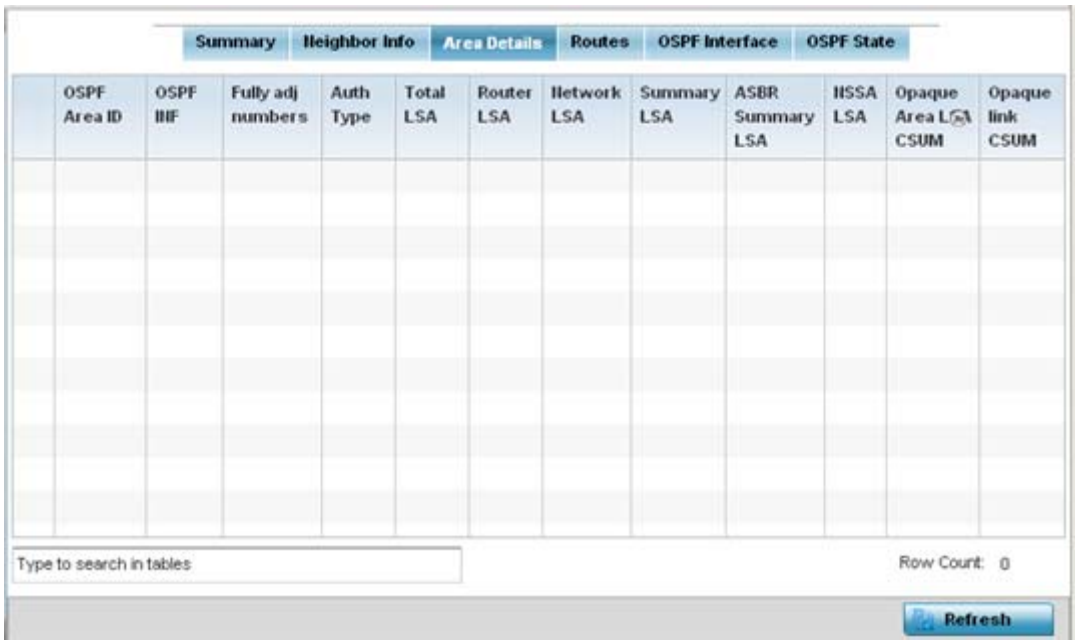


Figure 15-164 *Access Point - OSPF Area Details tab*

The **Area Details** tab describes the following:

OSPF Area ID	Displays either the integer (numeric ID) or IP address assigned to the OSPF area as a unique identifier.
OSPF INF	Lists the interface ID (virtual interface for dynamic OSPF routes) supporting each listed OSPF area ID.

Fully adj numbers	Fully adjusted numbers strip away the effects of other non OSPF and LSA factors and events, leaving only relevant OSPF area network route events counted.
Auth Type	Lists the authentication schemes used to validate the credentials of dynamic route connections and their areas.
Total LSA	Lists the *Link State Advertisements* (LSAs) of all entities using the dynamic route (in any direction) in the listed area ID.
Router LSA	Lists the Link State Advertisements of the router supporting each listed area ID. The router LSA reports active router interfaces, IP addresses, and neighbors.
Network LSA	Displays which routers are joined together by the designated router on a broadcast segment (e.g. Ethernet). Type 2 LSAs are flooded across their own area only. The link state ID of the type 2 LSA is the IP interface address of the designated route.
Summary LSA	The summary LSA is generated by ABR to leak area summary address info into another areas. ABR generates more than one summary LSA for an area if the area addresses cannot be properly aggregated by only one prefix.
ASBR Summary LSA	Originated by ABRs when an ASBR is present to let other areas know where the ASBR is. These are supported just like summary LSAs.
NSSA LSA	Routers in a *Not-so-stubby-area* (NSSA) do not receive external LSAs from Area Border Routers, but are allowed to send external routing information for redistribution. They use type 7 LSAs to tell the ABRs about these external routes, which the Area Border Router then translates to type 5 external LSAs and floods as normal to the rest of the OSPF network. Redistribution into an NSSA area creates a special type of LSA known as TYPE 7, which can exist only in an NSSA area. An NSSA ASBR generates this LSA, and an NSSA ABR router translates it into type 5 LSA which gets propagated into the OSPF domain.
Opaque Area LSA CSUM	Displays the Type-10 opaque link area checksum with the complete contents of the LSA. Type-10 Opaque LSAs are not flooded beyond the borders of their associated area.
Opaque link CSUM	Displays the Type-10 opaque link checksum with the complete contents of the LSA.

5 Select the **Refresh** button to update the statistics counters to their latest values.

15.4.17.4 OSPF Route Statistics

OSPF

Refer to the *Routes* tab to assess the status of OSPF *Border Routes, External Routes*, *Network Routes* and *Router Routes*.

To view OSPF route statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen), expand the default node and select an Access Point for statistical observation.

3 Select **OSPF**.

4 Select the **Routes** tab. The Border Routers tab display by default.

An *area border router* (ABR) connects (links) more than one area. Usually an ABR is used to connect non-backbone areas to the backbone. If OSPF virtual links are used an ABR will also be used to connect the area using the virtual link to another non-backbone area. Border routes use internal OSPF routing table entries to an ABR or *Autonomous System Boundary Router* (ASBR). Border routers maintain an LSDB for each area supported. They also participate in the backbone.

5 Refer to **External Routes** tab.

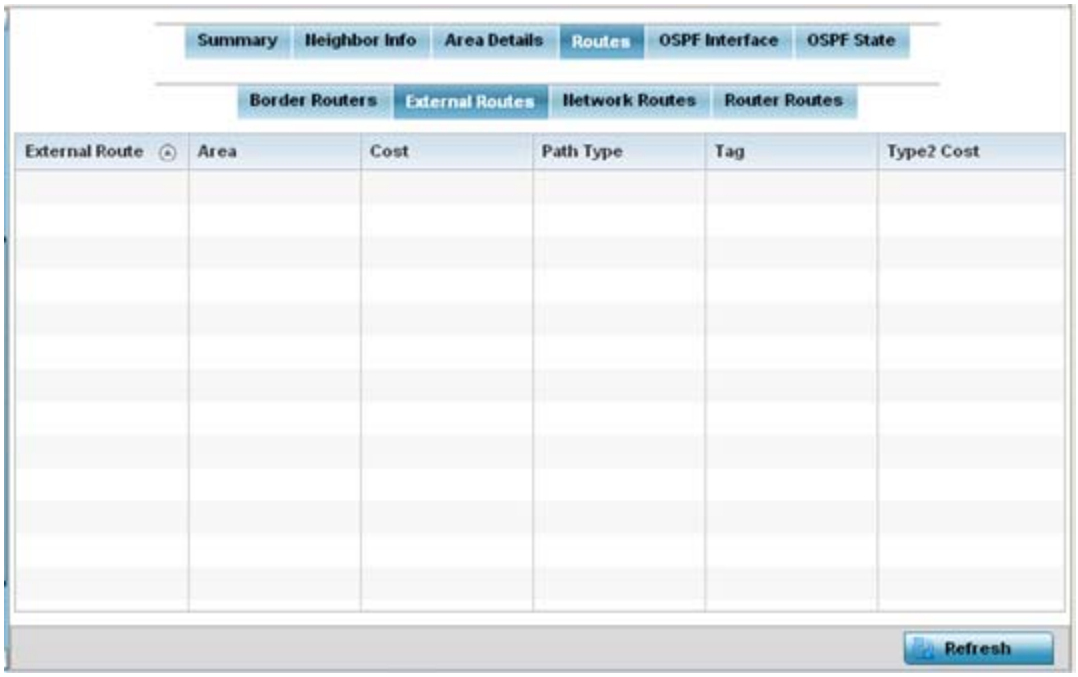


Figure 15-165 *Access Point - OSPF External Routes tab*

External routes are external to area, originate from other routing protocols (or different OSPF processes) and are inserted into OSPF using redistribution. A *stub* area is configured not to carry external routes. Each external route can be tagged by the advertising router, enabling the passing of additional information between routers. Each external route can also be tagged by the advertising router, enabling the passing of additional information between routers on the boundary of the autonomous system.

The External route tab displays a list of external routes, the area impacted, cost, path type, tag and type 2 cost. Cost factors may be the distance of a router (round-trip time), network throughput of a link, or link availability and reliability, expressed as simple unit-less numbers. This provides a dynamic process of traffic load balancing between routes of equal cost.

6 Refer to the **Network Routes** tab.

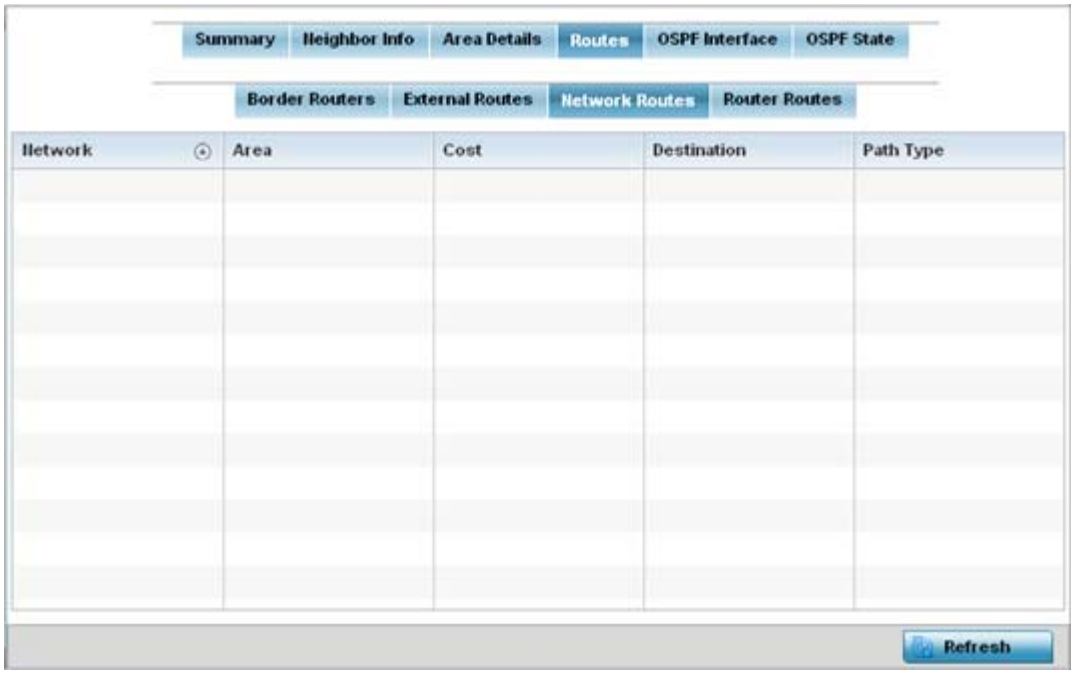


Figure 15-166 *Access Point - OSPF Network Routes tab*

Network routes support more than two routers, with the capability of addressing a single physical message to all attached routers (broadcast). Neighboring routers are discovered dynamically using OSPF hello messages. This use of the hello protocol takes advantage of broadcast capability. An OSPF network route makes further use of multicast capabilities, if they exist. Each pair of routers on the network is assumed to communicate directly.

The network tab displays the network name, impacted OSPF area, cost, destination and path type.

7 Select the **Router Routes** tab.

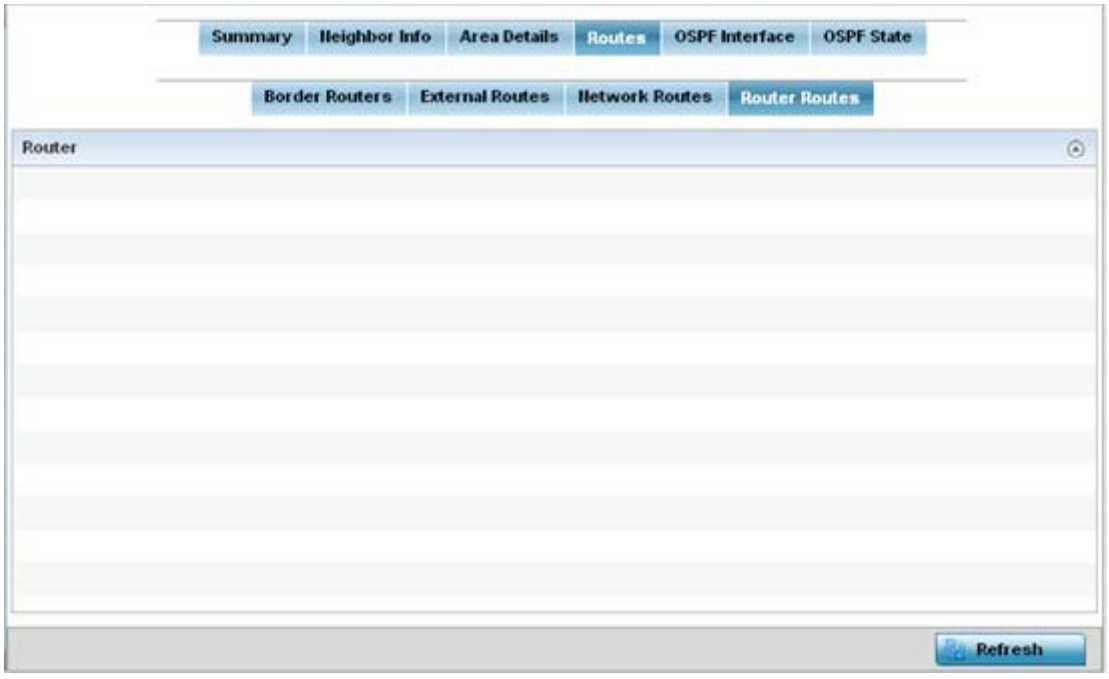


Figure 15-167 *Access Point - OSPF Router Routes tab*

An internal (or *router*) route connects to one single OSPF area. All of its interfaces connect to the area in which it is located and does not connect to any other area.

8 Select the **Refresh** button (within any of the four OSPF Routes tabs) to update the statistics counters to their latest values.

15.4.17.5 OSPF Interface

OSPF

An OSPF interface is the connection between a router and one of its attached networks. An interface has state information associated with it, which is obtained from the underlying lower level protocols and the routing protocol itself. A network interface has associated a single IP address and mask (unless the network is an unnumbered point-to-point network). An interface is sometimes also referred to as a link.

To view OSPF interface statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen), expand the default node and select an Access Point for statistical observation.

3 Select **OSPF**.

4 Select the **OSPF Interface** tab.

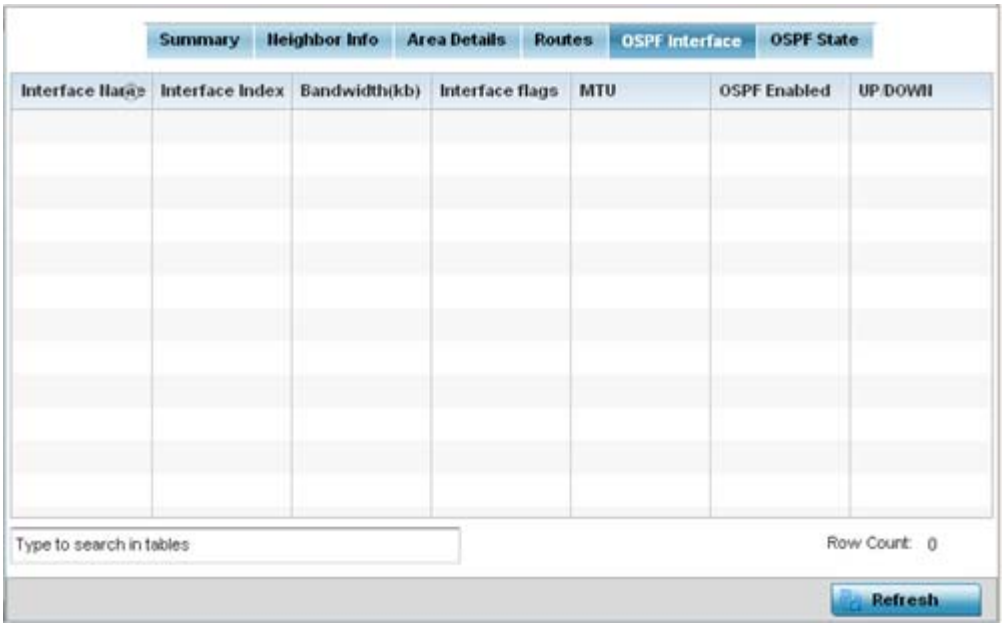


Figure 15-168 *Access Point - OSPF Interface tab*

The **OSPF Interface** tab describes the following:

Interface Name	Displays the IP addresses and mask defined as the virtual interface for dynamic OSPF routes. Zero config and DHCP can be used to generate route addresses, or a primary and secondary address can be manually provided.
Interface Index	Lists the numerical index used for the OSPF interface. This interface ID is in the hello packets establishing the OSPF network connection.
Bandwidth (kb)	Lists the OSPF interface bandwidth (in Kbps) in the range of 1 - 10,000,000.
Interface Flags	Displays the flag used to determine the interface status.

MTU	Lists the OSPF interface *maximum transmission unit* (MTU) size. The MTU is the largest physical packet size (in bytes) a network can transmit. Any packets larger than the MTU are divided into smaller packets before being sent.
OSPF Enabled	Lists whether OSPF has been enabled for each listed interface. OSPF is disabled by default.
UP/DOWN	Displays whether the OSPF interface (the dynamic route) is currently up or down for each listed interface. An OSPF interface is the connection between a router and one of its attached networks.

5 Select the **Refresh** button to update the statistics counters to their latest values.

15.4.17.6 OSPF State

OSPF

An OSPF enabled Access Point sends hello packets to discover neighbors and elect a designated router for dynamic links. The hello packet includes link *state* data maintained on each Access Point and is periodically updated on all OSPF members. The Access Point tracks link state information to help assess the health of the OSPF dynamic route.

To view OSPF state statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen), expand the default node and select an Access Point for statistical observation.

3 Select **OSPF**.

4 Select the **OSPF State** tab.

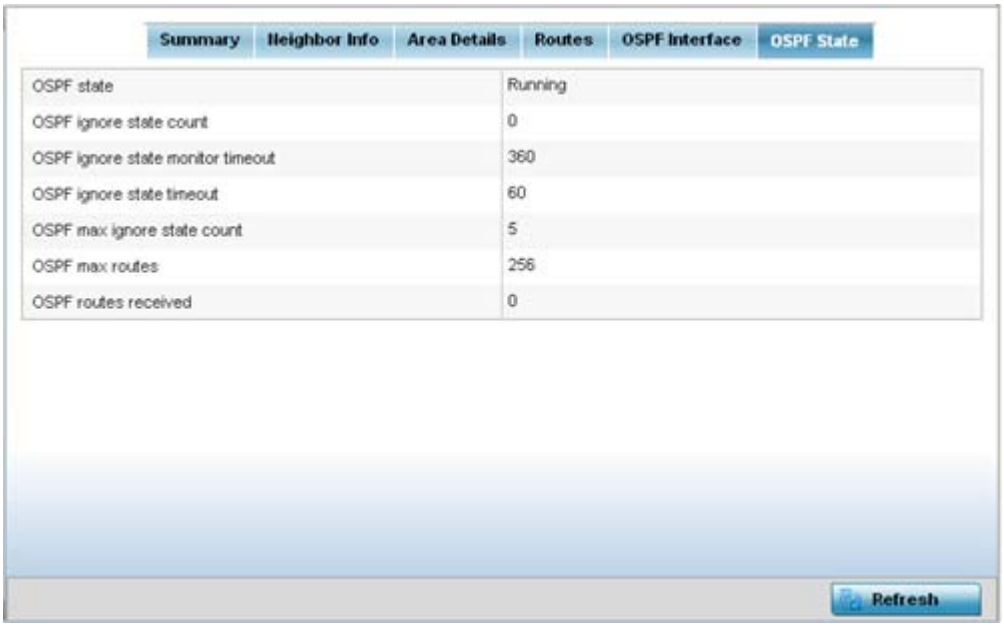


Figure 15-169 *Access Point OSPF - State tab*

The **OSPF State** tab describes the following:

OSPF state	Displays the OSPF link state amongst neighbors within the OSPF topology. Link state information is maintained in a *link-state database* (LSDB) which is a tree image of the entire network topology. Identical copies of the LSDB are periodically updated through flooding on all OSPF supported nodes. Flooding is the part of the OSPF protocol that distributes and synchronizes the link-state database between OSPF routers.
OSPF ignore state count	Lists the number of times state requests have been ignored between the Access Point and its peers within this OSPF supported broadcast domain.
OSPF ignore state monitor timeout	Displays the timeout that, when exceeded, prohibits the Access Point from detecting changes to the OSPF link state.
OSPF ignore state timeout	Displays the timeout that, when exceeded, returns the Access Point back to state assessment amongst neighbors in the OSPF topology.
OSPF max ignore state count	Displays whether an OSPF state timeout is being ignored and not utilized in the transmission of state update requests amongst neighbors within the OSPF topology.
OSPF max routes	States the maximum number of routes negotiated amongst neighbors within the OSPF topology.
OSPF routes received	Lists the routes received and negotiated amongst neighbors within the OSPF topology.

5 Select the **Refresh** button to update the statistics counters to their latest values.

15.4.18 L2TPv3 Tunnels

Access Point Statistics

Access Points use L2TP V3 to create tunnels for transporting layer 2 frames. L2TP V3 enables an Access Point to create tunnels for transporting Ethernet frames to and from bridge VLANs and physical ports. L2TP V3 tunnels can be defined between WING devices and other devices supporting the L2TP V3 protocol.

To review a selected Access Point's L2TPv3 statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **L2TPv3**.

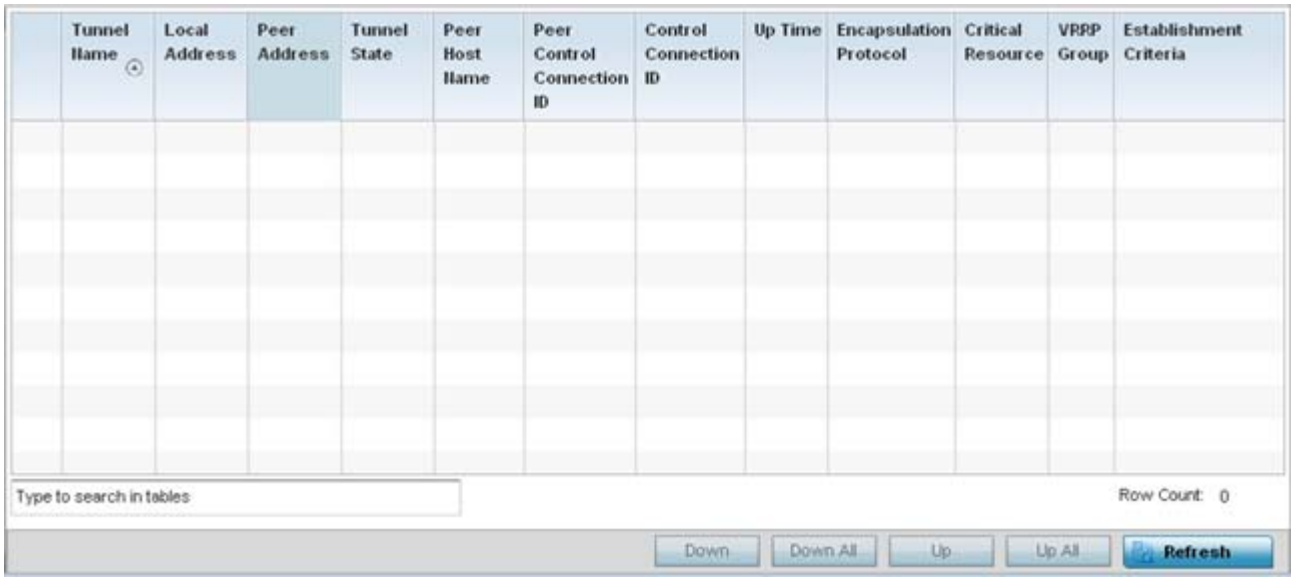


Figure 15-170 *Access Point - L2TPv3 screen*

The Access Point **L2TPv3 Tunnels** screen displays the following:

Tunnel Name	Displays the name of each listed L2TPv3 tunnel assigned upon creation. Each listed tunnel name can be selected as a link to display session data specific to that tunnel. The Sessions screen displays cookie size information as well as psuedowire information specific to the selected tunnel. Data is also available to define whether the tunnel is a trunk session and whether tagged VLANs are used. The number of transmitted, received and dropped packets also display to provide a throughput assessment of the tunnel connection. Each listed session name can also be selected as a link to display VLAN information specific to that session. The VLAN Details screen lists those VLANs used an Access Point interface in L2TP tunnel establishment.
Local Address	Lists the IP address assigned as the local tunnel end point address, not the tunnel interface's IP address. This IP is used as the tunnel source IP address. If a local address is not specified, the source IP address is chosen automatically based on the tunnel peer IP address.
Peer Address	Lists the IP address of the L2TP tunnel peer establishing the tunnel connection.
Tunnel State	States whether the tunnel is Idle (not utilized by peers) or is currently active.
Peer Host Name	Lists the assigned peer hostname used as matching criteria in the tunnel establishment process.
Peer Control Connection ID	Displays the numeric identifier for the tunnel session. This is the peer pseudowire ID for the session. This source and destination IDs are exchanged in session establishment messages with the L2TP peer.
CTRL Connection ID	Displays the router ID(s) sent in tunnel establishment messages with a potential peer device.
Up Time	Lists the amount of time the L2TP connection has remained established amongst peers sharing the L2TPv3 tunnel connection. The Up Time is displayed in a *Days*: *Hours*: *Minutes*: *Seconds*: format. If D:0 H:0 M:0 S:0 is displayed, the tunnel connection is not currently established.

Encapsulation Protocol	Displays either *IP* or *UDP* as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes. Tunneling is also called encapsulation. Tunneling works by encapsulating a network protocol within packets carried by the second network.
Critical Resource	Lists critical resources for this tunnel. Critical resources are device IP addresses on the network (gateways, routers etc.). These IP addresses are critical to the health of the network. These device addresses are pinged regularly by Access Points. If there's a connectivity issue, an event is generated stating a critical resource is unavailable.
VRRP Group	Displays the VRRP group name if configured. VRRP configurations support router redundancy in a wireless network requiring high availability.
Establishment Criteria	Displays the tunnel establishment criteria for this tunnel. Tunnel establishment involves exchanging 3 message types (SCCRQ, SCCRP and SCCN) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest value.

15.4.19 VRRP

Access Point Statistics

The *VRRP* statistics screen displays *Virtual Router Redundancy Protocol* (VRRP) configuration statistics supporting router redundancy in a wireless network requiring high availability.

To review a selected Access Point's VRRP statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **VRRP**.

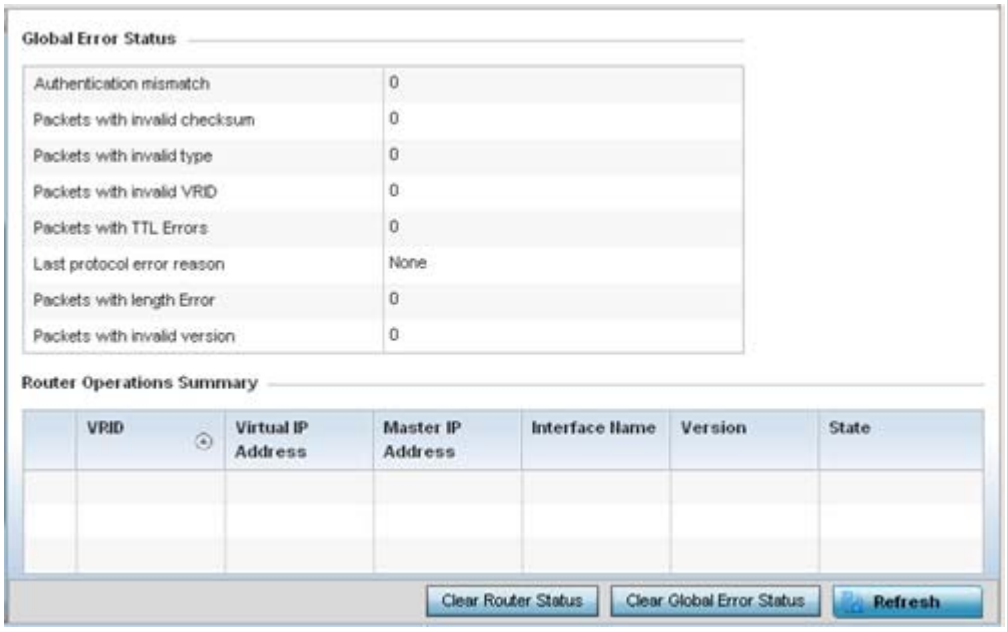


Figure 15-171 *Access Point - VRRP screen*

4 Refer to the **Global Error Status** field to review the various sources of packet errors logged during the implementation of the virtual route.

Errors include the mismatch of authentication credentials, invalid packet checksums, invalid packet types, invalid virtual route IDs, TTL errors, packet length errors and invalid (non matching) VRRP versions.

5 Refer to the **Router Operations Summary** for the following status:

VRID	Lists a numerical index (1 - 254) used to differentiate VRRP configurations. The index is assigned when a VRRP configuration is initially defined. This ID identifies the virtual router a packet is reporting status for.
Virtual IP Address	Lists the virtual interface IP address used as the redundant gateway address for the virtual route.
Master IP Address	Displays the IP address of the elected VRRP master. A VRRP master (once elected) responds to ARP requests, forwards packets with a destination link layer MAC address equal to the virtual router MAC address, rejects packets addressed to the IP address associated with the virtual router and accepts packets addressed to the IP address associated with the virtual router.
Interface Name	Displays the interfaces selected on the Access Point to supply VRRP redundancy failover support.
Version	Display VRRP version 3 (RFC 5798) or 2 (RFC 3768) as selected to set the router redundancy. Version 3 supports sub-second (centisecond) VRRP failover and support services over virtual IP.
State	Displays the current state of each listed virtual router ID.
Clear Router Status	Select the *Clear Router Status* button to clear the Router Operations Summary table values to zero and begin new data collections.
Clear Global Error Status	Select the *Clear Global Error Status* button to clear the Global Error Status table values to zero and begin new data collections.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.20 Critical Resources

Access Point Statistics

The *Critical Resources* statistics screen displays a list of device IP addresses on the network (gateways, routers etc.). These IP addresses are critical to the health of the controller or service platform managed network. These device addresses are pinged regularly by managed Access Points. If there's a connectivity issue, an event is generated stating a critical resource is unavailable. Thus, each device's VLAN, ping mode and state is displayed for the administrator.

To review a selected Access Point's critical resource statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Critical Resources**.

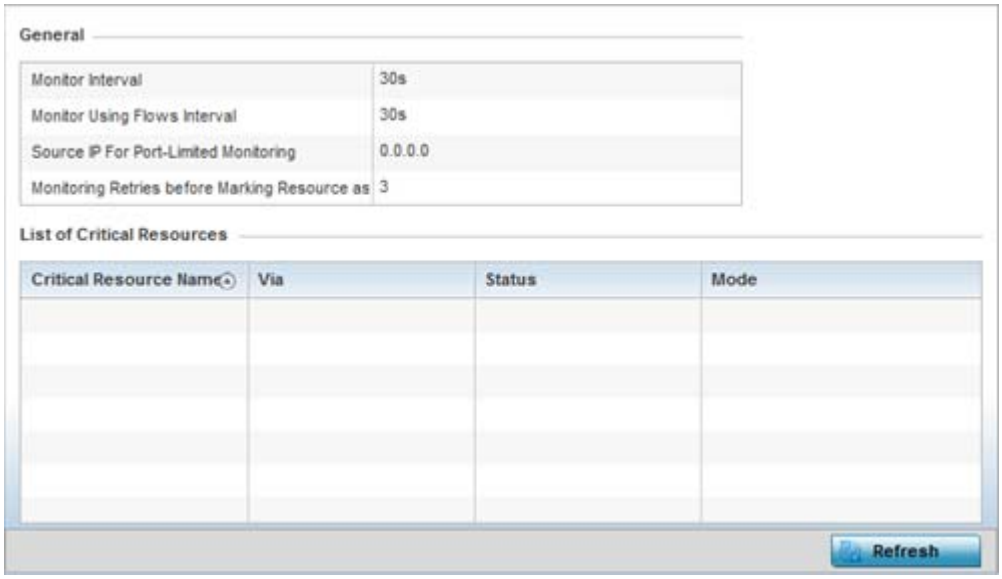


Figure 15-172 *Access Point - Critical Resources screen*

4 Refer to the **General** field to assess the **Monitor Interval** and **Monitor Using Flows Interval** used to poll for updates from the critical resource IP listed for **Source IP For Port-Limited Monitoring**. **Monitoring Retries before Marking Resource as DOWN** are the number of retry connection attempts permitted before this listed resource is defined as down (offline).

The Access Point **Critical Resource** screen displays the following:

Critical Resource Name	Lists the name of the critical resource monitored by the Access Point. Critical resources are device IP addresses on the network (gateways, routers etc.). These IP addresses are critical to the health of the network. These device addresses are pinged regularly by Access Points. If there's a connectivity issue, an event is generated stating a critical resource is unavailable.
Via	Lists the VLAN used by the critical resource as a virtual interface. The critical resource displays as a link than can be selected to list configuration and network address information in greater detail.

Status	Defines the operational state of each listed critical resource VLAN interface (either *Up* or *Down*).
Error Reason	Provides an error status as to why the critical resource is not available over its designated VLAN.
Mode	Displays the operational mode of each listed critical resource.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.21 LDAP Agent Status

Access Point Statistics

When LDAP has been specified as an external resource (as opposed to local Access Point RADIUS resources) to validate PEAP-MS-CHAP v2 authentication requests, user credentials and password information needs to be made available locally to successfully connect to the external LDAP server. Up to two LDAP Agents (primary and secondary external resources) can be defined as external resources for PEAP-MS-CHAP v2 authentication requests.

AP6521 model Access Point does not support this feature in Standalone AP or Controller AP mode. However, AP6521 model is supported when adopted and managed by a controller or service platform.

For more information on setting LDAP agents as part of the RADIUS server policy, see *Configuring RADIUS Server Policies on page 11-57*.

To view Access Point LDAP agent statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **LDAP Agent Status.**

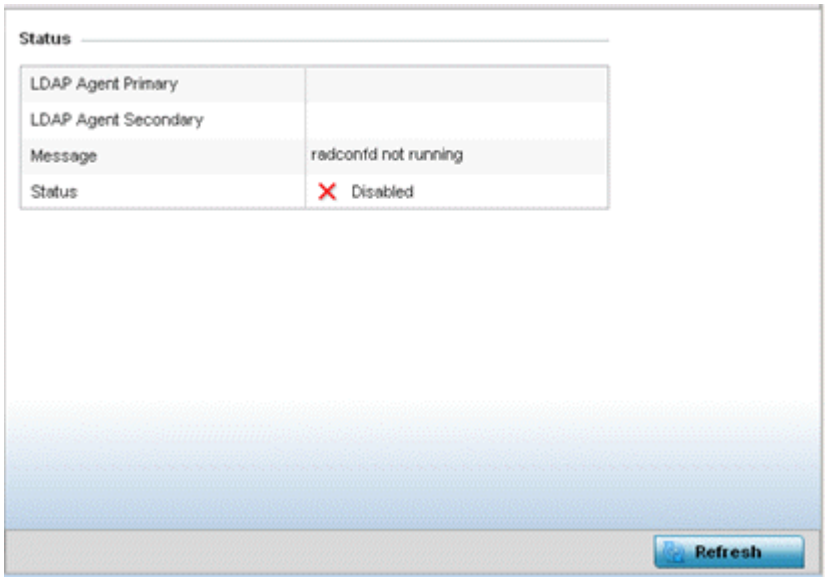


Figure 15-173 *Access Point - LDAP Agent Status screen*

The **LDAP Agent Status** screen displays the following:

LDAP Agent Primary	Lists the primary IP address of a remote LDAP server resource used by the Access Point to validate PEAP-MS-CHAP v2 authentication requests. When a RADIUS server policy's data source is set to LDAP, this is the first resource for authentication requests.
LDAP Agent Secondary	Lists the secondary IP address of a remote LDAP server resource used by the Access Point to validate PEAP-MS-CHAP v2 authentication requests. When a RADIUS server policy's data source is set to LDAP, this is the second resource for authentication requests.
Message	Displays any system message generated in the Access Point's connection with the primary or secondary LDAP agent. If there's a problem with the username and password used to connection to the LDAP agent, it would be listed here.
Status	Displays whether the Access Point has successfully joined the remote LDAP server domain designated to externally validate PEAP-MS-CHAP v2 authentication requests.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

15.4.22 Mint Links

Access Point Statistics

Wireless controllers and Access Points use the MiNT protocol as the primary means of device discovery and communication for Access point adoption and management. MiNT provides a mechanism to discover neighbor devices in the network, and exchange packets between devices regardless of how these devices are connected (L2 or L3).

MiNT provides the means to secure communications at the transport layer. Using MiNT, a device can be configured to only communicate with other authorized (MiNT enabled) devices of the same model. MiNT links can be established over a VLAN (Among Access Points on a VLAN) or IP (remote access point to controller).

MiNT Links are automatically created between controllers and Access Points during adoption using MLCP (*MiNT Link Creation Protocol*). They can also be manually created between a controller and Access Point (or) between Access Points. MiNT links are manually created between controllers while configuring a cluster.

Level 2 (or) remote MiNT links are controller aware links, and requires IP network for communication. This level 2 MiNT links at access points are intended for remote Adaptive AP deployment and management from NOC. With Level2 MiNT links, access points are only aware of the controllers and not about other Access points. Level 2 MiNT links also provide partitioning, between Access Points deployed at various remote sites.

To view an Access Point's Mint links:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Mint Links** from the left-hand side of the UI.

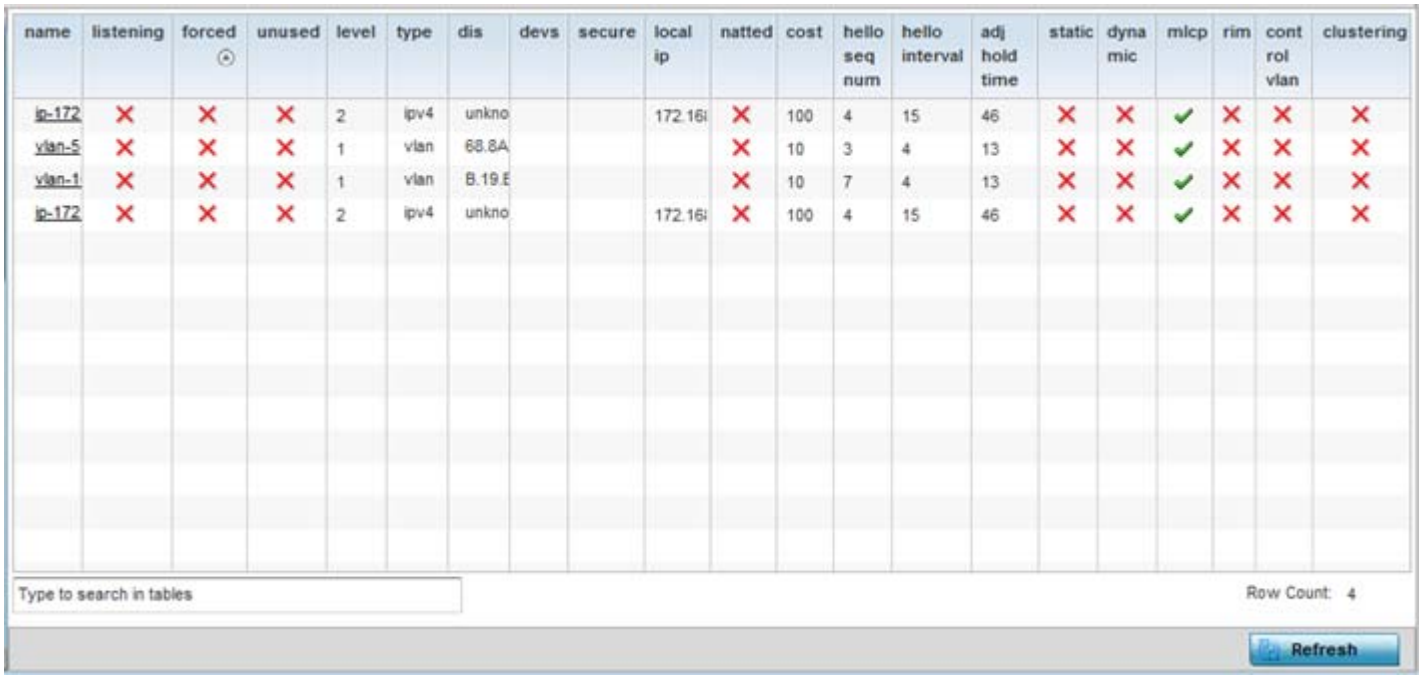


Figure 15-174 *Access Point - Mint Links screen*

The Mint Links screen lists the *name* of the impacted VLAN or link in the form of a link that can be selected to display more granular information about that VLAN. A green check mark or a red X defines whether the listed VLAN is *listening* to traffic, *forced* to stay up or *unused* with the Mint link. The *level* column specifies whether the listed Mint link is traditional switching link (level 2) or a routing link (level 3). The *type* column defines whether the listed Mint link is a VLAN or an IPv4 or IPv6 type network address. The *dis* column lists how each link was discovered.

Refer to the *secure* column to assess whether the listed links are isolated between peers. The *local ip* column lists the IP address assigned as the link's end point address, not the interface's IP address. The *natted* column lists whether the link is NAT enabled or disabled for modifying network address information in IP packet headers in transit. The *cost* defines the cost for a packet to travel from its originating port to its end point destination.

The *hello seq number* and *hello interval* define the interval between hello keep alive messages between link end points. While the *adj hold time* sets the time after the last hello packet when the connected between end points is defined as lost.

The *static* and *dynamic* link columns state whether each listed link is static route using a manually configured route entry, or a dynamic route characterized by its destination The *rim* column defines whether the listed link is managed remotely. The *control vlan* column states whether the listed link has enabled as a control VLAN. Lastly, the *clustering* column states whether listed link members discover and establish connections to other peers and provide self-healing in the event of cluster member failure.

4 Periodically select **Refresh** to update the screen's data counters to their latest values.

5 If needed, select a Mint link from the *name* column to display more granular information for that link.

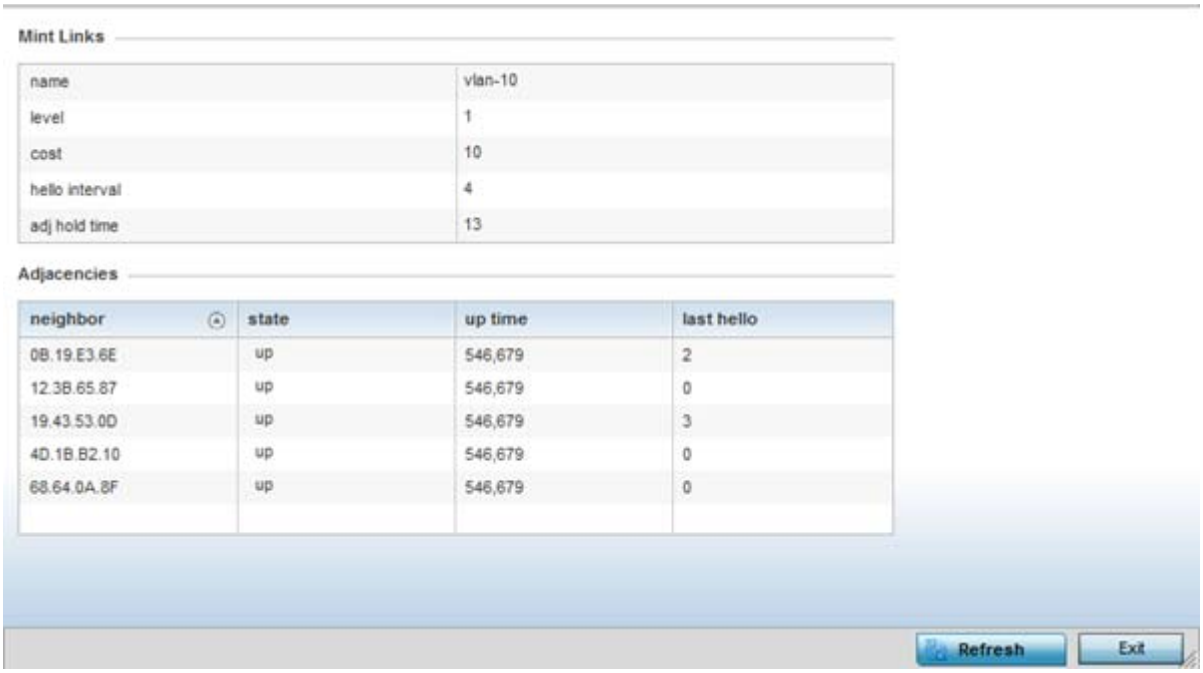


Figure 15-175 *Access Point - Mint Link Details screen*

The first table lists the Mint link's name and *level* specifying whether the Mint link is traditional switching link (level 2) or a routing link (level 3). The *cost* defines the cost for a packet to travel from its originating port to its end point destination. The *hello interval* lists the time between hello keep alive messages between link end points. The *adj hold time* sets the time after the last hello packet when the connected between end points is defined as lost.

The *Adjacencies* table lists *neighbor* devices by their hardware identifiers and operational *state* to help determine their availability as Mint link end points and peers. The *up time* lists the selected link's detection on the network and the last hello lists when the *last hello* message was exchanged.

6 Periodically select *Refresh* to update the statistics counters to their latest values.

15.4.23 Guest Users

Access Point Statistics

A *captive portal* is an access policy for providing guests temporary and restrictive access to the wireless network. A captive portal configuration provides secure authenticated access using a standard Web browser. Captive portals provide authenticated access by capturing and re-directing a wireless user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. Captive portals can have their access durations set by an administrator to either provide temporary access to the Access Point managed network or provide access without limitations.

For information on setting captive portal duration and authentication settings, refer to *Configuring Captive Portal Policies on page 11-1*.

To view current Access Point guest user utilization:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Guest Users**.

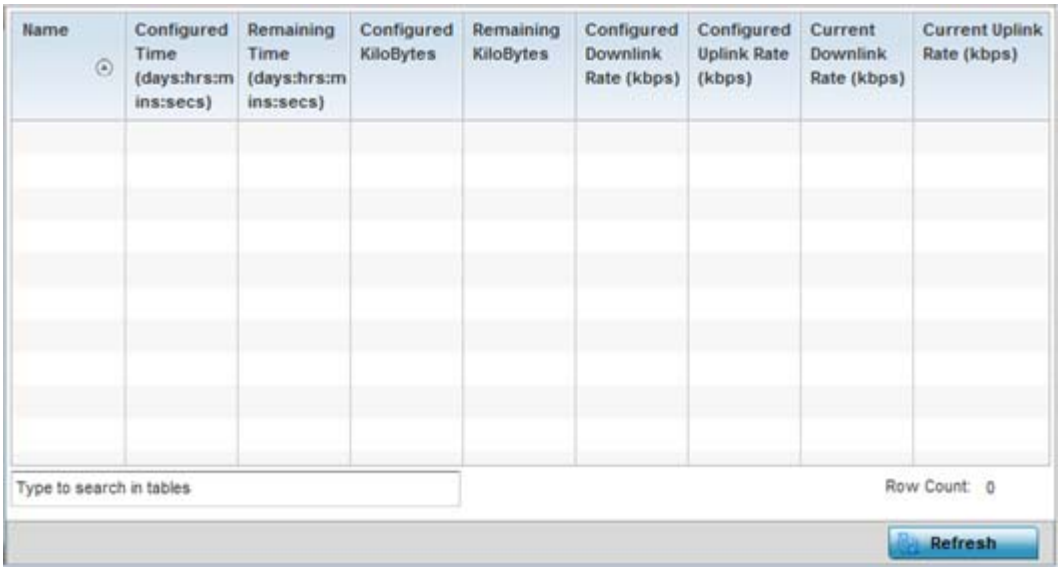


Figure 15-176 *Access Point – Guest Users screen*

The **Guest Users** screen describes the following:

Name	Lists the administrator assigned name of the client utilizing the Access Point for guest access to the WiNG managed wireless network.
Configured Time (days:hrs:mins:secs)	Displays the restricted permissions each listed client was initially configured for their captive portal guest user session with this managing Access Point.
Remaining Time (days:hrs:mins:secs)	Displays the time each listed client has remaining in their captive portal guest user session with this Access Point.
Configured Kilobytes	Lists the maximum configured bandwidth consumable by the listed guest user (in kilobytes).
Remaining Kilobytes	Lists the remaining bandwidth available to the listed guest user (in kilobytes). This is the difference between the configured (maximum) bandwidth and the users's current utilization.
Configured Downlink Rate (kbps)	Specifies the download speed configured for the listed guest user. When bandwidth is available, the user can download data at the specified rate (in kilobytes per second). If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to the defined reduced downlink rate. For more information, refer to *Defining User Pools on page 11-53*.
Configured Uplink Rate (kbps)	Specifies the upload speed dedicated to the listed guest user. When bandwidth is available, the user is able to upload data at the specified rate (in kilobytes per second). If a guest user has a bandwidth based policy and exceeds the specified data limit, their speed is throttled to the reduced uplink rate. For more information, refer to *Defining User Pools on page 11-53*.

Current Downlink Rate (Kbps)	Lists the listed guest user's current downlink rate in kbps. Use this information to assess whether this user's configured downlink rate is adequate for their session requirements and whether their reduced downlink rate need adjustment if the configured downlink rate is exceeded. For more information, refer to *Defining User Pools on page 11-53*.
Current Uplink Rate (Kbps)	Lists the listed guest user's current uplink rate in kbps. Use this information to assess whether this user's configured uplink rate is adequate for their session requirements and whether their reduced uplink rate need adjustment if the configured uplink rate is exceeded. For more information, refer to *Defining User Pools on page 11-53*.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest value.

15.4.24 GRE Tunnels

Access Point Statistics

Generic Routing Encapsulation (GRE) is one of the available tunneling mechanisms which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint.

To review a selected Access Point's GRE statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **GRE Tunnels**.

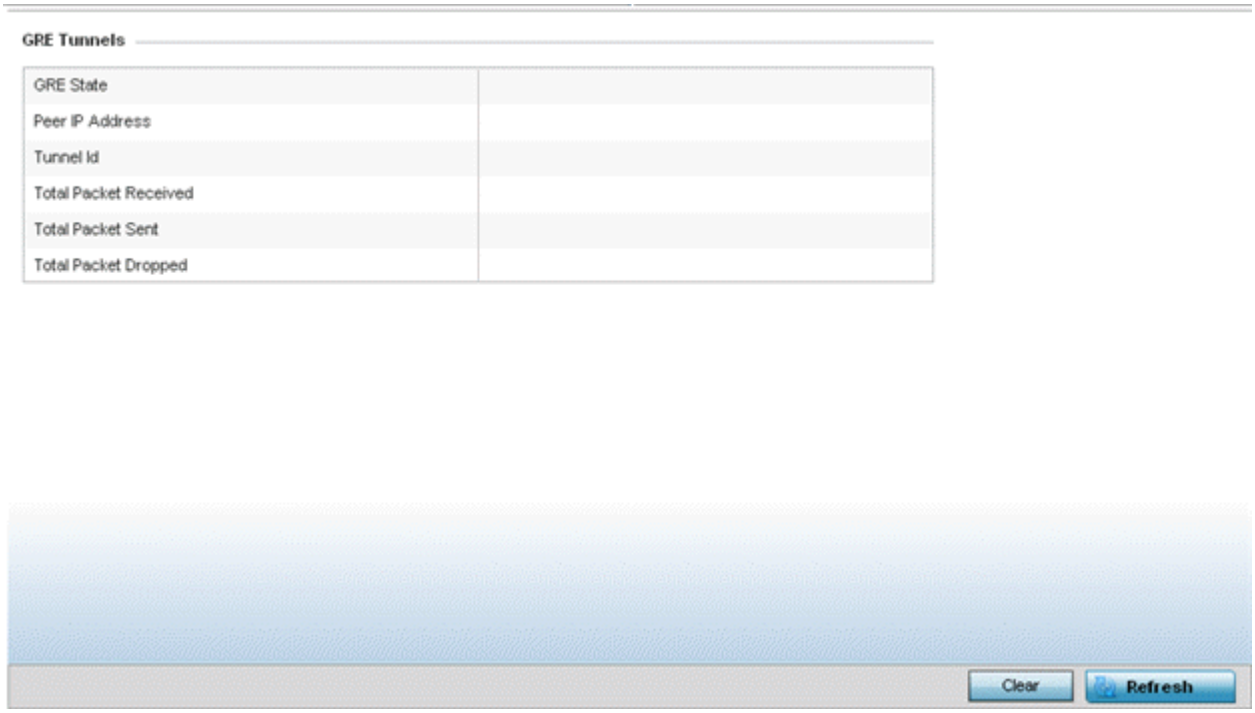


Figure 15-177 *Access Point - GRE Tunnels screen*

The Access Point **GRE Tunnels** screen displays the following:

GRE State	Displays the current operational state of the GRE tunnel.
Peer IP Address	Displays the IP address of the peer device on the remote end of the GRE tunnel.
Tunnel Id	Displays the session ID of an established GRE tunnel. This ID is only viable while the tunnel is operational.
Total Packets Received	Displays the total number of packets received from a peer at the remote end of the GRE tunnel.
Total Packets Sent	Displays the total number of packets sent from this Access Point to a peer at the remote end of the GRE tunnel.
Total Packets Dropped	Lists the number of packets dropped from tunneled exchanges between this Access Point and a peer at the remote end of the VPN tunnel
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest value.

15.4.25 Dot1x

Access Point Statistics

Dot1x (or 802.1x) is an IEEE standard for network authentication. Devices supporting Dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a Dot1x network, a device automatically connects and authenticates without needing to manually login.

To view the Dot1x statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Dot1x** from the left-hand side of the UI.

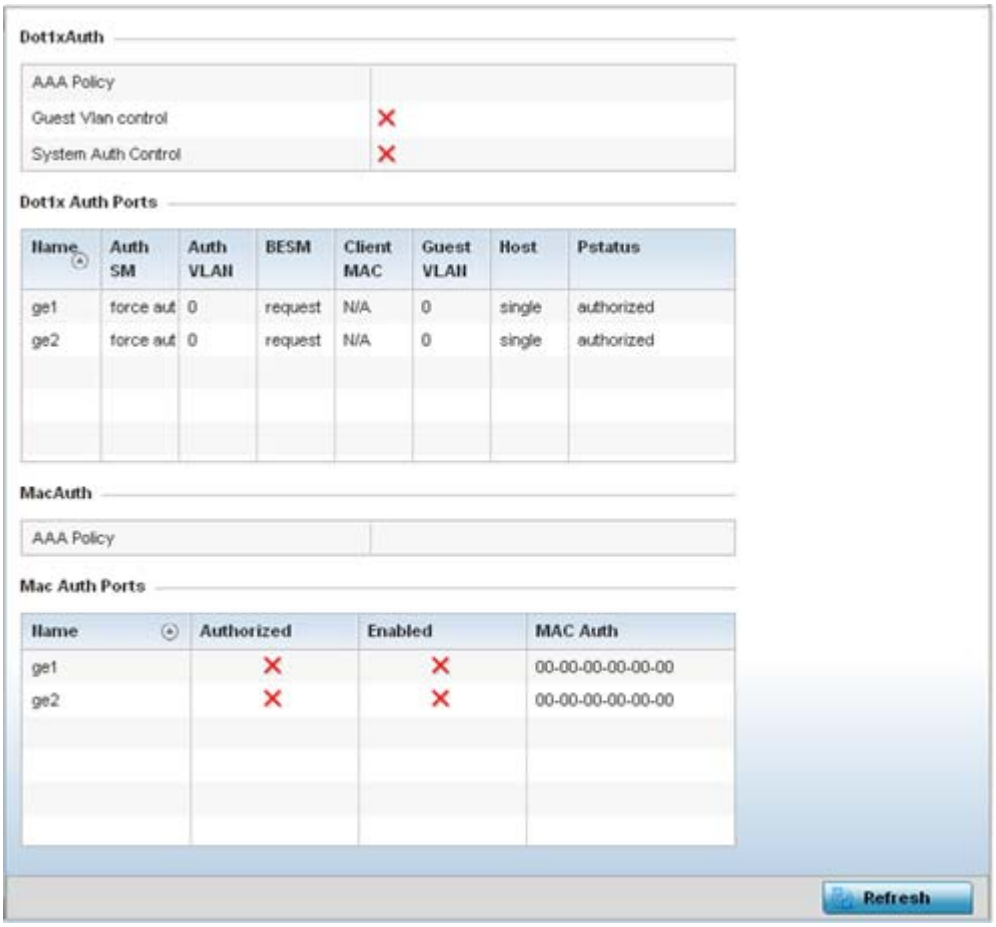


Figure 15-178 *Access Point – Dot1x screen*

4 Refer to the following **Dot1xAuth** statistics:

AAA Policy	Lists the AAA policy currently being utilized for authenticating user requests.
Guest Vlan Control	Lists whether guest VLAN control has been allowed (or enabled). This is the VLAN traffic is bridged on if the port is unauthorized and guest VLAN globally enabled. A green checkmark designates guest VLAN control as enabled. A red X defines guest VLAN control as disabled.
System Auth Control	Lists whether Dot1x authorization is globally enabled for the Access Point. A green checkmark designates Dot1x authorization globally enabled. A red X defines Dot1x as globally disabled.

5 Review the following **Dot1x Auth Ports** utilization information:

Name	Lists the Access Point ge ports subject to automatic connection and authentication using Dot1x.

Auth SM	Lists the current authentication state of the listed port.
Auth VLAN	Lists the virtual interface utilized post authentication.
BESM	Lists whether an authentication request is pending on the listed port.
Client MAC	Lists the MAC address of requesting clients seeking authentication over the listed port.
Guest VLAN	Lists the guest VLAN utilized for the listed port. This is the VLAN traffic is bridged on if the port is unauthorized and guest VLAN globally enabled.
Host	Lists whether the host is a single entity or not.
Pstatus	Lists whether the listed port has been authorized for Dot1x network authentication.

6 Refer to the **MacAuth** table to assess the AAA policy applied to MAC authorization requests.

7 Review the following **MAC Auth Ports** utilization information:

Name	Lists the Access Point ge ports subject to automatic connection and MAC authentication using Dot1x.
Authorized	Lists whether MAC authorization using Dot1x has been authorized (permitted) on the listed ge port. A green checkmark designates Dot1x authorization as authorized. A red X defines authorization as disabled.
Enabled	Lists whether MAC authorization using Dot1x has been enabled on the listed ge port. A green checkmark designates Dot1x authorization as allowed. A red X defines authorization as disabled.
MAC Auth	Lists the MAC address corresponding to the listed Access Point port interface on which authentication requests are made.

8 Select the **Refresh** button to update the screen's statistics counters to their latest value.

15.4.26 Network

Access Point Statistics

Use the *Network* screen to view information for performance statistics for ARP, DHCP, Routing and Bridging.For more information, refer to the following:

- *ARP Entries*
- *Route Entries*
- *Default Routes*
- *Bridge*
- *IGMP*
- *MLD*
- *Traffic Shaping*
- *DHCP Options*
- *Cisco Discovery Protocol*
- *Link Layer Discovery Protocol*
- *IPv6 Neighbor Discovery*
- *MSTP*

15.4.26.1 ARP Entries

Network

Address Resolution Protocol (ARP) is a protocol for mapping an IP address to a device address recognized in the local network. An address is 32 bits long. In an Ethernet local area network, however, addresses for attached devices are 48 bits long. (The physical machine address is also known as a MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

To view an Access Point's ARP statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Network** and expand the menu to reveal its submenu items.

4 Select **ARP Entries**.

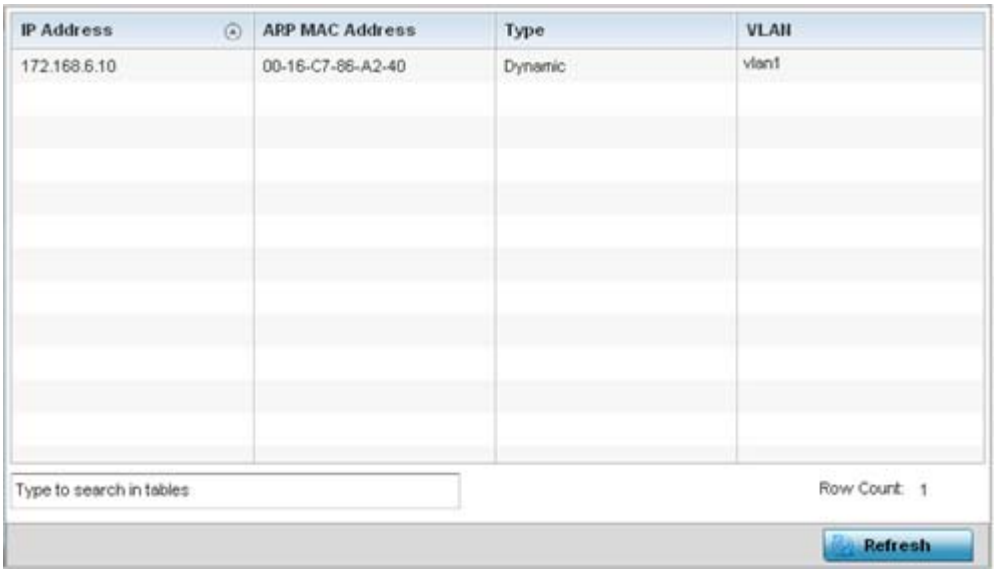


Figure 15-179 *Access Point - Network ARP screen*

The **ARP Entries** screen describes the following:

IP Address	Displays the IP address of the client resolved on behalf of the Access Point.
ARP MAC Address	Displays the MAC address corresponding to the IP address being resolved.
Type	Lists the type of ARP entry.
VLAN	Displays the system assigned VLAN ID where an IP address was found.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.26.2 Route Entries

Network

The *Route Entries* screen displays data for routing packets to a defined destination. When an existing destination subnet does not meet the needs of the network, add a new destination subnet, subnet mask and gateway as needed for either IPv4 or IPv6 formatted data packets.

IPv4 operates as a best effort delivery method, as it does not guarantee delivery, and does not ensure proper sequencing or duplicate delivery (unlike (TCP). IPv4 hosts can use link local addressing to provide local connectivity.

IPv6 is the latest revision of the *Internet Protocol* (IP) designed to replace IPv4. IPV6 provides enhanced identification and location information for devices on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

To view IPv4 and IPv6 route entries:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Network** and expand the menu to reveal its sub menu items.

4 Select **Route Entries**. The **IPv4 Route Entries** tab displays by default.

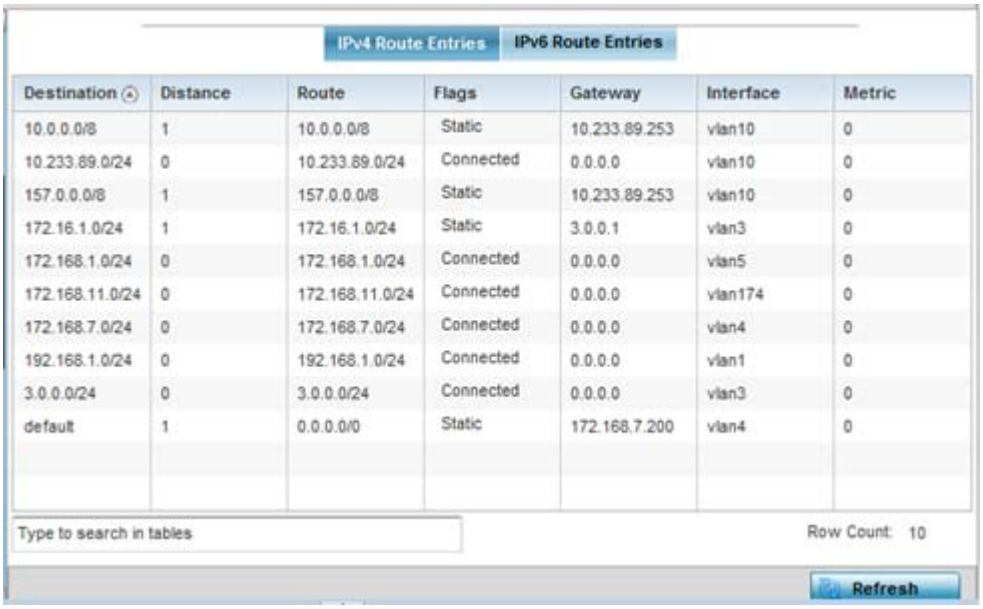


Figure 15-180 *Access Point - Network IPv4 Route Entries screen*

The **IPv4 Route Entries** screen lists the following:

Destination	Displays the IPv4 formatted address of the destination route address.

Distance	Lists the hop distance to a desired route. Devices regularly send neighbors their own assessment of the total cost to get to all known destinations. A neighboring device examines the information and compares it to their own routing data. Any improvement on what's already known is inserted in that device's own routing tables. Over time, each networked device discovers the optimal next hop for each destination.
Route	Lists the IPv4 formatted IP address used for routing packets to a defined destination.
Flags	The flag signifies the condition of the *direct* or *indirect* route.
Gateway	Displays the gateway IP address used to route packets to the destination subnet.
Interface	Displays the name of the controller interface or VLAN utilized by the destination subnet.
Metric	Lists the metric (or cost) of the route to select (or predict) the best route. The metric is computed using a routing algorithm, and covers information bandwidth, network delay, hop count, path cost, load, MTU, reliability, and communication cost.
Refresh	Select *Refresh* to update the display to the latest values.

5 Select the **IPv6 Route Entries** tab to review route data for IPv6 formatted traffic.

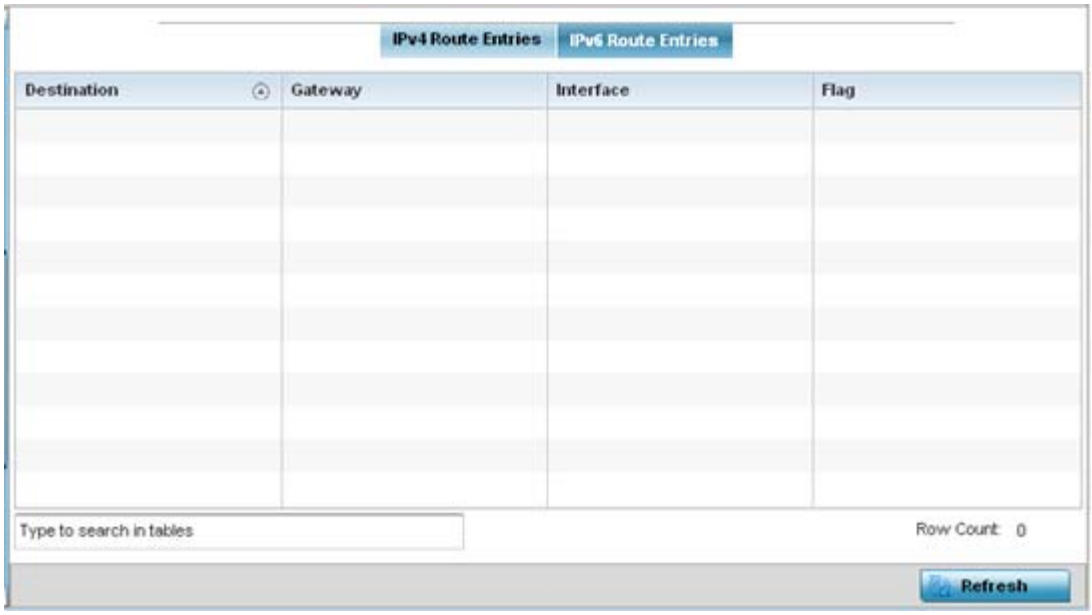


Figure 15-181 *Wireless Controller - IPv6 Route Entries screen*

The **IPv6 Route Entries** screen lists the following:

Destination	Displays the IPv6 formatted address of the destination route address.
Gateway	Displays the gateway IP address used to route packets to the destination subnet.
Interface	Displays the name of the controller interface or VLAN utilized by the destination subnet.
Flag	The flag signifies the condition of the *direct* or *indirect* route.
Refresh	Select *Refresh* to update the display to the latest values.

15.4.26.3 Default Routes

Network

In an IPv6 supported environment unicast routing is always enabled. A controller or service platform routes IPv6 formatted traffic between interfaces as long as the interfaces are enabled for IPv6 and ACLs allow IPv6 formatted traffic. However, an administrator can add a default routes as needed.

Static routes are manually configured. They work fine in simple networks. However, static routes with topology changes require an administrator to manually configure and modify the corresponding route revisions. Default routes are useful, as they forward packets that match no specific routes in the routing table.

To view Access Point default routes:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Network** and expand the menu to reveal its sub menu items.

4 Select **Default Routes**. The **IPv4 Default Routes** tab displays by default.

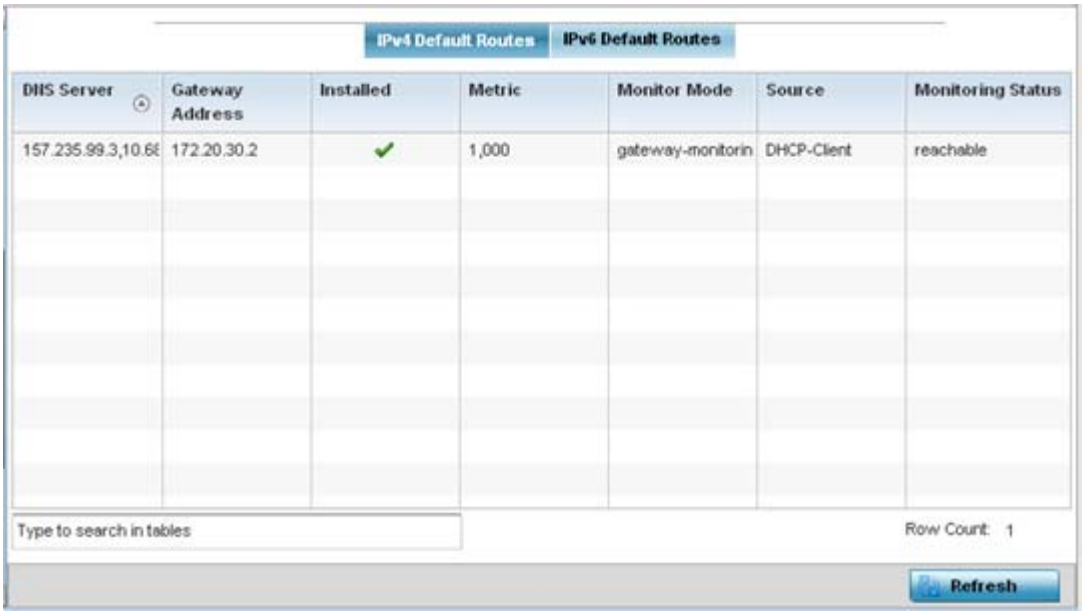


Figure 15-182 *Access Point - IPv4 Default Routes screen*

The **IPv4 Default Routes** screen provides the following information:

DNS Server	Lists the address of the DNS server providing IPv4 formatted address assignments on behalf of the Access Point.
Gateway Address	Lists the IP address of the gateway resource used with the listed route.
Installed	A green checkmark defines the listed route as currently installed on the Access Point. A red X defines the route as not currently installed and utilized.
Metric	The metric (or cost) could be the distance of a router (round-trip time), link throughput or link availability.

Monitor Mode	Displays where in the network the route is monitored for utilization status.
Source	Lists whether the route is *static,* a *DHCP-Client* or an administrator defined *default* route. Static routes are manually configured. Static routes work adequately in simple networks. However, static routes with topology changes require an administrator to manually configure and modify the corresponding route revisions. Default routes are useful, as they forward packets that match no specific routes in the routing table.
Monitoring Status	Lists whether the defined IPv4 route is currently reachable on the Access Point managed network. If not, perhaps a topology change has occurred to a static route requiring a default route be utilized.
Refresh	Select *Refresh* to update the display to the latest values.

5 Select the **IPv6 Default Routes** tab to review default route availabilities for IPv6 formatted traffic.

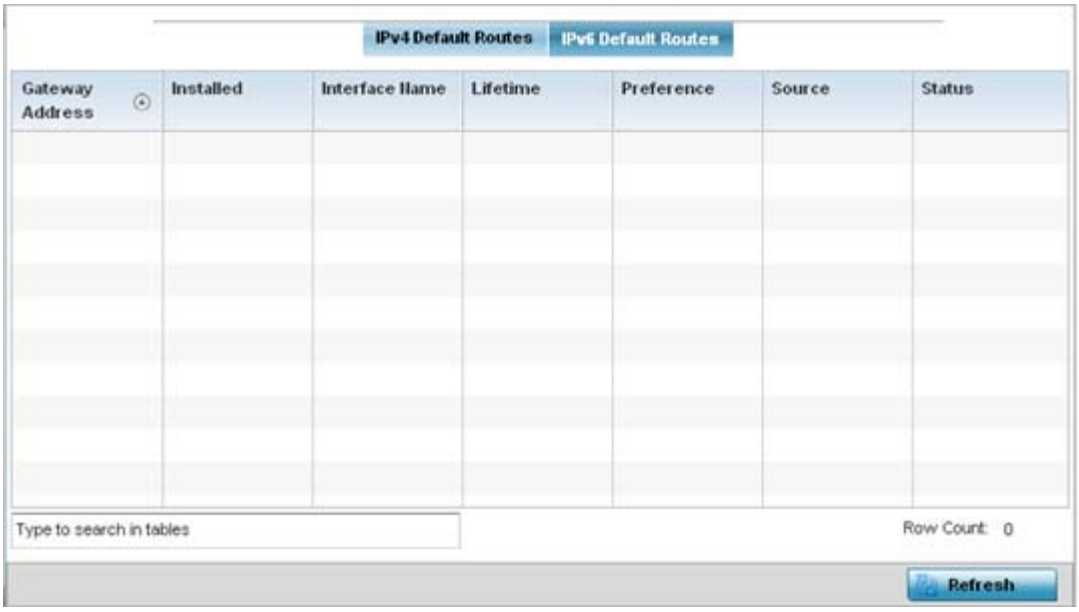


Figure 15-183 *Wireless Controller - IPv6 Default Routes screen*

The **IPv6 Default Routes** screen provides the following information:

Gateway Address	Lists the IP address of the gateway resource used with the listed route.
Installed	A green checkmark defines the listed IPv6 default route as currently installed on the Access Point. A red X defines the route as not currently installed and utilized.
Interface Name	Displays the interface on which the IPv6 default route is being utilized.
Lifetime	Lists the lifetime representing the valid usability of the default IPv6 route.
Preference	Displays the administrator defined IPv6 preferred route for IPv6 traffic.

Source	Lists whether the route is *static* or an administrator defined *default* route. Static routes are manually configured. Static routes work adequately in simple networks. However, static routes with topology changes require an administrator to manually configure and modify the corresponding route revisions. Default routes are useful, as they forward packets that match no specific routes in the routing table.
Status	Lists whether the defined IPv6 route is currently reachable on the Access Point managed network. If not, perhaps a topology change has occurred to a static route requiring a default route be utilized.
Refresh	Select *Refresh* to update the display to the latest values.

15.4.26.4 Bridge

Network

Bridging is a forwarding technique used in networks. Bridging makes no assumption about where a particular address is located. It relies on the flooding and examination of source addresses in received packet headers to locate unknown devices. Once a device is located, its location is stored in a table to avoid broadcasting to that device again. Bridging is limited by its dependency on flooding, and is used in local area networks only. A bridge and an Access Point are very much alike, as an Access Point can be viewed as a bridge with a number of ports.

The *Bridge* screen provides details about the *Integrate Gateway Server* (IGS), which is a router connected to an Access Point. The IGS performs the following:

- Issues IP addresses
- Throttles bandwidth
- Permits access to other networks
- Times out old logins

The Bridging screen also provides information about the *Multicast Router* (MRouter), which is a router program that distinguishes between multicast and unicast packets and how they should be distributed along the Multicast Internet. Using an appropriate algorithm, a multicast router instructs a switching device what to do with the multicast packet.

To view an Access Point's Bridge statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Network** and expand the menu to reveal its sub menu items.

4 Select **Bridge**.

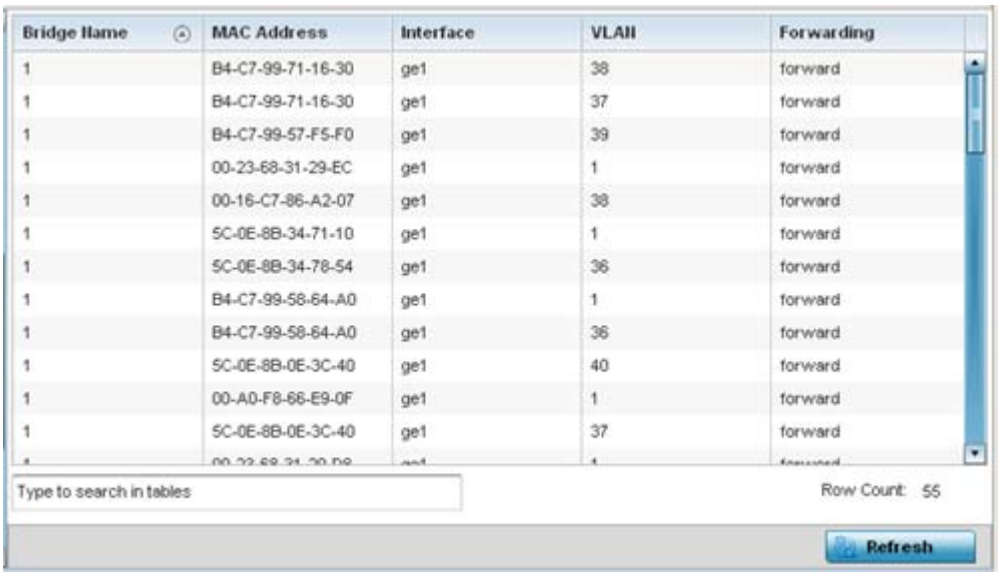


Figure 15-184 *Access Point - Network Bridge screen*

5 Review the following bridge configuration attributes:

Bridge Name	Displays the numeric ID of the network bridge.
MAC Address	Displays the MAC address of the bridge selected.
Interface	Displays the interface (Access Point physical port name) where the bridge transferred packets. Supported Access Points models have different port configurations.
VLAN	Displays the VLAN the bridge uses a virtual interface.
Forwarding	Displays whether the bridge is forwarding packets.

6 Select **Refresh** to update the counters to their latest values.

15.4.26.5 IGMP

Network

Internet Group Management Protocol (IGMP) is a protocol used for managing members of IP multicast groups. The Access Point listens to IGMP network traffic and forwards the IGMP multicast packets to radios on which the interested hosts are connected. On the wired side of the network, the Access Point floods all the wired interfaces. This feature reduces unnecessary flooding of multicast traffic in the network

To view a network's IGMP configuration:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Network** and expand the menu to reveal its sub menu items.

4 Select **IGMP**.

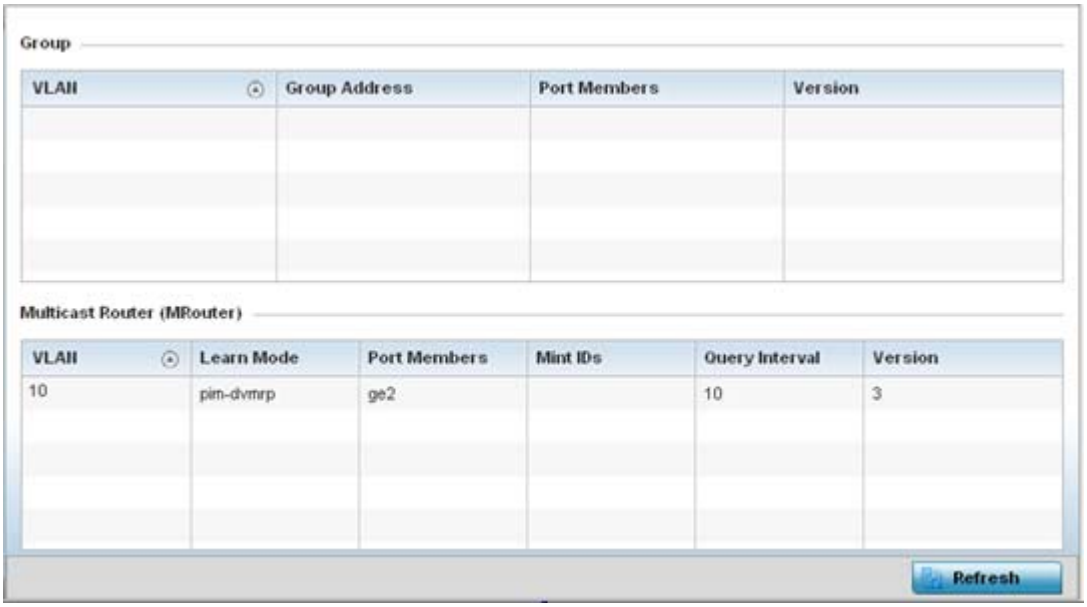


Figure 15-185 *Access Point - Network IGMP screen*

The **Group** field displays the following:

VLAN	Displays the group VLAN where the multicast transmission is conducted.
Group Address	Displays the Multicast Group ID supporting the statistics displayed. This group ID is the multicast address that hosts are listening to.
Port Members	Displays the ports on which multicast clients have been discovered by the Access Point. For example, ge1, radio1, etc.
Version	Displays each listed group IGMP version compatibility as either version 1, 2 or 3.

The **Multicast Router (MRouter)** field displays the following:

VLAN	Displays the group VLAN where the multicast transmission is conducted.
Learn Mode	Displays the learning mode used by the router as either *Static* or *PIM-DVMRP*.
Port Members	Displays the ports on which multicast clients have been discovered by the multicast router. For example, ge1, radio1, etc.
MiNT IDs	Lists MiNT IDs for each listed VLAN. MiNT provides the means to secure Access Point profile communications at the transport layer. Using MiNT, an Access Point can be configured to only communicate with other authorized (MiNT enabled) Access Points of the same model.
Query Interval	Lists the IGMP query interval implemented when the querier functionality is enabled. The default value is 60 seconds.
Version	Lists the multicast router IGMP version compatibility as either version 1, 2 or 3. The default setting is 3.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.26.6 MLD

Network

Multicast Listener Discovery (MLD) snooping enables a controller, service platform or Access Point to examine MLD packets and make forwarding decisions based on content. MLD is used by IPv6 devices to discover devices wanting to receive multicast packets destined for specific multicast addresses. MLD uses multicast listener queries and multicast listener reports to identify which multicast addresses have listeners and join multicast groups.

MLD snooping caps the flooding of IPv6 multicast traffic on controller, service platform or Access Point VLANs. When enabled, MLD messages are examined between hosts and multicast routers and to discern which hosts are receiving multicast group traffic. The controller, service platform or Access Point then forwards multicast traffic only to those interfaces connected to interested receivers instead of flooding traffic to all interfaces.

To view network MLD configuration options:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Network** and expand the menu to reveal its sub menu items.

4 Select MLD.

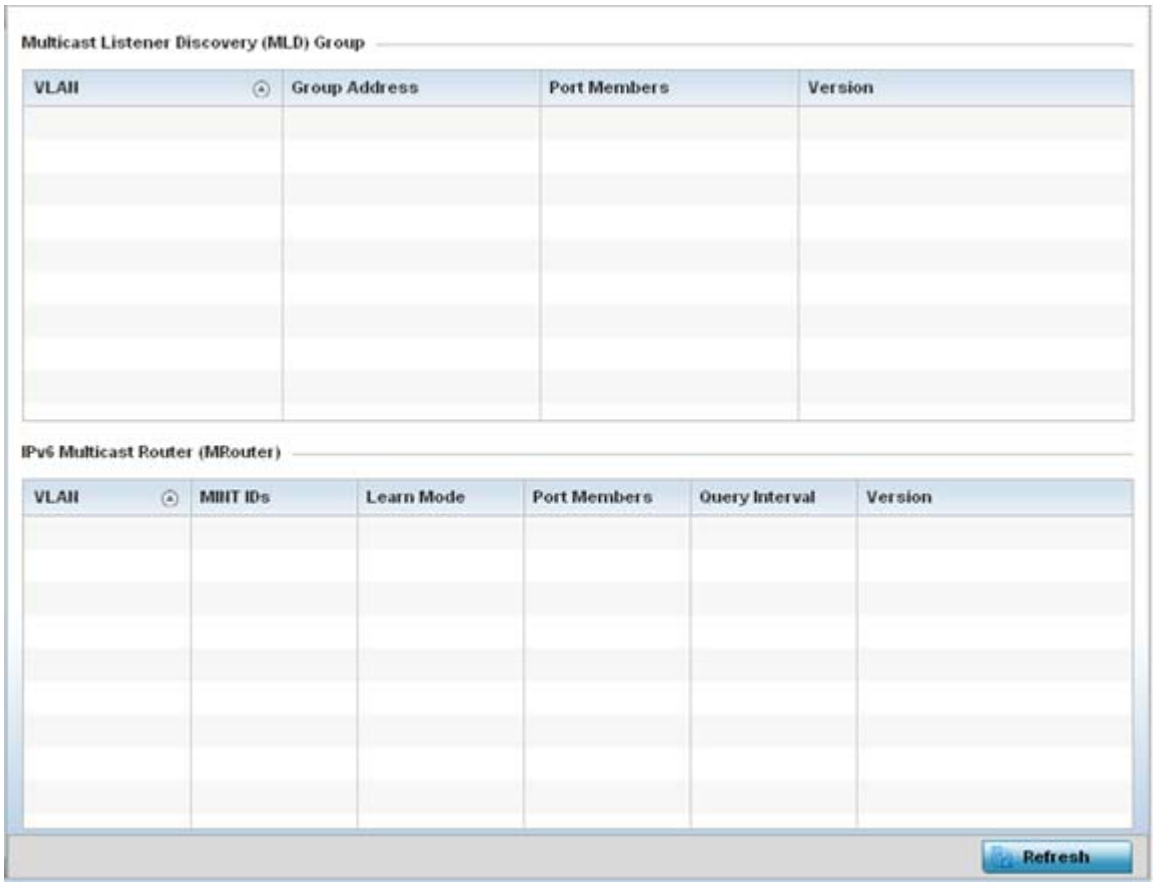


Figure 15-186 *Access Point - Network MLD screen*

The **Multicast Listener Discovery (MLD) Group** field describes the following:

VLAN	Displays the group VLAN where the MLD groups multicast transmission is conducted.
Group Address	Displays the Multicast Group ID supporting the statistics displayed. This group ID is the multicast address hosts are listening to.
Port Members	Displays the ports on which MLD multicast clients have been discovered. For example, ge1, radio1, etc. Ports can vary somewhat amongst supported Access Point models.
Version	Displays each listed group's version compatibility as either version 1, 2 or 3.

The **IPv6 Multicast Router (MRouter)** field describes the following:

VLAN	Displays the group VLAN where the multicast transmission is conducted.
MiNT IDs	Lists MiNT IDs for each listed VLAN. MiNT provides the means to secure communications at the transport layer. Using MiNT, an Access Point can be configured to only communicate with other authorized (MiNT enabled) devices.
Learn Mode	Displays the learning mode used by the router as either *Static* or *PIM-DVMRP.*
Port Members	Displays the physical ports on which multicast clients have been discovered by the multicast router. For example, ge1, radio1, etc. Ports can vary somewhat amongst supported Access Point models.
Query Interval	Lists the query interval implemented when the querier functionality is enabled. The default value is 60 seconds.
Version	Lists the multicast router version compatibility as either version 1, 2 or 3. The default setting is 3.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.26.7 Traffic Shaping

Network

Traffic shaping regulates network data transfers to ensure a specific performance level. Traffic shaping delays the flow of packets defined as less important than prioritized traffic streams. Traffic shaping enables traffic control out an interface to match its flow to the speed of a remote target's interface and ensure traffic conforms applied policies. Traffic can be shaped to meet downstream requirements and eliminate network congestion when data rates are in conflict.

Apply traffic shaping to specific applications to apply application categories. When application and ACL rules are conflicting, an application takes precedence over an application category, then ACLs.

To view network Access Point traffic shaping configuration:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **Traffic Shaping**. The Status screen displays by default, and lists the Access Point's traffic shaping status.

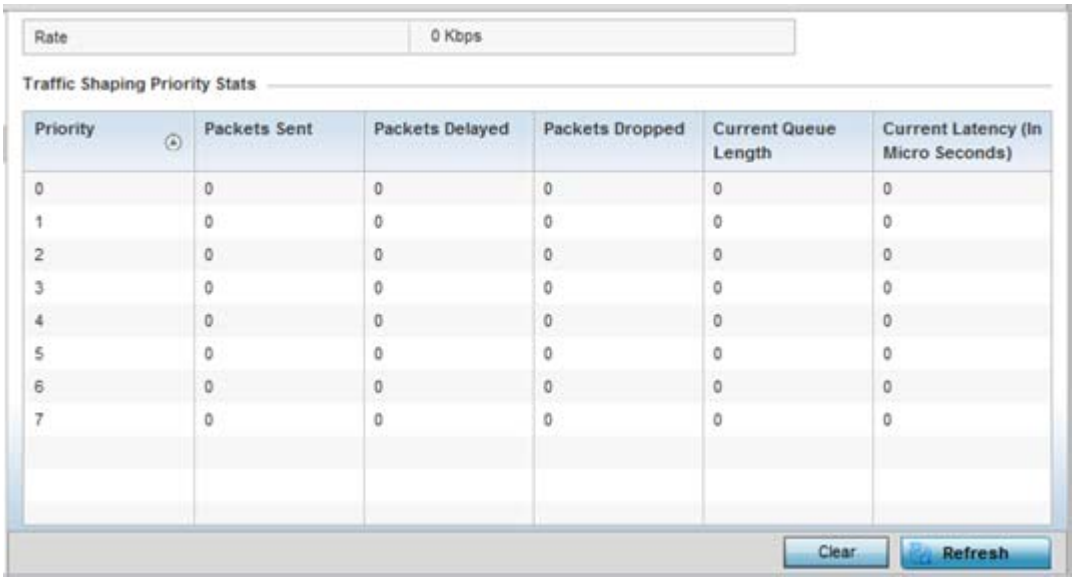


Figure 15-187 *Access Point - Network Traffic Shaping Statistics screen*

5 Select Statistics.

6 Refer to the following **Traffic Shaping** statistics:

Rate	The rate configuration controls the maximum traffic rate sent or received on an interface. Consider this form of rate limiting on interfaces at the edge of a network to limit traffic into or out of the network. Traffic within the set limit is sent and traffic exceeding the set limit is dropped or sent with a different priority.
Priority	Lists the traffic shaper queue priority. There are 8 queues (0 - 7), and traffic is queued in each based on incoming packets 802.1p markings.
Packets Sent	Provides a baseline of the total number of packets sent to assess packet delays and drops as a result of the filter rules applied in the traffic shaping configuration.
Packets Delayed	Lists the packets defined as less important than prioritized traffic streams and delayed as a result of traffic shaping filter rules applied.
Packets Dropped	Lists the packets defined as less important than prioritized traffic streams, delayed and eventually dropped as a result of traffic shaping filter rules applied.
Current Length	Lists the packet length of the data traffic *shaped* to meet downstream requirements.
Current Latency	Traffic shaping latency is the time limit after which packets start dropping as a result of the traffic prioritization filter rules applied.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.26.8 DHCP Options

Network

Supported Access Points can use a DHCP server resource to provide the dynamic assignment of IP addresses automatically. This is a protocol that includes IP address allocation and delivery of host-specific configuration parameters from a DHCP server to a host. Some of these parameters are IP address, gateway and network mask.

The DHCP Options screen provides the DHCP server name, image file on the DHCP server, and its configuration.

To view a network's DHCP Options:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Network** and expand the menu to reveal its sub menu items.

4 Select **DHCP Options**.

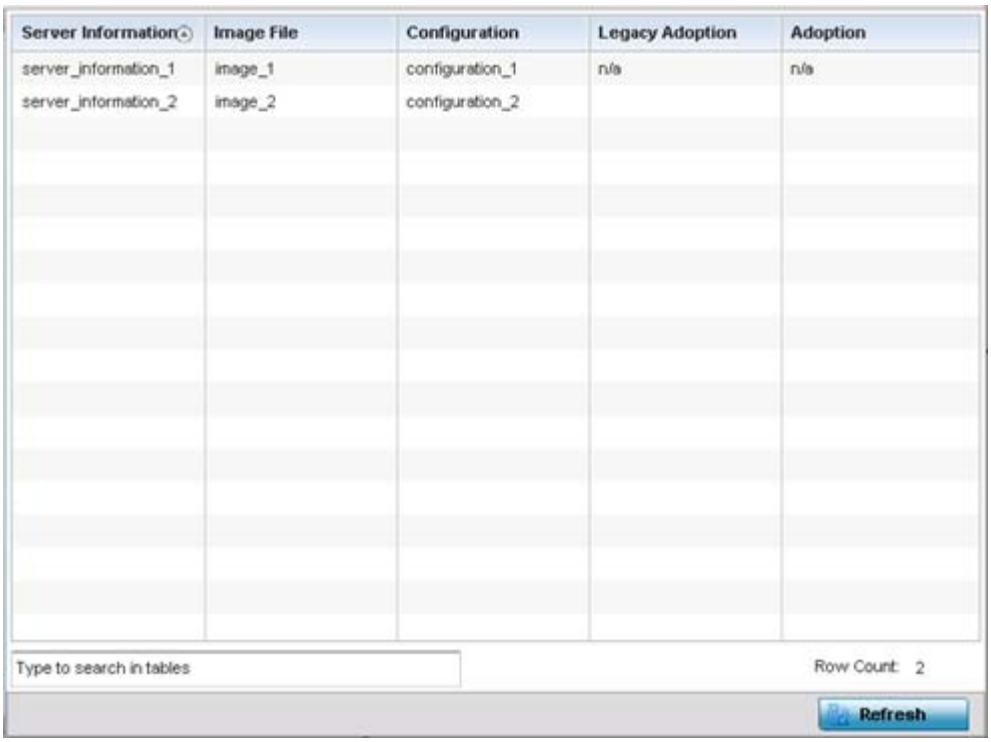


Figure 15-188 *Access Point - Network DHCP Options screen*

The **DHCP Options** screen displays the following:

Server Information	Displays the DHCP server hostname used on behalf of the Access Point.
Image File	Displays the image file name. BOOTP or the bootstrap protocol can be used to boot diskless clients. An image file is sent from the boot server. The image file contains the image of the operating system the client will run. DHCP servers can be configured to support BOOTP.
Configuration	Displays the name of the configuration file on the DHCP server.
Legacy Adoption	Displays historical device adoption information on behalf of the Access Point.
Adoption	Displays adoption information on behalf of the Access Point.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.26.9 Cisco Discovery Protocol

Network

The *Cisco Discovery Protocol* (CDP) is a proprietary Data Link Layer network protocol implemented in Cisco networking equipment and used to share information about network devices.

To view an Access Point's CDP statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select Network and expand the menu to reveal its sub menu items.

4 Select **Cisco Discovery Protocol**.

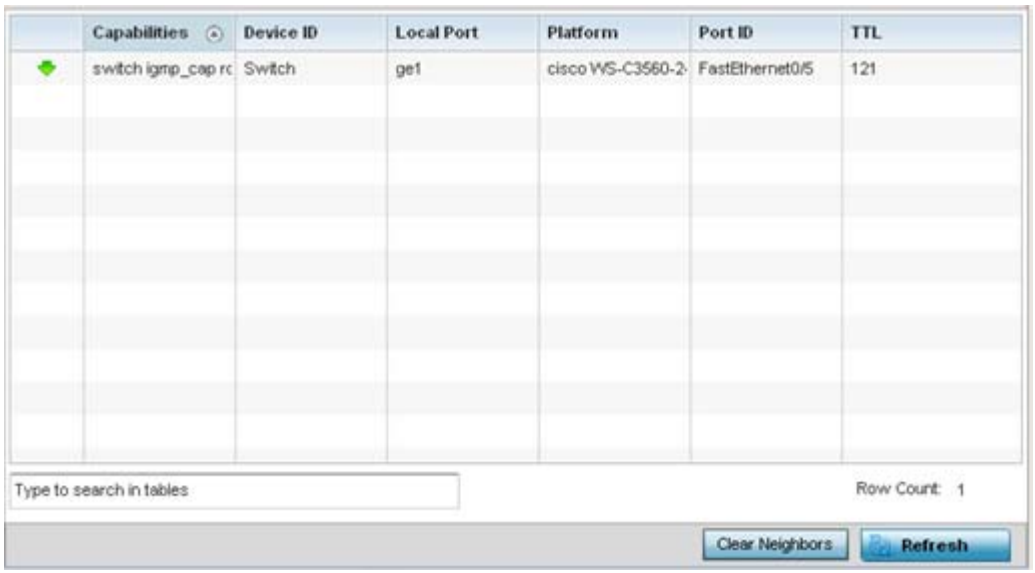


Figure 15-189 *Access Point - Network CDP screen*

The **Cisco Discovery Protocol** screen displays the following:

Capabilities	Displays the capabilities code for the device as either *Router, Trans Bridge, Source Route Bridge, Host, IGMP* or *Repeater.*
Device ID	Displays the configured device ID or name for each listed device.
Local Port	Displays the local port name (Access Point physical port) for each CDP capable device. Supported Access Point models have unique port configurations.
Platform	Displays the model number of the CDP capable device interoperating with the Access Point.
Port ID	Displays the Access Point's numeric identifier for the local port.
TTL	Displays the *time to live* (TTL) for each CDP connection.
Clear Neighbors	Select *Clear Neighbors* to remove CDP neighbors from the table and begin a new data collection.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

15.4.26.10 Link Layer Discovery Protocol

Network

The *Link Layer Discovery Protocol* (LLDP) or IEEE 802.1AB is a vendor-neutral Data Link Layer protocol used by network devices for advertising of (announcing) their identity, capabilities, and interconnections on a IEEE 802 LAN network. The protocol is formally referred to by the IEEE as *Station and Media Access Control Connectivity Discovery*.

To view a network's Link Layer Discovery Protocol statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Network** and expand the menu to reveal its sub menu items.

4 Select **Link Layer Discovery**.

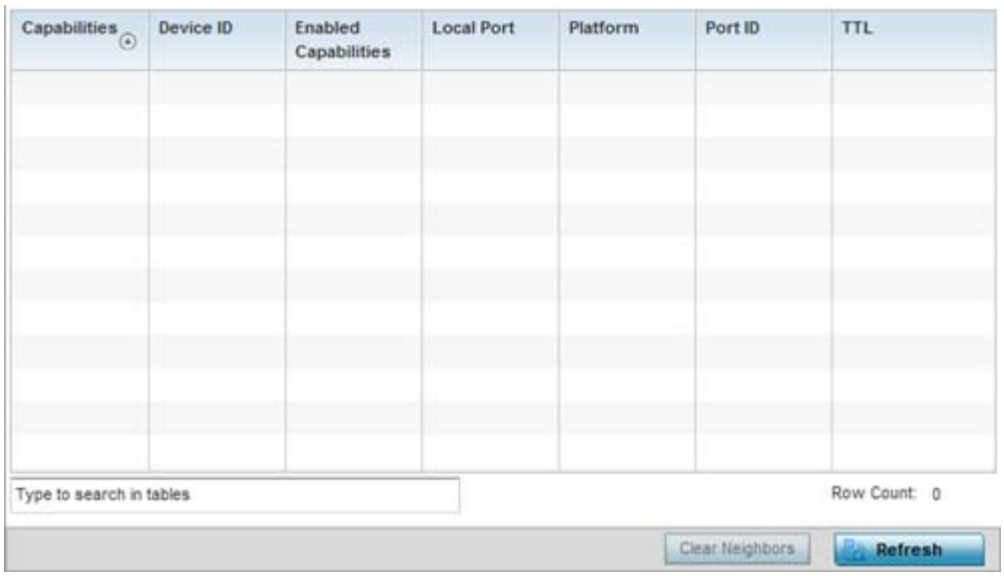


Figure 15-190 *Access Point - Network LLDP screen*

The **Link Layer Discovery Protocol** screen displays the following:

Capabilities	Displays the capabilities code for the device.
Device ID	Displays the configured device ID or name for each device in the table.
Enabled Capabilities	Displays which device capabilities are currently enabled.
Local Port	Displays the local port name (Access Point physical port) for each LLDP capable device. Supported Access Point models have unique port configurations.
Platform	Displays the model number of the LLDP capable device interoperating with the Access Point.
Port ID	Displays the identifier for the local port.
TTL	Displays the *time to live* (TTL) for each LLDP connection.
Clear Neighbors	Select *Clear Neighbors* to remove all known LDP neighbors from the table.
Refresh	Select *Refresh* to update the statistics counters to their latest values.

15.4.26.11 IPv6 Neighbor Discovery

Network

IPv6 neighbor discovery uses ICMP messages and solicited multicast addresses to find the link layer address of a neighbor on the same local network, verify the neighbor's reachability and track neighboring devices.

Upon receiving a neighbor solicitation message, the destination replies with *neighbor advertisement* (NA). The source address in the advertisement is the IPv6 address of the device sending the message. The destination address in the advertisement message is the IPv6 address of the device sending the neighbor solicitation. The data portion of the NA includes the link layer address of the node sending the neighbor advertisement.

Neighbor solicitation messages also verify the availability of a neighbor once its the link layer address is identified. When a node wants to verify the reachability of a neighbor, the destination address in a neighbor solicitation message is the unicast address of the neighbor.

A neighbor is interpreted as reachable when an acknowledgment is returned indicating packets have been received and processed. If packets are reaching the device, they're also reaching the next hop neighbor, providing a confirmation the next hop is reachable.

To view an Access Point's IPv6 neighbor statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **IPv6 Neighbor Discovery**

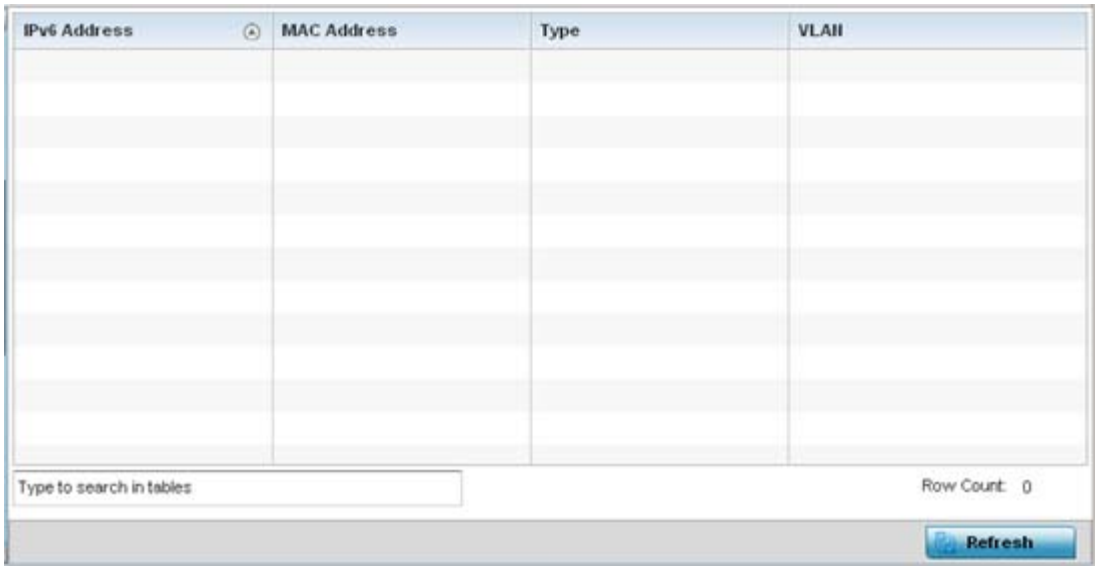


Figure 15-191 *Access Point - Network IPv6 Neighbor screen*

The **IPv6 Neighbor** screen displays the following:

IPv6 Address	Lists an IPv6 IP address for neighbor discovery. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via CMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
MAC Address	Lists the factory encoded hardware MAC address of the neighbor device using an IPv6 formatted IP address as its network identifier.
Type	Displays the device type for the neighbor solicitation. Neighbor solicitations request the link layer address of a target node while providing the sender's own link layer address to the target. Neighbor solicitations are multicast when the node needs to resolve an address and unicast when the node seeks to verify the reachability of a neighbor. Options include *Host, Router* and *DHCP Server.*
VLAN	Lists the virtual interface (from 1 - 4094) used for the required neighbor advertisements and solicitation messages used for neighbor discovery.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.26.12 MSTP

Network

The *Multiple Spanning Tree Protocol* (MSTP) provides an extension to RSTP to optimize the usefulness of VLANs. MSTP allows for a separate spanning tree for each VLAN group, and blocks all but one of the possible alternate paths within each spanning tree topology.

If there's just one VLAN in the Access Point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it's possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs.

MSTP includes all of its spanning tree information in a single *Bridge Protocol Data Unit* (BPDU) format. BPDUs are used to exchange information bridge IDs and root path costs. Not only does this reduce the number of BPDUs required to communicate spanning tree information for each VLAN, but it also ensures backward compatibility with RSTP. MSTP encodes additional region information after the standard RSTP BPDU as well as a number of MSTI messages. Each MSTI messages conveys spanning tree information for each instance. Each instance can be assigned a number of configured VLANs. The frames assigned to these VLANs operate in this spanning tree instance whenever they are inside the MST region. To avoid conveying their entire VLAN to spanning tree mapping in each BPDU, the Access Point encodes an MD5 digest of their VLAN to an instance table in the MSTP BPDU. This digest is used by other MSTP supported devices to determine if the neighboring device is in the same MST region as itself.

To view a controller or service platform's MSTP statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand the **Network** menu from the left-hand side of the UI.

4 Select **MSTP.**

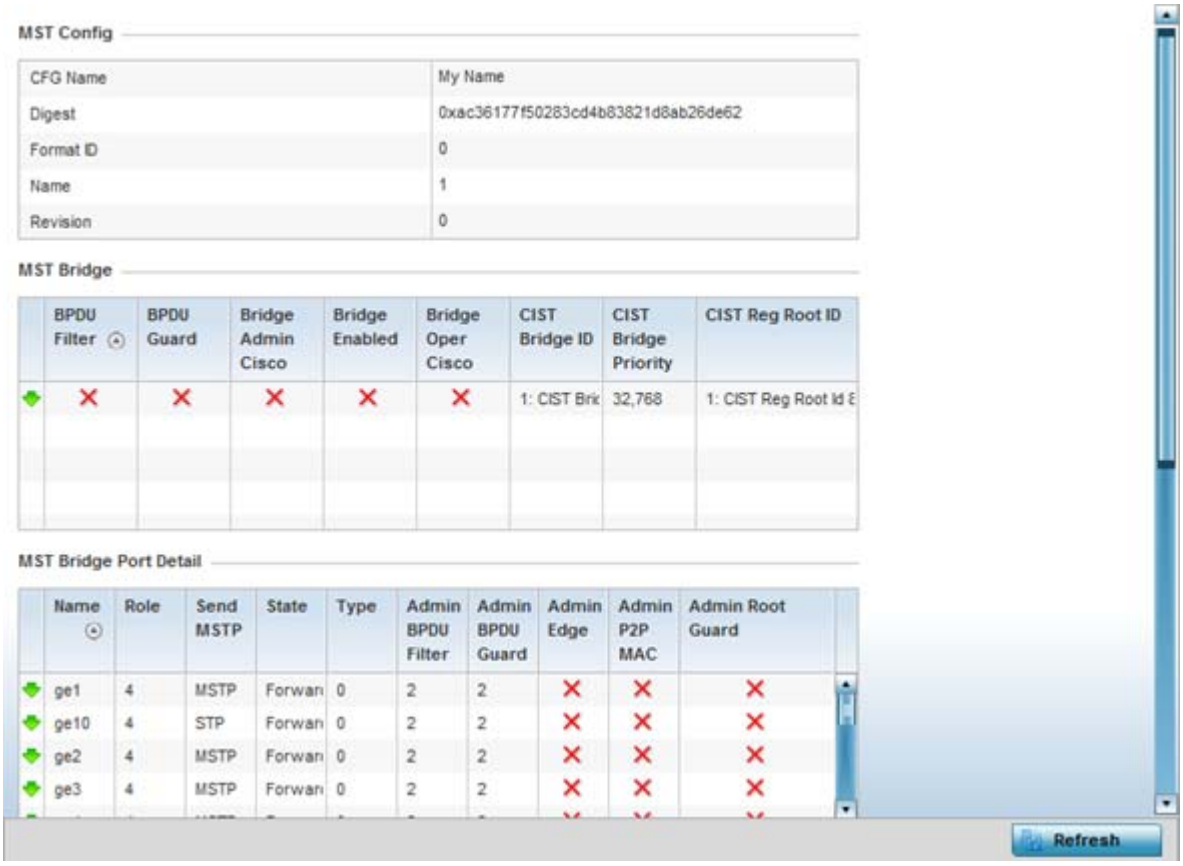


Figure 15-192 *Access Point- Network MSTP screen*

The **MST Config** field displays the name assigned to the MSTP configuration, its digest, format ID, name and revision.

The **MST Bridge** field lists the filters and guards that have been enabled and whether Cisco interoperability if enabled.

The **MST Bridge Port Detail** field lists specific Access Point port status and their current state.

15.4.27 DHCPv6 Relay & Client

Access Point Statistics

DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. DHCPv6 relay agents receive messages from clients and forward them a DHCPv6 server. The server sends responses back to the relay agent, and the relay agent sends the responses to the client on the local link

To assess an Access Point's DHCPv6 relay configuration:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **DHCP Relay & Client** from the left-hand side of the UI.

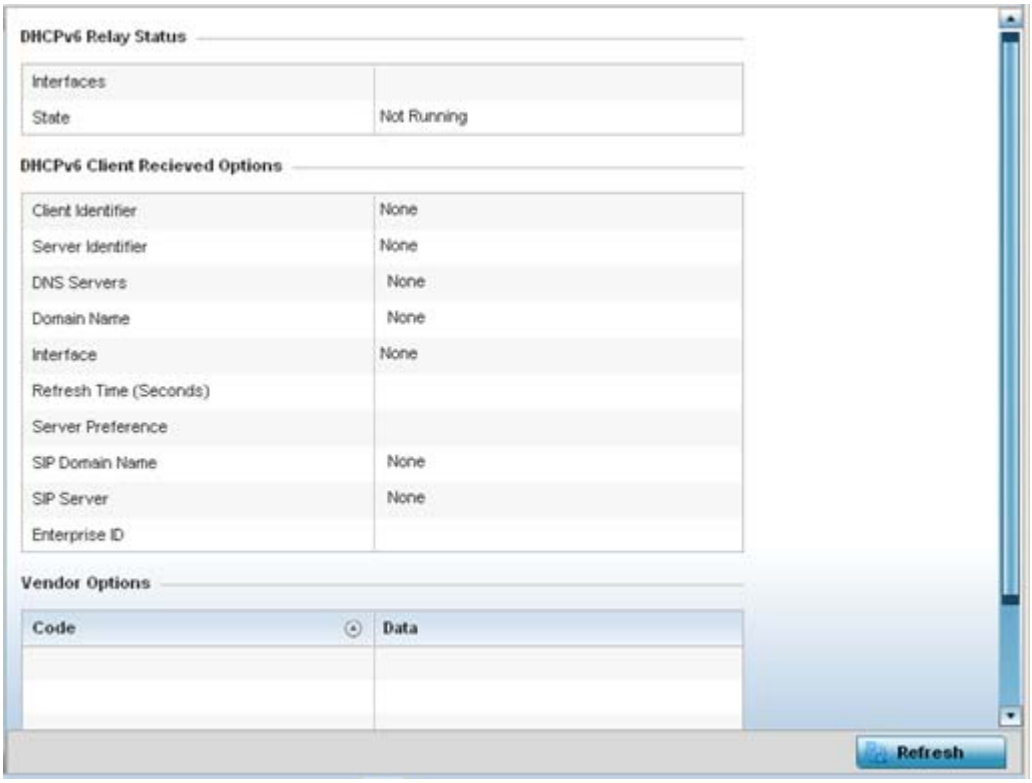


Figure 15-193 *Access Point - DHCPv6 Relay and Client screen*

4 The **DHCPv6 Status** tables defines the following:

Interfaces	Displays the Access Point interface used for DHCPv6 relay.
State	Displays the current operational state of the DHCPv6 server to assess its availability as a viable IPv6 provisioning resource.

5 The **DHCPv6 Status** tables defines the following:

Client Identifier	Lists whether the reporting client is using a *hardware address* or *client identifier* as its identifier type within requests to the DHCPv6 server.
Server Identifier	Displays the server identifier supporting client DHCPv6 relay message reception.
DNS Servers	Lists the DNS server resources supporting relay messages received from clients.
Domain Name	Lists the domain to which the remote server resource belongs.
Interface	Displays the interfaces dedicated to client DHCPv6 relay message reception.
Refresh Time (Seconds)	Lists the time (in seconds) since the data populating the DHCPv6 client received options table has been refreshed.
Server Preference	Lists the preferred DHCPv6 server resource supporting relay messages received from clients.
SIP Domain Name	Lists the SIP domain name supporting DHCPv6 client telephone extensions or voice over IP systems.

SIP Server	Displays the SIP server name supporting DHCPv6 telephone extensions or voice over IP systems.
Enterprise ID	Lists the enterprise ID associated with DHCPv6 received client options.

6 Refer to the **Vendor Options** table for the following:

Code	Lists the relevant numeric DHCP vendor code.
Data	Lists the supporting data relevant to the listed DHCP vendor code.

15.4.28 DHCP Server

Access Point Statistics

Access Point's utilize an internal *Dynamic Host Configuration Protocol* (DHCP) server. DHCP can provide IP addresses automatically. DHCP is a protocol that includes mechanisms for IP address allocation and delivery of host-specific configuration parameters (IP address, network mask gateway etc.) from a DHCP server to a host.

To review DHCP server statistics, refer to the following:

- *Viewing General DHCP Information*
- *Viewing DHCP Binding Information*
- *Viewing DHCP Server Networks Information*

15.4.28.1 Viewing General DHCP Information

DHCP Server

To view *General* DHCP status and binding information for both DHCPv4 and DHCPv6:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand the **DHCP Server** menu from the left-hand side of the UI.

4 Select **General.**

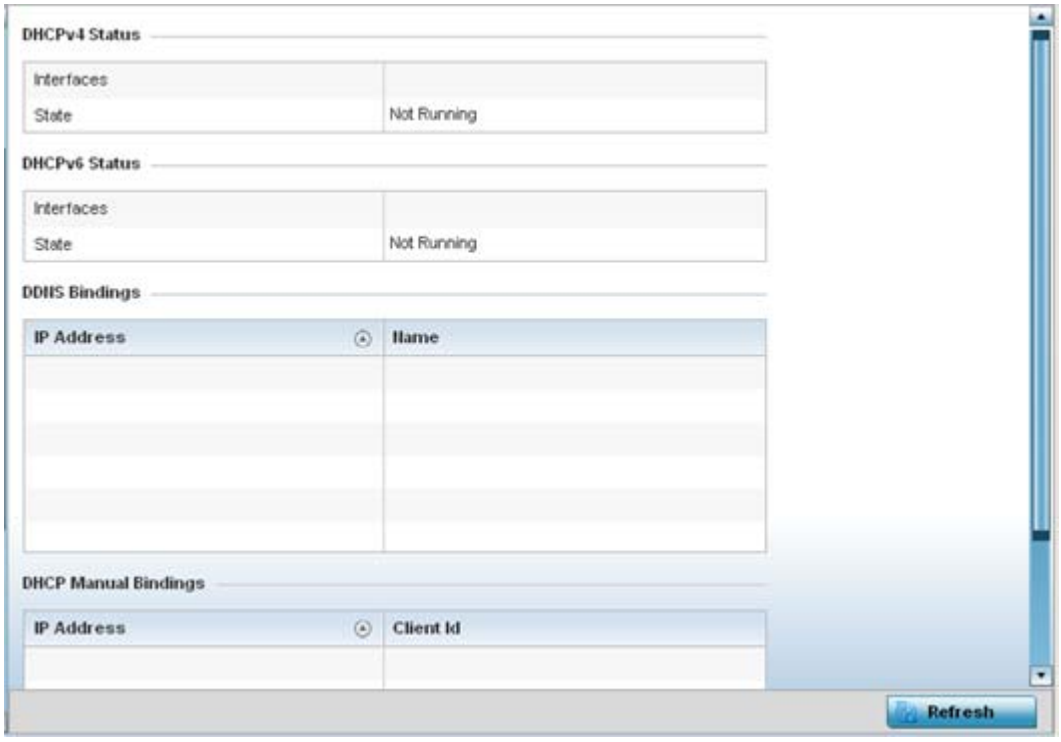


Figure 15-194 *Access Point - DHCP Server General screen*

5 The **DHCPv4 Status** and **DHCPv6 Status** tables defines the following:

Interfaces	Displays the Access Point interface used with the DHCPv4 or DHCPv6 resource for IP address provisioning.
State	Displays the current operational state of the DHCPv4 or DHCPv6 server to assess its availability as a viable IP provisioning resource.

6 The **DDNS Bindings** table displays the following:

IP Address	Displays the IP address assigned to the requesting client.
Name	Displays the domain name mapping corresponding to the listed IP address.

7 The **DHCP Manual Bindings** table displays the following:

IP Address	Displays the IP address for clients requesting DHCP provisioning resources.
Client Id	Displays the client's ID used to differentiate requesting clients.

8 Select the **Refresh** button to update the screen's statistics counters to their latest values.

15.4.28.2 Viewing DHCP Binding Information

DHCP Server

The *DHCP Binding* screen displays DHCP binding information such as expiry time, client IP addresses and their MAC address.

Access Points build and maintain a DHCP snooping table (DHCP binding database). An Access Point uses the snooping table to identify and filter untrusted messages. The DHCP binding database keeps track of DHCP

addresses assigned to ports, as well as filtering DHCP messages from untrusted ports. Incoming packets received on untrusted ports, are dropped if the source MAC address does not match the MAC in the binding table.

To view the DHCP binding information:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand the **DHCP Server** menu from the left-hand side of the UI.

4 Select **Bindings.**

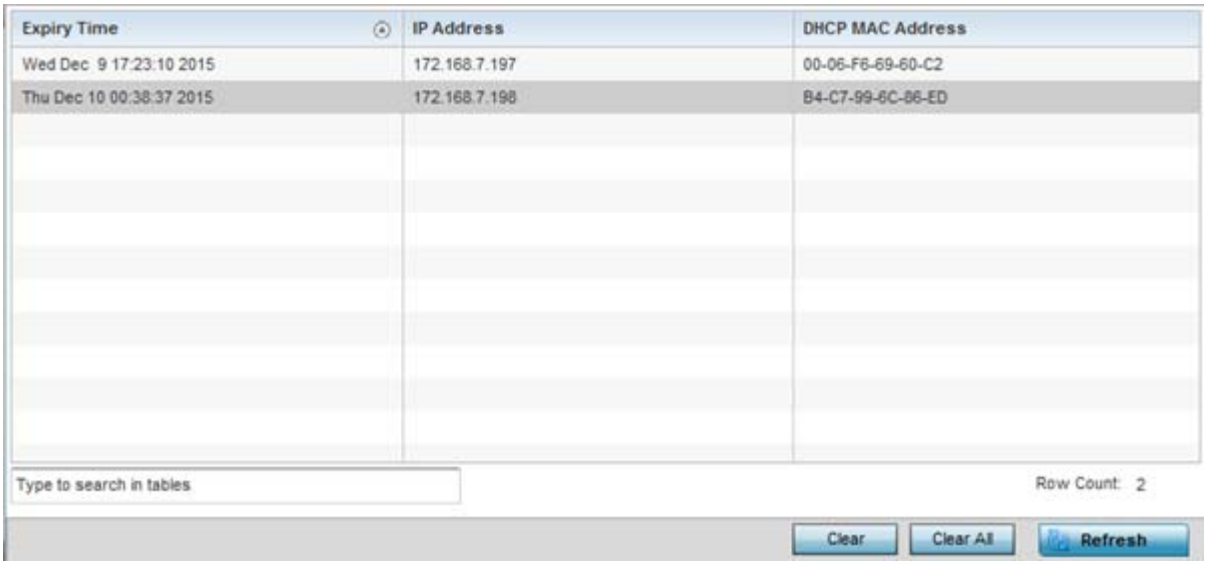


Figure 15-195 *Access Point - DHCP Server Bindings screen*

The **Bindings** screen displays the following:

Expiry Time	Displays the expiration of the lease used by the client for Access Point DHCP resources.
IP Address	Displays the IP address of each listed client requesting DHCP services.
DHCP MAC Address	Displays the MAC address of each listed client requesting DHCP services.
Clear	Select a table entry and select *Clear* to remove the client from the list of devices requesting DHCP services from the Access Point.
Clear All	Select *Clear All* to remove all listed clients from the list of requesting clients.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.28.3 Viewing DHCP Server Networks Information

DHCP Server

The DHCP server maintains a pool of IP addresses and client configuration parameters (default gateway, domain name, name servers etc). On receiving a valid client request, the server assigns the requestor an IP address, a lease (the validity of time), and other IP configuration parameters.

The *Networks* screen provides network pool information such as the subnet for the addresses you want to use from the pool, the pool name, the used addresses and the total number of addresses.

To view the **DHCP Server Networks** information:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand the **DHCP Server** menu from the left-hand side of the UI.

4 Select **Networks.**

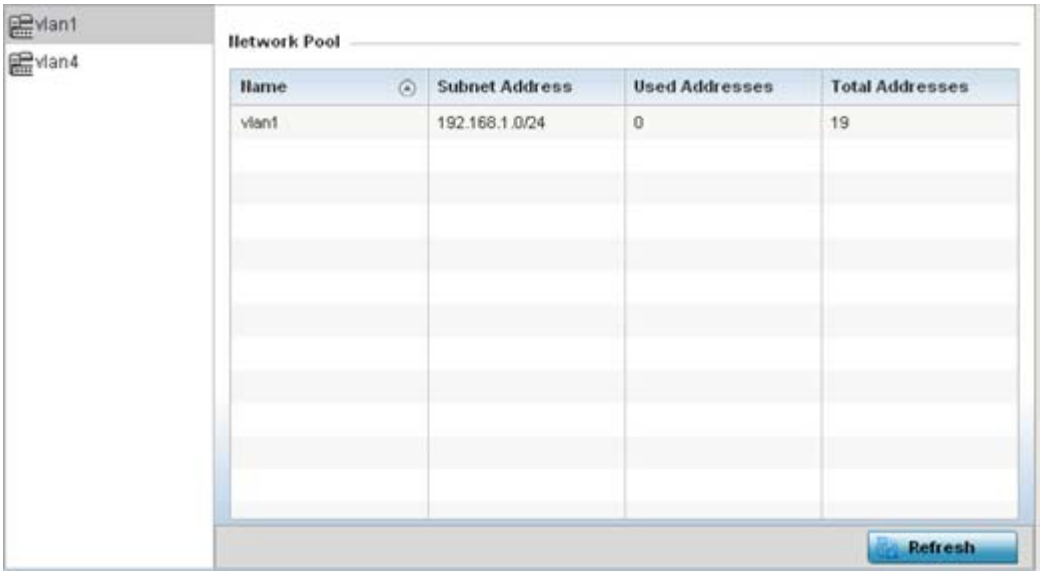


Figure 15-196 *Access Point - DHCP Server Networks screen*

The **Networks** screen displays the following:

Name	Displays the name of the virtual network (VLAN) from which IP addresses can be issued to DHCP client requests on the listed Access Point interface.
Subnet Address	Displays the subnet for the IP addresses used from the network pool.
Used Addresses	Displays the number of host IP addresses allocated by the DHCP server.
Total Addresses	Displays the total number of IP addresses available in the network pool for requesting clients.

5 Select the **Refresh** button to update the screen's statistics counters to their latest values.

15.4.29 Firewall

Access Point Statistics

A firewall is a part of a computer system or network designed to block unauthorized access while permitting authorized communications. It's a device or set of devices configured to permit or deny access to the controller or service platform managed network based on a defined set of rules.

This screen is partitioned into the following:

- *Packet Flows*

- *Denial of Service*
- *IP Firewall Rules*
- *IPv6 Firewall Rules*
- *MAC Firewall Rules*
- *NAT Translations*
- *DHCP Snooping*
- *IPv6 Neighbor Snooping*

15.4.29.1 Packet Flows

Firewall

The *Packet Flows* screen displays data traffic packet flow utilization. The chart represents the different protocol flows supported, and displays a proportional view of the flows in respect to their percentage of data traffic utilized.

The Total Active Flows graph displays the total number of flows supported. Other bar graphs display for each individual packet type.

To view Access Point packet flows statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Firewall** and expand the menu to reveal its sub menu items.

4 Select **Packet Flows**.

5 Periodically select **Refresh** to update the statistics counters to their latest values. **Clear All** clears all the statistics counters and begins a new data collection.

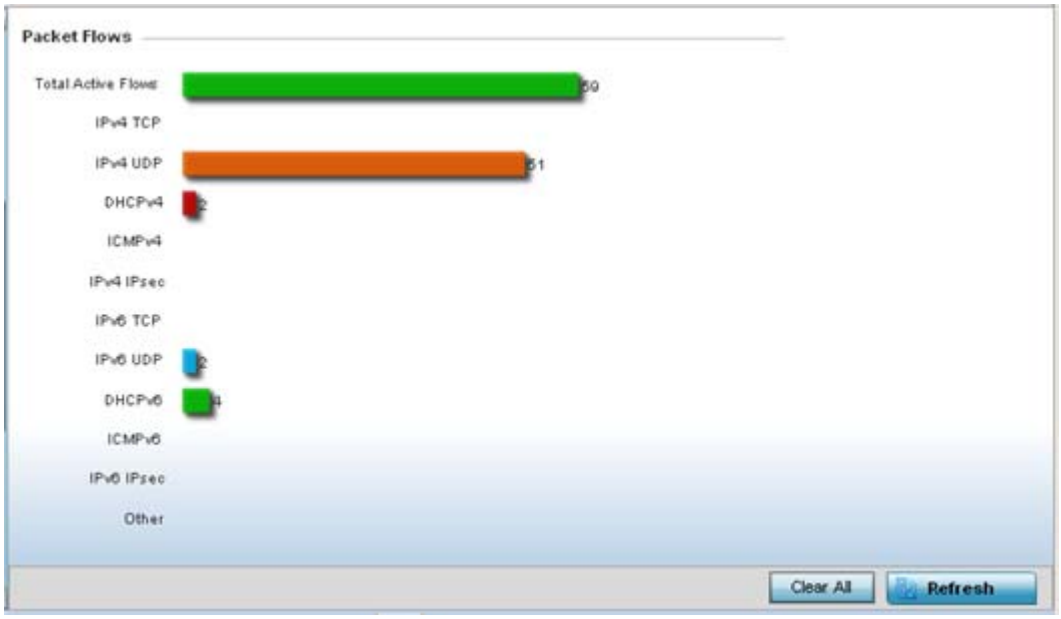


Figure 15-197 *Access Point - Firewall Packet Flows screen*

15.4.29.2 Denial of Service

Firewall

A *denial-of-service attack* (DoS attack) or distributed denial-of-service attack is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out a DoS attack may vary, it generally consists of concerted efforts to prevent an Internet site or service from functioning efficiently.

One common method involves saturating the target's machine with external communications requests, so it cannot respond to legitimate traffic or responds so slowly as to be rendered effectively unavailable. DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consume its resources so it can't provide its intended service.

The DoS screen displays the types of attack, number of times it occurred and the time of last occurrence.

To view Access Point DoS attack information:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Firewall** and expand the menu to reveal its sub menu items.

4 Select **Denial of Service**.

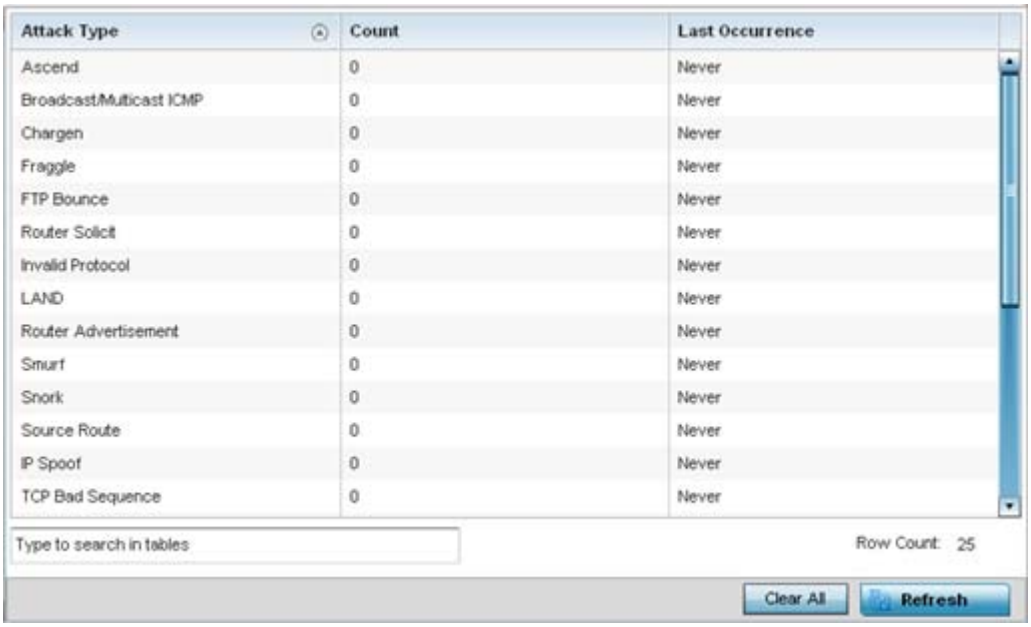


Figure 15-198 *Access Point - Firewall Denial of Service screen*

The **Denial of Service** screen displays the following:

Attack Type	Displays the *Denial of Service* (DoS) attack type.
Count	Displays the number of times the Access Point's firewall has detected each listed DoS attack.
Last Occurrence	Displays the when the attack event was last detected by the Access Point firewall.

Clear All	Select the *Clear All* button to clear the screen of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.29.3 IP Firewall Rules

Firewall

Create firewall rules to let any computer to send IPv4 formatted traffic to, or receive traffic from, programs, system services, computers or users. Firewall rules can be created to take one of the three actions listed below that match the rule's criteria:

- *Allow an IPv4 connection*
- *Allow an IPv4 connection only if it is secured through the use of Internet Protocol security*
- *Block a connection*

Rules can be created for either inbound or outbound IPv4 formatted packet traffic. To view IPv4 firewall rules:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Firewall** and expand the menu to reveal its sub menu items.

4 Select **IP Firewall Rules**.

Figure 15-199 *Access Point - Firewall IP Firewall Rules screen*

The **IP Firewall Rules** screen displays the following:

Precedence	Displays the precedence value applied to packets. The rules within an *Access Control Entries* (ACL) list are based on precedence values. Every rule has a unique precedence value between 1 and 5000. You cannot add two rules with the same precedence.

Friendly String	The friendly string provides information as to which firewall the rules apply.
Hit Count	Displays the number of times each firewall rule has been triggered.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.29.4 IPv6 Firewall Rules

Firewall

IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. These hosts require firewall packet protection unique to IPv6 traffic, as IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the *neighbor discovery* (ND) protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet layer configuration parameters.

- *Allow an IPv6 formatted connection*
- *Allow a connection only if it is secured through the use of IPv6 security*
- *Block a connection and exchange of IPv6 formatted packets*

To view existing IPv6 firewall rules:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand the **Firewall** menu from the left-hand side of the UI.

4 Select **IPv6 Firewall Rules.**

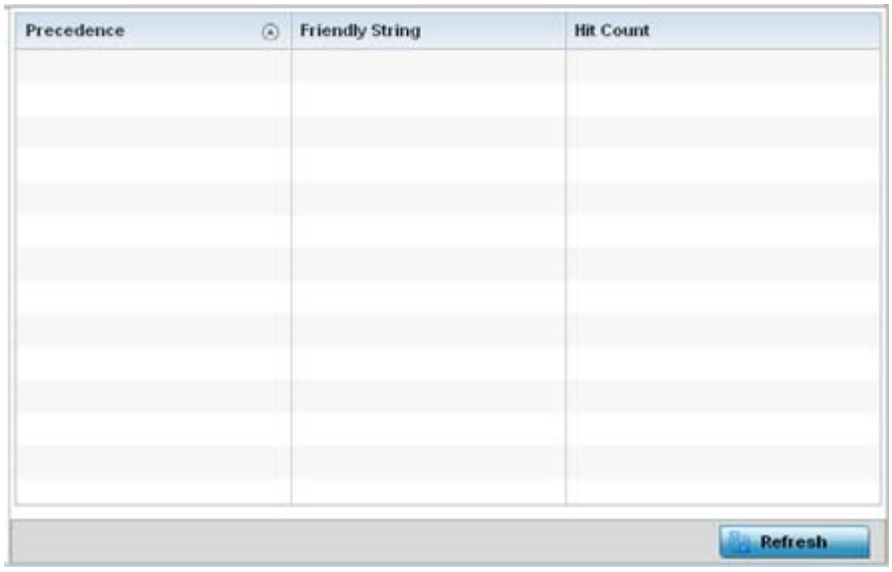


Figure 15-200 *Access Point- Firewall IPv6 Firewall Rules screen*

The **IPv6 Firewall Rules** screen displays the following:

Precedence	Displays the precedence (priority) applied to IPV6 formatted packets. Unlike IPv4, IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons. Every rule has a unique precedence value between 1 - 5000. You cannot add two rules with the same precedence value.
Friendly String	This is a string that provides more information as to the contents of the IPv6 specific IP rule. This is for information purposes only.
Hit Count	Displays the number of times each IPv6 ACL has been triggered.
Hardware Hit Count	On NX4500 and NX6500 series service platforms, intra-vlan packets are switched locally (on the service platform), preventing ACL or stateful firewall inspection. However, a unique ACL is available on NX4500 and NX6500 service platform GE ports providing a stateless firewall using IP based ACLs. The *Hardware Hit Count* constitutes the number of times one of the service platform's 1024 IP hardware rules has been triggered on one of its GE ports. NX4500 and NX6500 models have 2 GE ports, and NX4524 and NX6524 models have 24 GE ports.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.29.5 MAC Firewall Rules

Firewall

The ability to allow or deny Access Point connectivity by client MAC address ensures malicious or unwanted clients are unable to bypass the Access Point's security filters. Firewall rules can be created to support one of the three actions listed below that match the rule's criteria:

- *Allow a connection*
- *Allow a connection only if it's secured through the MAC firewall security*
- *Block a connection*

To view the Access Point's MAC Firewall Rules:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Firewall** and expand the menu to reveal its sub menu items.

4 Select **MAC Firewall Rules**.

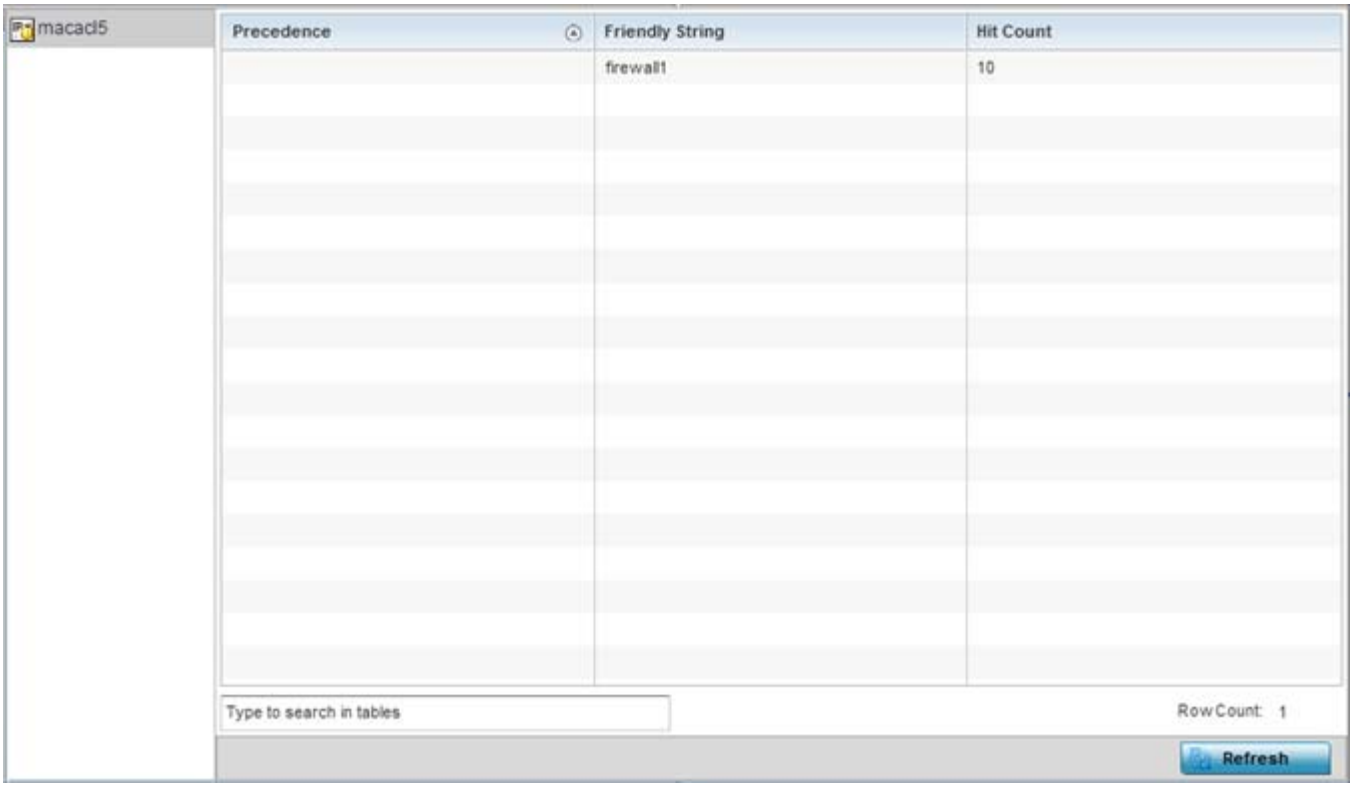


Figure 15-201 *Access Point - Firewall MAC Firewall Rules screen*

The **MAC Firewall Rules** screen displays the following information:

Precedence	Displays a precedence value, which are applied to packets. The rules within an *Access Control Entries* (ACL) list are based on their precedence. Every rule has a unique precedence between 1 and 5000. You cannot add two rules with the same precedence value.
Friendly String	This is a string that provides information as to which firewall the rules apply.
Hit Count	Displays the number of times each WLAN ACL has been triggered.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.29.6 NAT Translations

Firewall

Network Address Translation (NAT) is a technique to modify network address information within IP packet headers in transit. This enables mapping one IP address to another to protect wireless controller managed network address credentials. With typical deployments, NAT is used as an IP masquerading technique to hide private IP addresses behind a single, public facing, IP address.

NAT can provide a profile outbound Internet access to wired and wireless hosts connected to either an Access Point or a wireless controller. Many-to-one NAT is the most common NAT technique for outbound Internet access. Many-to-one NAT allows an Access Point or wireless controller to translate one or more internal private IP addresses to a single, public facing, IP address assigned to a 10/100/1000 Ethernet port or 3G card.

To view the Firewall's NAT translations:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Firewall** and expand the menu to reveal its sub menu items.

4 Select **NAT Translations**.

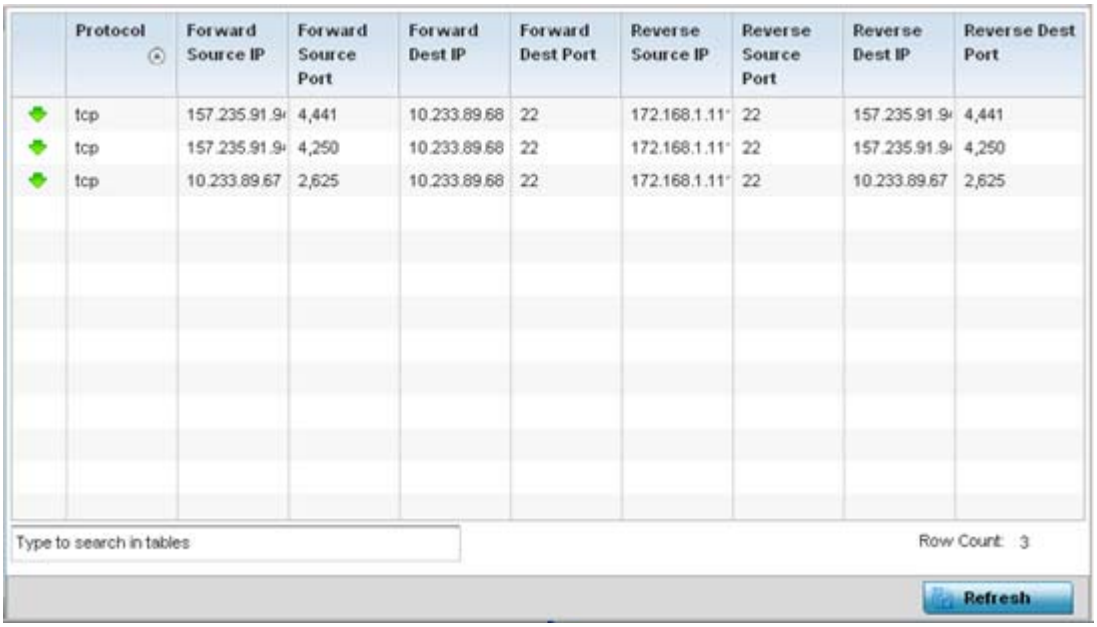


Figure 15-202 *Access Point - Firewall NAT Translation screen*

The **NAT Translations** screen displays the following:

Protocol	Lists the NAT translation IP protocol as either *TCP*, *UDP* or *ICMP*.
Forward Source IP	Displays the source IP address for the forward NAT flow.
Forward Source Port	Displays the source port for the forward NAT flow (contains ICMP ID if it is an ICMP flow).
Forward Dest IP	Displays the destination IP address for the forward NAT flow.
Forward Dest Port	Destination port for the forward NAT flow (contains ICMP ID if it is an ICMP flow).
Reverse Source IP	Displays the source IP address for the reverse NAT flow.
Reverse Source Port	Displays the source port for the reverse NAT flow (contains ICMP ID if it is an ICMP flow).
Reverse Dest IP	Displays the destination IP address for the reverse NAT flow.
Reverse Dest Port	Displays the destination port for the reverse NAT flow (contains ICMP ID if it is an ICMP flow).
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.29.7 DHCP Snooping

Firewall

When DHCP servers are allocating IP addresses to clients on the LAN, DHCP snooping can be configured to better enforce the security on the LAN to allow only clients with specific IP/MAC addresses.

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Firewall** and expand the menu to reveal its sub menu items.

4 Select **DHCP Snooping**.

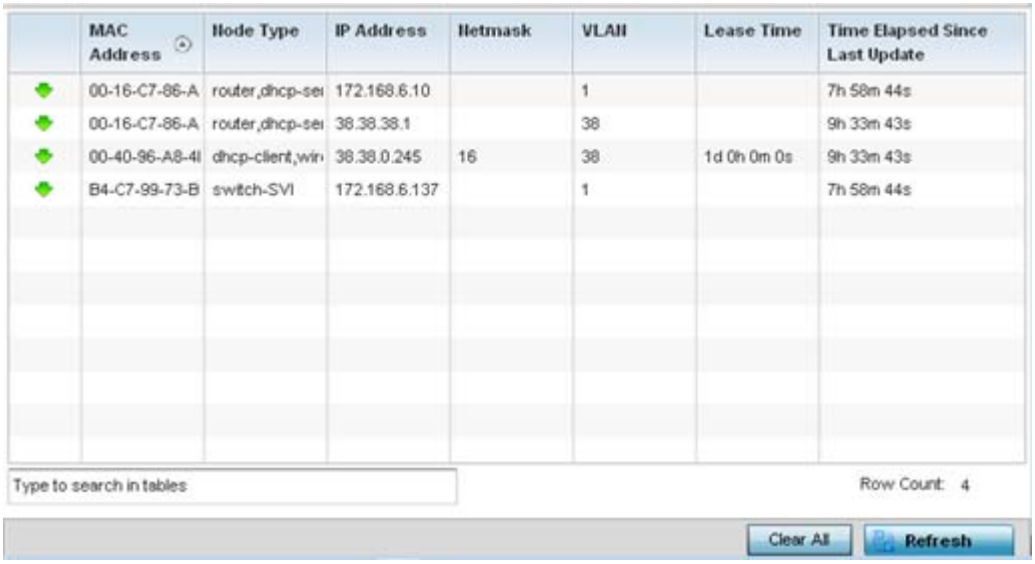


Figure 15-203 *Access Point - Firewall DHCP Snooping screen*

The **DHCP Snooping** screen displays the following:

MAC Address	Displays the MAC address of the client requesting DHCP resources from the controller or service platform.
Node Type	Displays the NetBios node from which IP addresses can be issued to client requests on this interface.
IP Address	Displays the IP address used for DHCP discovery, and requests between the DHCP server and DHCP clients.
Netmask	Displays the subnet mask used for DHCP discovery, and requests between the DHCP server and DHCP clients.
VLAN	Displays the VLAN used as a virtual interface for the newly created DHCP configuration.
Lease Time	When a DHCP server allocates an address for a DHCP client, the client is assigned a lease (which expires after a designated interval defined by the administrator). The lease time is the time an IP address is reserved for re-connection after its last use. Using very short leases, DHCP can dynamically reconfigure networks in which there are more computers than there are available IP addresses. This is useful, for example, in education and customer environments where client users change frequently. Use longer leases if there are fewer users.

Time Elapsed Since Last Updated	Displays the time the server was last updated.
Clear All	Select the *Clear All* button to clear the screen of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.29.8 IPv6 Neighbor Snooping

Firewall

Access Points listen to IPv6 formatted network traffic and forward IPv6 packets to radios on which the interested hosts are connected.

To review IPv6 neighbor snooping statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Expand the **Firewall** menu from the left-hand side of the UI.

4 Select **IPv6 Neighbor Snooping.**

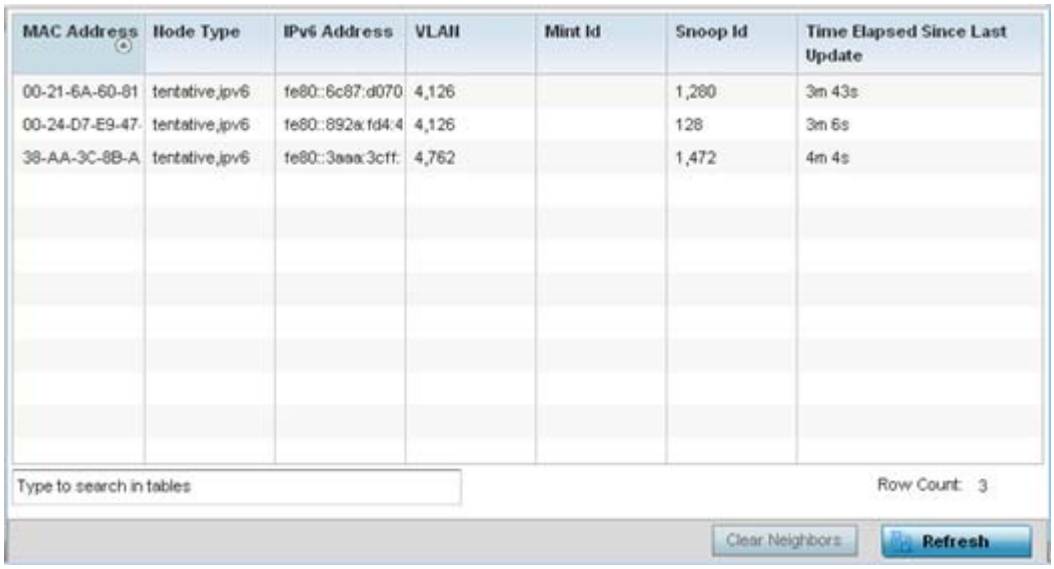


Figure 15-204 *Access Point- Firewall IPv6 Neighbor Snooping screen*

The **IPv6 Neighbor Snooping** screen displays the following:

MAC Address	Displays the MAC address of the IPv6 client.
Node Type	Displays the NetBios node with an IPv6 address pool from which IP addresses can be issued to client requests on this interface.
IPv6 Address	Displays the IPv6 address used for DHCPv6 discovery and requests between the DHCPv6 server and DHCP clients.
VLAN	Displays an Access Point virtual interface ID used for a new DHCPv6 configuration.

Mint Id	Lists MiNT IDs for each listed VLAN. MiNT provides the means to secure communications at the transport layer. Using MiNT, a device can be configured to only communicate with other authorized (MiNT enabled) devices of the same model.
Snoop Id	Lists the numeric snooping session ID generated when Access Points listen to IPv6 formatted network traffic and forward IPv6 packets to radios.
Time Elapsed Since Last Update	Displays the amount of time elapsed since the DHCPv6 server was last updated.
Clear Neighbors	Select *Clear Neighbors* to revert the counters to zero and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's counters to their latest values.

15.4.30 VPN

Access Point Statistics

IPSec VPN provides a secure tunnel between two networked peer controllers or service platforms. Administrators can define which packets are sent within the tunnel, and how they are protected. When a tunnelled peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its remote peer destination.

Tunnels are sets of *security associations* (SA) between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunnelled peers. SAs are unidirectional and exist in both the inbound and outbound direction. SAs are established per the rules and conditions of defined security protocols (AH or ESP).

Crypto maps combine the elements comprising IPSec SAs. Crypto maps also include *transform sets*. A transform set is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic. One crypto map is utilized for each IPsec peer, however for remote VPN deployments one crypto map is used for all the remote IPsec peers.

Internet Key Exchange (IKE) protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs, and enables secure communications without time consuming manual pre-configuration.

VPN statistics are partitioned into the following:

IKESA

IPSec

15.4.30.1 IKESA

VPN

The *IKESA* screen allows for the review of individual peer security association statistics.

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **VPN** and expand the menu to reveal its sub menu items.

4 Select **IKESA**.

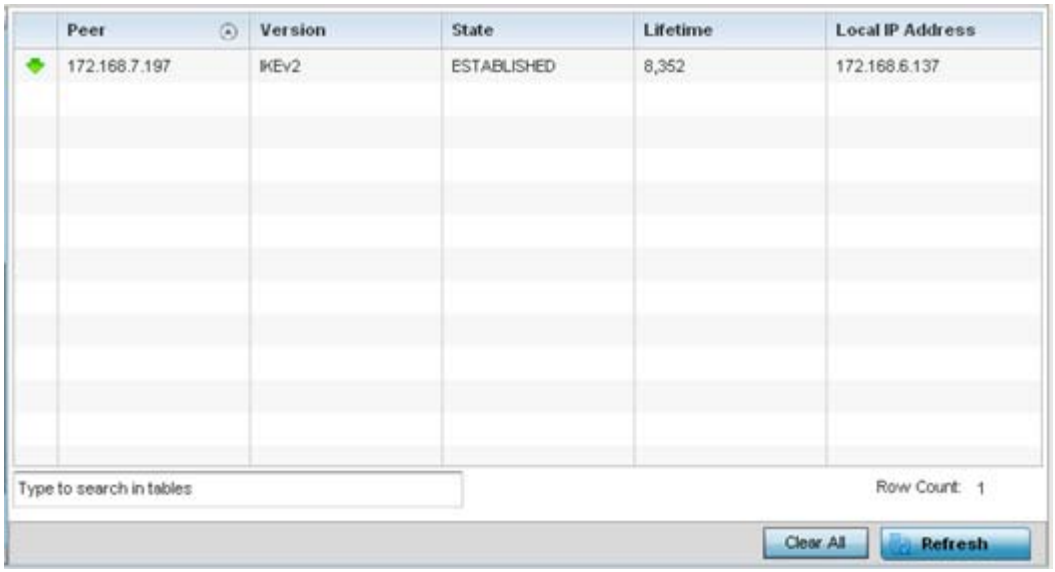


Figure 15-205 *Access Point - VPN IKESA screen*

5 Review the following VPN peer security association statistics:

Peer	Lists peer IDs for peers sharing *security associations* (SA) for tunnel interoperability. When a peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its destination.
Version	Displays each peer's IKE version used for auto IPSec secure authentication with the IPSec gateway and other controllers or service platforms.
State	Lists the state of each listed peer's security association (whether established or not).
Lifetime	Displays the lifetime for the duration of each listed peer IPSec VPN security association. Once the set value is exceeded, the association is timed out.
Local IP Address	Displays each listed peer's local tunnel end point IP address. This address represents an alternative to an interface IP address.
Clear All	Select the *Clear All* button to clear each peer of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.30.2 IPSec

VPN

Use the *IPSec* VPN screen to assess tunnel status between networked peers.

To view IPSec VPN status for tunnelled peers:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points

3 Select **VPN** and expand the menu to reveal its sub menu items.

4 Select **IPSec**.

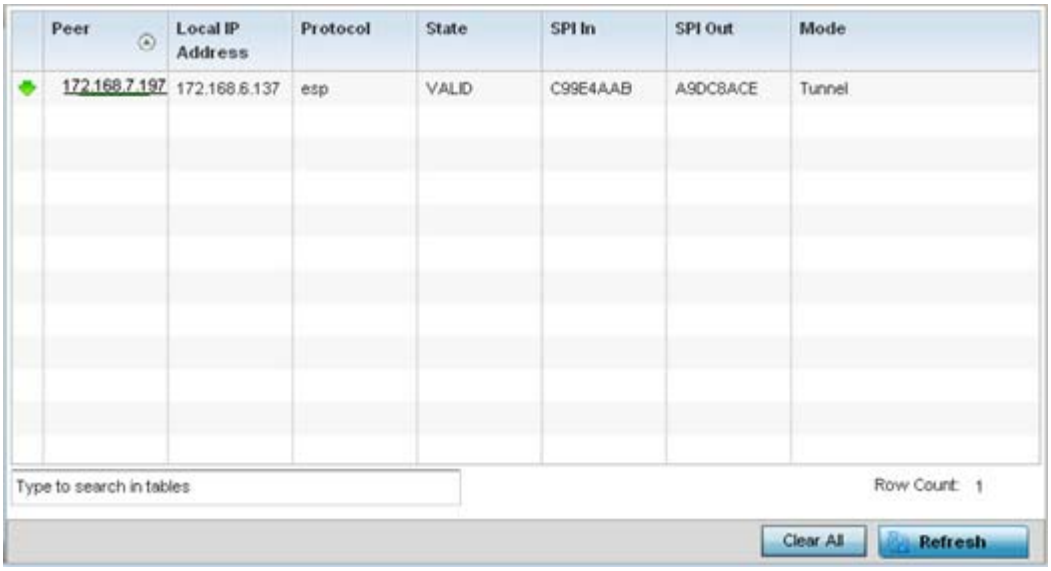


Figure 15-206 *Access Point - VPN IPSec screen*

5 Review the following VPN peer security association statistics:

Peer	Lists IP addresses for peers sharing *security associations* (SAs) for tunnel interoperability. When a peer sees a sensitive packet, it creates a secure tunnel and sends the packet through the tunnel to its destination.
Local IP Address	Displays each listed peer's local tunnel end point IP address. This address represents an alternative to an interface IP address.
Protocol	Lists the security protocol used with the VPN IPSec tunnel connection. SAs are unidirectional, existing in each direction and established per security protocol. Options include *ESP* and *AH*.
State	Lists the state of each listed peer's security association.
SPI In	Lists *stateful packet inspection* (SPI) status for incoming IPSec tunnel packets. SPI tracks each connection traversing the IPSec VPN tunnel and ensures they are valid.
SPI Out	Lists SPI status for outgoing IPSec tunnel packets. SPI tracks each connection traversing the IPSec VPN tunnel and ensures they are valid.
Mode	Displays the IKE mode. IPSEC has two modes in IKEv1 for key exchanges. Aggressive mode requires 3 messages be exchanged between the IPSEC peers to setup the SA, Main requires 6 messages.
Clear All	Select the *Clear All* button to clear each peer of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.31 Certificates

Access Point Statistics

The *Secure Socket Layer* (SSL) protocol ensures secure transactions between Web servers and browsers. SSL uses a third-party certificate authority to identify one (or both) ends of a transaction. A browser checks the certificate issued by the server before establishing a connection.

This screen is partitioned into the following:

- *Trustpoints*
- *RSA Keys*

15.4.31.1 Trustpoints

Certificates

Each certificate is digitally signed by a trustpoint. The trustpoint signing the certificate can be a certificate authority, corporate or individual. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters and an association with an enrolled identity certificate.

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points

3 Select **Certificates** and expand the menu to reveal its sub menu items.

4 Select **Trustpoints**.

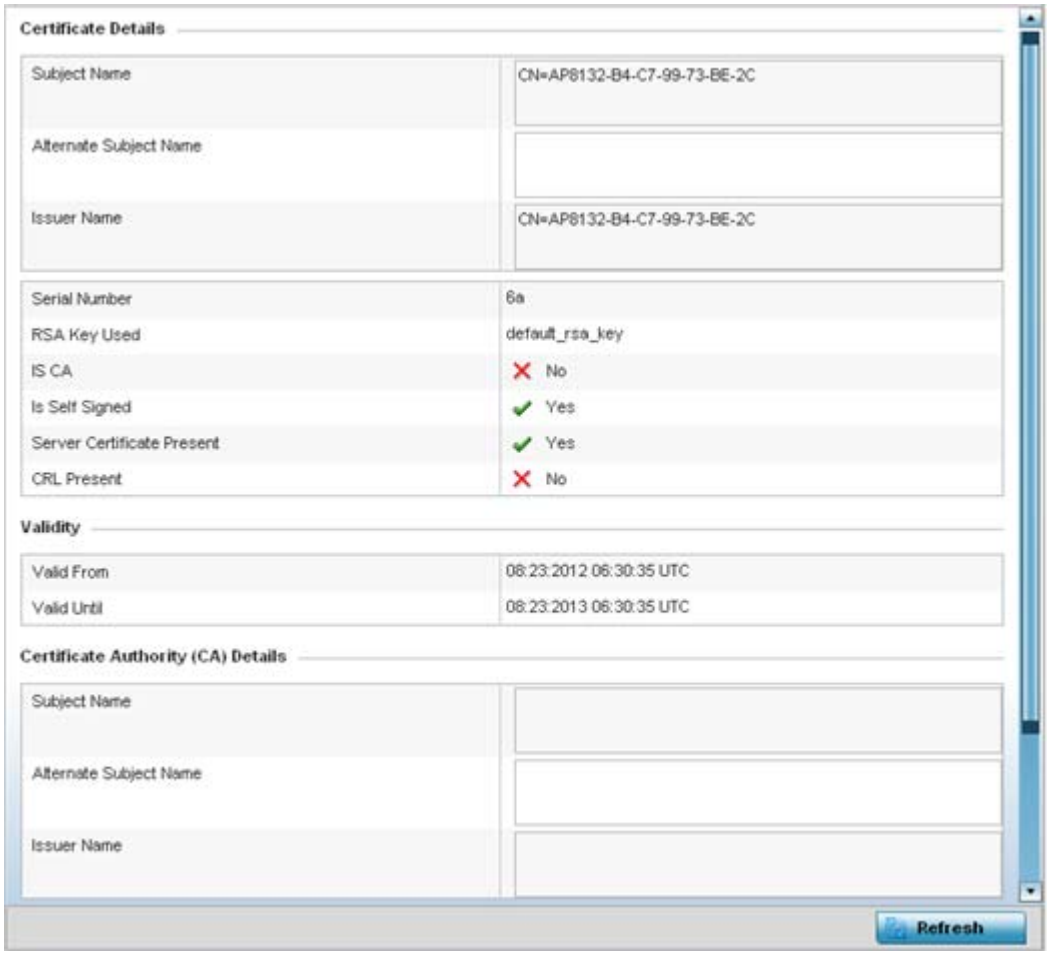


Figure 15-207 *Access Point - Certificate Trustpoint screen*

The Certificate Details field displays the following:

Subject Name	Lists details about the entity to which the certificate is issued.
Alternate Subject Name	Displays alternative details to the information specified under the Subject Name field.
Issuer Name	Displays the name of the organization issuing the certificate.
Serial Number	The unique serial number of the certificate issued.
RSA Key Used	Displays the name of the key pair generated separately, or automatically when selecting a certificate.
IS CA	Indicates whether this certificate is an authority certificate (Yes/No).
Is Self Signed	Displays whether the certificate is self-signed (Yes/No).
Server Certificate Present	Displays whether a server certification is present or not (Yes/No).
CRL Present	Displays whether a *Certificate Revocation List* (CRL) is present (Yes/No). A CRL contains a list of subscribers paired with digital certificate status. The list displays revoked certificates along with the reasons for revocation. The date of issuance and the entities that issued the certificate are also included.

5 Refer to the **Validity** field to assess the certificate duration beginning and end dates.

6 Review the *Certificate Authority* (CA) Details and Validity information to assess the subject and certificate duration periods.

7 Periodically select the **Refresh** button to update the screen's statistics counters to their latest values.

15.4.31.2 RSA Keys

Certificates

Rivest, Shamir, and Adleman (RSA) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing, as well as encryption.

The *RSA Keys* screen displays a list of RSA keys installed in the selected Access Point. RSA Keys are generally used for establishing a SSH session, and are a part of the certificate set used by RADIUS, VPN and HTTPS.

To view the RSA Key details:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points

3 Select **Certificates** and expand the menu to reveal its sub menu items.

4 Select **RSA Keys**.

Figure 15-208 *Access Point - Certificate RSA Keys screen*

The **RSA Key Details** field displays the size (in bits) of the desired key. If not specified, a default key size of 1024 is used.

The **RSA Public Key** field lists the public key used for encrypting messages.

5 Periodically select the **Refresh** button to update the screen's statistics counters to their latest values.

15.4.32 WIPS

Access Point Statistics

A *Wireless Intrusion Prevention System* (WIPS) monitors the radio spectrum for the presence of unauthorized Access Points and take measures to prevent an intrusion. Unauthorized attempts to access a controller or service platform managed WLAN is generally accompanied by anomalous behavior as intruding clients try to find network vulnerabilities. Basic forms of this behavior can be monitored and reported without a dedicated WIPS. When the parameters exceed a configurable threshold, a SNMP trap is generated that reports the results via management interfaces.

The WIPS screens provide details about the blacklisted clients (unauthorized Access Points) intruded into the network. Details include the name of the blacklisted client, the time when the client was blacklisted, the total time the client remained in the network, etc. The screen also provides WIPS event details.

For more information, see:

- *WIPS Client Blacklist*
- *WIPS Events*

15.4.32.1 WIPS Client Blacklist

WIPS

This *Client Blacklist* displays blacklisted clients detected by this Access Point using WIPS. Blacklisted clients are not allowed to associate to this Access Points.

To view the WIPS client blacklist for this Access Point:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **WIPS** and expand the menu to reveal its sub menu items.

4 Select **Client Blacklist**.

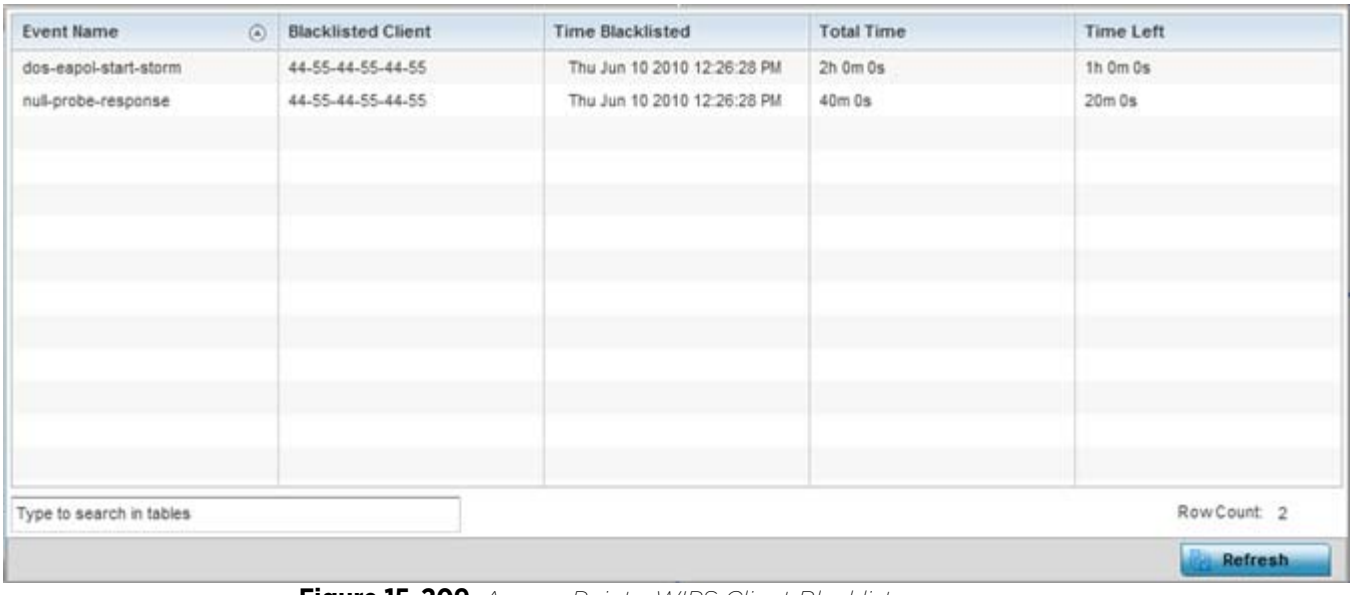


Figure 15-209 *Access Point - WIPS Client Blacklist screen*

The WIPS **Client Blacklist** screen displays the following:

Event Name	Displays the name of the event that resulted in the blacklisting.
Blacklisted Client	Displays the MAC address of the unauthorized and blacklisted device intruding this Access Point's radio coverage area.
Time Blacklisted	Displays the time when the client was blacklisted by this Access Point.
Total Time	Displays the time the unauthorized (now blacklisted) device remained in this Access Point's WLAN.
Time Left	Displays the time the blacklisted client remains on the list.
Refresh	Select the *Refresh* button to update the statistics counters to their latest values.

15.4.32.2 WIPS Events

WIPS

To view the WIPS events statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **WIPS** and expand the menu to reveal its sub menu items.

4 Select **WIPS Events**.

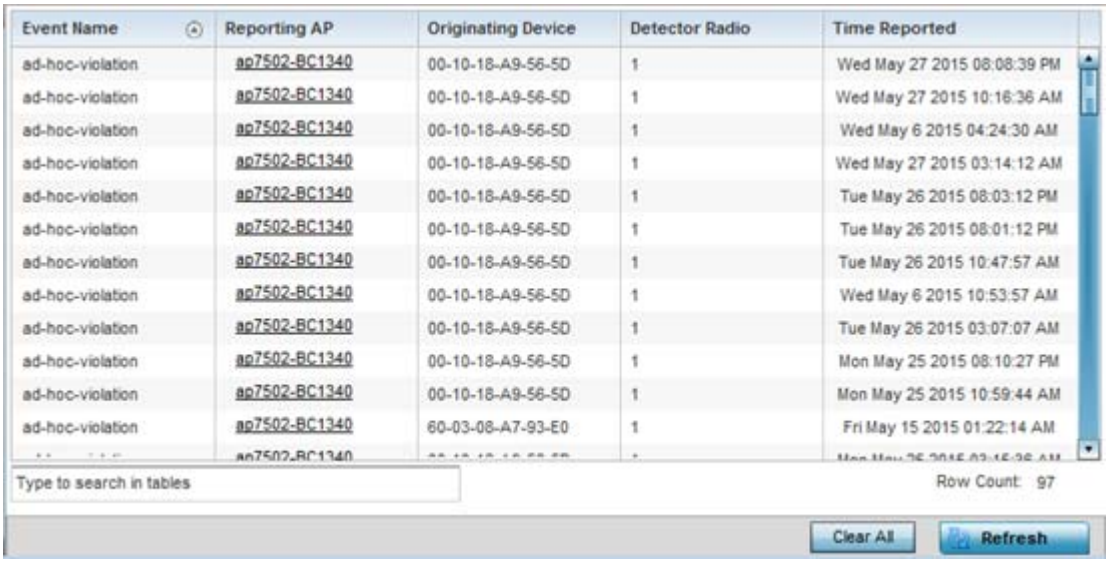


Figure 15-210 *Access Point - WIPS Events screen*

The **WIPS Events** screen provides the following:

Event Name	Displays the name of the detected wireless intrusion event.
Reporting AP	Displays the MAC address of the Access Point reporting the listed intrusion.
Originating Device	Displays the MAC address of the intruding device.
Detector Radio	Displays the number of the detecting Access Point radio.

Time Reported	Displays the time when the intrusion event was detected.
Clear All	Select the *Clear All* button to clear the screen of its current status and begin a new data collection.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.33 Sensor Servers

Access Point Statistics

Sensor servers allow the monitor and download of data from multiple sensors and remote locations using Ethernet TCP/IP or serial communication. Repeaters are available to extend the transmission range and combine sensors with various frequencies on the same receiver.

To view the network address and status information of the sensor server resources available to the Access Point:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Sensor Servers**.

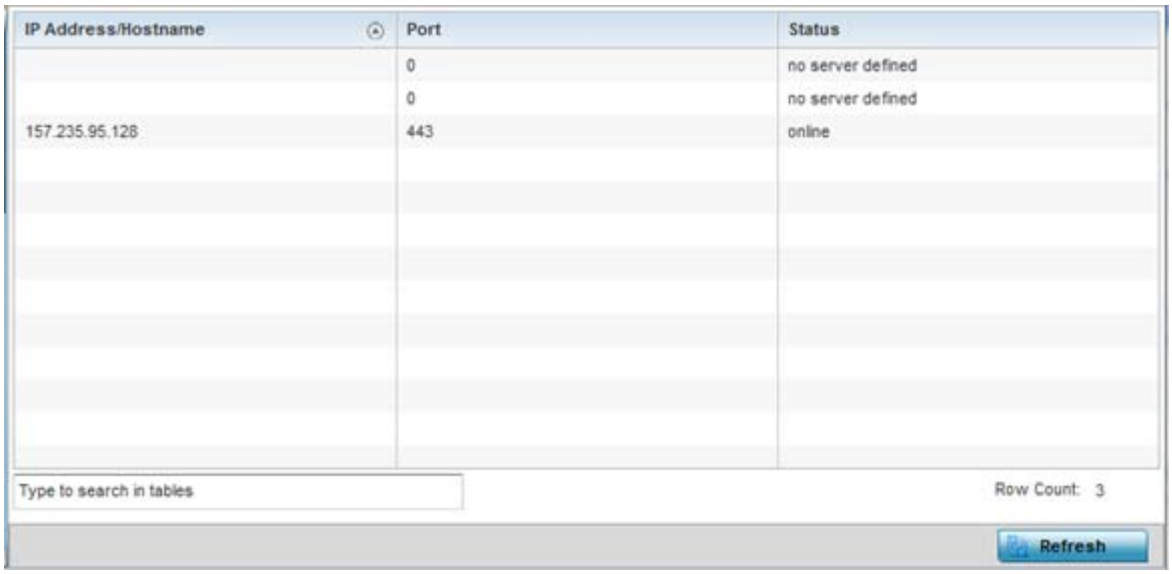


Figure 15-211 *Access Point - Sensor Servers screen*

The **Sensor Servers** screen displays the following:

IP Address/ Hostname	Displays a list of sensor server IP addresses or administrator assigned hostnames. These are the server resources available to the Access Point for the management of data uploaded from dedicated sensors.
Port	Displays the numerical port where the sensor server is listening. Unconnected server resources are not able to provide sensor reporting.
Status	Displays whether the server resource is connected or not.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.34 Bonjour Services

Access Point Statistics

Bonjour is Apple's zero-configuration networking (Zeroconf) implementation. Zeroconf is a group of technologies that include service discovery, address assignment and hostname resolution. Bonjour locates the devices (printers, computers etc.) and services these computers provide over a local network.

Bonjour provides a method to discover services on a LAN. Bonjour allows users to set up a network without any configuration. Services such as printers, scanners and file-sharing servers can be found using Bonjour. Bonjour only works within a single broadcast domain. However, with a special DNS configuration, it can be extended to find services across broadcast domains.

To view the Bonjour service statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Bonjour Services** from the left-hand side of the Access Point UI.

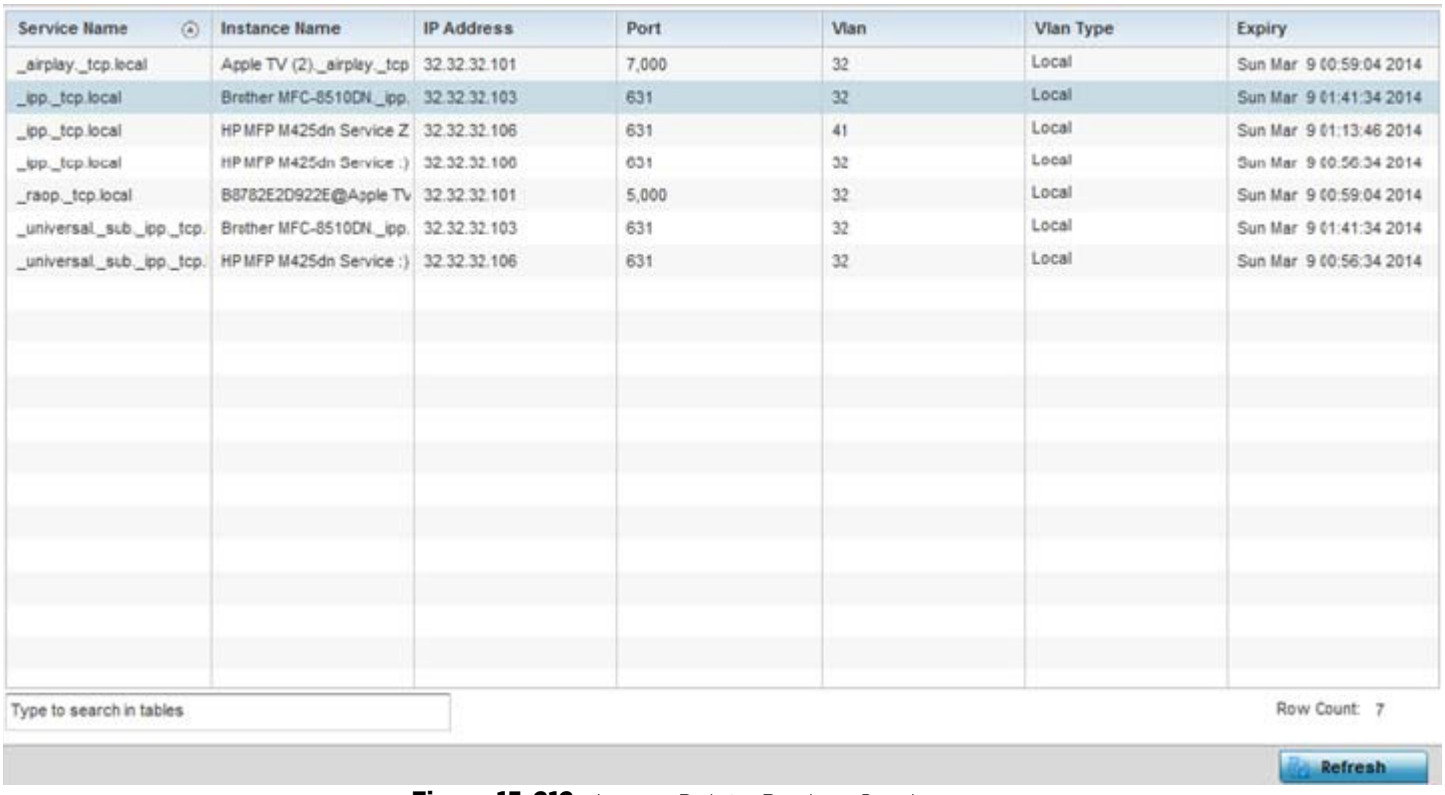


Figure 15-212 *Access Point - Bonjour Services screen*

Refer to the following Bonjour service utilization stats.:

Service Name	Lists the services discoverable by the Bonjour gateway. Services can either be *pre-defined* Apple services (scanner, printer etc.) or an *alias* not available on the predefined list.
Instance Name	Lists the name of each Bonjour service instance (session) utilized by the Access Point.

IP Address	Lists the network IP address utilized by the listed Bonjour service providing resources to the Access Point.
Port	Displays the port used to secure a connection with the listed Bonjour service.
Vlan	Lists the VLAN(s) on which a listed Bonjour service is routable.
Vlan Type	Lists the VLAN type as either a *local* bridging mode or a shared *tunnel*.
Expiry	Lists the expiration date of the listed Bonjour service, and its availability to discover resources on the LAN.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.35 Captive Portal

Access Point Statistics

A captive portal forces a HTTP client to use a special Web page for authentication before using the Internet. A captive portal turns a Web browser into a client authenticator. This is done by intercepting packets regardless of the address or port, until the user opens a browser and tries to access the Internet. At that time, the browser is redirected to a Web page.

To view the captive portal statistics of an Access Point:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Captive Portal**.

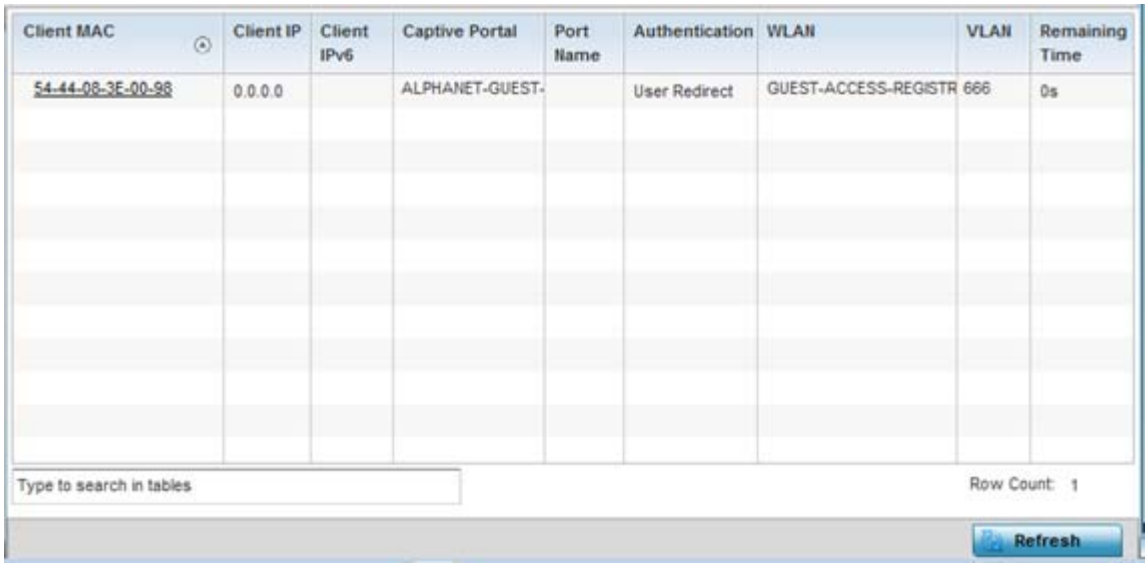


Figure 15-213 *Access Point - Captive Portal screen*

The **Captive Portal** screen displays the following:

Client MAC	Displays the requesting client's MAC address. The MAC displays as a link that can be selected to display client configuration and network address information in greater detail.

Client IP	Displays the requesting client's IPv4 formatted IP address.
Client IPv6	Displays the requesting client's IPv6 formatted IP address.
Captive Portal	Displays the captive portal name that each listed client is utilizing for guest access to Access Point resources.
Port Name	Lists the Access Point port name supporting the captive portal connection with the listed client MAC address.
Authentication	Displays the authentication status of the requesting client.
WLAN	Displays the name of the WLAN the client belongs to.
VLAN	Displays the name of the requesting client's VLAN interface.
Remaining Time	Displays the time after which the client is disconnected from the captive portal managed Internet.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.36 Network Time

Access Point Statistics

Network Time Protocol (NTP) is central to networks that rely on their Access Point(s) to supply system time. Without NTP, Access Point supplied network time is unpredictable, which can result in data loss, failed processes, and compromised security. With network speed, memory, and capability increasing at an exponential rate, the accuracy, precision, and synchronization of network time is essential in an Access Point managed enterprise network. The Access Point can use a dedicated server to supply system time. The Access Point can also use several forms of NTP messaging to sync system time with authenticated network traffic.

The Network Time screen provides detailed statistics of an associated NTP Server of an Access Point. Use this screen to review the statistics for each Access Point.

The Network Time statistics screen consists of two tabs:

- *NTP Status*
- *NTP Association*

15.4.36.1 NTP Status

Network Time

To view the Network Time statistics of an Access Point:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Network Time.**

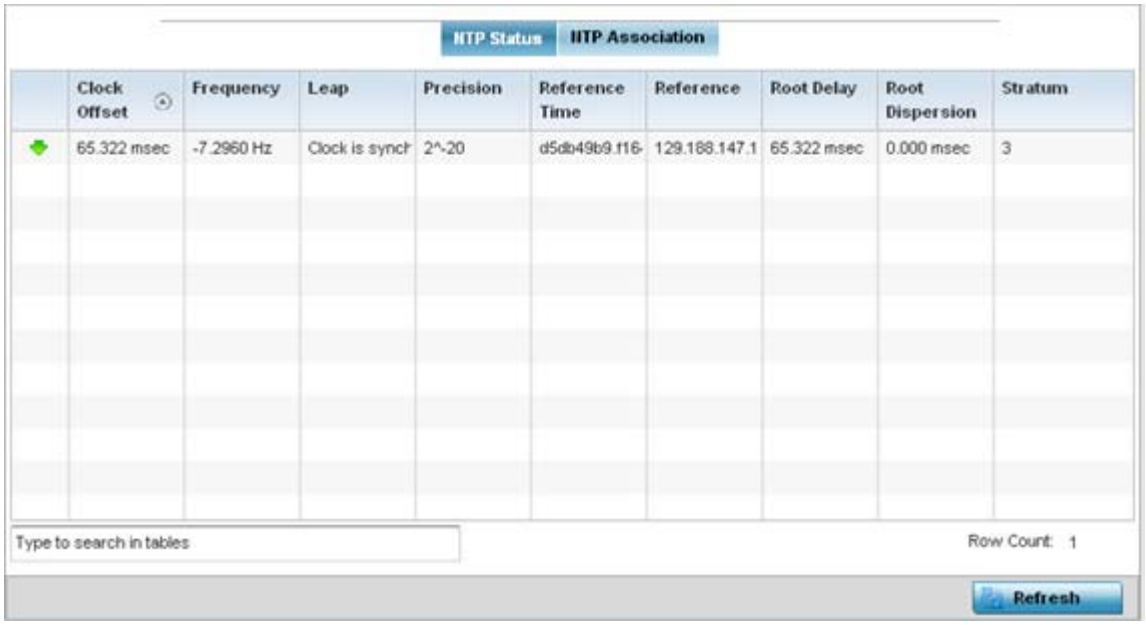


Figure 15-214 *Access Point - NTP Status screen*

The **NTP Status** tab displays by default with the following information:

Clock Offset	Displays the time differential between the Access Point's time and its NTP resource's time.
Frequency	Indicates the SNTP server clock's skew (difference) for the Access Point.
Leap	Indicates if a second is added or subtracted to SNTP packet transmissions, or if transmissions are synchronized.
Precision	Displays the precision of the time clock (in Hz). The values that normally appear in this field range from -6, for mains-frequency clocks, to -20 for microsecond clocks.
Reference Time	Displays the time stamp the Access Point's clock was last synchronized or corrected.
Reference	Displays the address of the time source the Access Point is synchronized to.
Root Delay	The total round-trip delay in seconds. This variable can take on both positive and negative values, depending on relative time and frequency offsets. The values that normally appear in this field range from negative values (a few milliseconds) to positive values (several hundred milliseconds).
Root Dispersion	The difference between the time on the root NTP server and its reference clock. The reference clock is the clock used by the NTP server to set its own clock.
Stratum	Displays how many hops the Access Point is from its current NTP time resource.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.36.2 NTP Association

Network Time

The interaction between the Access Point and an NTP server constitutes an association. NTP associations can be either peer associations (the Access Point synchronizes to another system or allows another system to synchronize to it), or a server associations (only the Access Point synchronizes to the NTP resource, not the other way around).

To view the Access Point's NTP association statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Network Time**.

4 Select the **NTP Association** tab.

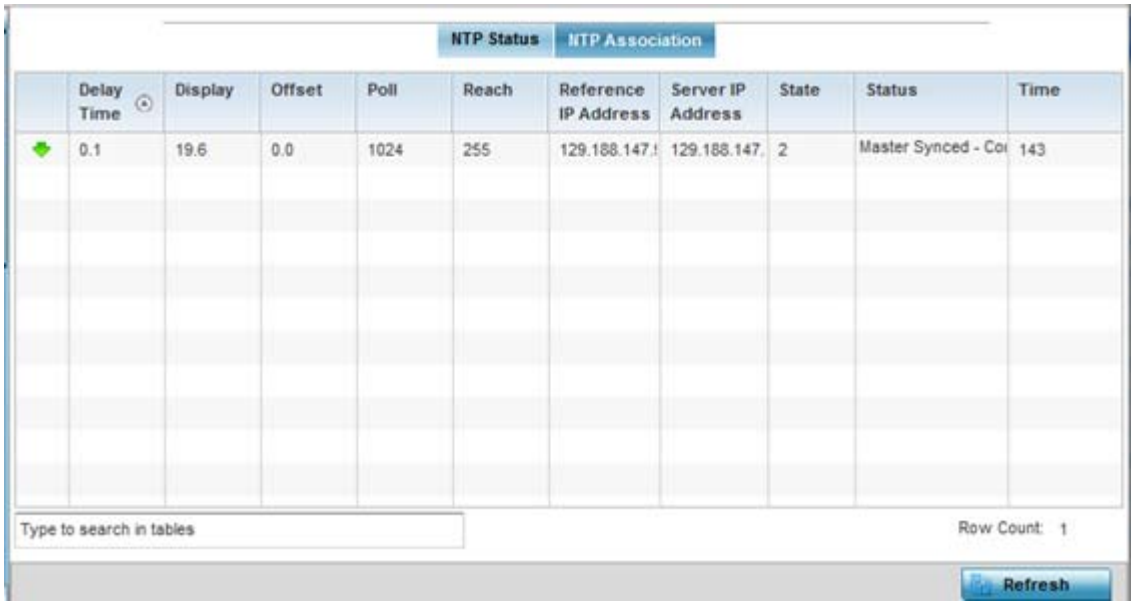


Figure 15-215 *Access Point - NTP Association screen*

The **NTP Association** screen displays the following:

Delay Time	Displays the round-trip delay (in seconds) for broadcasts between the NTP server and the Access Point.
Display	Displays the time difference between the peer NTP server and the Access Point's clock.
Offset	Displays the calculated offset between the Access Point and the NTP server. The Access Point adjusts its clock to match the server's time value. The offset gravitates towards zero, but never completely reduces its offset to zero.
Poll	Displays the maximum interval between successive messages (in seconds) to the nearest power of two.
Reach	Displays the status of the last eight SNTP messages. If an SNTP packet is lost, the lost packet is tracked over the next eight SNTP messages.

Reference IP Address	Displays the address of the time source the Access Point is synchronized to.
Server IP Address	Displays the numerical IP address of the SNTP resource (server) providing SNTP updates to the Access Point.
State	Displays the NTP association status code.
Status	Displays how many hops the Access Point is from its current NTP time source.
Time	Displays the time of the last statistics update.
Refresh	Select the *Refresh* button to update the screen's statistics counters to their latest values.

15.4.37 Load Balancing

Access Point Statistics

An Access Point load can be viewed in a graph and filtered to display different load attributes. The Access Point's entire load can be displayed, as well as the separate loads on the 2.4 and 5 GHz radio bands. The channels can also be filtered for display. Each element can either be displayed *individually* or *collectively* in the graph.

To view the Access Point's load balance in a filtered graph format:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Load Balancing**.

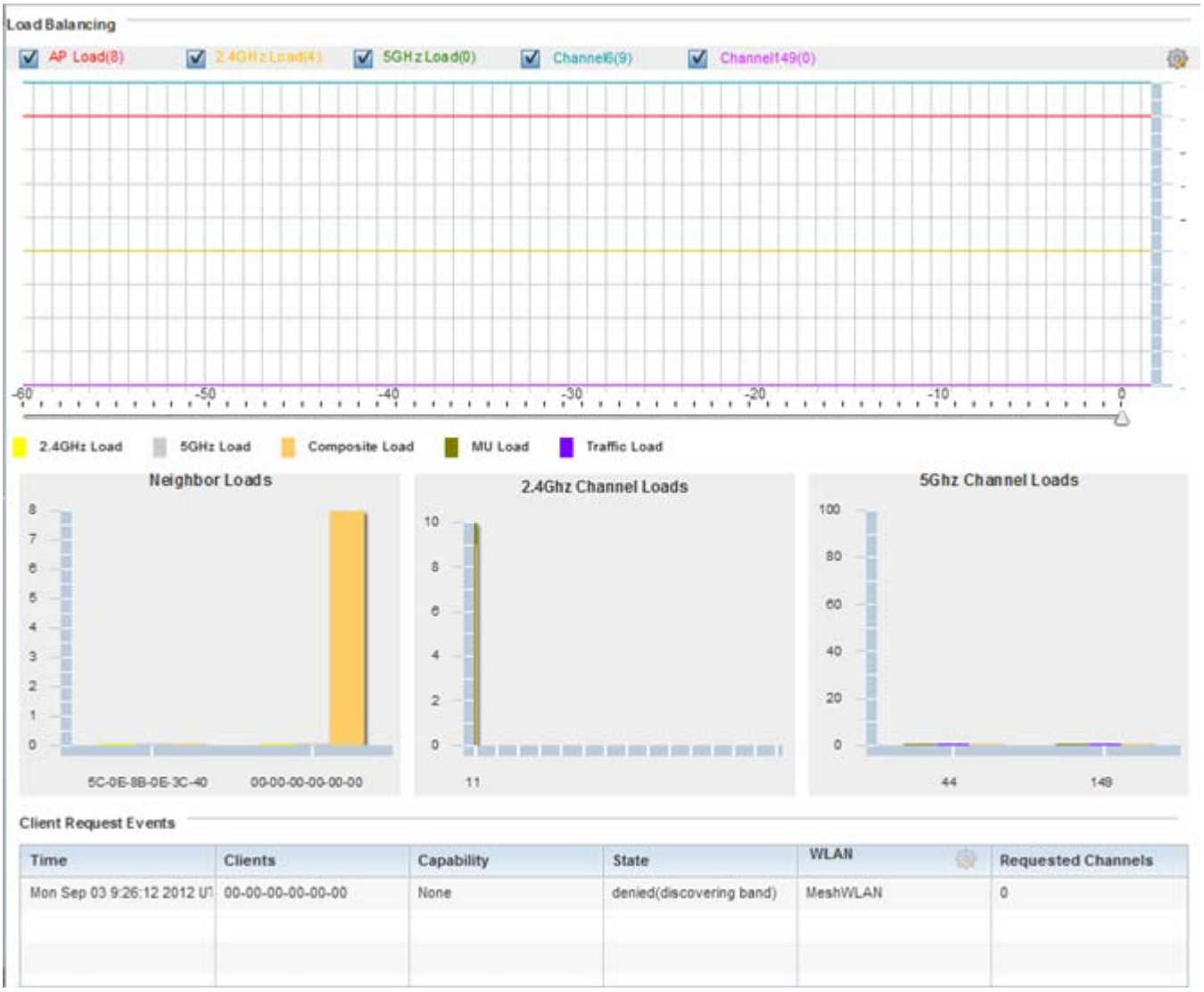


Figure 15-216 *Access Point - Load Balancing screen*

The **Load Balancing** screen displays the following:

Load Balancing	Select any of the options to display any or all of the following information in the graph below: *AP Load*, *2.4GHz Load*, *5GHz Load*, and *Channel*. The graph section displays the load percentages for each of the selected variables over a period of time, which can be altered using the slider below the upper graph.
Client Requests Events	The Client Request Events displays the Time, Client, Capability, State, WLAN and Requested Channels for all client request events on the Access Point. Remember, AP6532 and AP71xx models can support up to 256 clients per Access Point and AP6511 and AP6521 models support up to 128 clients per Access Point.

15.4.38 Environmental Sensors (AP8132 Models Only)

Access Point Statistics

A sensor module is a USB environmental sensor extension to an AP8132 model Access Point. It provides a variety of sensing mechanisms, allowing the monitoring and reporting of the radio coverage area. The output of the sensor's detection mechanisms are viewable using either the Environmental Sensor screen.

To view an AP8132 model Access Point's environmental statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, and select one of its connected Access Points.

3 Select **Environment**.

Figure 15-217 *Access Point - Environmental Sensor screen (Light tab)*

The **Light** tab displays by default, with additional *Temperature, Motion* and *Humidity* tabs available for unique sensor reporting. Each of these sensor measurements helps the administrator determine whether the immediate deployment area is occupied by changes in the Access Point's environment.

4 Refer to the **Light** table to assess the sensor's detected light intensity within the Access Point's immediate deployment area.

Light intensity is measured by the sensor in lumens. The table displays the **Current Light Intensity (lumens)** and a **20 Minute Average of Light Intensity (lumens)**. Compare these two items to determine whether the deployment location remains consistently lit, as an administrator can power off the Access Point's radios when no activity is detected in the immediate deployment area. For more information, see *Profile Environmental Sensor Configuration (AP8132 Only) on page 8-222*.

5 Refer to the **Light Intensity Trend Over Last Hour** graph to assess the fluctuation in lighting over the last hour. Use this graph to assess the deployment areas light intensity of particular hours of the day as needed to conjunction with the daily graph immediately below it.

6 Refer to the **Light Intensity Trend Over Last Day** graph to assess whether lighting is consistent across specific hours of the day. Use this information to help determine whether the Access Point can be upgraded or powered off during specific hours of the day.

7 Select the **Temperature** tab.

Figure 15-218 *Access Point - Environmental Sensor screen (Temperature tab)*

8 Refer to the **Temperature** table to assess the sensor's detected temperature within the Access Point's immediate deployment area.

Temperature is measured in centigrade. The table displays the **Current Temperature (centigrade)** and a **20 Minute Average Temperature (centigrade)**. Compare these two items to determine whether the deployment location remains consistently heated. For more information on enabling the sensor, see *Profile Environmental Sensor Configuration (AP8132 Only) on page 8-222*.

9 Refer to the **Temperature Trend Over Last Hour** graph to assess the fluctuation in ambient temperature over the last hour. Use this graph in combination with the Light and Motions graphs (in particular) to assess the deployment area's activity level.

10 Refer to the **Temperature Trend Over Last Day** graph to assess whether deployment area temperature is consistent across specific hours of the day. Use this information to help determine whether the Access Point can be upgraded or powered off during specific hours of the day.

11 Select the **Motion** tab.

Figure 15-219 *Access Point - Environmental Sensor screen (Motion tab)*

12 Refer to the **Motion** table to assess the sensor's detected movement within the Access Point's immediate deployment area.

Motion is measured in intervals. The table displays the **Current Motion (count per interval)** and a **20 Minute Average Motion (count per interval)**. Compare these two items to determine whether the Access Point's deployment location remains consistently occupied by client users. For more information on enabling the sensor, see *Profile Environmental Sensor Configuration (AP8132 Only) on page 8-222*.

13 Refer to the **Motion Trend Over Last Hour** graph to assess the fluctuation in user movement over the last hour. Use this graph in combination with the Light and Temperature graphs (in particular) to assess the deployment area's activity level.

14 Refer to the **Motion Trend Over Last Day** graph to assess whether deployment area user movement is consistent across specific hours of the day. Use this information to help determine whether the Access Point can be upgraded or powered off during specific hours of the day.

15 Select the **Humidity** tab.

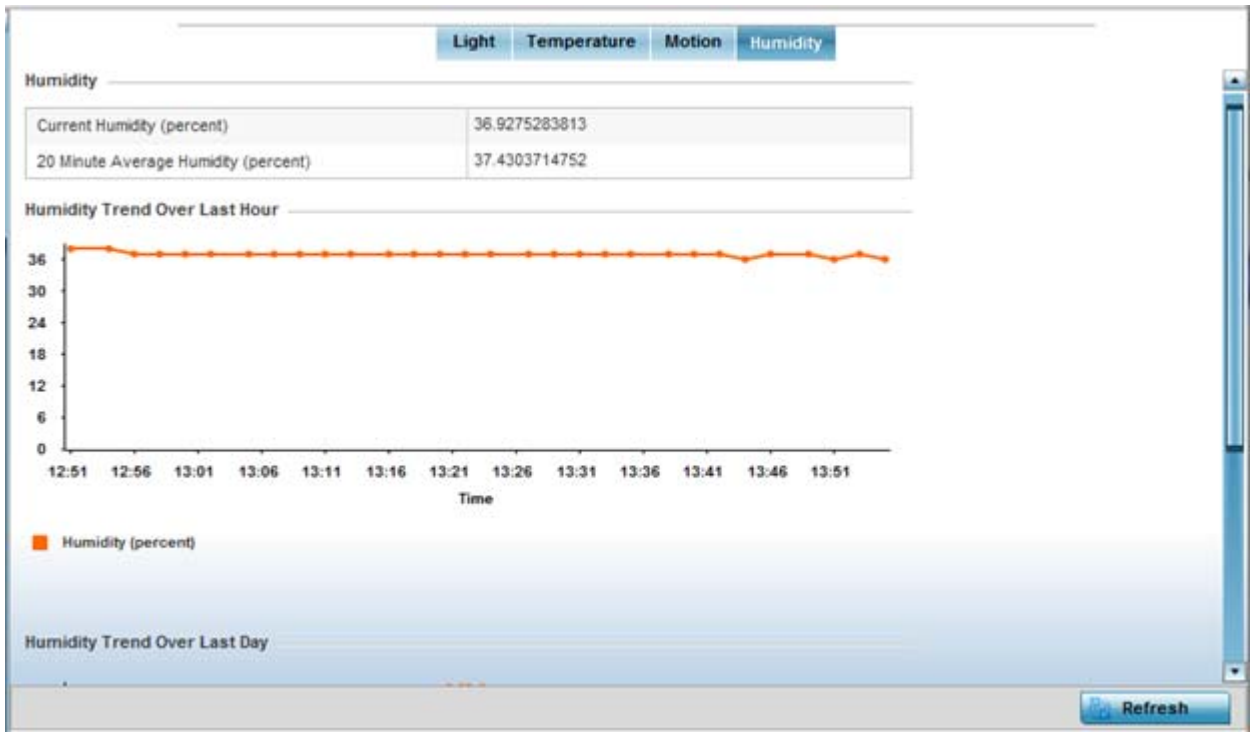


Figure 15-220 *Access Point - Environmental Sensor screen (Humidity tab)*

16 Refer to the **Humidity** table to assess the sensor's detected humidity fluctuations within the Access Point's immediate deployment area.

Humidity is measured in percentage. The table displays the **Current Humidity (percent)** and a **20 Minute Average Humidity (percent)**. Compare these two items to determine whether the deployment location remains consistently humid (often a by-product of temperature). For more information on enabling the sensor, see *Profile Environmental Sensor Configuration (AP8132 Only) on page 8-222*.

17 Refer to the **Humidity Trend Over Last Hour** graph to assess the fluctuation in humidity over the last hour. Use this graph in combination with the Temperature and Motions graphs (in particular) to assess the deployment area's activity levels.

18 Refer to the **Humidity Trend Over Last Day** graph to assess whether deployment area humidity is consistent across specific hours of the day. Use this information to help determine whether the Access Point can be upgraded or powered off during specific hours of the day.

15.5 Wireless Client Statistics

- *Statistics*

The wireless client statistics display read-only statistics for a client selected from within its connected Access Point and controller or service platform directory. It provides an overview of the health of wireless clients in the controller or service platform managed network. Use this information to assess if configuration changes are required to improve client performance.

Wireless clients statistics can be assessed using the following criteria:

- *Health*

- *Details*
- *Traffic*
- *WMM TSPEC*
- *Association History*
- *Graph*

15.5.1 Health

Wireless Client Statistics

The *Health* screen displays information on the overall performance of a selected wireless client.

To view the health of a wireless client:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, an Access Point, then a connected client.

3 Select **Health**.

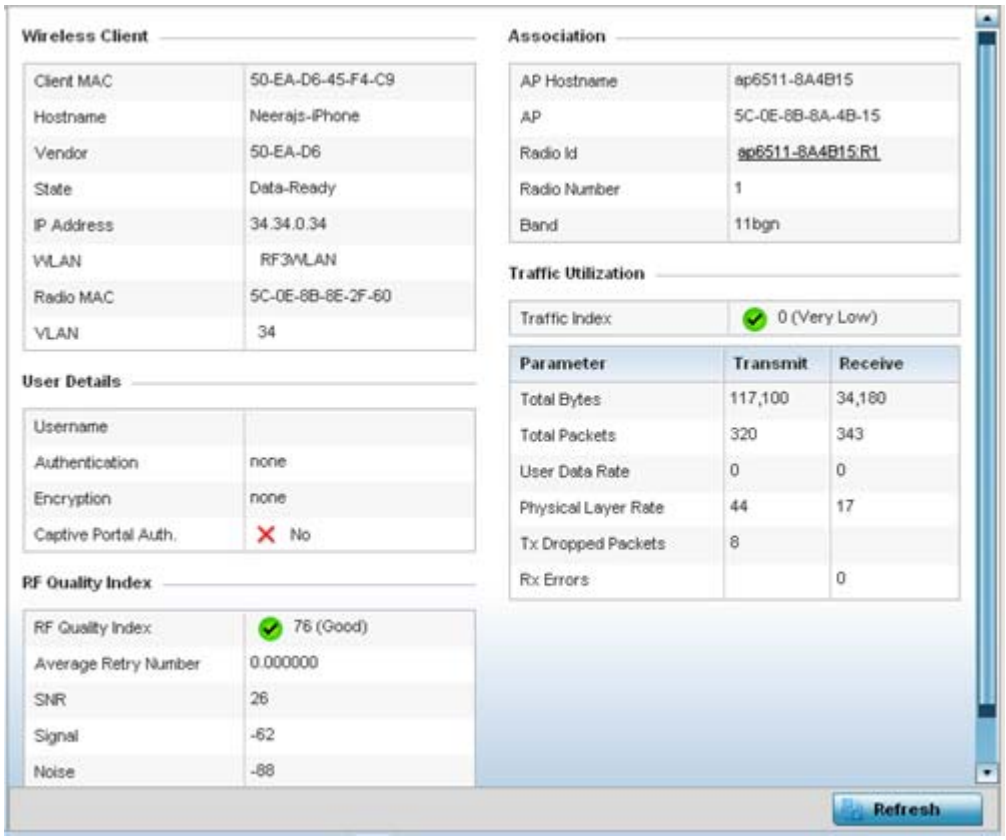


Figure 15-221 *Wireless Client - Health screen*

The **Wireless Client** field displays the following:

Client MAC	Displays the factory encoded MAC address of the selected wireless client.
Hostname	Lists the hostname assigned to the client when initially managed by the controller, service platform or Access Point.
Vendor	Displays the vendor name (manufacturer) of the wireless client.

State	Displays the current operational state of the wireless client. The client's state can be *idle*, *authenticated*, *roaming*, *associated* or *blacklisted*.
IP Address	Displays the IP address the selected wireless client is currently utilizing as a network identifier.
WLAN	Displays the client's connected Access Point WLAN membership. This is the WLAN whose QoS settings should account for the clients's radio traffic objective.
Radio MAC	Displays the Access Point radio MAC address the wireless client is connected to on the network.
VLAN	Displays the VLAN ID the Access Point has defined for use as a virtual interface with the client.

The **User Details** field displays the following:

Username	Displays the unique name of the administrator or operator managing the client's connected Access Point, controller or service platform.
Authentication	Lists the authentication scheme applied to the client for interoperation with the Access Point.
Encryption	Lists the encryption scheme applied to the client for interoperation with the Access Point.
Captive Portal Auth.	Displays whether captive portal authentication is enabled for the client as a guest access medium to the controller or service platform managed network.

The **RF Quality Index** field displays the following:

RF Quality Index	Displays information on the RF quality for the selected wireless client. The RF quality index is the overall effectiveness of the RF environment as a percentage of the connect rate in both directions, as well as the retry and error rate. RF quality index can be interpreted as: *0 – 20* (Very poor quality) *20 – 40* (Poor quality) *40 – 60* (Average quality) *60 – 100* (Good quality)
Average Retry Number	Displays the average number of retries per packet. A high number indicates possible network or hardware problems.
SNR	Displays the *signal to noise* (SNR) ratio of the connected wireless client.
Signal	Displays the power of the radio signals in - dBm.
Noise	Displays the disturbing influences on the signal by interference of signals in - dBm.
Error Rate	Displays the number of received bit rates altered due to noise, interference and distortion. It's a unitless performance measure.

The **Association** field displays the following:

AP Hostname	Lists the administrator assigned device name of the client's connected Access Point.

AP	Displays the MAC address of the client's connected Access Point.
Radio	Lists the target Access Point that houses the radio. Select the Access Point to view performance information in greater detail.
Radio ID	Lists the hardware encoded MAC address the radio uses as a hardware identifier that further distinguishes the radio from others within the same device.
Radio Number	Displays the Access Point's radio number (either 1, 2 or 3) to which the selected client is associated.
Radio Type	Displays the radio type. The radio can be 802.11b, 802.11bg, 802.11bgn, 802.11a or 802.11an.

4 The **Traffic Utilization** field displays statistics on the traffic generated and received by the selected client. This area displays the traffic index, which measures how efficiently the traffic medium is utilized. It's defined as the percentage of current throughput relative to the maximum possible throughput.

Traffic indices are:

- *0 – 20* (Very low utilization)
- *20 – 40* (Low utilization)
- *40 – 60* (Moderate utilization)
- *60 and above* (High utilization)

The Traffic Utilization table displays the following:

Total Bytes	Displays the total bytes processed by the Access Point's connected wireless client.
Total Packets	Displays the total number of packets processed by the wireless client.
User Data Rate	Displays the average user data rate in both directions.
Physical Layer Rate	Displays the average packet rate at the physical layer in both directions.
Tx Dropped Packets	Displays the number of packets dropped during transmission.
Rx Errors	Displays the number of errors encountered during data transmission. The higher the error rate, the less reliable the connection or data transfer between the client and connected Access Point.

5 Select the **Refresh** button to update the screen's statistics counters to their latest values.

15.5.2 Details

Wireless Client Statistics

The *Details* screen provides granular performance information for a selected wireless client.

To view the details screen of a connected wireless client:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, an Access Point, then a connected client.

3 Select **Details**.

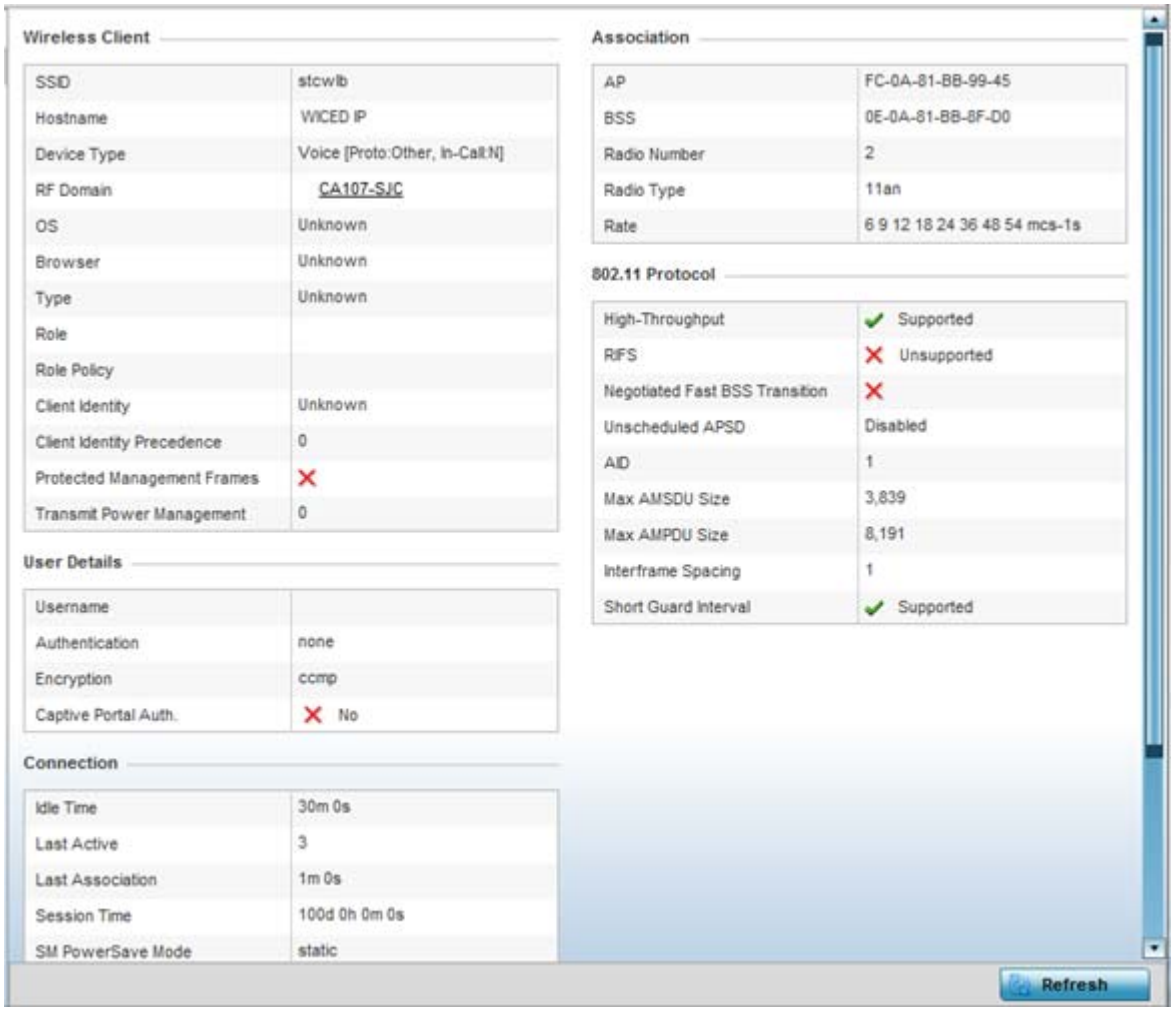


Figure 15-222 *Wireless Client - Details screen*

The **Wireless Client** field displays the following:

SSID	Displays the client's *Service Set ID* (SSID).
Hostname	Lists the hostname assigned to the client when initially managed by the controller, service platform or Access Point managed network.
Device Type	Displays the client device type providing the details to the operating system.
RF Domain	Displays the RF Domain to which the connected client is a member via its connected Access Point, controller or service platform. The RF Domain displays as a link that can be selected to display configuration and network address information in greater detail.
OS	Lists the client's operating system (Android etc.).
Browser	Displays the browser type used by the client to facilitate its wireless connection.
Type	Lists the client manufacturer (or vendor).
Role	Lists the client's defined role in the controller, service platform or Access Point managed network.

Role Policy	Lists the user role set for the client as it became a controller, service platform or Access Point managed device.
Client Identity	Displays the unique vendor identity of the listed device as it appears to its adopting controller or service platform.
Client Identity Precedence	Lists the numeric precedence this client uses in establishing its identity amongst its peers.
Protected Management Frames	A green checkmark defines management frames as protected between this client and its associated Access Point radio. A red X states that management frames are disabled for the client and its connected radio.
Transmit Power Management	Lists the number power management frames exchanged between this client and its connected Access Point radio. Lists zero when disabled.

The **User Details** field displays the following:

Username	Displays the unique name of the administrator or operator managing the client's connected Access Point.
Authentication	Lists the authentication scheme applied to the client for interoperation with its connected Access Point radio.
Encryption	Lists the encryption scheme applied to the client for interoperation with its connected Access Point radio.
Captive Portal Auth.	Displays whether captive portal authentication is enabled. When enabled, a restrictive set of access permissions may be in effect.

The **Connection** field displays the following:

Idle Time	Displays the time for which the wireless client remained idle.
Last Active	Displays the time in seconds the wireless client was last interoperating with its connected Access Point.
Last Association	Displays the duration the wireless client was in association with its connected Access Point.
Session Time	Displays the duration for which a session can be maintained by the wireless client without it being dis-associated from the Access Point.
SM Power Save Mode	Displays whether this feature is enabled on the wireless client. The *spatial multiplexing* (SM) power save mode allows an 802.11n client to power down all but one of its radios. This power save mode has two sub modes of operation: *static operation* and *dynamic operation*.
Power Save Mode	Displays whether this feature is enabled or not. To prolong battery life, the 802.11 standard defines an optional Power Save Mode, which is available on most 80211 clients. End users can simply turn it on or off via the card driver or configuration tool. With power save off, the 802.11 network card is generally in receive mode listening for packets and occasionally in transmit mode when sending packets. These modes require the 802.11 NIC to keep most circuits powered-up and ready for operation.
WMM Support	Displays whether WMM is enabled or not in order to provide data packet type prioritization between the Access Point and connected client.
40 MHz Capable	Displays whether the wireless client has 802.11n channels operating at 40 MHz.

Max Physical Rate	Displays the maximum data rate at the physical layer.
Max User Rate	Displays the maximum permitted user data rate.
MC2UC Streams	Lists the number or multicast to unicast data streams detected.

The **Association** field displays the following:

AP	Displays the MAC address of the client's connected Access Point.
BSS	Displays the *Basic Service Set* (BSS) the Access Point belongs to. A BSS is a set of stations that can communicate with one another.
Radio Number	Displays the Access Point radio the wireless client is connected to.
Radio Type	Displays the radio type. The radio can be 802.11b, 802.11bg, 802.11bgn, 802.11a or 802.11an.
Rate	Displays the permitted data rate for Access Point and client interoperation.

The **802.11 Protocol** field displays the following:

High-Throughput	Displays whether high throughput is supported. High throughput is a measure of the successful packet delivery over a communication channel.
RIFS	Displays whether this feature is supported. RIFS is a required 802.11n feature that improves performance by reducing the amount of dead time between OFDM transmissions.
Negotiated Fast BSS Transition	Lists whether Fast BSS transition is negotiated. This indicates support for a seamless fast and secure client handoff between two Access Points, controllers or service platforms.
Unscheduled APSD	Displays whether APSD is supported. APSD defines an unscheduled service period, which is a contiguous period of time during which the Access Point is expected to be awake.
AID	Displays the *Association ID* (AID) established by an AP. 802.11 association enables the Access Point to allocate resources and synchronize with a client. A client begins the association process by sending an association request to an Access Point. This association request is sent as a frame. This frame carries information about the client and the SSID of the network it wishes to associate. After receiving the request, the Access Point considers associating with the client, and reserves memory space for establishing an AID for the client.
Max AMSDU Size	Displays the maximum size of AMSDU. AMSDU is a set of Ethernet frames to the same destination that are wrapped in a 802.11n frame. This values is the maximum AMSDU frame size in bytes.
Max AMPDU Size	Displays the maximum size of AMPDU. AMPDU is a set of Ethernet frames to the same destination that are wrapped in an 802.11n MAC header. AMPDUs are used in a very noisy environment to provide reliable packet transmission. This value is the maximum AMPDU size in bytes.
Interframe Spacing	Displays the interval between two consecutive Ethernet frames.

Short Guard Interval	Displays the guard interval in micro seconds. Guard intervals prevent interference between data transmissions. The guard interval is the space between characters being transmitted. The guard interval eliminates *inter-symbol interference* (ISI). ISI occurs when echoes or reflections from one character interfere with another character. Adding time between transmissions allows echo's and reflections to settle before the next character is transmitted. A shorter guard interval results in shorter character times which reduces overhead and increases data rates by up to 10%.

4 Select the **Refresh** button to update the screen's statistics counters to their latest values.

15.5.3 Traffic

Wireless Client Statistics

The traffic screen provides an overview of client traffic utilization in both the transmit and receive directions. This screen also displays a RF quality index.

To view the traffic statistics of a wireless clients:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, an Access Point, then a connected client.

3 Select **Traffic**.

Figure 15-223 *Wireless Client - Traffic screen*

Traffic Utilization statistics employ an index, which measures how efficiently the traffic medium is used. It's defined as the percentage of current throughput relative to the maximum possible throughput.

Traffic indices are:

- 0 – 20 (Very low utilization)
- 20 – 40 (Low utilization)
- 40 – 60 (Moderate utilization)
- 60 and above (High utilization)

This screen also provides the following:

Total Bytes	Displays the total bytes processed (in both directions) by the Access Point's connected client.
Total Packets	Displays the total number of data packets processed (in both directions) by the Access Point's connected wireless client.
User Data Rate	Displays the average user data rate.
Packets per Second	Displays the packets processed per second.
Physical Layer Rate	Displays the data rate at the physical layer level.
Bcast/Mcast Packets	Displays the total number of broadcast/multicast packets processed by the client.
Management Packets	Displays the number of management (overhead) packets processed by the client.
Tx Dropped Packets	Displays the client's number of dropped packets while transmitting to its connected Access Point.
Tx Retries	Displays the total number of client transmit retries with its connected Access Point.
Rx Errors	Displays the errors encountered by the client during data transmission. The higher the error rate, the less reliable the connection or data transfer between client and connected Access Point.
Rx Actions	Displays the number of receive actions during data transmission with the client's connected Access Point.
Rx Probes	Displays the number of probes sent. A probe is a program or other device inserted at a key juncture in a for network for the purpose of monitoring or collecting data about network activity.
Rx Power Save Poll	Displays the power save using the *Power Save Poll* (PSP) mode. Power Save Poll is a protocol, which helps to reduce the amount of time a radio needs to powered. PSP allows the WiFi adapter to notify the Access Point when the radio is powered down. The Access Point holds any network packet to be sent to this radio.

The **RF Quality Index** area displays the following information:

RF Quality Index	Displays information on the RF quality of the selected wireless client. The RF quality index is the overall effectiveness of the RF environment as a percentage of the connect rate in both directions as well as the retry rate and the error rate. The RF quality index value can be interpreted as: *0 – 20* (Very low utilization) *20 – 40* (Low utilization) *40 – 60* (Moderate utilization) *60 and above* (High utilization)
Retry Rate	Displays the average number of retries per packet. A high number indicates possible network or hardware problems.

SNR (dBm)	Displays the connected client's *signal to noise ratio* (SNR). A high SNR could warrant a different Access Point connection to improve performance.
Signa (dBm)	Displays the power of the radio signals in - dBm.
Noise (dBm)	Displays the disturbing influences on the signal in - dBm.
Error Rate (ppm)	Displays the number of received bit rates altered due to noise, interference and distortion. It's a unitless performance measure.
MOS Score	Displays average voice call quality using the *Mean Opinion Score* (MOS) call quality scale. The MOS scale rates call quality on a scale of 1-5, with higher scores being better. If the MOS score is lower than 3.5, it's likely users will not be satisfied with the voice quality of their call.
R-Value	R-value is a number or score used to quantitatively express the quality of speech in communications systems. This is used in digital networks that carry *Voice over IP* (VoIP) traffic. The R-value can range from 1 (worst) to 100 (best) and is based on the percentage of users who are satisfied with the quality of a test voice signal after it has passed through a network from a source (transmitter) to a destination (receiver). The R-value scoring method accurately portrays the effects of packet loss and delays in digital networks carrying voice signals.

4 Select the **Refresh** button to update the screen's statistics counters to their latest values.

15.5.4 WMM TSPEC

Wireless Client Statistics

The 802.11e *Traffic Specification* (TSPEC) provides a set of parameters that define the characteristics of the traffic stream, (operating requirement and scheduling etc.). The sender TSPEC specifies parameters available for packet flows. Both sender and the receiver use TSPEC.

The TSPEC screen provides information about TSPEC counts and TSPEC types utilized by the selected wireless client.

To view the TSPEC statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, an Access Point, then a connected client.

3 Select **WMM TSPEC**.

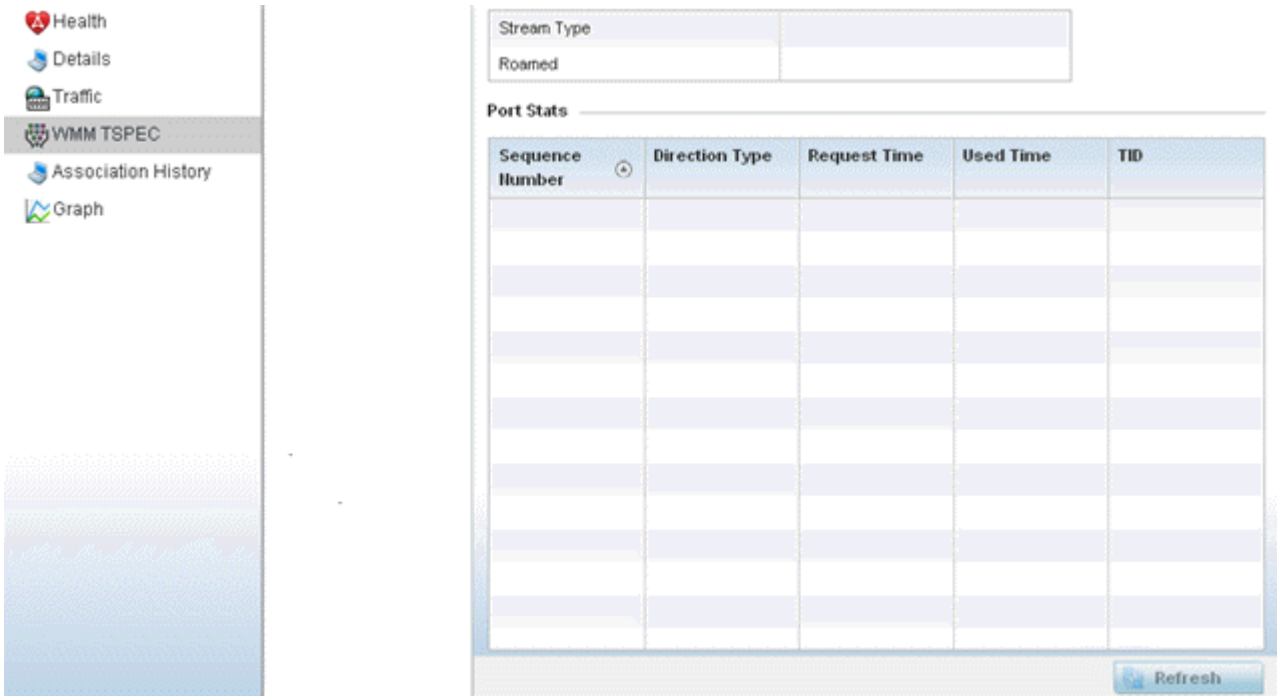


Figure 15-224 *Wireless Client - WMM TSPEC screen*

The top portion of the screen displays the TSPEC stream type and whether the client has roamed.

The Ports Stats field displays the following:

Sequence Number	Lists a sequence number that's unique to this WMM TSPEC *uplink* or *downlink* data stream.
Direction Type	Displays whether the WMM TSPEC data stream is in the *uplink* or *downlink* direction.
Request Time	Lists each sequence number's request time for WMM TSPEC traffic in the specified direction. This is time allotted for a request before packets are actually sent.
Used Time	Displays the time the client used TSPEC. The client sends a *delete traffic stream* (DELTS) message when it has finished communicating.
TID	Displays the parameter for defining the traffic stream. TID identifies data packets as belonging to a unique traffic stream.

4 Periodically select **Refresh** to update the screen to its latest values.

15.5.5 Association History

Wireless Client Statistics

Refer to the **Association History** screen to review this client's Access Point connections. Hardware device identification, operating channel and GHz band data is listed for each Access Point. The Association History can help determine whether the client has connected to its target Access Point and maintained its connection, or has roamed and been supported by unplanned Access Points in the controller or service platform managed network.

To view a selected client's association history:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, an Access Point, then a connected client.

3 Select **Association History**.

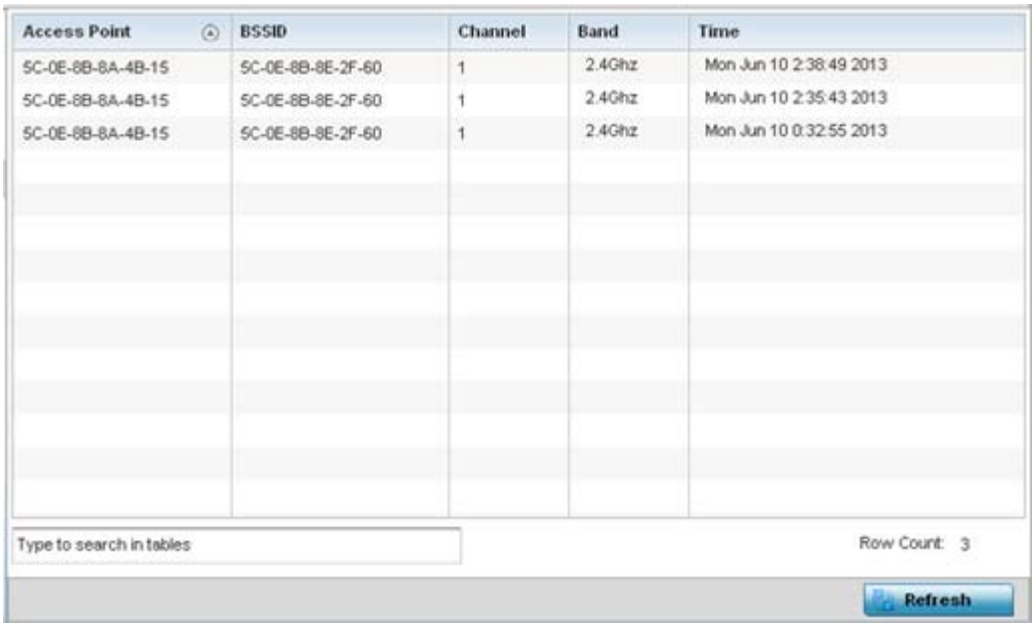


Figure 15-225 *Wireless Client - Association History screen*

Refer to the following to discern this client's Access Point association history:

Access Point	Lists the Access Point MAC address this client has connected to, and is being managed by.
BSSID	Displays the BSSID of each previously connected Access Point.
Channel	Lists the channel shared by both the Access Point and client for interoperation, and to avoid congestion with adjacent channel traffic.
Band	Lists the 2.4 or 5GHz radio band this clients and its connect Access Point are using for transmit and receive operations.
Time	Lists the historical connection time between each listed Access Point and this client.

4 Select **Refresh** to update the screen to its latest values.

15.5.6 Graph

Wireless Client Statistics

Use the client **Graph** to assess a connected client's radio performance and diagnose performance issues that may be negatively impact performance. Up to three selected performance variables can be charted at one time. The graph uses a Y-axis and a X-axis to associate selected parameters with their performance measure.

To view a graph of this client's statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **System** from the navigation pane (on the left-hand side of the screen). Expand a RF Domain, select a controller or service platform, an Access Point then a connected client.

3 Select **Graph**.

4 Use the **Parameters** drop down menu to define from 1- 3 variables assessing client signal noise, transmit or receive values.

5 Use the **Polling Interval** drop-down menu to define the interval the chart is updated. Options include *30 seconds*, *1 minute*, *5 minutes, 20 minutes* or *1 hour*. 30 seconds is the default value.

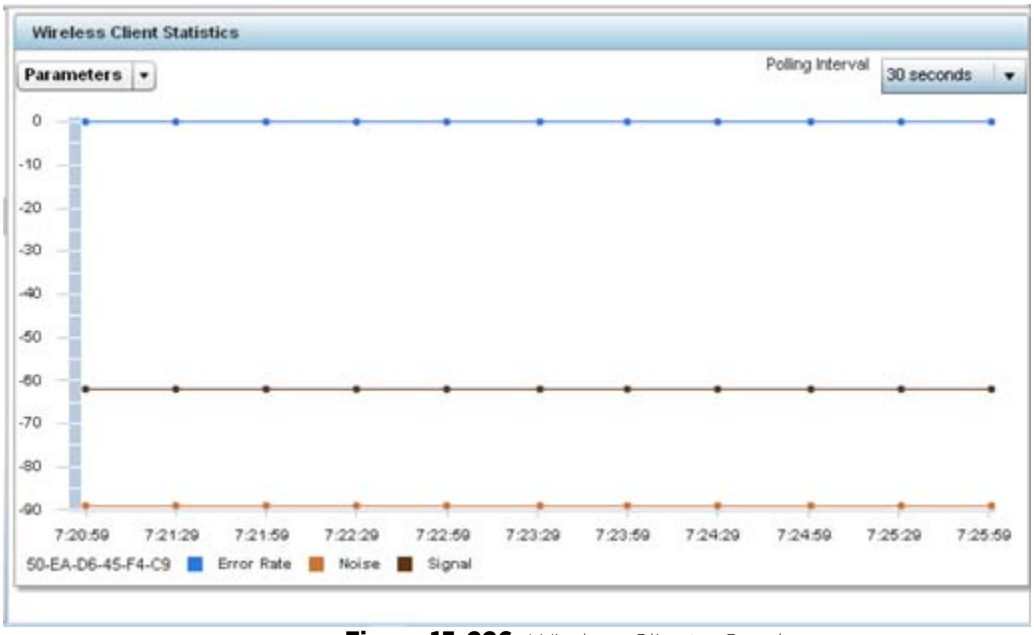


Figure 15-226 *Wireless Client - Graph*

6 Select an available point in the graph to list the selected performance parameter, and display that parameter's value and a time stamp of when it occurred.

15.6 Guest Access Statistics

Statistics

Guest client statistics are uniquely available for wireless clients requesting the required pass code, authentication and access into the WiNG managed guest client network

Guest Access statistics can be assessed for the following:

- *Guest Access Cumulative Statistics*
- *Social Media Statistics*
- *Reports*
- *Notifications*
- *Guest Access Database*

15.6.1 Guest Access Cumulative Statistics

Guest Access Statistics

The *Statistics* screen displays information on the WiNG managed guest client network. Its includes browser utilization, new versus returning user trends, client user age, client operating system, device type proliferation and gender trending.

To view a cumulative set of client guest access statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **Guest Access** above the navigation pane (on the upper left-hand side of the screen, directly to the right of System).

3 Select **Statistics**.

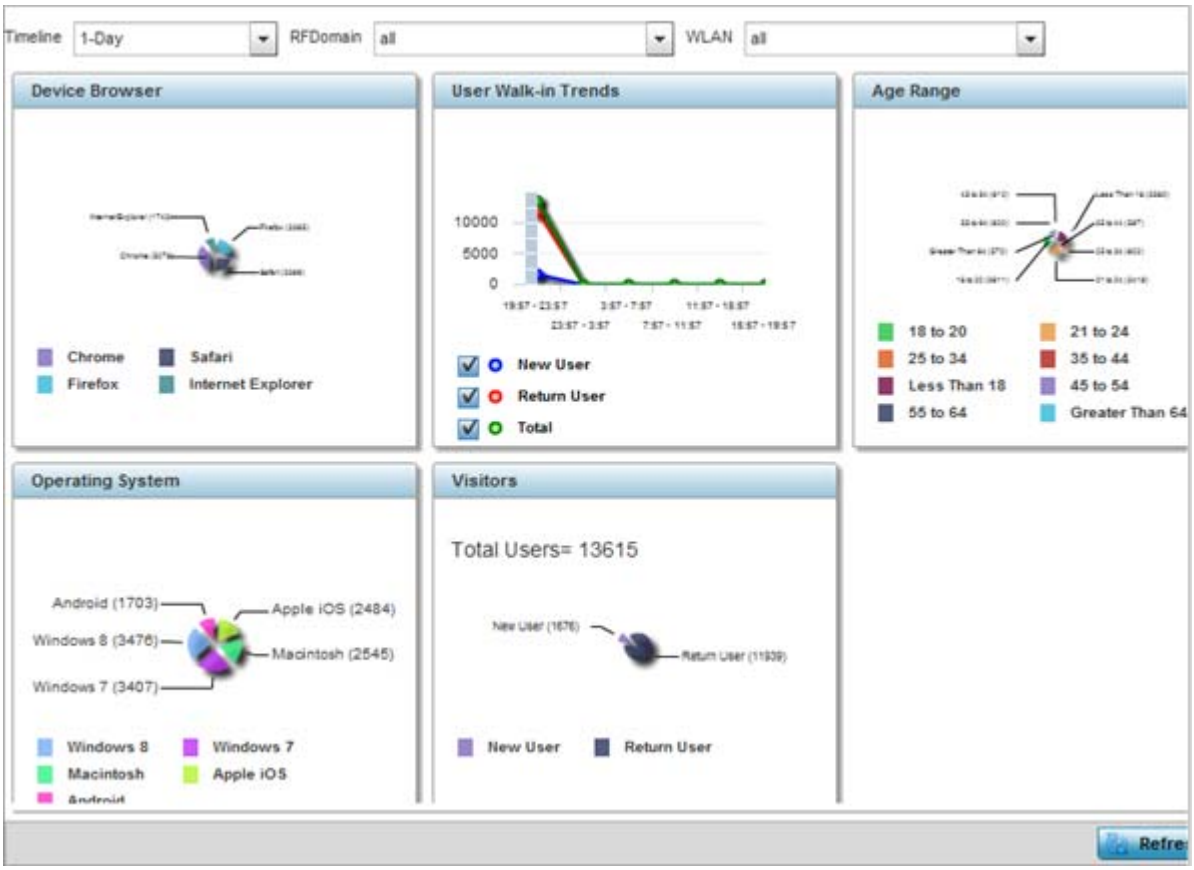


Figure 15-227 *Guest Access - Statistics screen*

4 Refer to the top of the screen to configure how the following trending periods and user filters are set for guest access statistics trending and reporting:

Timeline	Use the drop-down menu to specify whether statistics are gathered for *1-Day, 1-Month, 1-Week, 2-Hours, 30-Mins* or *5-Hours*. Timelines support the latest time period from present. For example, specifying 30-Mins displays statistics for the most recent 30 minutes trended.
RF Domain	Use the drop-down menu to select a single RF Domain from which to filter guest access statistics. Optionally select *All* to include data from each RF Domain supported.

WLAN	Use the drop down menu to filter guest access statistics to a specific WLAN. A single WLAN can belong to more then one RF Domain.

5 Refer to the following to assess guest client browser, operating system, age, gender and new versus returning status to assess whether guest client utilization is in line with WiNG guest access deployment objectives:

Device Browser	Displays guest user browser utilization in pie-chart format. Each client browser type (*Chrome, Firefox, Safari* and *Internet Explorer)* detected within the defined trending period displays uniquely in its own color for easy differentiation. The number of guest clients utilizing each browser also displays numerically.
User Walk-in Trends	Walk-in trending enables an administrator to filter new guest access clients versus return guest clients out of the total reported for the trending period and selected RF Domain and WLAN. New guest users (blue), return guests (red) or total guests can either be collectively displayed or individually displayed by selecting one, two or all three of the options.
Age Range	Displays guest user age differentiation in pie-chart format. Age ranges are uniquely color coded as *Less Than 18, 18 to 20, 21 to 24, 25 to 34, 35 to 44, 45 to 54, 55 to 64* and *Greater Than 64*. Each age group detected within the trending period displays uniquely in its own color for easy differentiation. Each age range also displays numerically. Periodically assess whether the age ranges meet expectations for guest client access within the WiNG managed guest network.
Operating System	Displays guest client operating system utilization in pie-chart format. Each client operating system type (*Android, Windows 7, Windows 8, Apple iOS* and *Macintosh*) displays uniquely in its own color for easy differentiation. The number of guest clients utilizing each operating system also displays numerically.
Visitors	Displays return guest clients versus new guest clients in pie-chart format. Both new and returning clients display uniquely in their own color for easy differentiation. Periodically assess whether the number of returning guest clients is line with the guest network's deployment objectives in respect to the RF Domain(s) and WLAN(s) selected for trending.
Customer Loyalty App	Graphically displays the number of guest clients with loyalty application presence enabled. Loyalty application detection occurs on the Access Point to which the client is associated, allowing a retail administrator to assess whether a captive portal client is using specific retail (loyalty) applications in their captive portal. This setting is enabled by default.
Devices	Displays guest client device type utilization in pie-chart format. Each client device type (*Windows PC, Macintosh, Apple iPad, Android Mobile* and *Motorola Droid*) displays uniquely in its own color for easy differentiation. The number of each device type detected also displays numerically to help assess their proliferation with WiNG managed guest network.
Gender	Displays guest client gender in pie-chart format. Detected male and female guest users display uniquely in their own color for easy differentiation. Guest clients whose gender is unspecified also displays to help assess the undetermined gender client count out of total. The number of male, female and unspecified guest clients also displays numerically.

6 Select the **Refresh** button to update the screen's statistics counters to their latest values.

15.6.2 Social Media Statistics

Guest Access Statistics

Device registration using social media login credentials requires user validation through the guest user's social media account. The guest user authenticates with an administrator configured social media server like Facebook or Google. Upon successful authentication, the guest user's social media profile data (collected from the social media server) is registered on the device.

To view guest access social media utilization for guest clients:

1 Select the **Statistics** menu from the Web UI.

2 Select **Guest Access** above the navigation pane (on the upper left-hand side of the screen, directly to the right of System).

3 Select **Social**.

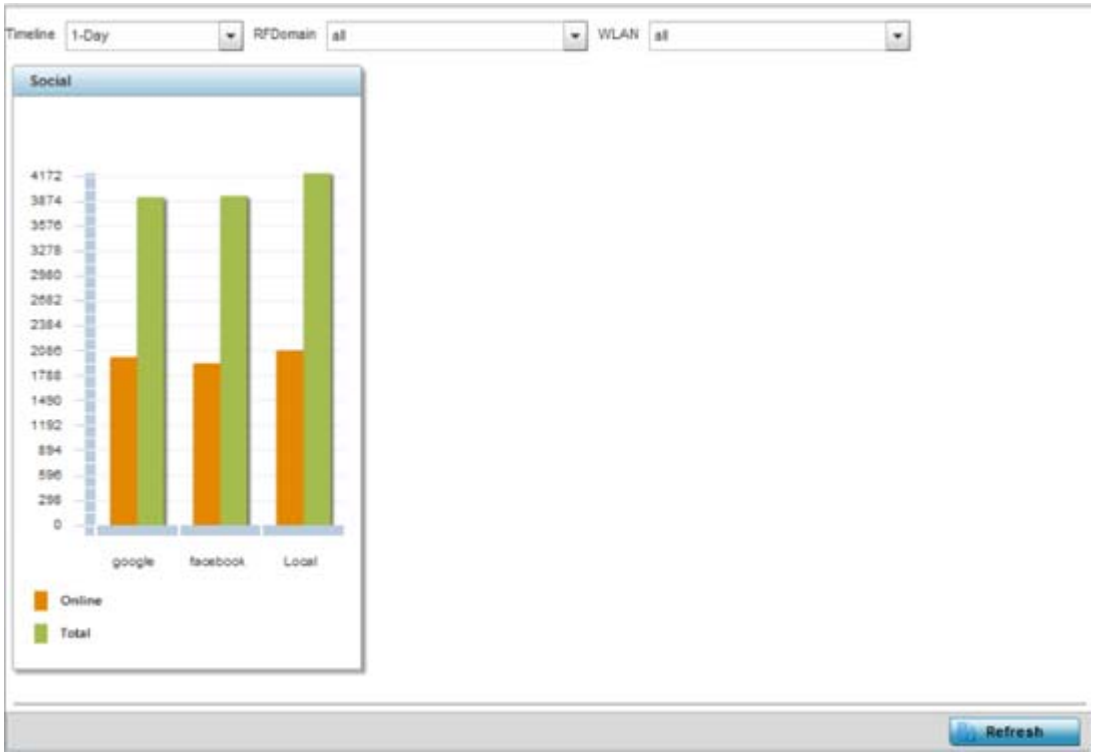


Figure 15-228 *Guest Access - Social screen*

4 Refer to the top of the screen to configure how the following trending periods and user filters are set for guest access social media trending:

Timeline	Use the drop-down menu to specify whether social media statistics are gathered for *1-Day, 1-Month, 1-Week, 2-Hours, 30-Mins* or *5-Hours*. Timelines support the latest time period from present. For example, specifying 30-Mins displays statistics for the most recent 30 minutes trended.

RF Domain	Use the drop-down menu to select a single RF Domain from which to filter social media guest access statistics. Optionally select *All* to include data from each RF Domain supported.
WLAN	Use the drop down menu to filter guest access social media statistics to a specific WLAN. A single WLAN can belong to more then one RF Domain.

The data displays in bar graph format, with the total number of social media authenticating clients listed in green, and those currently online displayed in orange for both Google and Facebook authenticating clients. Refer to the **Local** graph to assess those clients requiring captive portal authentication as a fallback mechanism for guest registration through social media authentication.

5 Periodically select **Refresh** to update the statistics counters to their latest values.

15.6.3 Reports

- *Guest Access Statistics*

Report queries can be filtered and run to obtain information on targeted guest clients within the WiNG guest network.

To generate customized guest client reports:

1 Select the **Statistics** menu from the Web UI.

2 Select **Guest Access** above the navigation pane (on the upper left-hand side of the screen, directly to the right of System).

3 Select **Reports**.

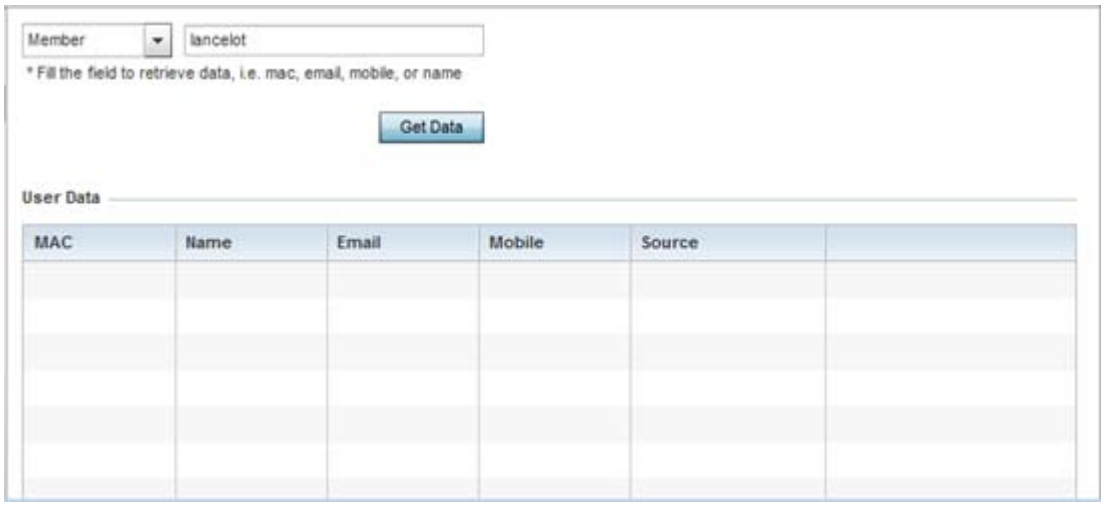


Figure 15-229 *Guest Access - Reports screen*

4 Select the drop-down menu at the top, left-hand, side of the screen to define whether the guest client's report data is fetched based on its *MAC, Name, Mobile, Email, Member* or *Time*. Once provided, enter an appropriate search string to generate a report for the target guest client. When completed with the report's search strings, select **Get Data**.

5 Refer to the **User Data** table to review the following report output:

MAC	Displays the factory encoded hardware MAC address assigned to this guest client at the factory by the manufacturer. This is the guest client's hardware identifier added to the guest user database. If the guest client requests access later, this MAC address is validated against the guest user database, and the client is allowed access to the WiNG managed guest network.
Name	Lists the name used for guest access authentication and pass code generation.
Email	Lists the E-Mail address used for guest access authentication and the receipt of the required passcode.
Mobile	Lists the guest client's registered mobile number used for guest access authentication requests and the receipt of the required passcode.
Source	Lists the source (Facebook, Google) whose username and password were used as the clients's social media authenticator.

15.6.4 Notifications

- *Guest Access Statistics*

For each registered guest user, a passcode is sent by E-mail, SMS or both. A guest management policy defines E-mail host and SMS gateway commands, along with credentials required for sending a passcode to guest client via E-mail and SMS Users can configure up to 32 different guest management policies. Each policy enables the user to configure the SMS gateway, SMS message body, E-mail SMTP server, E-mail subject contents and E-mail message body. There can be only one guest management policy active per device at any one time.

The *short message service* (SMS) is the text messaging service component of phone, E-Mail and mobile systems. SMS uses standardized communications protocols to allow fixed or mobile phone devices to exchange text messages.

To review guest client notification statistics:

1 Select the **Statistics** menu from the Web UI.

2 Select **Guest Access** above the navigation pane (on the upper left-hand side of the screen, directly to the right of System).

3 Select **Notification**.

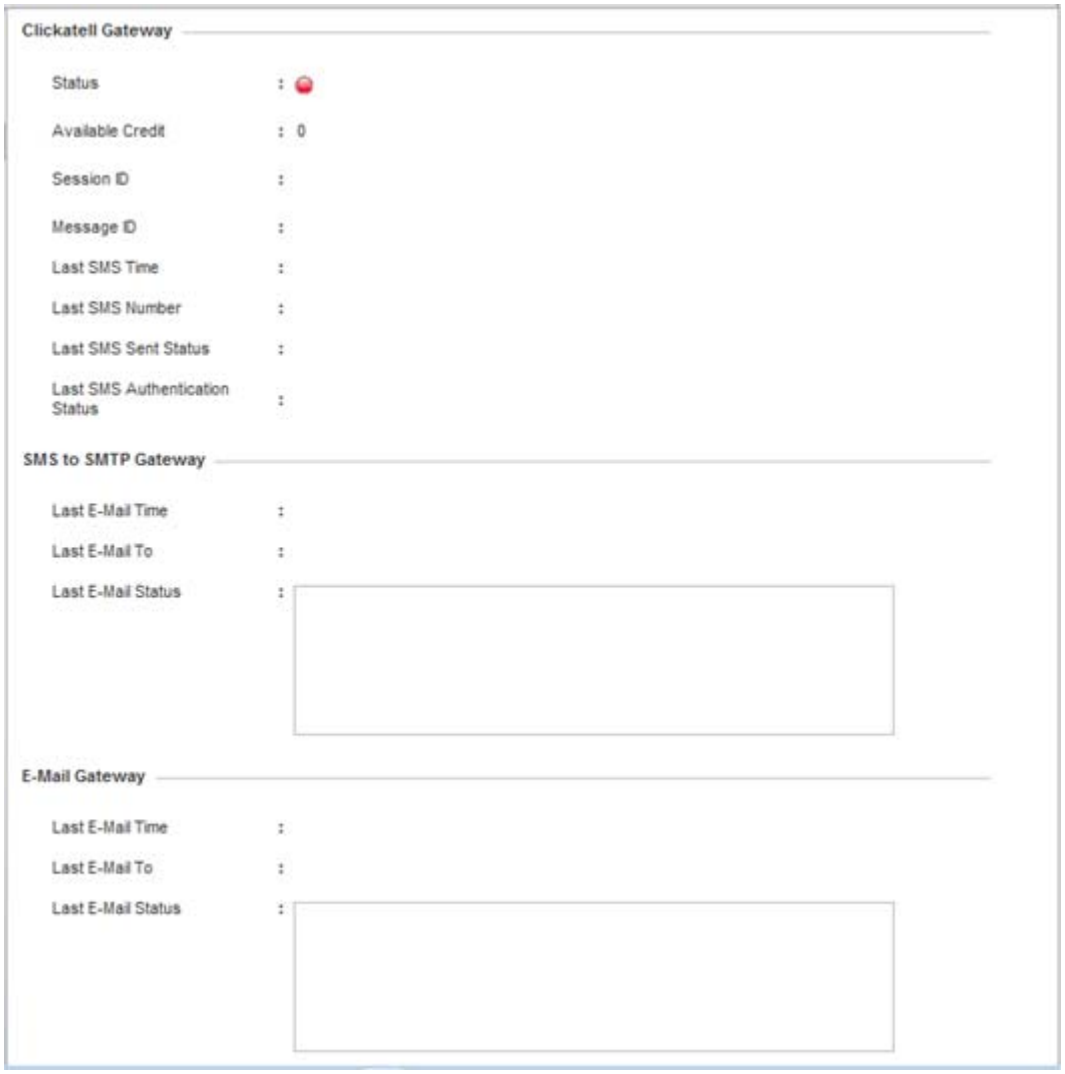


Figure 15-230 *Guest Access - Notification screen*

4 Review the following **Clickatell Gateway** information. By default, clickatell is the host SMS gateway server resource for guest access.

Status	Displays an icon as a visual indicator of the gateway status. Green defines the gateway as available. Red indicates the gateway is down and unavailable.
Session ID	Lists an event ID for the clickatell gateway session credential and passcode exchange.
Message ID	Lists the unique SMS message ID created for the successful message exchange with the clickatell host SMS gateway server.
Last SMS Time	Lists the timestamp appended to the sent time of the clickatell SMS gateway message.
Last SMS Number	Lists the numeric status code returned in response to a SMS gateway server guest access request.
Last SMS Sent Status	Lists the associated status strings returned in response to a SMS gateway server guest access request.

Last SMS Authentication Status	Lists the SMS authentication credential and validation message exchange status for the listed clieckatell gateway session ID.

5 Review the following **SMS to SMTP Gateway** information.

Last E-Mail Time	Displays the most recent E-Mailed passcode to a guest via SMS. SMS enables guest users to register with their E-Mail or mobile device ID as the primary key for authentication.
Last E-Mail To	Lists the recipient of the most recent SMS to SMTP server credential E-mail exchange containing the required passcode for the registered guest.
Last E-Mail Status	Lists the completion status of the most recent server SMS to SMTP gateway credential exchange containing the required passcode for the authenticating guest client.

6 Review the following **Email Gateway** information.

Last E-Mail Time	Displays the time of the most recent E-Mailed passcode to a guest access requesting client. Guest users can register with their E-mail credentials as the primary means of authentication.
Last E-Mail To	Lists the recipient of this session's server E-Mail credential exchange containing the required passcode for the authenticating guest client.
Last E-Mail Status	Lists the completion status of the most recent server E-Mail credential exchange containing the required passcode for the authenticating guest client.

15.6.5 Guest Access Database

Guest Access Statistics

Refer to the **Database** screen to periodically *import* or *export* guest access information to and from a WiNG managed device. The import or export of the guest access database is supported in JSON format only. Archiving guest access utilization data is a good way to assess periods of high and low utilization and better plan for client guest access consumption of controller or Access Point network resources.

To administrate the guest access database:

1 Select the **Statistics** menu from the Web UI.

2 Select **Guest Access** above the navigation pane (on the upper left-hand side of the screen, directly to the right of *System*).

3 Select **Database**.

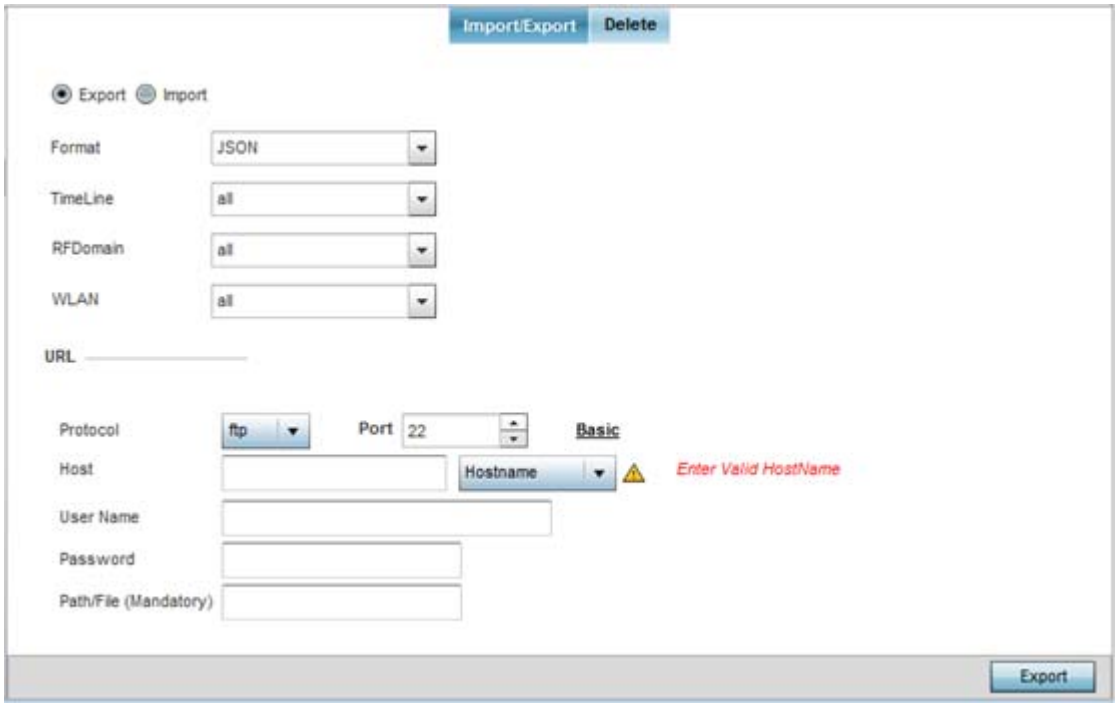


Figure 15-231 *Guest Access - Database Import/Export screen*

4 Select **Export** to archive guest access data (in JSON or CSV format) to a designated remote location, or **Import** to upload guest access utilization data back to the WiNG managed controller, service platform or Access Point.

5 If conducting an **Export** operation, provide the following to refine the data exported:

Format	Define whether the guest access data is exported in *JSON* or *CSV* format. *JavaScript Object Notation* (JSON) is an open standard format using text to export data objects consisting of attribute value pairs. A *comma-separated values* (CSV) file stores tabular data in plain text. Plain text means that the file is interpreted a sequence of characters, so that it is human-readable with a standard text editor. Each line of the file is a data record. Each record consists of one or more fields, separated by commas.
Timeline	Use the drop-down menu to specify whether guest access statistics are exported for the previous 1-Day, 1-Month, 1-Week, 2-Hours, 30-Mins or 5-Hours. Timelines support the latest time period from present. For example, specifying 30-Mins exports statistics trended over the most recent 30 minutes.
RF Domain	Use the drop-down menu to select a single RF Domain from which to filter social media guest access statistics. Optionally select *All* to include data from each RF Domain supported.
WLAN	Use the drop down menu to filter guest access social media statistics to a specific WLAN. A single WLAN can belong to more then one RF Domain.

6 When exporting or importing guest access data (regardless or format), provide the following **URL** data to accurately configure the remote host.

Format	Select the data transfer protocol used for exporting or importing guest access data. Available options include: *tftp* *ftp* *sftp*
Port	Use the spinner control to set the virtual port for the for the export or import operation.
Host	Provide a textual *hostname* or numeric IP address of the server used for guest access data transfer operations. Hostnames cannot include an underscore character. Select *IPv4 Address* to use an IPv4 formatted address as the host. Select *IPv6 Address* to use an IPv6 formatted address as the host. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
User Name	If using FTP or SFTP and the data transfer protocol, enter the *username* required by the remote FTP or SFTP server resource.
Password	If using FTP or SFTP and the data transfer protocol, enter the password required by the remote FTP or SFTP server resource.
Path/File	Specify the path to the server resource where guest access data is either exported or imported. Enter the complete relative path to the file on the server. If electing to use SFTP as the file transfer protocol, its recommended the path/file be set using the *command line interface* (CLI).

7 When the URL data is accurately entered, select the **Export** or **Import** button respectively to initiate the operation.

8 Optionally select the **Delete** tab to purge either all or part of the guest user database.

Figure 15-232 *Guest Access - Database Deletion screen*

9 Select **All** to remove the contents of the entire database. Select **Any** to invoke a drop-down menu where *Mac, Name, Mobile, Email* or a *WLAN* can be selected to refine the database removal to just a selected entity. Enter the name of the MAC address, user, mobile number or WLAN you wish to remove from the database, then select **Delete**.

15.7 Analytics Developer Interface

Statistics

The analytics developer interface is an additional tool available to administrators to review specific APIs in granular detail. The developer interface is available to elected NOC controllers or service platforms capable of provisioning all of its peer controllers, service platforms and adopted devices. NOC controllers include NX9000, NX9500, NX9510, NX7500, NX6500, NX6524 and RFS6000 models.

To access the developer interface:

1 Connect to controller using its existing IP address, but append **/stats** to the end of the IP address as follows:
http://<CONTROLLER_IP_ADDRESS>/stats or *https://<CONTROLLER_IP_ADDRESS>/stats*
The following login screen displays for the developer interface:

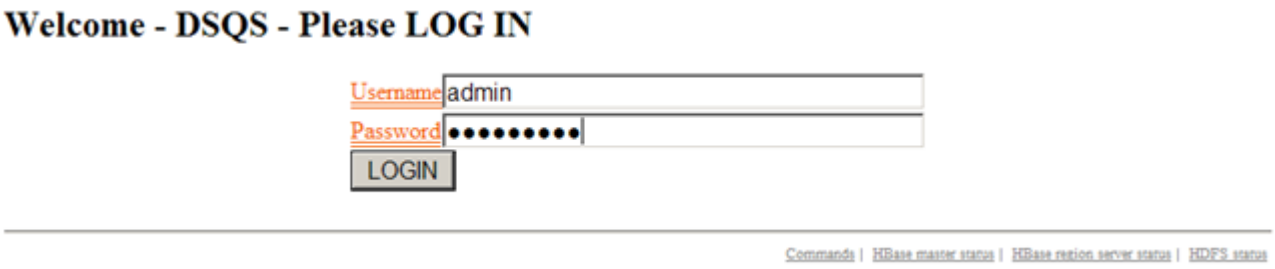


Figure 15-233 *Developer Interface - Login screen*

2 Provide the same **Username** and **Password** credentials you're currently utilizing for a typical controller login.
Once the login credentials are successfully entered, the following screen displays:

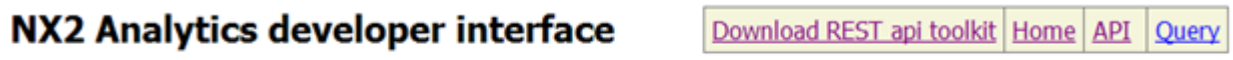


Figure 15-234 *Developer Interface - Main screen*

Refer to the following for more detailed descriptions of the functionality available to administrators using the analytics developer interface:

- *Download REST API Toolkit*
- *API Assessment*

15.7.1 Download REST API Toolkit

Analytics Developer Interface

Sample *Representational State Transfer* (REST) code can be downloaded from the toolkit. REST is a software design schema for Web application development.

To download sample REST API code:

1 Select **Download REST api toolkit** from the Web UI.

A **File Download** screen displays prompting for the desired location of the download or whether the files should be opened directly.

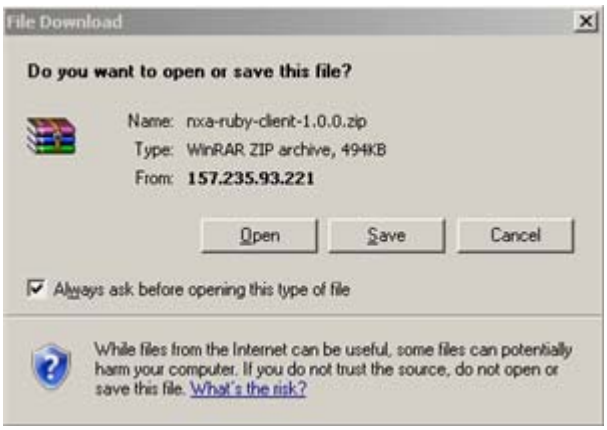


Figure 15-235 *Developer Interface -File Download screen*

2 Open the zip archive and review the **Readme** file to assess the contents and how they can be leveraged for API creation and modification.

Sample Ruby Client

A sample ruby client is provided as part of this package. The Ruby client can be used as a sample to pull statistics data from NXAnalytics. The response from NXAnalytics is in JSON format.

Contents

Readme.txt file.

Ruby script files:

NXAStatsClient.rb

NXARESTClient.rb

NXAResultsJSONParser.rb

NXALogin.rb

NXAException.rb

NXAConstants.rb

NXAConnectionParams.rb

Requirements To Run Sample Ruby Client

Ruby 2.0 or above. The sample has been tested with Ruby 2.0. To download Ruby use the following:

https://www.ruby-lang.org/en/downloads/or http://rubyinstaller.org/

Additional Ruby Gems needed to run the sample client are the following.

- ipaddress
- json
- rest-client

Please install the gems before running the sample client.

How To Run the Program From Command Line

```
ruby NXAStatsClient <IPAddress Of Controller>
        <Protocol[http|https]> <Port [8080|443]>
        <Stats_Type>[wlan | rfdomain | radio | client | captive-portal | client-assoc-disassoc]
        <lookback_duration_in_seconds [ 1 - 2592000]>
        <username> <password>
        <number_of_results_to_return [ 1 - 100]>
```

Sample:

```
ruby NXAStatsClient 172.20.33.45 https 443 rfdomain 600 admin admin 30
```

How To Run the Program From IDE

If you are using Eclipse or APTANA or any other IDE please do the following.

- Choose appropriate network proxy settings
- Configure IDE to choose appropriate Ruby interpreter
- Create a Ruby project
- Copy the Ruby files as part of package to the new Ruby project
- Define the arguments required for the main Ruby program
- Run the main Ruby program

15.7.2 API Assessment

Analytics Developer Interface

Refer to the toolkit's API functionality to review a collection of APIs for specific feature groups, including captive portals, client associations and disassociations, client stats, RF Domains.

To review the toolkit's built-in set of APIs:

1 Select **API** from the Web UI.

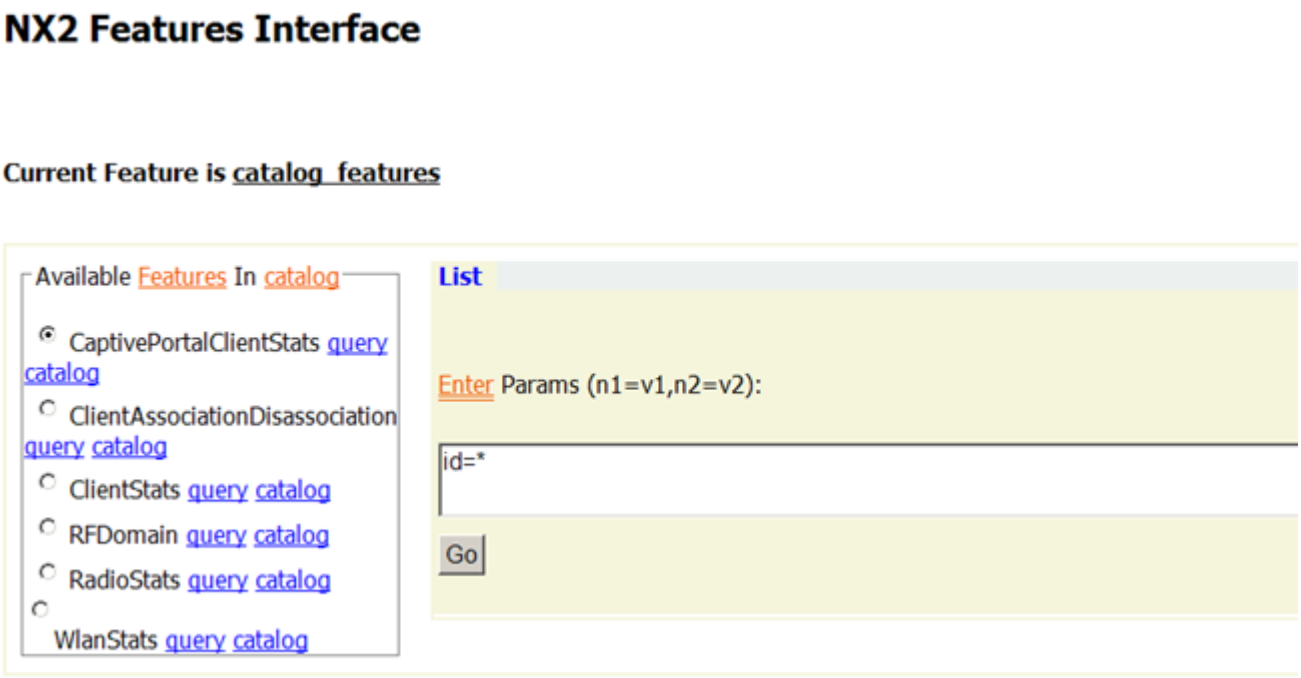


Figure 15-236 *Developer Interface - API*

2 Select an available feature from the catalog of features.

An administrator can either launch a **query** for a selected feature or select **catalog** to expose the schema for a selected feature.

3 Select **query** to display the **NX2 Raw Query Interface**.

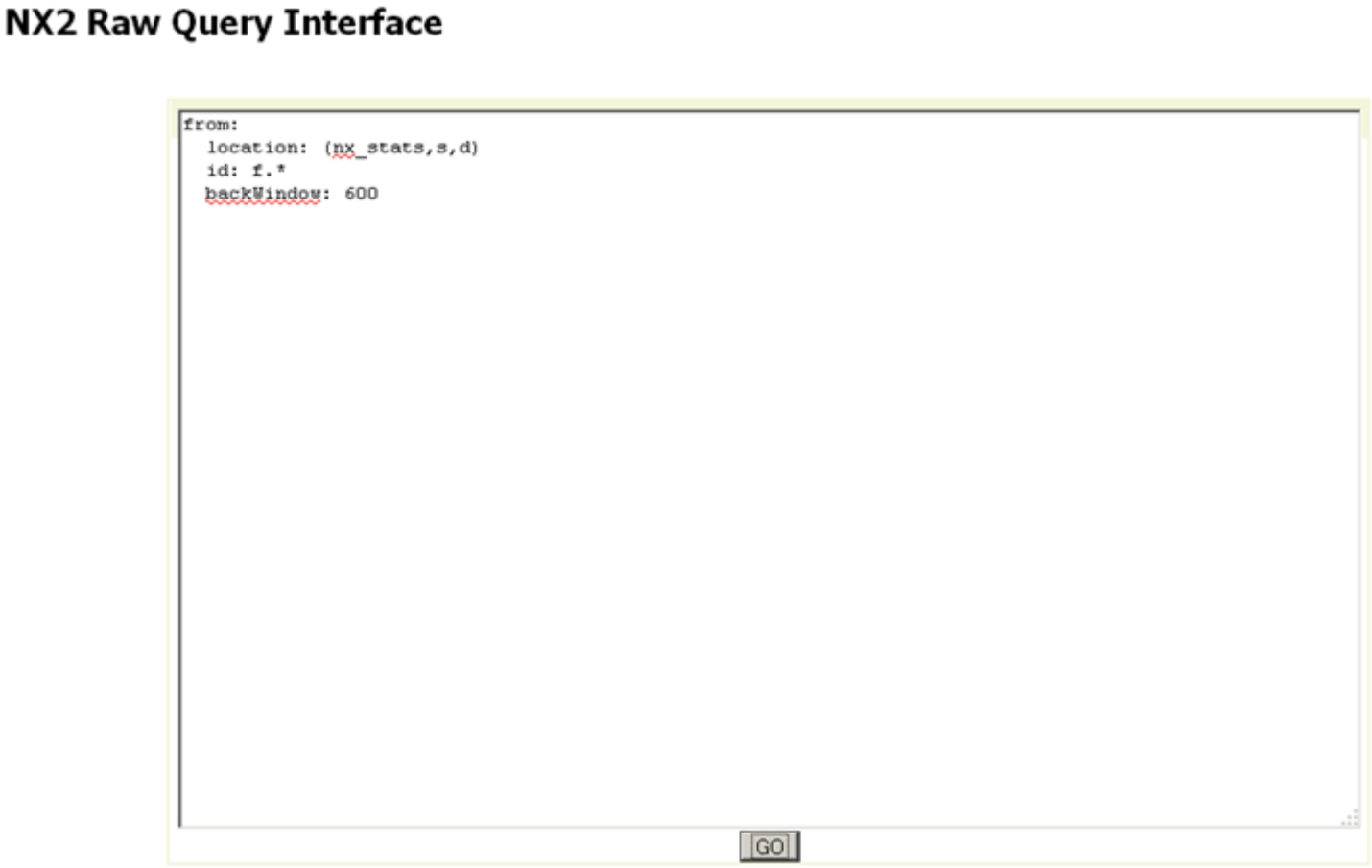


Figure 15-237 *Developer Interface - API Raw Query Interface*

4 Select **Go** to initiate the query for the selected item.

Figure 15-238 *Developer Interface - API Raw Query Results*

The results of the query display the values currently set for the selected feature. This information cannot be manipulated as a configurable API attribute, though this information can be utilized as criteria for API attribute creation.

5 From the NX2 Features Interface, select a feature from those available and select **catalog**.

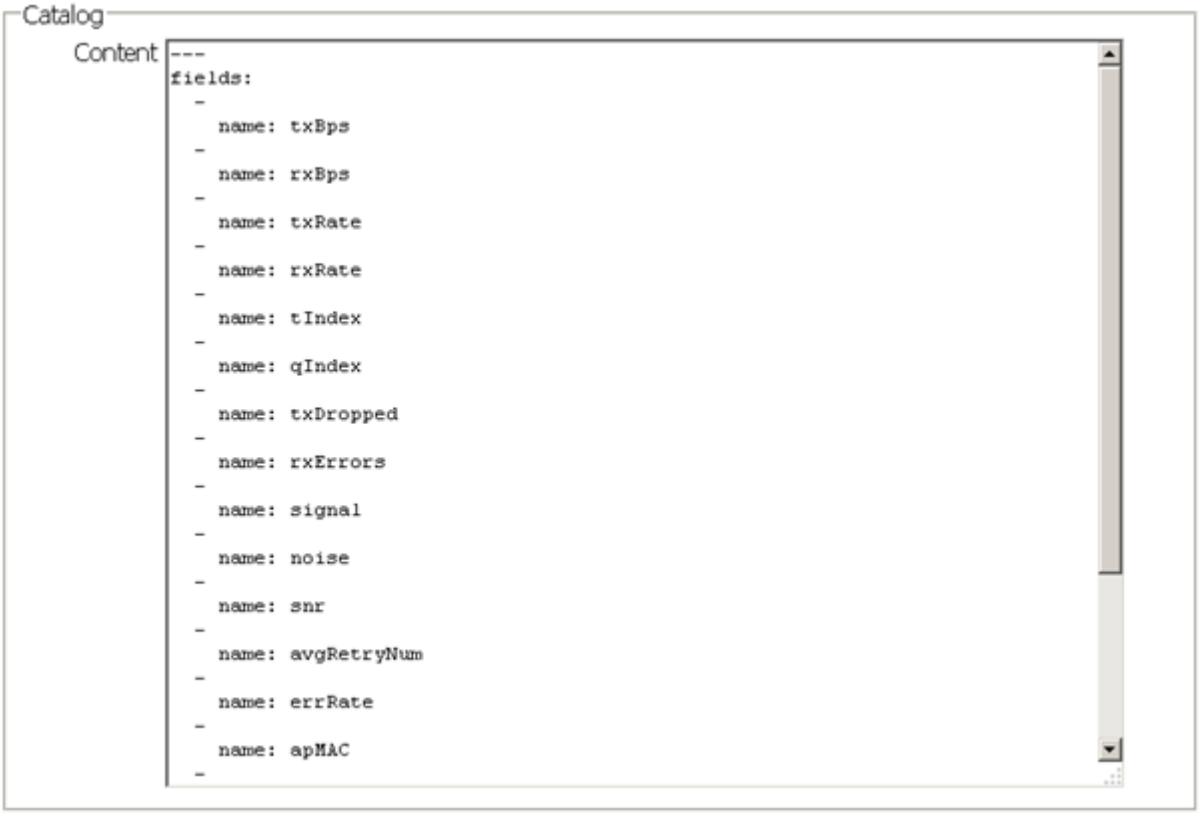


Figure 15-239 *Developer Interface - API Catalog*

The catalog item selection displays the values currently set for the selected feature. As with queries, this information cannot be manipulated as a configurable API attribute, though this information can be utilized as criteria for API attribute creation.

16 Analytics

A NX9500 and NX9510 model service platforms can provide granular and robust analytic reporting for a RFS4000 and RFS6000 controller managed network or a NX45xx/NX65xx service platform managed network. Using analytics, data is collected and reported at varying intervals. Analytic data is culled from WLANs at either the system, RF Domain, controller/service platform or Access Point level.

Analytics can parse and process events within the NOC managed network as events are received.

The analytics display resembles the *Health* and *Inventory* pages available to controllers and Access Points, though Analytics provides performance information at a far more granular level.

The analytics user interface populates information within a *data store*, with multiple displays partitioned by performance function. The data store is a customizable display managed with just the content the administrator wants viewed. The data store is purged after 90 days if no administration is conducted sooner.

A separate analytics license is enforced at the NOC. The license restricts the number of Access Point streams processed at the NOC or forwarded to partner systems for further processing. The analytics feature can be turned on at select APs by enabling them in configuration. This way the customer can enable analytics on a select set of APs and not the entire system as long as the number of APs on which it is enabled is less than or equal to the total number of AP analytics licenses available at the NOC controller.

For more information, see:

- *System Analytics*
- *RF Domain Analytics*
- *Wireless Controller Analytics*
- *Access Point Analytics*
- *Analytic Event Monitoring*

16.1 System Analytics

Analytics can be administrated at the system level to include all RF Domains, their controller or service platform memberships, adopted Access Points and their connected clients. For information on monitoring analytic events, refer to *Analytic Event Monitoring*.

To administrate analytics system-wide:

1 Select **Statistics** from the Web UI.

2 Select the **Analytics** menu item directly to the right of the System menu item within Statistics.

The analytics screen displays with **Captive Portal** data displayed by default.

Refer to the arrow icon located in the top, right-hand, side of each panel to define whether the display is in Chart format, a Table or whether you would like the output for that parameter saved as a PDF report at a user specified location.

Figure 16-1 *System Analytics - Captive Portal screen*

3 Refer to the upper, right-hand, portion of the analytics interface and define the trending period for the data displayed. Options include *Last 1 Day*, *Last 3 Days*, *Last 1 Week*, *Last 2 Weeks*, *Last 3 Weeks, Last 1 Month*, *Last 2 Months* or *Last 3 Months*. Today is the default setting for trending analytics data.

4 Refer to the following **Captive Portal** analytic data trended and reported in real-time on the selected interval:

Device Types	Displays a pie chart (by default) of the captive portal clients (smart phones, tablets, laptops etc.). Select the table icon from the top, right-hand, side of the field to display the data in table format. Both the pie chart and table display the device type and the percentage of those devices only within the captive portal.
Device OS	Displays a pie chart (by default) of connected devices (using captive portal authentication), differentiated by their operating system (*Windows*, *Linux*, *Android* etc.). Select the table icon from the top, right-hand, side of the field to display the data in table format. Both the pie chart and table display the OS type and the percentage of that device OS type only within the captive portal.
Browser Types	Displays a pie chart (by default) of the browser types utilized by captive portal authenticated devices. Select the table icon from the top, right-hand, side of the field to display the data in table format. Both the pie chart and table display the OS type by percentage of utilization only within the captive portal.

Top X URLs	Reports the top visited URLs by connected clients using captive portal authentication. Use the spinner control to refine the number of URLs reported, then select *Reload* to update the display. Set whether the content is displayed as a chart or as a table.
Search Terms	Lists the number of unique clients who searched for using a search term. Each display option lists the search term and the number of times each term was searched by a connected captive portal client. For example, if there's two clients (clients *A* and *B),* and client *A* searched for "extremenetworks" 5 times and *B* searched for "extremenetworks" 2 times. The count would be 2 and not 7. As with URLs, search terms are normalized (aggregated daily).
Normalized URLs	Reports URLs visited most often, *normalized* (aggregated daily), by devices using captive portal authentication. Select the arrow to the left of each listed URL timestamp to populate the URL and Count columns with the specific URLs visited and the number of times they've been visited.
Unique vs Repeat Users	Displays a breakdown of repeat versus new users to the captive portal. Both a chart and a table display are available, each with a timestamp of when the data was collected.
Device Count Per AP	Displays the number of top performing Access Points reporting connected client counts using captive portal authentication.
Clients in WLAN	Displays the number of managed WLANs reporting connected client counts. Client analytics are trended every 75 minutes.

5 Select **Client Analytics** to display analytic level data for connected wireless clients.

NOTE: Be sure to select the **Search** button adjacent to the **Search for Wireless Client** parameter to ensure the tables are populated and refreshed with detected wireless clients. Client analytics are trended every 75 minutes.

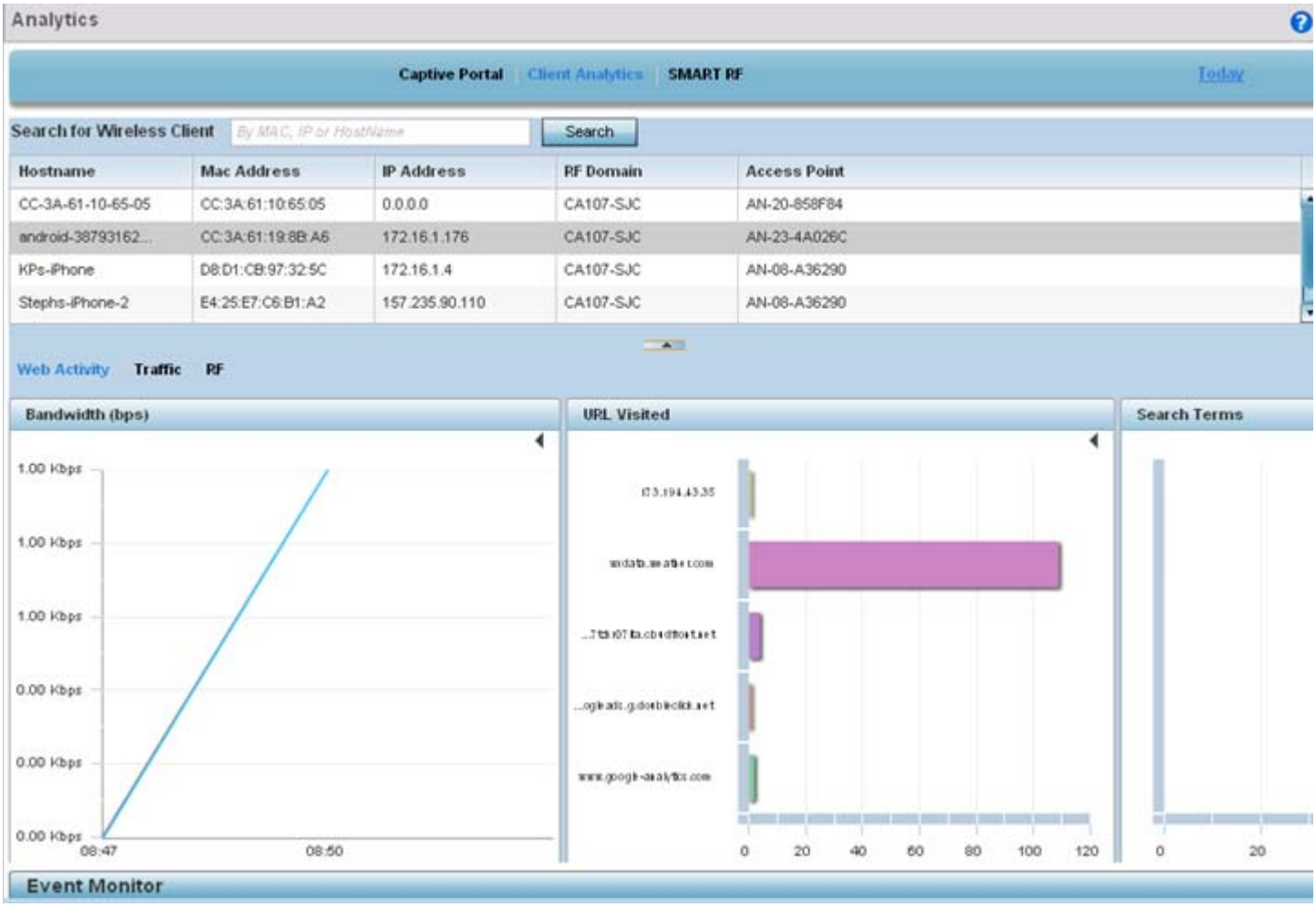


Figure 16-2 *System Analytics - Client Analytics screen*

6 Refer to the following **Client Analytics** trended at the selected interval:

Hostname	Lists the administrator assigned hostname set for each listed client when connected to the controller, service platform or Access Point managed network.
Mac Address	Displays the factory encoded MAC address for the listed client as a hardware manufacturing ID.
IP Address	Lists the IP addresses the client is using as a wireless network identifier within the controller, service platform or Access Point managed network.
RF Domain	Lists the client's current RF Domain membership. RF Domains allow administrators to assign regional, regulatory and RF configuration to devices deployed in a common coverage area such as on a building floor, or site. Each RF Domain contains regional, regulatory and sensor server configuration parameters and may also be assigned policies that determine access, Smart RF and WIPS configuration.
Access Point	Displays an administrator assigned hostname for each listed Access Point whose radio is providing a network connection for the wireless network.

The Client Analytics screen contains **Web Activity**, **Traffic** and **RF** displays within the lower half of the screen. Each of these analytics display an administrator's choice of graphical or tabled data for the client's Web activity, SNR, network interference, signal quality and packet retries.

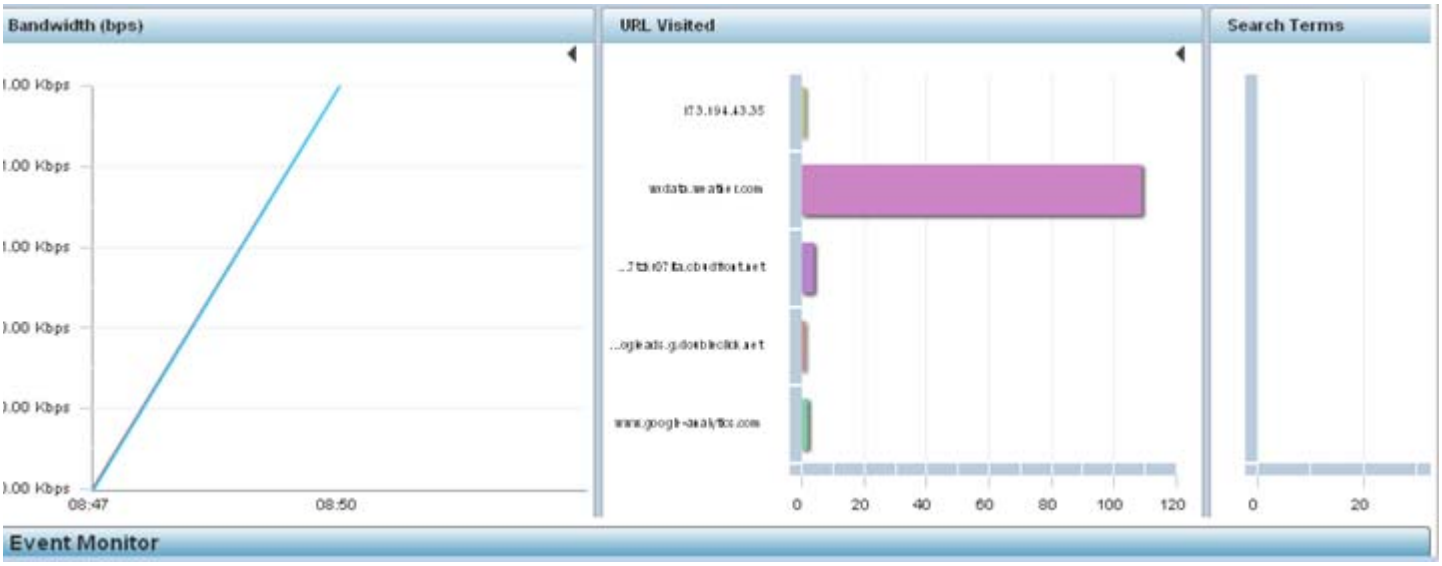


Figure 16-3 *System Analytics - Client Web Activity screen*

7 The **Web Activity** field displays by default with the following content trended in the selected interval:

Bandwidth	Displays the client's Web activity bandwidth utilization in *Bits per second* (Bps) in either chart or table format.
URL Visited	Displays URLs visited by a selected client in either chart or table format. Either display contains the Web destination URL and the number of times the URL was accessed by the client.
Search Terms	Displays terms used as search Web search criteria by connected clients in either chart or table format. Either display contains the search item and the number of times the term was searched by the client.

8 Select **Traffic**.

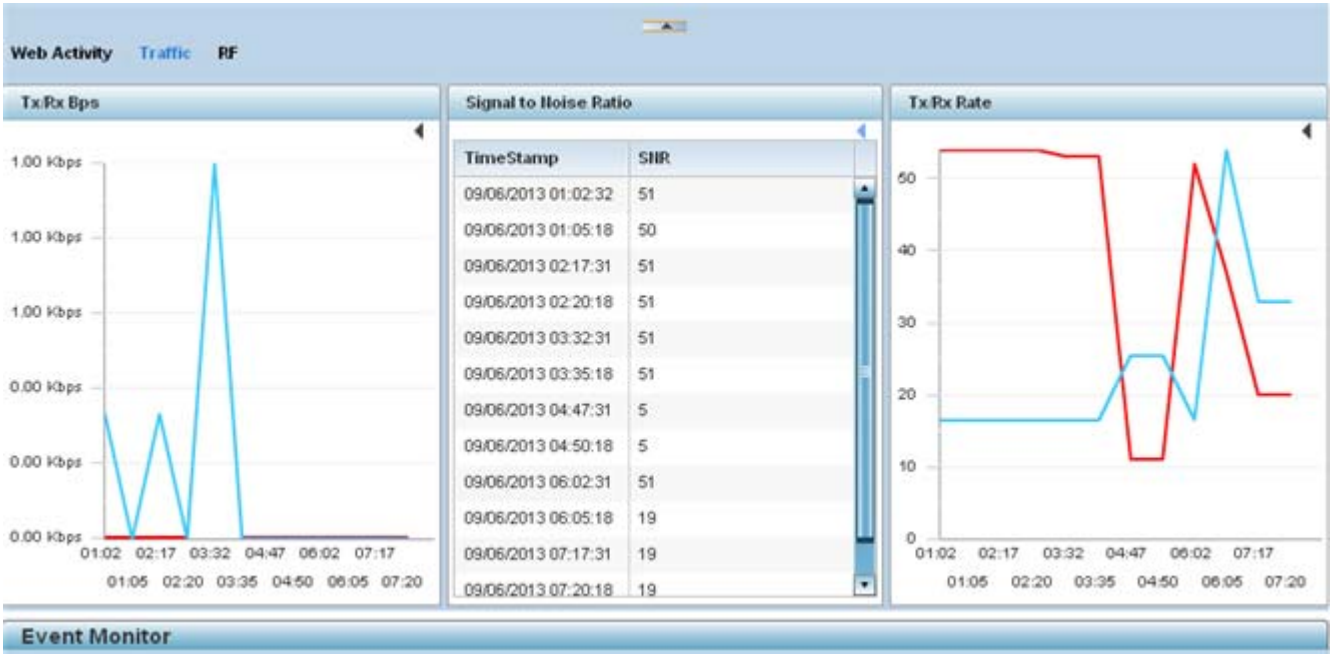


Figure 16-4 *System Analytics - Client Traffic screen*

9 Refer to the following client **Traffic** analytics trended at the selected interval:

Tx/Rx Bps	Displays the *Bits per second* (Bps) speed of data both transmitted from and received at the listed client, in either chart or table format.
Signal to Noise Ratio	Displays the connected client's *signal to noise ratio* (SNR) and a time stamp of its reporting. A high SNR could warrant a different Access Point connection to improve performance.
Tx/Rx Rate	Displays the connected client's transmit and receive data rate in either chart or table format.

10 Select **RF**.

Figure 16-5 *System Analytics - Client RF screen*

11 Refer to the following client **RF** analytics trended in the selected interval:

RF Quality Index	Displays the overall effectiveness of the system-wide RF environment as a percentage of the connect rate in both directions. The RF quality index value can be interpreted as: 0 – 20 *(Very low utilization)* 20 – 40 *(Low utilization)* 40 – 60 *(Moderate utilization)* 60 and above *(High utilization)*
Average Retries	Displays the rate of client connection retry attempts and a timestamp of their occurrence in either chart or table format. A high number indicates potential network or hardware issues.

12 Select **Smart RF** to display system-level power and channel compensation analytics:

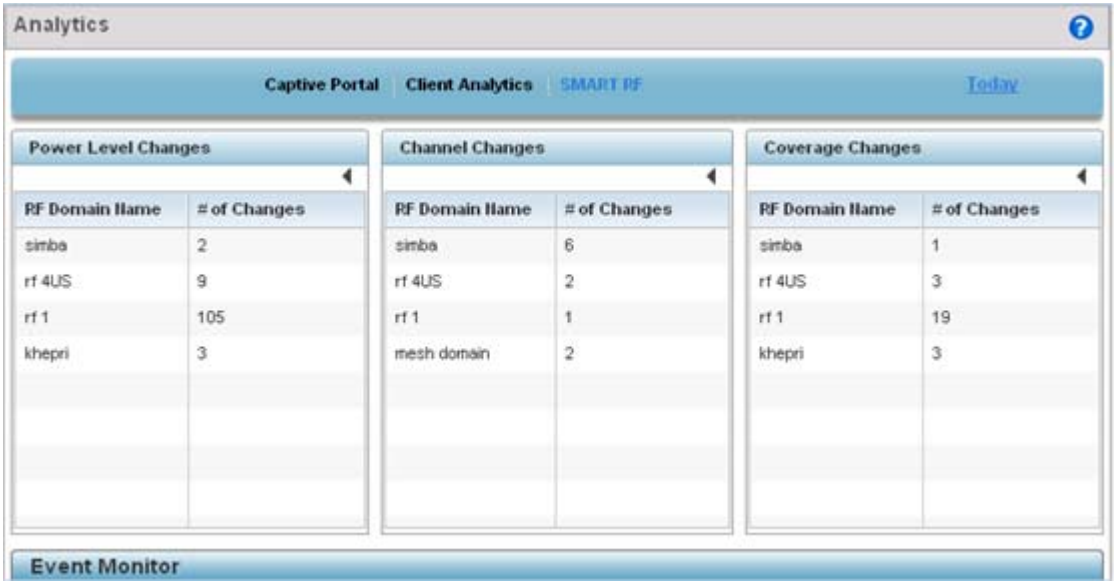


Figure 16-6 *System Analytics - Smart RF screen*

13 Refer to the following system-wide power level, channel and coverage **Smart RF** analytics trended in real-time at the administrator defined interval:

Power Level Changes	Displays the number of Smart RF power level compensations made for the system's RF Domains during the defined analytic reporting interval. This helps an administrator assess the device power changes needed to accommodate a potentially failed or poorly performing device and provides an overall insight into the overall duty cycle requirements of a particular RF Domain.
Channel Changes	Displays the number of Smart RF channel change compensations made for the system's RF Domains during the defined analytic reporting interval.
Coverage Changes	Displays the number of Smart RF coverage change compensations made for the system's RF Domains during the defined analytic reporting interval.

16.2 RF Domain Analytics

Additional analytics are available at the RF Domain level of the user interface for trending data for specific groups of RF Domain member devices. RF Domain analytics are trended every 60 minutes. For information on monitoring analytic events, refer to *Analytic Event Monitoring*.

To administrate RF Domain level analytics:

1 Select **Statistics** from the Web UI.

2 Select the **Analytics** menu item directly to the right of the System menu item within Statistics.

3 Expand the System hierarchy on the left-hand side of the user interface and select a RF Domain.

The Analytics screen displays with the **Captive Portal** tab displayed by default. This is the same data presented at the system level of the user interface. For more information on captive portal analytics, see *System Analytics on page 16-1*.

4 Select **Traffic** to assess throughput and bandwidth utilization information reported collectively for selected RF Domain member devices. Use the **WLAN** drop-down menu to refine whether traffic statistics are reported for a particular RD Domain WLAN or reported collectively for all WLANs.

Refer to the arrow icon located in the top, right-hand, side of each panel to define whether the display is in Chart format, a Table or whether you would like the output for that parameter saved as a PDF report at a user specified location.

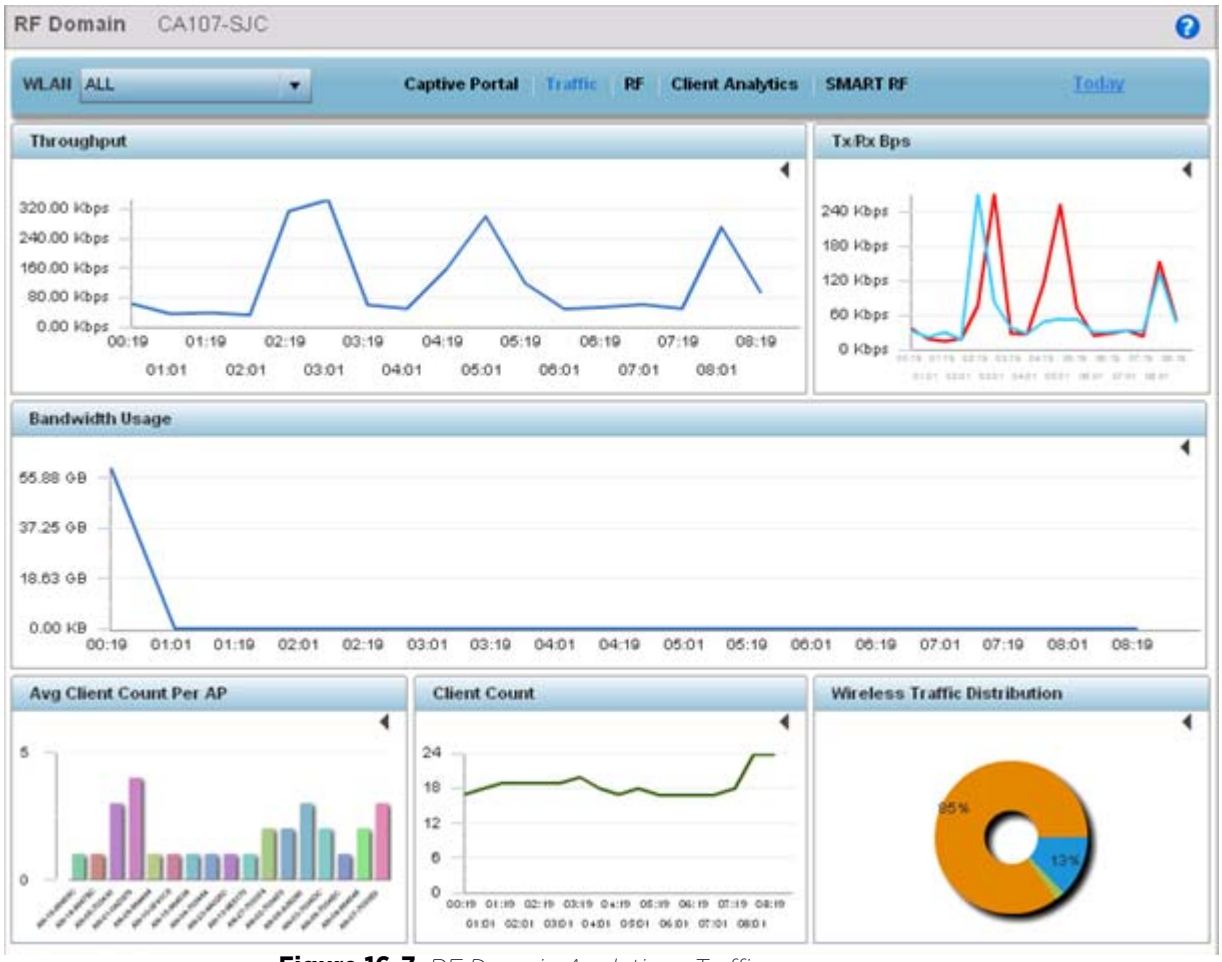


Figure 16-7 *RF Domain Analytics - Traffic screen*

5 Refer to the upper, right-hand, portion of the analytics interface and define the trending period for the data displayed. Options include *Yesterday, Last 24 Hours*, *Last 3 Days*, *Last 1 Week*, *Last 2 Weeks*, *Last 3 Weeks, Last 1 Month*, *Last 2 Months* or *Last 3 Months*. Today is the default setting for trending analytics data.

6 Refer to the following **Traffic** analytic data trended and reported for RF Domain member devices:

Throughput	Lists RF Domain member device throughput (in Mbps) as an overall indicator of RF traffic activity of all RF Domain member devices. Assess whether specific times of the day require additional RF domain member device support to adequately support RF traffic requirements.
Tx/Rx Bps	Displays *transmit* and *receive* data (in Bps) for RF Domain member devices over the listed trending period.
Bandwidth Usage	Lists RF Domain member bandwidth utilization (in Kbps) to help an administrator assess periods os sustainable versus unsustainable activity.
Average Client Count per AP	Displays RF Domain member Access Points and their connected client counts. Assess whether particular client counts are excessive, and whether loads can be better distributed amongst RF Domain member Access Points. Client analytics are trended every 75 minutes.
Client Count	Lists RF Domain member Access Point connected client counts. Use the trending data to assess periods of high versus low client connection activity. Client analytics are trended every 75 minutes.

Wireless Traffic Distribution	Displays a chart of unicast versus management frames transmitted by RF Domain member devices.

7 Select **RF** to display RF Domain member device RF quality, detected network interference (noise) and device connection retries.

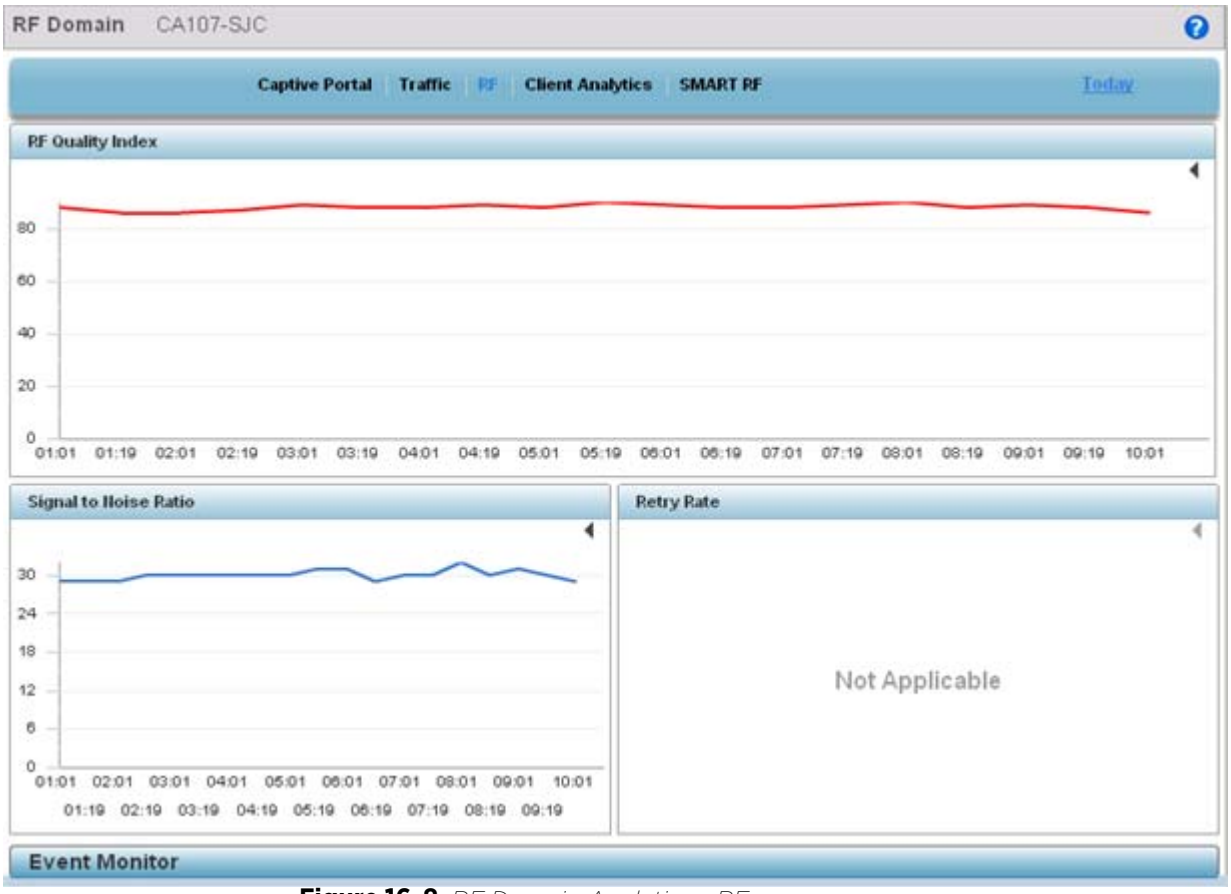


Figure 16-8 *RF Domain Analytics - RF screen*

8 Refer to the following **RF** analytics trended for a selected RF Domain:

RF Quality Index	Displays the trended graph of the effectiveness of a selected RF Domain's RF environment as a percentage of the connect rate in both directions. The RF quality index value can be interpreted as: 0 – 20 *(Very low utilization)* 20 – 40 *(Low utilization)* 40 – 60 *(Moderate utilization)* 60 and above *(High utilization)*.
Signal to Noise Ratio	Displays a selected RF Domain's connected client *signal to noise ratio* (SNR) and a time stamp of its reporting. A high SNR could warrant power compensation to account for poorly performing radios.
Retry Rate	Lists the number of retry attempts for requesting client connections to RF Domain member device radios.

9 Select **Client Analytics** to display analytic level data for connected wireless clients. This data is the same client analytic data available at the system level of the user interface, only displayed for the selected RF Domain as opposed to the entire system. For more information on client analytics, see *System Analytics on page 16-1*.

NOTE: When trending client analytics, be sure to select the **Search** button adjacent to the **Search for Wireless Client** parameter to ensure the tables are populated with detected wireless clients. Client analytics are trended every 75 minutes.

10 Select **Smart RF**.

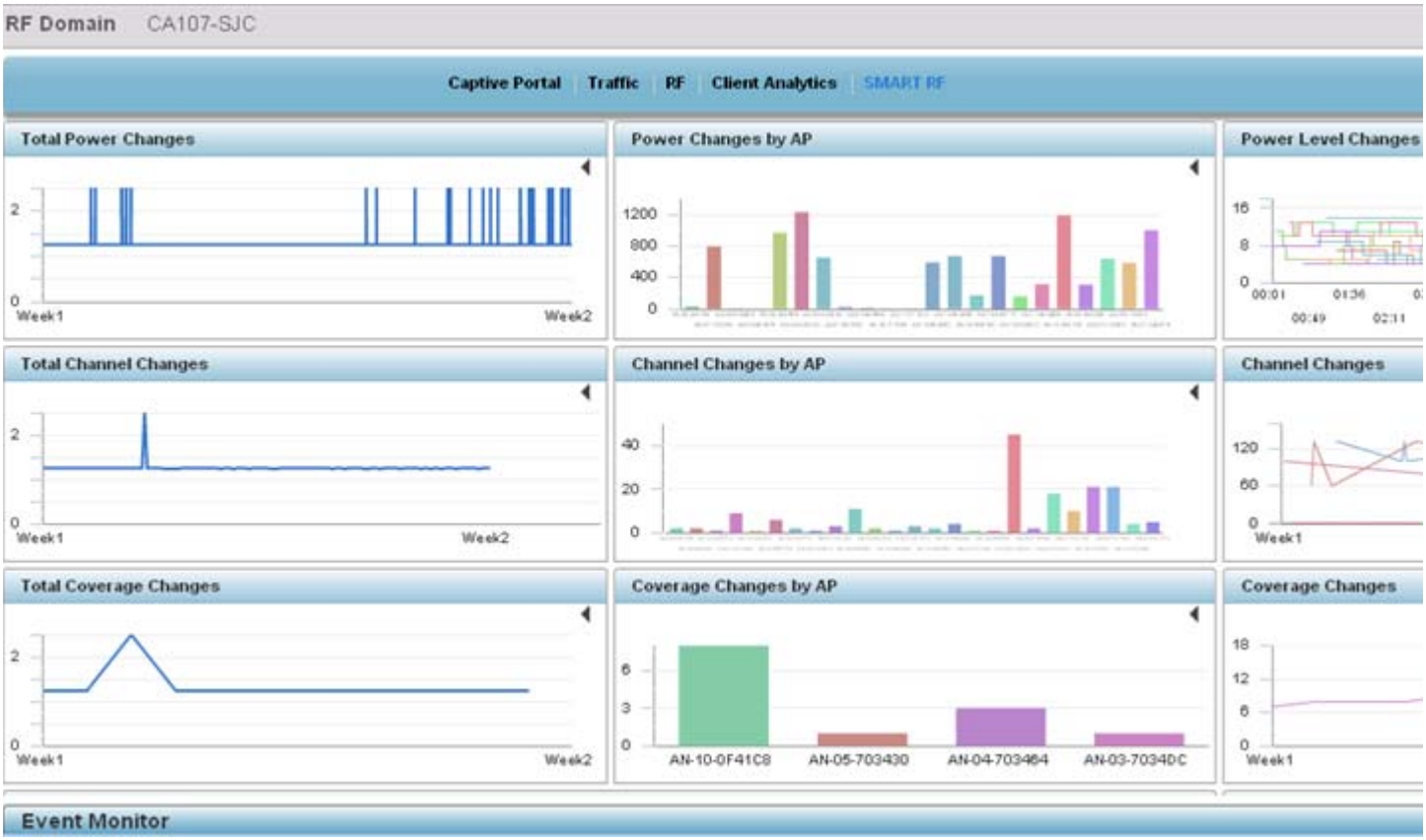


Figure 16-9 *RF Domain Analytics - Smart RF screen*

11 Refer to the following RF Domain power level, channel and coverage adjustment **Smart RF** analytics:

Total Power Changes	Lists the total trended number of power compensations required by RF Domain member radios to account for the power load requirements of offline or poor performing radios.
Total Channel Changes	Lists the total trended number of channel compensations required by RF Domain member radios to account for the channel support requirements offline or poor performing radios.
Total Coverage Changes	Displays the total trended number of coverage compensations required by RF Domain member radios to account for the load requirements of offline or poor performing radios.
Power Changes by AP	Lists the total trended number of power compensations made by individual RF domain member Access Points to account for the power load requirements of offline or poor performing radios.

Channel Changes by AP	Lists the total trended number of channel compensations made by individual RF domain member Access Points to account for the channel support requirements of offline or poor performing radios.
Coverage changes by AP	Displays the total trended number of coverage compensations made by individual RF domain member Access Points to account for the load requirements of offline or poor performing radios.
Power Level Changes	Lists all the power level changes made by RF Domain member radios separately within the same to graph help administrators assess periods of power compensations by numerous devices within the same RF Domain.
Channel Changes	Provides a timeline (using the selected trending period) when channel changes occur amongst RF Domain member connected clients. Use this data to assess whether multiple device channel changes occur at the same time and whether the channel ch nag es are to the same channel. RF Domain channel analytics are trended every 90 minutes.
Coverage Changes	Provides a timeline (using the selected trending period) when coverage changes occur amongst RF Domain member connected clients. Use this data to assess whether multiple device coverage changes occur at the same time.
Channel Distribution	Displays a chart for both the 2.4 and 5 GHz radio bands showing the channels currently being utilized by RF Domain member devices. This is helpful to assess whether devices are utilizing channels properly spaced to avoid interference. RF Domain channel analytics are trended every 90 minutes.
Coverage Changes by Client	Lists the factory encoded MAC addresses of connected clients that have made Smart RF initiated coverage changes with RF Domain member devices.

16.3 Wireless Controller Analytics

Refined analytics are available at the individual controller or service platform level of the user interface for trending data for specific controllers or service platforms undergoing configuration updates. Wireless controller analytics are trended every 75 minutes. For information on monitoring analytic events, refer to *Analytic Event Monitoring*.

A facility is also available for the comparison of configuration files to assess the specific updates made to configurations.

To review analytics for individual controllers or service platforms:

1 Select **Statistics** from the Web UI.

2 Select the **Analytics** menu item directly to the right of the System menu item within Statistics.

3 Expand the System hierarchy on the left-hand side of the user interface, expand a RF Domain and select a wireless controller.

Figure 16-10 *Wireless Controller Analytics screen*

4 Optionally select the **Resource Usage** button to display a subscreen trending the service platform's **RAM Usage** (in MB) and **Disk Usage** (in GB). Periodically revisit the service platform's resource usage to assess whether resources are jeopardized at certain times of the day or repeatable patterns are observable that can assist in administration.

5 Refer to the following analytic data trended for the selected controller or service platform:

Timestamp	Displays a timestamp when an update was made to the selected controller or service platform's configuration.
User	Lists the user name initiating the controller update.
Comments	Lists any comments made relative to a configuration update.

6 Select the **Diff Files** button to display the updates made to the selected controller or service platform's configuration versus the previous configuration utilized.

16.4 Access Point Analytics

Refined analytics are available at the individual Access Point level of the user interface for trending data for specific Access Points. For information on monitoring analytic events, refer to *Analytic Event Monitoring*.

To review analytics for individual Access Points:

1 Select **Statistics** from the Web UI.

2 Select the **Analytics** menu item directly to the right of the System menu item within Statistics.

3 Expand the System hierarchy on the left-hand side of the user interface, expand a RF Domain and select an member Access Point.

The Access Point analytics screen displays with **Traffic** tab displayed by default.

4 Use the **Radio** drop-down menu to refine whether traffic statistics are reported an Access Point's 2.4 or 5 GHz radio.

Refer to the arrow icon located in the top, right-hand, side of each panel to define whether the display is in Chart format, a Table or whether you would like the output for that parameter saved as a PDF report at a user specified location.

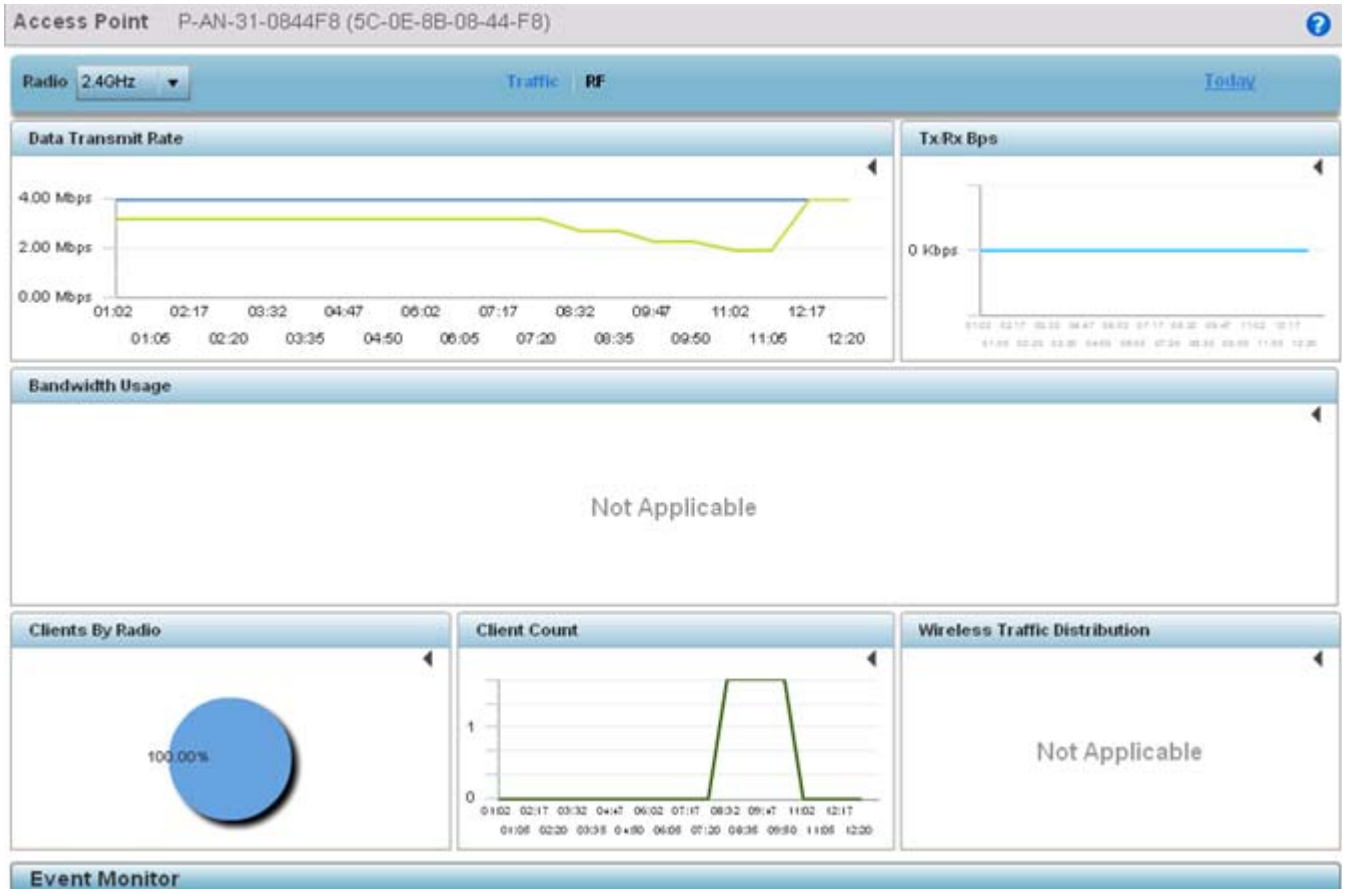


Figure 16-11 *Access Point Analytics - Traffic screen*

5 Refer to the upper, right-hand, portion of the analytics interface and define the trending period for the data displayed. Options include *Last 1 Day*, *Last 3 Days*, *Last 1 Week*, *Last 2 Weeks*, *Last 3 Weeks, Last 1 Month*, *Last 2 Months* or *Last 3 Months*. Today is the default setting for trending analytics data.

6 Refer to the following **Traffic** analytic data trended for the selected Access Point:

Data Transmit Rate	Lists the selected Access Point's throughput (in Mbps) as an indicator of RF traffic activity on the selected 2.4 or 5 GHz radio.
Tx/Rx BPs	Displays *transmit* and *receive* data (in Bps) for the selected Access Point radio over the defined trending period.
Bandwidth Usage	Lists Access Point radio bandwidth utilization (in Kbps) to help an administrator assess periods os sustainable versus unsustainable activity for the selected 2.4 or 5 GHz Access Point radio.

Clients by Radio	Displays a pie chart depicting the ratio of clients operating on different 802.11 bands (11BGN, 11AN etc.). This client data is trended every 75 minutes.
Client Count	Lists the selected Access Point's connected client count. Use this trending data to assess periods of high versus low client connection activity, and whether this particular Access Point is properly load balanced.
Wireless Traffic Distribution	Displays a chart depicting the ratio of unicast versus management frames transmitted by the selected Access Point.

7 Select **RF** to display Access Point RF quality analytics.

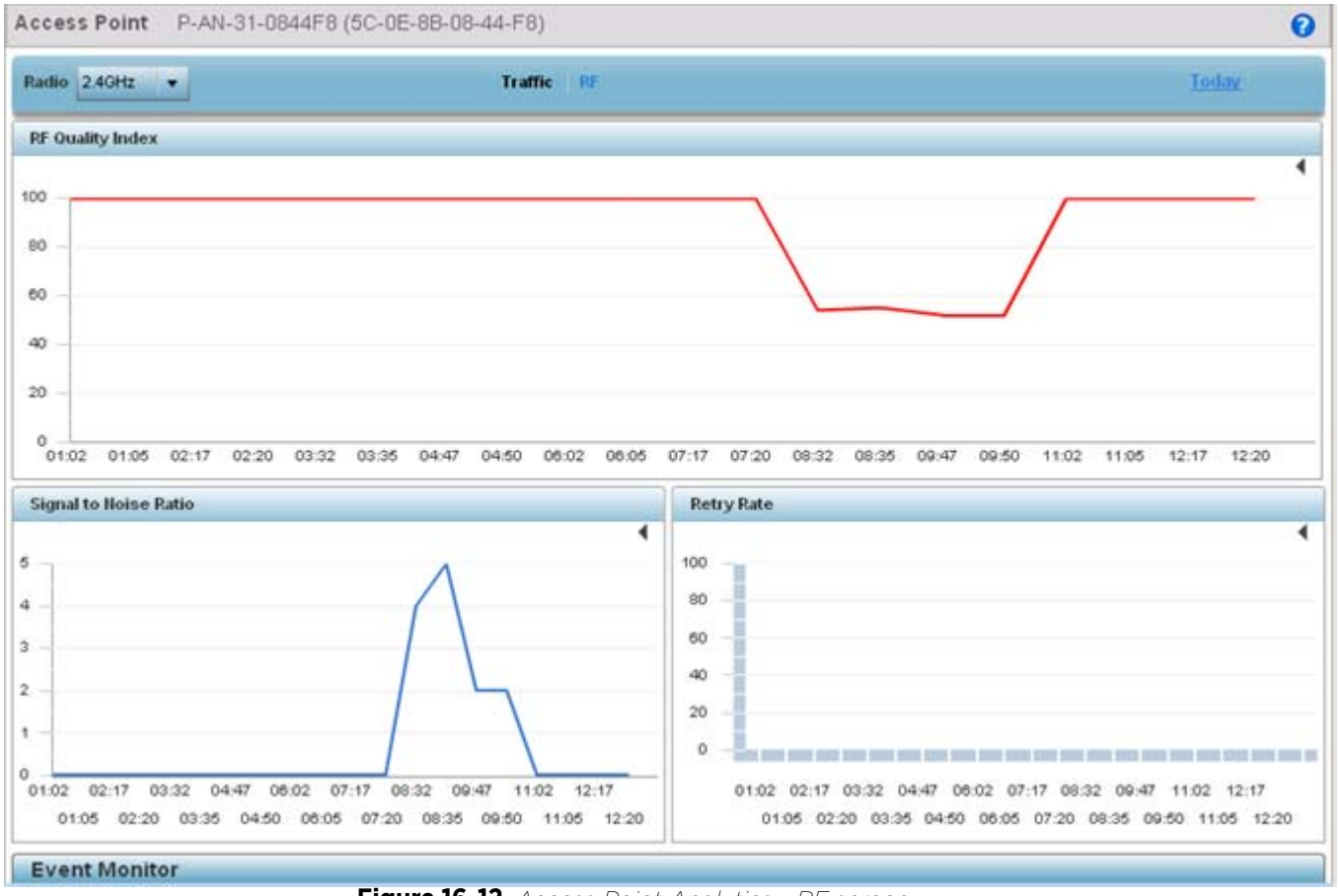


Figure 16-12 *Access Point Analytics - RF screen*

8 Refer to the following **RF** analytics trended for a selected Access Point:

RF Quality Index	Displays the trended graph of the effectiveness of a selected Access Point's RF environment as a percentage of the connect rate in both directions. The RF quality index value can be interpreted as: 0 – 20 *(Very low utilization)* 20 – 40 *(Low utilization)* 40 – 60 *(Moderate utilization)* 60 and above *(High utilization)*.
Signal to Noise Ratio	Displays a selected Access Point's connected client *signal to noise ratio* (SNR) and a time stamp of its reporting. A high SNR could warrant power compensation to account for poorly performing Access Point radios.

Retry Rate	Lists the number of retry attempts for requesting client connections to the selected Access Point's radios.

16.5 Analytic Event Monitoring

Display the **Event Monitor** on the bottom portion of the analytic display, at any time or place in the user interface hierarchy, to review individual analytic events by their severity, originating device, reporting module and timestamp (occurrence).

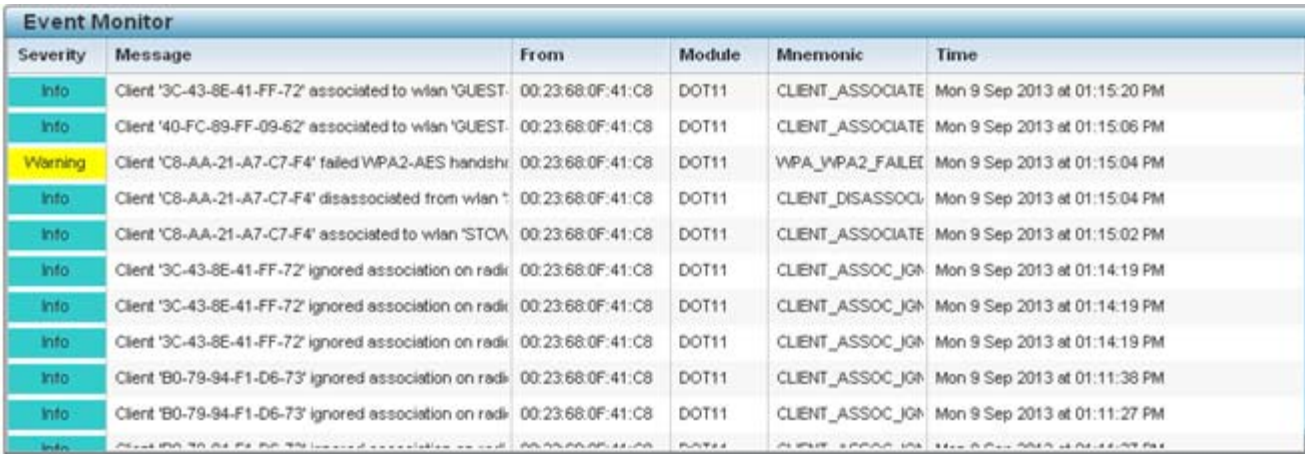


Figure 16-13 *Analytic Event Monitor*

Review the following within the Event Monitor to assess if an individual event requires further administration to improve network performance:

Severity	Lists the severity for each analytic event. Severity levels include *Emergency*, *Alert*, *Critical*, *Errors*, *Warning*, *Notice*, *Info* and *Debug*.
Message	Displays an event description to assist the administrator in assessing the significance of the event and (in conjunction with the severity) whether corrective action is immediately needed.
From	Displays the hardware encoded MAC address of the device impacted by the listed event.
Module	Lists the module from which analytic events are tracked and reported.
Mnemonic	Lists the service platform or controller mnemonic that translates the listed event into a string that's meaningful to the network administrator.
Time	Displays the date and time when each listed event was detected within the network.

17 WiNG Events

WiNG outputs an event message for configuration changes and status updates to enable an administrator to assess the success or failure of specific configuration activities. Use the information in this chapter to review system generated event messages and their descriptions.

Each listed event can have customized notification settings defined and saved as part of an event policy. Thus, policies can be configured and administrated in respect to specific sets of client association, authentication/ encryption and performance events. Once policies are defined, they can be mapped to device profiles strategically as the likelihood of an event applies to particular devices. By default, there's no enabled event policy and one needs to be created and implemented.

For more information on the UI's descriptions of events, refer to *Fault Management on page 13-1*.

17.1 Event Messages

To review event history messages:

1 Select **Configuration** > **Diagnostics** > **Fault Management** > **Event History** to display the Event History screen.

2 Select **Fetch Historical Events** to display the diagnostic events in the Event History table.

3 Refer to the following (read only) information to assess logged diagnostic events.

ADOPT-SERVICESNMP_SUCCESS6	SNMP framework success
ADOPT-SERVICESNMP_FAILURE6	SNMP framework failure
ADOPT-SERVICETUT_TEMPERATURE_ALARM_RAISED ([str])	Temperature alarm raised on sensor
ADOPT-SERVICETUT_TEMPERATURE_ALARM_CLEARED([str])	Temperature alarm cleared on sensor
ADOPT-SERVICETUT_TEMPERATURE_ALARM_CLEARED([str])	Temperature alarm cleared on sensor
ADOPT-SERVICETUT_FAN_ALARM_CLEARED5IPX ([str])	Fan alarm cleared on ID
ADOPT-SERVICETUT_PWRCTRL_ALARM_RAISED5IPX ([str])	Power controller alarm raised
ADOPT-SERVICETUT_PWRCTRL_ALARM_CLEARED5IPX ([str])	Power controller alarm cleared
ADOPT-SERVICETUT_LINE_POWER_ALARM_RAISED5IPX ([str]) Line power alarm raised on id [str]	Line power alarm raised
ADOPT-SERVICETUT_LINE_POWER_ALARM_CLEARED5IPX ([str]) Line power alarm cleared on id [str]	Line power alarm cleared
ADOPT-SERVICETUT_WLAN_CLIENT_ASSOC6IPX ([str]) Client [str] on interface index [str] associated	Client associated

ADOPT-SERVICETUT_WLAN_CLIENT_DISASSOC6IPX ([str]) Client [str] on interface index [str] disassociated with status code [str], [str]	Client disassociated
ADOPT-SERVICETUT_WLAN_CLIENT_ASSOC_FAILURE3IPX ([str]) Association failed for Client [str] on interface index [str] with status code [str], [str]	Association failed for client on specified interface index
ADOPT-SERVICETUT_WLAN_CLIENT_AUTH6IPX ([str])	Client on interface index authenticated
ADOPT-SERVICETUT_WLAN_CLIENT_DEAUTH6 IPX ([str])	Client on interface index deauthenticated with status code
ADOPT-SERVICETUT_WLAN_CLIENT_AUTH_FAILURE3IPX ([str])	Authentication failed for client on interface index with status code
ADOPT-SERVICETUT_RADIO_ADAPTIVE_POWER_CHANGE5 IPX ([str])	Interface with operational status and power levels
ADOPT-SERVICETUT_RF_MONITOR_MODE_CHANGE5 IPX ([str])	RF monitor status changed to on interface
ADOPT-SERVICEIPX_EVENT_FAILURE3IPX ([str])	Failed to raise WiNG event
AP NO_IMAGE_FILE [str] firmware image is not present on controller	Access Point firmware not on controller
AP IMAGE_PARSE_FAILURE Format of [str] firmware image on controller is invalid	Invalid Access Point firmware file
AP LEGACY_AUTO_UPDATE Legacy Access Point [str] [mac] being updated	Legacy Access Point updated
AP AP_ADOPTED [str] [mac] adopted	Access Point adopted
AP AP_UNADOPTED [str] [mac] un-adopted	Access Point unadopted
AP AP_RESET_DETECTED 6 [str] [mac] reset itself	Access Point reset detected
AP AP_RESET_REQUEST 6 [str] [mac] reset request	Access Point user requested reset
AP AP_TIMEOUT 6 str] [mac] timed out, reset sent to AP	Access Point timed out
AP ADOPTED Access Point([qstr]/[qstr]/[dev]) at rf-domain:[qstr] adopted and configured. Radios: Count=[str], Bss: [str]	Access Point adopted and configured
AP UNADOPTED Access Point([qstr]/[qstr]/[dev]) at rf-domain:[qstr] unadopted. Radios: Count=[str], Bss: [str]	Access Point unadopted
APADOPTED_TO_CONTROLLER Joined successfully with controller [qstr]([str])	Access Point adopted to controller
APONLINE Access Point [dev] is now online. Offline Reason is [str]. Offline count is [int]	Access Point online
APOFFLINE Access Point [dev] is now offline. Offline Reason is [str]. Offline count is [int]	Access Point offline

APOFFLINE Device [dev]([str]) is offline, last seen:[int] minutes ago on switchport [str]	Adopted device offline
APRESET Reset Access Point mac [dev], [str]	Access Point reset
APADOPTION_REDIRECTED Access Point([qstr]/[qstr]/[dev]) cdp:[qstr] lldp:[qstr] redirected to the controller host/pair [qstr] - [qstr]	Access Point redirected
APAP_AUTOUP_TIMEOUT4 AUTOUPGRADE: [str] mac [str] Autoupgrade timed out	Time out while auto upgrading an AP
APAP_AUTOUP_REBOOT5 AUTOUPGRADE: [str] mac [str] Autoupgrade rebooting	Rebooting AP after upgrade
APAP_AUTOUP_NO_NEED6 AUTOUPGRADE: [str] mac [str] ver [str] Autoupgrade not required or not available	Auto upgrade not initiated
APAP_AUTOUP_NEEDED6 AUTOUPGRADE: [str] mac [str] ver [str] Autoupgrade will be applied	Auto upgrade is initiated on AP
APAP_AUTOUP_DONE5 AUTOUPGRADE: [str] mac [str] Autoupgrade complete	Auto upgrade successful
APAP_AUTOUP_FAIL4 AUTOUPGRADE: [str] mac [str] Autoupgrade failed	Failed auto upgrade attempt
APAP_AUTOUP_VER6 AUTOUPGRADE: version [str] available for [str] equipment	Available Access Point firmware versions for auto upgrade
AAA RADIUS_DISCON_MSG Received Radius dynamic authorization Disconnect Message for [qstr] from server [qstr]	Received RADIUS disconnect request
AAA RADIUS_VLAN_UPDATE6 Assigning Radius server specified vlan [uint] to client [qstr] on wlan [qstr]	Client VLAN updated by RADIUS
AAA RADIUS_SESSION_NOT_STARTED5 Radius server indicates session time has not started for client [qstr]	Start time from RADIUS resource not yet valid
AAA RADIUS_SESSION_EXPIRED5 Radius server indicates session has already expired for client [qstr]	Session time from RADIUS resource already expired
ADV-WIPS ADV-WIPS-EVENT-14 Detected DoS Deauthentication attack against [mac] [str]	DoS Deauthentication attack
ADV-WIPSADV-WIPS-EVENT-24 Detected DoS Disassociation attack against [mac] [str]	DoS disassociation attack
ADV-WIPSADV-WIPS-EVENT-34 Detected DoS EAP failure spoof attack by [mac] [str]	EAP failure spoof attack
ADV-WIPSADV-WIPS-EVENT-104 Detected ID-Theft out of sequence attack for [mac] [str]	ID theft out of sequence attack
ADV-WIPSADV-WIPS-EVENT-114 Detected possible ID-Theft EAPoL Success spoof attack by [mac] [str]	Possible ID theft EAPoL success spoof attack
ADV-WIPSADV-WIPS-EVENT-124 Detected possible WLAN-Jack attack by [mac] [str]	Possible WLAN jack attack
ADV-WIPSADV-WIPS-EVENT-134 Detected possible ESSID-Jack attack against [mac] [str]	Possible ESSID jack attack

ADV-WIPSADV-WIPS-EVENT-144 Detected possible Monkey-Jack attack by [mac] [str]	Possible monkey jack attack
ADV-WIPSADV-WIPS-EVENT-164 Detected possible NULL Probe Response attack by [mac] [str]	Possible NULL probe response attack
ADV-WIPSADV-WIPS-EVENT-1054 Sanctioned MU [mac] detected associated with unsanctioned/ neighboring AP [str]	Sanctioned MU detected associated with unsanctioned/neighboring AP
ADV-WIPSADV-WIPS-EVENT-1094 Multicast all systems traffic found from [mac] [str]	Multicast all systems traffic
ADV-WIPSADV-WIPS-EVENT-11044 Multicast all routers traffic found from [mac] [str]	Multicast all routers traffic
ADV-WIPSADV-WIPS-EVENT-1114 Multicast OSPF all traffic found from [mac] [str]	Multicast OSPF all traffic
ADV-WIPSADV-WIPS-EVENT-1124 Multicast OSPF Deisgnated Routers traffic found from [mac] [str]	Multicast OSPF designated routers traffic
ADV-WIPSADV-WIPS-EVENT-1134 Multicast RIP-2 Routers traffic found from [mac] [str]	Multicast RIP 2 routers traffic
ADV-WIPSADV-WIPS-EVENT-1144 Multicast IGRP Routers traffic found from [mac] [str]	Multicast IGRP routers traffic
ADV-WIPSADV-WIPS-EVENT-1154 Multicast DHCP Server Relay Agent traffic found from [mac] [str]	Multicast DHCP server relay agent traffic
ADV-WIPSADV-WIPS-EVENT-1164 Multicast VRRP Agent traffic found from [mac] [str]	Multicast VRRP agent traffic
ADV-WIPSADV-WIPS-EVENT-1174 Multicast HSRP Agent traffic found from [mac] [str]	Multicast HSRP agent traffic
ADV-WIPSADV-WIPS-EVENT-1184 Multicast IGMP traffic found from [mac] [str]	Multicast IGMP traffic
ADV-WIPSADV-WIPS-EVENT-1194 Detected NETBIOS traffic from [mac] [str]	Detected NETBIOS traffic
ADV-WIPSADV-WIPS-EVENT-1204 Detected STP traffic from [mac] [str]	Detected STP traffic
ADV-WIPSADV-WIPS-EVENT-1134 Multicast RIP-2 Routers traffic found from [mac] [str]	Multicast RIP 2 routers traffic
ADV-WIPSADV-WIPS-EVENT-1214 Detected IPX traffic from [mac] [str]	Detected IPX traffic
ADV-WIPSADV-WIPS-EVENT-1424 Detected possible Probe Response attack by [mac] [str]	Possible probe response attack
ADV-WIPSADV-WIPS-EVENT-2214 Detected Invalid Management Frames from [mac] [str]	Invalid management frames
ADV-WIPSADV-WIPS-EVENT-264 Detected DoS RTS flood attack against [mac] [str]	DoS RTS flood attack
ADV-WIPSADV-WIPS-EVENT-2224 Detected Invalid Channel Advertisement for [mac] [str]	Invalid channel advertisement
ADV-WIPSADV-WIPS-EVENT-634 Detected Windows ZERO Configuration Memory Leak on [mac] [str]	Windows ZERO configuration memory leak

ADV-WIPSADV-WIPS-EVENT-2204 Detected Unauthorized Bridge [mac] [str]	Unauthorized bridge
APSW_CONN_LOST0 Lost connectivity with controller after config update. Rebooting and reverting to older working configuration	Controller connectivity lost
AAARADIUS_DISCON_MSG5 Received Radius dynamic authorization Disconnect Message for [qstr] from server [qstr]	Received RADIUS disconnect request
AAA RADIUS_VLAN_UPDATE6 Assigning Radius server specified vlan [uint] to client [qstr] on wlan [qstr]	Client VLAN updated by RADIUS resource
AAA RADIUS_SESSION_NOT_STARTED5 Radius server indicates session time has not started for client [qstr]	Start time from RADIUS resource not yet valid
AAA RADIUS_SESSION_EXPIRED5 Radius server indicates session has already expired for client [qstr]	Session time from RADIUS resource already expired
CAPTIVE-PORTAL AUTH_SUCCESS6 Captive-portal authentication success for client [mu] ([qstr-ip]) user [qstr]	Authentication success
ADV-WIPSADV-WIPS-EVENT-264 Detected DoS RTS flood attack against [mac] [str]	DoS RTS flood attack
ADV-WIPSADV-WIPS-EVENT-2224 Detected Invalid Channel Advertisement for [mac] [str]	Invalid channel advertisement
ADV-WIPSADV-WIPS-EVENT-634 Detected Windows ZERO Configuration Memory Leak on [mac] [str]	Windows ZERO configuration memory leak
ADV-WIPSADV-WIPS-EVENT-2204 Detected Unauthorized Bridge [mac] [str]	Unauthorized bridge
APSW_CONN_LOST0 Lost connectivity with controller after config update. Rebooting and reverting to older working configuration	Controller connectivity lost
AAA RADIUS_DISCON_MSG5 Received Radius dynamic authorization Disconnect Message for [qstr] from server [qstr]	Received RADIUS resource disconnect request
AAA RADIUS_VLAN_UPDATE6 Assigning Radius server specified vlan [uint] to client [qstr] on wlan [qstr]	Client VLAN updated by RADIUS
AAA RADIUS_SESSION_NOT_STARTED5 Radius server indicates session time has not started for client [qstr]	Start time from RADIUS resource not yet valid
AAA RADIUS_SESSION_EXPIRED5 Radius server indicates session has already expired for client [qstr]	Session time from RADIUS resource already expired
CAPTIVE-PORTAL AUTH_SUCCESS6 Captive-portal authentication success for client [mu] ([qstr-ip]) user [qstr]	Authentication success
CAPTIVE-PORTAL AUTH_FAILED6 Captive-portal authentication failed for client [mu] ([qstr-ip])	Authentication failed
CAPTIVE-PORTAL SESSION_TIMEOUT6 Captive-portal session timed out for client [mu] ([qstr-ip])	Session timed out

CAPTIVE-PORTAL CLIENT_DISCONNECT6 Captive-portal session disconnected for client [mu] ([qstr-ip])	Client disconnected
CAPTIVE-PORTAL PURGE_CLIENT6 Captive-portal: Purge client [mu] by new client [mu] for user [qstr]	Client purged
CAPTIVE-PORTAL FLEX_LOG_ACCESS6 [qstr]: [qstr] allowed access for client [mu] ([qstr-ip])	Flex log access granted for client
CAPTIVE-PORTAL INACTIVITY_TIMEOUT6 Captive-portal session cleared for client [mu] ([qstr-ip]) after inactivity timeout	Client timed out due to inactivity
CAPTIVE-PORTAL ALLOW_ACCESS6 Captive-portal allow access for client [mu] ([qstr-ip])	Client allowed access
CAPTIVE-PORTAL CLIENT_REMOVED6 Captive-portal session removed for client [mu] ([qstr-ip]) on policy change/admin action	Client removed due to admin changes
CAPTIVE-PORTAL PAGE_CRE_FAILED3 Page creation failed for policy [qstr], file [qstr], Error [qstr]	Page creation failure
CAPTIVE-PORTAL DATA_LIMIT_EXCEED6 Data limit exceed, Usage:[int] KBytes, Action:[str], client [mu] ([ip])	Client data limit exceeded
CAPTIVE-PORTAL VLAN_SWITCH6 Client [mu] ([ip]) switching from vlan [int] to vlan [int]	Client VLAN switch
CAPTIVE-PORTAL SERVER_MONITOR_STATE_CHANGE6 Captive-portal policy [qstr]: service monitor [str] server status changing from [qstr] to [qstr]	Captive portal server monitor state changed
CAPTIVE-PORTAL NO_SERVICE_PAGE_SENT6 Captive-portal sent no service page to client [mu] ([ip]) as [str] server is down	No service page sent to client
CERTMGRRSA_KEY_ACTIONS_SUCCESS6 [str] of RSA key [str] successful	Successful completion of RSA key related actions (import, export etc.)
CERTMGRRSA_KEY_ACTIONS_FAILURE3 [str] of RSA key [str] failed: [str]	Failure of RSA key related actions (import, export etc.)
CERTMGRCA_CERT_ACTIONS_SUCCESS6 [str] of CA certificate for trustpoint [str] successful	Successful completion of CA certificate related actions (import, export etc.)
CERTMGRCA_CERT_ACTIONS_FAILURE3 [str] of CA certificate for trustpoint [str] failed: [str]	Failure of CA certificate actions (import, export etc.)
CERTMGRSRV_CERT_ACTIONS_SUCCESS6 [str] of Server Certificate of trustpoint [str] successful	Successful completion of server certificate actions (import, export etc.)
CERTMGRSVR_CERT_ACTIONS_FAILURE3 [str] of Server Certificate of trustpoint [str] failed: [str]	Failure of server certificate actions (import, export etc.)
CERTMGRCSR_EXPORT_SUCCESS6 Export of Certificate Signing Request for [str] successful	Successful export of certificate signing request
CERTMGRCSR_EXPORT_FAILURE3 Export of Certificate Signing Request for [str] failed: [str]	Failed to export certificate signing request
CERTMGRCRL_ACTIONS_SUCCESSS6 [str] of CRL for trustpoint [str] successful	Successful completion of certificate revocation list action

CERTMGRCRL_ACTIONS_FAILURE3 [str] of CRL for trustpoint [str] failed: [str]	Certificate revocation list action failure
CERTMGRDELETE_TRUSTPOINT_ACTION6 Deletion of trustpoint [str] successful	Deletion of trustpoint
CERTMGRIMPORT_TRUSTPOINT6 Import of Trustpoint [str] [str]	Import of trustpoint
CERTMGREXPORT_TRUSTPOINT6 Export of Trustpoint [str] [str]//	Export of trustpoint
CERTMGRCERT_EXPIRY4 [str] certificate for trustpoint [str] [str]	Certificate expiration
CERTMGRCA_KEY_ACTIONS_SUCCESS6 [str] of CA private key for trustpoint [str] successful	Successful completion of CA private key actions
CERTMGRCA_KEY_ACTIONS_FAILURE3 [str] of CA private key for trustpoint [str] failed: [str]	Failure of CA private key actions
CLUSTERCMASTER_CFG_UPDATE_FAIL3 Cluster master config update to [str] failed, Err: [str]	Cluster master config update failed
CLUSTERMAX_EXCEEDED4 Max cluster members ([uint]) exceeded, clustering will not function properly until corrected	Max cluster count exceeded
CLUSTERSTATE_CHANGE4 Active cluster member changed. Present active [str]. Previous active [str].	Active cluster membership change
CLUSTERSTATE_CHANGE_INACTIVE4 Member [str] (load[int]) changing state from Active to Standby. New member [str] standby load [int].	Cluster member change from active to standby
CLUSTERSTATE_CHANGE_ACTIVE4 Member [str] (load[int]) changing state from Standby to Active. New member [str] standby load [int]	Cluster member change from standby to active
CLUSTERSTATE_RETAIN_ACTIVE4 Member [str] (load[int]) retaining Active state. New member [str] standby load [int]	Cluster member retaining active state
CRM CRITICAL_RESOURCE_UP5 Critical Resource [str] is UP	Critical resource is up
CRM CRITICAL_RESOURCE_DOWN 5 Critical Resource [str] is DOWN	Critical resource is down
CERTMGR-LITE INVALIDCACERT5 CA Certificate imported for the trustpoint [str] is invalid	CA certificate is invalid
CERTMGR-LITE INVALIDSERVCERT5 Server Certificate imported for the trustpoint [str] is invalid	Server certificate is invalid
CERTMGR-LITE INVALIDCERTCRL5 Certificate Crl Imported for trustpoint [str] is invalid	CRL is invalid
CERTMGR-LITE CERTEXPIRED5 [str] Certificate of trustpoint [str] is expired//	Certificate is expired
CERTMGR-LITE INVALIDCERTKEY5 Private key imported for trustpoint [str] is not valid	Private key is invalid
CERTMGR-LITE INVALIDRSAKEY5 Rsakey imported is not valid [str] is invalid//	RSA key import operation

CERTMGR-LITE KEYDECRYPTFAILE4 Rsakey cannot be decrypted with the password provided	RSA key cannot be decrypted with provided password
CERTMGR-LITE CERTIMPORTED6 [str] Certificate imported for the trustpoint [str]	Certificate imported for trustpoint
CERTMGR-LITE CERTKEYIMPORTED6 Private key imported for the trustpoint [str]	Private key imported for trustpoint
CERTMGR-LITE RSAKEYIMPORTED6 Rsakey imported with the name [str]	RSA key imported
CERTMGR-LITE DELETETRUSTPOINT6Trustpoint [str] is deleted	Trustpoint deleted
CERTMGR-LITE DELETERSAKEY6 Rsakey [str] is deleted	RSA Key deleted
CERTMGR-LITE CERTREQUESTGEN6 Certificate request generated for the trustpoint [str]	Certificate requested generated
CERTMGR-LITE CERTSELFSIGNEDGEN6 Selfsigned certificate generated for the trustpoint [str]	Self signed certificate generated
CERTMGR-LITE RSAKEYGEN6 Rsa key [str] generated	RSA key generated
CERTMGR-LITE ERROR5 [str]	Certificate manager general error
CERTMGR-LITE CERT_EXPIRY4 [str] certificate for trustpoint [str] [str]	Certificate about to expire
CERTMGR CERT_RENEW_FAILED1 Certificate renew in field failed reason [str]	Certificate renew failure reason
DHCPSVRDHCPSVR_STOP6 DHCP server is stopped	DHCP server stopped
DIAGWD_RESET_SYS2 The system has been RESET by the Watchdog	Log watchdog reset
DIAGCPU_USAGE_TOO_HIGH4 CPU Usage too high. Limit of [int]*(0.1%) exceeded. Current CPU usage is [int]*(0.1%)	Log CPU load detected as too high
DIAGCPU_USAGE_TOO_HIGH_RECOVER4 CPU Usage too high recover. Limit is [int]*(0.1%)	Current CPU usage is too high
DIAGCPU_LOAD4 [str] minute average load limit exceeded, value is [str]% limit is [str]% (top processes: [str])	CPU average load limit exceeded
DIAGRAM_USAGE6 [str], pid [uint], has exceeded ram usage limit [uint].[uint]%, now using [uint].[uint]%	Log processor RAM usage has exceeded RAM limit
DIAGMEM_USAGE_TOO_HIGH6 Memory Usage too high. Current Usage is [int]*(0.1%). Memory Usage Threshold is [int]*(0.1%)	Memory usage too high
DIAGMEM_USAGE_TOO_HIGH_RECOVER6 Memory Usage too high recover. Current Usage is [int]*(0.1%). Memory Usage Threshold is [int]*(0.1%)	Memory usage detected as too high
DIAGBUF_USAGE6 [uint] byte buffer usage greater than expected, [uint] used, warning level [uint]	Log buffer usage greater than anticipated

DIAGHEAD_CACHE_USAGE6 socket buffer head cache usage is greater than expected, usage [uint], warning level [uint]	Log head cache usage greater than anticipated
DIAGIP_DEST_USAGE6 IP destination cache usage is greater than expected, usage [uint], warning level [uint]	Log destination cache usage greater than anticipated
DIAGFREE_RAM6 Free RAM, [str]% is less than limit [str]%. Top Memory process: [str]/[uint] using [uint].[uint]% , [str]/[uint] using [uint].[uint]%, [str]/[uint] using [uint].[uint]%	Log RAM space less than limit
DIAGFREE_FLASH_DISK4 Free [str] file system space, [str]% is less than limit [str]%	Log free disk space less than limit
DIAGDISK_USAGE4 Disk usage too high	Log disk usage too high
DIAGNEW_LED_STATE6 LED state message [str] from module [str]	Log LED message from module
DIAGFREE_FLASH_INODES4 [uint] Free INodes on [str] file system is less than limit [uint]	Log INodes less than system limit
DIAGFREE_NVRAM_DISK4 Free [str] file system space, [str]% is less than limit [str]%	Log file system space less than limit
DIAGFREE_NVRAM_INODES4 [uint] Free INodes on [str] file system is less than limit [uint]	Log free INodes on file system less than limit
DIAGFREE_RAM_DISK4 Free [str] file system space, [str]% is less than limit [str]%	Log free file system space less than limit
DIAGFREE_RAM_INODES4 [uint] Free INodes on [str] file system is less than limit [uint]	LOG_FREE_VARFS_INODES
DIAGFD_COUNT4 FD Usage [uint] is over limit [uint]	HUMM
DIAGDISK_USAGE4 Disk usage too high	Log disk utilization usage too high
DIAGNEW_LED_STATE6 LED state message [str] from module [str]]	Log LED state message from module
DIAGLED_IDENTIFY6 LED identify sequence [str]	Log identification sequence
DHCPSVRRELAY_NO_IFACE4 Dhcp relay cannot be allowed on interface [str] as it does not exist	No interface for DHCP relay
DHCPSVRRELAY_IFACE_NO_IP4 Dhcp relay cannot be allowed on interface [str] as it does not have an IP address	No IP address on DHCP relay interface
DHCPSVRRELAY_START6 DHCP relay agent started on [str]	DHCP relay agent started
DHCPSVRRELAY_STOP6 DHCP relay agent stopped	DHCP relay agent stopped
DHCPSVRDHCPSVR_START6 DHCP server is started	DHCP server started
DIAGFAN_UNDERSPEED4 Fan [str] under speed: [uint] RPM is under limit [uint] RPM	Fan speed under set RPM limit
DIAGELAPSED_TIME7 Elapsed time since last diag run appears to be zero	Log elapsed time since last diagnostic run
DIAGAUTOGEN_TECH_SPRT6 Auto generated tech-support dump file [str] [str]	Log generation of tech support dump file

DIAGPOE_INIT_FAIL3 Could not initialize the PoE manager	Log PoE manager intialization failure
DIAGPOE_POWER_LEVEL4 POE power consumption is [uint]W which exceeds [uint]% of [uint]W power budget	Log power consumption exceeds power budget limit
DIAGPOE_READ_FAIL3 Could not read from the PoE	Log PoE read failure
DIAGPOE_STATE_CHANGE4 port [uint] POE state changed to [str]	Log PoE state change
DIAGRAID_DEGRADED4 RAID array is degraded	Log RAID array degraded
DIAGRAID_ERROR4 RAID array management error [uint]	Log RAID array management error
DIAGPWRSPLY_FAIL4 Power supply failure, no longer redundant	Log power supply failure
DIAGHDD_FAILING4 HDD is failing	Log HDD failure
DIAGUNDER_VOLTAGE4 Voltage [str]V under low limit [str]V	Log voltage sensor under low limit
DIAGOVER_VOLTAGE4 Voltage [str]V over high limit [str]V	Log voltage sensor over high limit
DIAGLOW_TEMP6 Temp sensor [str] [str]C under low limit [str]C	Log temperature sensor under low limit
DIAGHIGH_TEMP4 Temp sensor [str] [str]C over high limit [str]C	Log temperature sensor over high limit
DIAGOVER_TEMP0 Temp sensor [str] [str]C over maximum limit [str]C Shutdown switch	Log temperature sensor over max limit
DIAGWD_STATE_CHANGE6 Watchdog is now [str]	Log watchdog state
DOT1X DOT1X_SUCCESS 6 Client [qstr] 802.1x/EAP authentication success on interface [qstr]//802.1x authentication successful	802.1X authentication successful
DOT1X DOT1X_FAILED 5 Client [qstr] failed 802.1x/ EAP authentication on interface [qstr]//802.1x authentication failure	802.1X authentication failed
DOT11COUNTRY_CODE 5 Country of operation configured to [str]	Country of operation configured
DOT11 COUNTRY_CODE_ERROR 1 Error setting country of operation. [str]	Error setting country of operation
DOT11CLIENT_ASSOCIATED 6 Client [qstr] associated to wlan [qstr] ssid [qstr] on radio [qstr]	Client associated event
DOT11CLIENT_DISASSOCIATED 6 Client [qstr] disassociated from wlan [qstr] radio [qstr]: [str] (reason code:[uint])	Client disassociated
DOT11CLIENT_DENIED_ASSOC 5 Client [qstr] denied association on radio [qstr] [str]: [str]	Client denied association
DOT11CLIENT_ASSOC_IGNORED 6 Client [qstr] ignored association on radio [qstr] [str]: [str]	Client ignored association
DOT11WPA_WPA2_SUCCESS 6 Client [qstr] completed [str] handshake on wlan [qstr] radio [qstr]	Client completed WPA/WPA2 handshake

DOT11WPA_WPA2_FAILED 5 Client [qstr] failed [str] handshake on wlan [qstr] radio [qstr]	Client failed WPA/WPA2 handshake
DOT11WPA_WPA2_KEY_ROTN 6 Rotating wpa/wpa2 group keys on wlan [qstr] /	Rotating WPA/WPA2 group keys on WLAN
DOT11TKIP_MIC_FAIL_REPORT 5 TKIP message integrity check failure reported by [mac] on wlan [qstr]	TKIP MIC failure report
DOT11TKIP_MIC_FAILURE 5 TKIP message integrity check failed in packet from [mac] on wlan [qstr]	TKIP MIC check failed
DOT11TKIP_CNTRMEAS_START 4 Initiating TKIP countermeasures on wlan [qstr] ssid [qstr]	TKIP countermeasures initiated
DOT11TKIP_CNTRMEAS_END 4 TKIP countermeasures ended on wlan [qstr] ssid [qstr] //	TKIP countermeasures ended
DOT11EAP_SUCCESS 6 Client [qstr] 802.1x/EAP (type:[str]) authentication success on wlan [qstr] radio [qstr] username [str]	EAP authentication success
DOT11EAP_FAILED 5 Client [qstr] failed 802.1x/EAP authentication on wlan [qstr] radio [qstr]	EAP authentication failure
DOT11EAP_CLIENT_TIMEOUT 5 Client [qstr] timeout attempting 802.1x/EAP authentication on wlan [qstr] radio [qstr]	EAP authentication timed out
DOT11EAP_SERVER_TIMEOUT 5 Radius server [str] timeout authenticating client [qstr] on wlan [qstr] radio [qstr]	RADIUS server timed out
DOT11EAP_CACHED_KEYS 6 Key Cache used for client [qstr] on wlan [qstr] radio [qstr]. Skipping 802.1x	Key cache used for authentication
DOT11EAP_OPP_CACHED_KEYS 6 Opportunistic Key Cache used for client [qstr] on wlan [qstr] radio [qstr]. Skipping 802.1x.	Opportunistic key caching used for authentication
DOT11EAP_PREAUTH_SUCCESS 6 Client [qstr] 802.1x/EAP (type:[str]) pre-authentication success on wlan [qstr] bss [mac]	EAP pre authentication success
DOT11EAP_PREAUTH_FAILED 5 Client [qstr] failed 802.1x/EAP pre-authentication on wlan [qstr] bss [mac]	EAP pre-authentication failed
DOT11EAP_PREAUTH_CLIENT_TIMEOUT 5 Client [qstr] timeout attempting 802.1x/EAP pre-authentication on wlan [qstr]	EAP pre-authentication client timeout detected
DOT11EAP_PREAUTH_SERVER_TIMEOUT 5 Radius server [qstr] timeout pre-authenticating client [qstr] on wlan [qstr]	EAP pre-authentication server timeout detected
DOT11 FT_ROAM_SUCCESS 6 Client [qstr] fast bss transition roam to wlan [qstr] ssid [qstr] on radio [qstr]	Client fast BSS transition roam to WLAN SSD ID on radio
DOT11 GAL_RX_REQUEST 6 Received request to validate [qstr] on global assoc-list [qstr] from [qstr] on rf-domain [qstr]	Received request to validate global association request for RF Domain

DOT11 GAL_TX_RESPONSE 6 Sending global assoc-list [qstr] response for [qstr] to [qstr] on rf-domain [qstr], result: [str]	Sending global association response for RF Domain
DOT11 GAL_VALIDATE_REQ 6 Sending global assoc-list validation request to controller for [qstr]	Sending global association list validation to controller
DOT11 GAL_VALIDATE_FAILED 6 Received global assoc-list validation failure for [qstr]	Received global association list validation failures
DOT11 GAL_VALIDATE_SUCCESS 6 Received global assoc-list validation success for [qstr]	Received global association list validation successes
FWUFWUDONE6Firmware update successful, new version is [str]	Update successfully completed
FWUFWUABORTED6Firmware update aborted	Update aborted
FWUFWUNONEED6Firmware update not required, running and update versions same [str]	Update not required, running and update version are the same
FWUFWUSYSERR3Firmware update unsuccessful, system cmd [str] failed	Update unsuccessful, system cmd failed
FWUFWUBADCONFIG3Firmware update unsuccessful, unable to read configuration file	Update unsuccessful, unable to read config file
FWUFWUSERVERUNDEF3Firmware update unsuccessful, update server undefined	Update unsuccessful, server undefined
FWUFWUFILEUNDEF3Firmware update unsuccessful, update file undefined	Update unsuccessful, update file undefined
FWUFWUSERVERUNREACHABLE3 Firmware update unsuccessful, server [str] unreachable	Update unsuccessful, server unreachable
FWUFWUCOULDNTGETFILE3 Firmware update unsuccessful, couldn't get file, [str] //	Update unsuccessful, could not get file
FWUFWUVERMISMATCH3 Firmware update unsuccessful, version mismatch, expected [str], actual [str] //	Update unsuccessful, version mismatch
FWUFWUPRODMISMATCH3 Firmware update unsuccessful, product mismatch, expected [str], actual [str]	Update unsuccessful, product mismatch
FWUFWUCORRUPTEDFILE3 Firmware update unsuccessful, corrupted firmware file	Update unsuccessful, corrupted file
FWUFWUSIGNMISMATCH3 Firmware update unsuccessful, signature mismatch, [str]	Update unsuccessful, signature mismatch
FWUFWUUNSUPPORTEDHW 3 Firmware update unsuccessful, unsupported hardware	Update unsuccessful, unsupported hardware version
FWU FWUUNSUPPORTEDMODELNUM 3 Firmware update unsuccessful, unsupported FIPS model number	Update unsuccessful, unsupported FIPS model number
ISDN_EMERG 0 Emergency: [str]	ISDN emergency
ISDN_ALERT 1 Alert: [str]	ISDN alert
ISDN_CRIT 2 Critical: [str]	ISDN critical
ISDN_ERR 3 Error: [str]	ISDN error

ISDN_WARNING 4 Warning: [str]	ISDN warning
ISDN_NOTICE 5 Notice: [str]	ISDN notice
ISDN_INFO 6 Info: [str]	ISDN information
ISDN_DEBUG 7 Debug: [str]	ISDN debug
L2TPV3 L2TPV3_TUNNEL_UP 5 L2TPV3 tunnel [str] is UP	L2TPV3 tunnel is up
L2TPV3 L2TPV3_TUNNEL_DOWN 5 L2TPV3 tunnel [str] is DOWN	L2TPV3 tunnel is down
LICMGRLIC_INSTALLED6 [str] license installed	License installation
LICMGRLIC_INSTALL_DEFAULT6 [str] default license installed, count: [int]	Default license installation
LICMGRLIC_INSTALL_COUNT6 [str] license installed, count: [int]	License count
LICMGRLIC_REMOVED6 [str] license removed	License removed
LICMGRLIC_INVALID3 [str] license invalid Error: [str]	License installation failed
MESH MESH_LINK_UP 5 Mesh link up between radio [qstr] and radio [qstr]	Mesh link up
MESH MESH_LINK_DOWN 5 Mesh link down between radio [qstr] and radio [qstr]	Mesh link down
MGMTLOG_KEY_DELETED 4 Rsakey [str] associated with ssh is deleted so ssh is restarted with default rsa key	RSA key associated with SSH is deleted
MGMTLOG_KEY_RESTORED6Rsakey [str] associated with ssh is added so ssh is restarted with new key	RSA key associated with SSH is added
MGMTLOG_TRUSTPOINT_DELETED4 Trustpoint [str] associated with https is deleted or expired so https is restarted with default trustpoint	Trustpoint associated with HTTPS is deleted
MGMTLOG_HTTP_START5 [str] started in external mode	Web server started in external mode
MGMTLOG_HTTP_LOCAL_START5 thttpd started in localhost mode	Web server started in local mode
MGMTLOG_HTTPS_START5 stunnel started	Secure Web server started
MGMTLOG_HTTPS_WAIT5 waiting for thttpd to start	Waiting for Web server to start
MGMTLOG_HTTP_INIT5[str] status started is [uint] and external mode is [uint]	Web server started
MESH MESHPOINT_LOOP_PREVENT_ON 4 Meshpoint [qstr] loop prevention on (port [str]), wired traffic is blocked	Wired traffic is blocked
MESH MESHPOINT_LOOP_PREVENT_OFF 4 Meshpoint loop prevention off (port [str]), all wired traffic is allowed	Wired traffic is allowed
MESH MESHPOINT_ROOT_CHANGE 6 Meshpoint [qstr] root changed from [mac] to [mac] via next hop [mac]	Meshpoint root changed

MESH MESHPOINT_PATH_CHANGE 6 Meshpoint [qstr] next hop changed from [mac] to [mac] for [mac]	Meshpoint next hop changed
NSM IFUP4 Interface [str] is up	Interface up
NSM IFDOWN4 Interface [str] is down	Interface down
NSM DHCPIP6 Interface [str] acquired IP address [ip]/[uint] via DHC	Interface assigned DHCP IP address
NSM DHCPDEFRT6 Default route with gateway [ip] learnt via DHC	Default route learnt via DHCP
NSM DHCPIPCHG5 Interface [str] changed DHCP IP - old IP: [ip]/[uint], new IP: [ip]/[uint]	DHCP Interface IP changed
NSM DHCPNODEFRT5 Interface [str] lost its DHCP default route	Interface no default route
NSM IFIPCFG3 Interface [str] IP address [str] Interface [str]	Interface IP address
NSM DHCPC_ERR3 Both, DHCP client and server are configured for interface [str]. DHCP Client has been enabled on the interface and dhcp server is shut down	DHCP server-client config conflict
NSM DHCPIPNOADD5 Interface [str] lost its DHCP IP address to interface [str]'s overlapping static configured IP address	DHCP IP overlaps static IP address
NSM DHCPLSEXP5 Interface [str] lost its DHCP IP address [ip] due to lease expiration	Interace DHCP lease expired
NSM DHCPNAK5 Interface [str] lost its DHCP IP address [ip], DHCP NAK response from server	DHCP Server returned DHCP NAK response
NSM NSM_NTP6 Look up host [str] [str]//	Translate host name
NSM IF_FAILOVER5 Interface [str] failover to Interface [str]	Interface failover
NSM IF_FAILBACK5 Interface [str] failback to Interface [str]	Interface failback
PM PROCSTART6 Starting process [str]	Process started
PM PROCRSTRT3 Process str]"is not responding. Restarting process	Process restarted
PM PROCMAXRSTRT1 Process [str] reached its maximum number of allowed restarts	Process reached max number of restarts
PM PROCSYSRSTRT0 Process [str] reached its maximum number of allowed restarts. Rebooting the system.	Process reached max restarts. Rebooting system.
PM PROCSTOP5 Process [str] has been stopped	Process has been stopped
PM PROCID5 Process [str] changed its PID from [int] to [int]	Process changed PID
PM STARTUPCOMPLETE5 System startup complete	System startup completed
PM PROCNORESP4Process [str] is not responding ([uint]/[uint])	Process is not responding

RADCONFRADIUSDSTART6 Radius Server Started	RADIUS server started
RADCONFRADIUSDSTOP6 Radius Server Stopped	RADIUS server stopped
RADCONF COULD_NOT_STOP_RADIUSD3 radiusd could not be stopped	RADIUS server failed to stop
RADIORADIO_STATE_CHANGE 5 Radio [qstr] changing state from [qstr] to [qstr]	Radio state changed
RADIORADAR_SCAN_STARTED 6 Radar scan on primary channel [uint] freq [uint] MHz for a duration [uint] secs on radio [qstr]	Radar scan started
RADIORADAR_SCAN_COMPLETED 6 Radar scan done on primary channel [uint] freq [uint] MHz on radio [qstr]	Radar scan completed
RADIORADAR_DETECTED 4 Radar found on channel [uint] freq [uint] MHz	Radar detected
RADIORADAR_DET_INFO 4 Radar info: Radio: [qstr]. New channel: [uint] freq [uint] MHz. Scan time: [uint] secs	Radar info
RADIORESUME_HOME_CHANNEL 6 Operation on home channel [uint] freq [uint] MHz resumes on radio [qstr] after earlier radar detect	Radio resuming on home channel
RADIO ACS_SCAN_STARTED 6 ACS scan started on radio [qstr]	ACS scan started
RADIO ACS_SCAN_COMPLETE 6 ACS scan done, channel [uint] selected on radio [qstr]	ACS scan complete
RADIO_ANTENNA_ERROR 3 antenna type [str] in is not supported on radio [uint] of device [str]	Invalid (unsupported) antenna detected on this radio
RADIOCHANNEL_COUNTRY_MISMATCH3 Channel [str] not valid in country of operation [str] for [str] [str]	Channel and country of operation mismatch
SYSTEM HTTP_ERR3 [str] did not start	Web server did not start
SYSTEMLOGIN_FAIL_BAD_ROLE3 Log-in failed - [qstr] is an undefined user role - user [qstr] from [qstr]	Failed login attempt - no such user role
SYSTEMLOGOUT6 Logged out user [qstr] with privilege [qstr] from [qstr]	Logout event
SYSTEMWARM_START6 System Warm Start Reason : [str] Timestamp: [str]	System warm start
SYSTEMWARM_START_RECOVER6 Warm Start Recover. Reason: [str] Timestamp: [str]	System wam start recovery
SYSTEMCOLD_START6 System Cold start. System came up at [str]	System cold start
SYSTEMSERVER_UNREACHABLE5 Server not reachable, trying authentication using local database.	Authentication using the local database
SYSTEMPERIODIC_HEART_BEAT3Periodic Heart Beat. Interval:[int]. Ip address [str].	Periodic heartbeat detected

SYSTEMCONFIG_COMMIT6Configuration commit by user [qstr] ([str]) from [qstr]	Configuration commit
SYSTEMCONFIG_REVISION6Configuration revision updated to [str] from [str]	Configuration updated
SYSTEMSYSTEM_AUTOUP_ENABLE6 Autoupgrade enabled for [str]	Auto upgrade module is enabled
SYSTEMSYSTEM_AUTOUP_DISABLE6 Autoupgrade disabled for [str]	Auto upgrade module is disabled
SYSTEMMAAT_LIGHT5MAAT Light module [str]	Notice on action on RIM radio(s) from Maat Light module
SYSTEMDEVUP_RFD_FAIL4Upgrade failed on mac [str] in RF domain [str]	Upgrade for device failed on rf-domain manager
SMTPNOT SMTPAUTH5 Authentication failure for user: [str] on server [str].//	User authentication failure
SMTPNOT NET 5 Network error contacting server: [str].	Cannot contact server
SMTPNOT SMTPINFO6[str].	SMTP information notice
SMTPNOT CFG5 Error reading configuration file.	Cannot read configuration
SMTPNOT CFGINC5 Incomplete Configuration.	Incomplete configuration
SMTPNOT SMTPERR5 [str].	SMTP 5XX errors
SMTPNOT PROTO5Protocol Error: [str].	SMTP protocol errors
SYSTEMPROC_STOP6 Stopping process [qstr]	Stopping process
SYSTEMCLOCK_RESET6 System clock reset, Time: [str]	System clock reset
SYSTEMLOGIN5 Successfully logged in user [qstr] with privilege [qstr] from [qstr]	Successful login
SYSTEMLOGIN_FAIL3 Log-in failed for user [qstr] from [qstr]	Failed login attempt - user authentication failed
SYSTEMLOGIN_FAIL_ACCESS3 Log-in failed - user [qstr] is not allowed access from [qstr]	Failed login attempt - access violation
VRRP VRRP_STATE_CHANGE 5 [str]: VRRP Group [uint] transitioned to [str] state	VRRP state transition
VRRP VRRP_VIP_SUBNET_MISMATCH 2 VRRP Group [uint] VIP [ip] does not overlap with any of the interface addresses	VRRP IP not overlapping with interface addresses
VRRP VRRP_MONITOR_CHANGE 5 [str]: VRRP Group [uint] monitored [str] state change to [str]; priority change from [uint] to [uint]	VRRP monitor link state change
WIPSUNSANCTIONED_AP_ACTIVE 6 Unsanctioned AP [mac] vendor [str] on channel [int] with rssi [int] active from [str]	Unsanctioned AP active
WIPSUNSANCTIONED_AP_INACTIVE 6 Unsanctioned AP [mac] vendor [str] inactive from [str]	Unsanctioned AP inactive

WIPSUNSANCTIONED_AP_STATUS_CHANGE 6 Unsanctioned AP [mac] vendor [str] status has been administratively changed	Unsanctioned AP changed state
WIPSROGUE_AP_ACTIVE 4 Rogue AP [mac] vendor [str] on channel [int] with vlan [int] and rssi [int] active from [str] //	Rogue AP active
WIPSROGUE_AP_INACTIVE 4 Rogue AP [mac] vendor [str] inactive from [str]	Rogue AP inactive
WIPSAIR_TERMINATION_INITIATED 4 Air termination of [mac] vendor [str] on channel [int] initiated	Air termination initiated
WIPSAIR_TERMINATION_ENDED 4 Air termination of [mac] vendor [str] ended	Air termination ended

A Publicly Available Software

A.1 General Information

This document contains information regarding licenses, acknowledgments and required copyright notices for open source packages used in the following products:

Access Points

- AP6521, AP6522, AP6522M, AP6532, AP6562, AP7161, AP7502, AP7522, AP7532, AP7562, AP8122, AP8132, AP8163, AP8232, AP8432 and AP8533.

Wireless Controllers and Service Platforms

- Wireless Controllers – RFS4000, RFS6000
- Service Platforms – NX5500, NX5500E, NX7500, NX75XX, NX7510E, NX9500, NX9510, NX9600, NX9610, VX9000, VX9000E

A.2 Open Source Software Used

The Support site, located at www.extremenetworks.com/support provides information and online assistance including developer tools, software downloads, product manuals, support contact information and online repair requests.

Name	Version	URL	License
Apache Web Server	1.3.41	*http://www.apache.org/*	*Apache License, Version 2.0*
Asterisk	1.2.24	*http://www.asterisk.org/*	*GNU General Public License 2.0*
accepts	1.2.10	*http://registry.npmjs.org/accepts/-/accepts-1.2.10.tgz*	*MIT License*
advas	0.2.3	*http://advas.sourceforge.net/*	*GNU General Public License, version 2*
alivepdf	0.1.4.9	*https://code.google.com/p/alivepdf/*	*MIT License*
apscheduler	3.0.1	*https://pypi.python.org/pypi/APScheduler/*	*MIT License*
async	1.3.0	*http://registry.npmjs.org/async/-/async-1.3.0.tgz*	*MIT License*
autoconf	2.69	*http://www.gnu.org/software/autoconf/*	*GNU General Public License, version 2*
automake	1.11.6	*http://www.gnu.org/software/automake/*	*GNU General Public License, version 2*
bash	4.2	*http://www.gnu.org/software/bash/*	*GNU General Public License, version 2*
binutils	2.23	*http://www.gnu.org/software/binutils/*	*GNU General Public License, version 2*

Name	Version	URL	License
bison	2.3	*http://www.gnu.org/software/bison/*	*GNU General Public License, version 2*
bluez	5.7	*http://www.bluez.org/*	*GNU General Public License, version 2*
body-parser	1.13.2	*http://registry.npmjs.org/body-parser/-/body-parser-1.13.2.tgz*	*MIT License*
bridge	1.0.4	*http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge/*	*GNU General Public License, version 2*
bridge-utils	1.0.4	*http://sourceforge.net/projects/bridge/*	*GNU General Public License, version 2*
buffer-crc32	0.2.5	*http://registry.npmjs.org/buffer-crc32/-/buffer-crc32-0.2.5.tgz*	*MIT License*
busybox	1.14.4	*http://www.busybox.net/*	*GNU General Public License, version 2*
bytes	2.1.0	*http://registry.npmjs.org/bytes/-/bytes-2.1.0.tgz*	*MIT License*
colors	1.1.2	*http://registry.npmjs.org/colors/-/colors-1.1.2.tgz*	*MIT License*
compression	1.5.1	*http://registry.npmjs.org/compression/-/compression-1.5.1.tgz*	*MIT License*
conect-mongo	0.8.2	*http://registry.npmjs.org/connect-mongo/-/connect-mongo-0.8.2.tgz*	*MIT License*
cookie	0.1.3	*http://registry.npmjs.org/cookie/-/cookie-0.1.3.tgz*	*MIT License*
cookie-parser	1.3.5	*http://registry.npmjs.org/cookie-parser/-/cookie-parser-1.3.5.tgz*	*MIT License*
cookie-signature	1.0.6	*http://registry.npmjs.org/cookie-signature/-/cookie-signature-1.0.6.tgz*	*MIT License*
cuint	0.2.0	*http://registry.npmjs.org/cuint/-/cuint-0.2.0.tgz*	*MIT License*
cycle	1.0.3	*https://registry.npmjs.org/cycle/-/cycle-1.0.3.tgz*	*MIT License*
czjson	1.0.8	*https://pypi.python.org/pypi/czjson/1.0.8*	*GNU Lesser General Public License 2.1*
dash	0.5.7	*http://gondor.apana.org.au/~herbert/dash/*	*The BSD License*
debug	2.2.0	*https://registry.npmjs.org/debug/-/debug-2.2.0.tgz*	*MIT License*
depd	1.0.1	*http://registry.npmjs.org/depd/-/depd-1.0.1.tgz*	*MIT License*
dfu-util	0.8	*http://dfu-util.gnumonks.org/*	*GNU General Public License, version 2*
dhcp	3.0.3	*http://www.isc.org/software/dhcp*	*ISC License*

Name	Version	URL	License
diffutils	2.8.1	*http://www.gnu.org/software/diffutils/*	*GNU General Public License, version 2*
dmalloc	5.5.2	*http://dmalloc.com/*	None
dmidecode	2.11	*http://savannah.nongnu.org/projects/dmidecode/*	*GNU General Public License, version 2*
dnsmasq	2.47	*http://www.thekelleys.org.uk/dnsmasq/doc.html*	*GNU General Public License, version 2*
dosfstools	2.11	*http://www.daniel-baumann.ch/software/dosfstools/*	*GNU General Public License, version 2*
dropbear	0.55	*http://matt.ucc.asn.au/dropbear/dropbear.html*	*DropBear License*
e2fsprogs	1.41.13	*http://e2fsprogs.sourceforge.net/*	*GNU General Public License, version 2*
ejs	2.3.3	*http://registry.npmjs.org/ejs/-/ejs-2.3.3.tgz*	*Apache License, Version 2.0*
engine.io	1.5.2	*http://registry.npmjs.org/engine.io/-/engine.io-1.5.2.tgz*	*MIT License*
escape-html	1.0.2	*http://registry.npmjs.org/escape-html/-/escape-html-1.0.2.tgz*	*MIT License*
ethtool	2.6.35	*http://www.kernel.org/pub/software/network/ethtool/*	*GNU General Public License, version 2*
event-loop-lag	1.1.0	*http://registry.npmjs.org/event-loop-lag/-/event-loop-lag-1.1.0.tgz*	*MIT License*
express	4.13.1	*http://registry.npmjs.org/express/-/express-4.13.1.tgz*	*MIT License*
express-session	1.11.3	*http://registry.npmjs.org/express-session/-/express-session-1.11.3.tgz*	*MIT License*
eyes	0.1.8	*http://github.com/cloudhead/eyes.js*	*MIT License*
finalhandler	0.4.0	*http://registry.npmjs.org/finalhandler/-/finalhandler-0.4.0.tgz*	*MIT License*
flashrom	0.9.4	*http://flashrom.org/Flashrom*	*GNU General Public License, version 2*
flex	4.5.1.21328	*http://flex.sourceforge.net/*	*The BSD License*
fluks	0.2	*https://github.com/markuspeloquin/fluks*	*MIT License*
freedos	4.5.1.21328	*http://www.freedos.org/download/*	*GNU General Public License, version 2*
freeipmi	1.1	*http://www.gnu.org/software/freeipmi/*	*GNU General Public License, version 3*
fresh	0.3.0	*http://registry.npmjs.org/fresh/-/fresh-0.3.0.tgz*	*MIT License*
futures	2.2.0	*https://github.com/agronholm/pythonfutures*	*The BSD License*

Name	Version	URL	License
gcc	4.1.2	*http://gcc.gnu.org/*	*GNU General Public License, version 2*
gdb	7.2	*http://www.gnu.org/software/gdb/*	*GNU General Public License, version 3*
gdbm	1.8.3	*http://www.gnu.org/s/gdbm/*	*GNU General Public License, version 2*
genext2fs	1.4.1	*http://genext2fs.sourceforge.net/*	*GNU General Public License, version 2*
glib2	2.30.2	*http://www.gtk.org/*	*GNU Lesser General Public License 2.1*
glibc	2.7	*http://www.gnu.org/software/libc/*	*GNU General Public License, version 2*
has-binary-data	0.1.5	*http://registry.npmjs.org/has-binary-data/-/has-binary-data-0.1.5.tgz*	*MIT License*
hdparm	9.38	*http://sourceforge.net/projects/hdparm/*	*GNU General Public License, version 2*
hooks	0.3.2	*http://registry.npmjs.org/hooks/-/hooks-0.3.2.tgz*	*MIT License*
hostapd	0.6.9	*http://hostap.epitest.fi/hostapd/*	*GNU General Public License, version 2*
hotplug	1.3	*http://sourceforge.net/projects/linux-hotplug/*	*GNU General Public License, version 2*
hotplug2	0.9	*http://isteve.bofh.cz/~isteve/hotplug2/*	*GNU General Public License, version 2*
i2ctools	3.0.3	*http://www.lm-sensors.org/wiki/I2CTools*	*GNU General Public License, version 2*
iconv-lite	0.4.11	*http://registry.npmjs.org/iconv-lite/-/iconv-lite-0.4.11.tgz*	*MIT License*
igb	5.2.9.4	*http://sourceforge.net/projects/e1000/*	*GNU General Public License, version 2*
ipaddr	2.1.0	*http://code.google.com/p/ipaddr-py/*	*Apache License, Version 2.0*
ipkg-utils	1.7	*http://www.handhelds.org/sources.html*	*GNU General Public License, version 2*
ipmitool	1.8.11	*http://ipmitool.sourceforge.net/*	*The BSD License*
iproute2	050816	*http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2*	*GNU General Public License, version 2*
iptables	1.4.3	*http://www.netfilter.org/projects/iptables/index.html*	*GNU General Public License, version 2*

Name	Version	URL	License
ipxe	1.0.0	*http://ipxe.org/*	*GNU General Public License, version 2*
isstream	0.1.2	*https://registry.npmjs.org/isstream/-/isstream-0.1.2.tgz*	*MIT License*
js-yaml	3.3.1	*http://registry.npmjs.org/js-yaml/-/js-yaml-3.3.1.tgz*	*MIT License*
kerberos	None	*http://web.mit.edu/Kerberos/*	*GNU General Public License, version 2*
kexec-tools	2.0.3	*http://kernel.org/pub/linux/utils/kernel/kexec/*	*GNU General Public License, version 2*
libbson	1.1.0	*http://github.com/mongodb/libbson*	*Apache License, Version 2.0*
libcares	1.7.1	*http://c-ares.haxx.se/*	*The BSD License*
libcurl	7.30.0	*http://curl.haxx.se/libcurl/*	*The BSD License*
libdevmapper	2.02.66	*ftp://sources.redhat.com/pub/lvm2/old*	*GNU Lesser General Public License 2.1*
libexpat	2.0.0	*http://expat.sourceforge.net/*	*MIT License*
libffi	3.0.7	*http://sourceware.org/libffi/*	*MIT License*
libgcrypt	1.4.5	*ftp://ftp.gnupg.org/GnuPG/libgcrypt/*	*GNU Lesser General Public License 2.1*
libgmp	4.2.2	*http://gmplib.org/*	*GNU Lesser General Public License, version 3.0*
libgnutls	3.2.12	*ftp://ftp.gnupg.org/GnuPG/gnutls/v3.0/*	*GNU Lesser General Public License, version 3.0*
libgpg-error	1.6	*ftp://ftp.gnupg.org/GnuPG/libgpg-error/*	*GNU Lesser General Public License 2.1*
libharu	2.1.0	*http://libharu.org/*	*MIT License*
libhttp-parser	None	*None*	*MIT License*
libiconv	1.14	*http://savannah.gnu.org/projects/libiconv/*	*GNU General Public License 2.0*
libjson	0.10	*http://sourceforge.net/projects/libjson/*	*The BSD License*
libkerberos	0.1	*http://web.mit.edu/kerberos/dist/*	*The BSD License*
libncurses	5.4	*http://www.gnu.org/software/ncurses/*	*MIT License*
libnettle	2.7	*http://www.lysator.liu.se/~nisse/nettle/*	*GNU Lesser General Public License 2.1*
libnuma	2.0.10	*https://github.com/numactl/numactl/*	*GNU Lesser General Public License, version 2.0*
libpam	1.1.1	*http://www.kernel.org/pub/linux/libs/pam/*	*The BSD License*

Name	Version	URL	License
libpcap	1.0.0	*http://www.tcpdump.org/*	*The BSD License*
libpcre	8.21	*ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/*	*The BSD License*
libpopt	1.14	*http://freecode.com/projects/popt*	*MIT License*
libraryopt	1.01	*http://sourceforge.net/projects/libraryopt/*	*GNU General Public License, version 2*
libreadline	4.3	*http://cnswww.cns.cwru.edu/php/chet/readline/rltop.html*	*GNU General Public License, version 2*
libtool	2.4.2	*http://www.gnu.org/software/libtool/*	*GNU General Public License, version 2*
libusb	0.1.12	*http://www.libusb.org/*	*GNU Lesser General Public License, version 2.0*
libusb	1.0.18	*http://www.libusb.org/*	*GNU Lesser General Public License, version 2.0*
libvirt	0.9.11	*http://libvirt.org/sources/*	*GNU Lesser General Public License 2.1*
libxml2	2.8.0	*http://xmlsoft.org/*	*MIT License*
libxslt	1.1.26	*http://xmlsoft.org/xslt/*	*MIT License*
lighttpd	1.4.37	*http://www.lighttpd.net/*	*MIT License*
lilo	22.6	*http://lilo.alioth.debian.org/*	*The BSD License*
linux	2.6.28.9	*http://www.kernel.org/*	*GNU General Public License, version 2*
linux	2.6.35.9	*http://www.kernel.org/*	*GNU General Public License, version 2*
lodash	3.10.0	*http://registry.npmjs.org/lodash/-/lodash-3.10.0.tgz*	*MIT License*
log-timestamp	0.1.2	*http://registry.npmjs.org/log-timestamp/-/log-timestamp-0.1.2.tgz*	*MIT License*
ltp	20130904	*https://github.com/linux-test-project/ltp*	*GNU General Public License, version 2*
lxml	2.3beta1	*http://lxml.de/*	*The BSD License*
lzma	4.32	*http://www.7-zip.org/sdk.html*	*GNU Lesser General Public License, version 2.0*
lzma	4.57	*http://www.7-zip.org/sdk.html*	*GNU Lesser General Public License, version 2.0*
lzo	2.03	*http://www.oberhumer.com/opensource/lzo/*	*GNU General Public License, version 2*

Name	Version	URL	License
M2Crypto	0.21.1	*http://chandlerproject.org/bin/view/Projects/MeTooCrypto*	*The BSD License*
m4	1.4.16	*http://www.gnu.org/software/m4/*	*GNU General Public License, version 2*
madwifi	trunk-r3314	*http://madwifi-project.org/*	*The BSD License*
mdadm	3.2.2	*http://neil.brown.name/blog/mdadm*	*GNU General Public License, version 2*
media-typer	0.3.0	*http://registry.npmjs.org/media-typer/-/media-typer-0.3.0.tgz*	*MIT License*
memtester	4.0.8	*http://pyropus.ca/software/memtester/*	*GNU General Public License, version 2*
merge-descriptors	1.0.0	*http://registry.npmjs.org/merge-descriptors/-/merge-descriptors-1.0.0.tgz*	*MIT License*
method-override	2.3.4	*http://registry.npmjs.org/method-override/-/method-override-2.3.4.tgz*	*MIT License*
methods	1.1.1	*http://registry.npmjs.org/methods/-/methods-1.1.1.tgz*	*MIT License*
mii-diag	2.09	*http://freecode.com/projects/mii-diag*	*GNU General Public License, version 2*
mkyaffs	None	*http://www.yaffs.net/*	*GNU General Public License, version 2*
mod_ssl	2.8.3.1-1.3.41	*http://www.modssl.org/*	*The BSD License*
mongo-c-driver	1.1.0	*http://github.com/mongodb/mongo-c-driver*	*Apache License, Version 2.0*
mongo-python-driver	2.7.1	*http://github.com/mongodb/mongo-python-driver*	*Apache License, Version 2.0*
mongodb	3.0.5	*http://www.mongodb.org/*	*GNU Lesser General Public License, version 3.0*
mongoose	4.0.7	*http://registry.npmjs.org/mongoose/-/mongoose-4.0.7.tgz*	*MIT License*
mpath	0.2.1	*http://registry.npmjs.org/mpath/-/mpath-0.2.1.tgz*	*MIT License*
mpromise	0.5.5	*http://registry.npmjs.org/mpromise/-/mpromise-0.5.5.tgz*	*MIT License*
mquery	1.6.2	*http://registry.npmjs.org/mquery/-/mquery-1.6.2.tgz*	*MIT License*
ms	0.7.1	*http://registry.npmjs.org/ms/-/ms-0.7.1.tgz*	*MIT License*
mtd	2009-05-05	*http://www.linux-mtd.infradead.org/*	*GNU General Public License, version 2*
mtd-utils	1.4.4	*http://www.linux-mtd.infradead.org/*	*GNU General Public License, version 2*

Name	Version	URL	License
mtd-utils	2009-05-05	*http://www.linux-mtd.infradead.org/*	*GNU General Public License, version 2*
muri	1.1.0	*http://registry.npmjs.org/muri/-/muri-1.1.0.tgz*	*MIT License*
nano	1.2.4	*http://www.nano-editor.org/*	*GNU General Public License, version 2*
net-snmp	5.3.0.1	*http://net-snmp.sourceforge.net/*	*The BSD License*
no-vnc	None	*http://kanaka.github.io/noVNC/*	*Mozilla Public License, version 2*
node-mongodb-native	1.4.35	*http://github.com/mongodb/node-mongodb-native*	*Apache License, Version 2.0*
node.js	0.12.7	*http://nodejs.org/*	*MIT License*
ntp	4.2.6p4	*http://www.ntp.org/index.html*	*The BSD License*
numactl	2.0.10	*https://github.com/numactl/numactl/*	*GNU General Public License, version 2*
Open Scales	2.2	*http://openscales.org/*	*GNU Lesser General Public License, version 3.0*
OpenStreetMap		*http://www.openstreetmap.org/*	*Creative Commons Attribution-ShareAlike License, version 3.0*
on-headers	1.0.0	*http://registry.npmjs.org/on-headers/-/on-headers-1.0.0.tgz*	*MIT License*
openldap	2.4.40	*http://www.openldap.org/foundation/*	*The Open LDAP Public License*
openllpd	0.0.3alpha	*http://openlldp.sourceforge.net/*	*GNU General Public License, version 2*
openssh	6.6p1	*http://www.openssh.com/*	*The BSD License*
openssl	0.9.8zg	*http://www.openssl.org/*	*OpenSSL License*
openssl	1.0.0i	*http://www.openssl.org/*	*OpenSSL License*
openssl	1.0.1g	*http://www.openssl.org/*	*OpenSSL License*
openssl-fips	1.2.3	*http://www.openssl.org/*	*OpenSSL License*
openwrt	trunk-r15025	*http://www.openwrt.org/*	*GNU General Public License, version 2*
opkg	trunk-r4564	*http://code.google.com/p/opkg/*	*GNU General Public License, version 2*
oprofile	0.9.2	*http://oprofile.sourceforge.net/news/*	*GNU Lesser General Public License 2.1*

Name	Version	URL	License
ProGuard	4.8	*http://proguard.sourceforge.net/*	*GNU General Public License, version 2*
PyPDF2	1.23	*http://mstamy2.github.com/PyPDF2*	*The BSD License*
parseurl	1.3.0	*http://registry.npmjs.org/parseurl/-/parseurl-1.3.0.tgz*	*MIT License*
path-to-regexp	1.2.0	*http://registry.npmjs.org/path-to-regexp/-/path-to-regexp-1.2.0.tgz*	*MIT License*
pciutils	3.1.8	*http://mj.ucw.cz/sw/pciutils/*	*GNU General Public License, version 2*
pdnsd	1.2.5	*http://members.home.nl/p.a.rombouts/pdnsd/*	*GNU General Public License, version 2*
picocom	1.6	*http://code.google.com/p/picocom/*	*GNU General Public License, version 2*
pillow	2.8.1	*http://python-pillow.github.io/*	*MIT License*
ping	1.0	*None*	*The BSD License*
pkg-config	0.22	*http://pkg-config.freedesktop.org/wiki/*	*GNU General Public License, version 2*
portmap	6.0	*http://neil.brown.name/portmap/*	*The BSD License*
posix	2.0.1	*http://registry.npmjs.org/posix/-/posix-2.0.1.tgz*	*MIT License*
ppp	2.4.5	*http://ppp.samba.org/ppp/*	*The BSD License*
ppp	2.4.3	*http://ppp.samba.org/ppp/*	*The BSD License*
preppy	2.3.1	*https://bitbucket.org/rptlab/preppy*	*The BSD License*
procname	0.2	*http://code.google.com/p/procname/*	*GNU Lesser General Public License, version 2.0*
procps	3.2.8	*http://procps.sourceforge.net/*	*GNU General Public License, version 2*
proxy-addr	1.0.8	*http://registry.npmjs.org/proxy-addr/-/proxy-addr-1.0.8.tgz*	*MIT License*
psmisc	22.8	*http://sourceforge.net/projects/psmisc/*	*GNU General Public License, version 2*
pure-ftpd	1.0.22	*http://www.pureftpd.org/project/pure-ftpd*	*The BSD License*
pychecker	0.8.18	*http://pychecker.sourceforge.net/*	*The BSD License*
pyparsing	1.5.1	*http://sourceforge.net/projects/pyparsing/*	*The BSD License*
pytz	2014.10	*http://pythonhosted.org/pytz*	*MIT License*
pyxapi	0.1	*http://www.pps.jussieu.fr/%7Eylg/PyXAPI/*	*GNU General Public License, version 2*

Name	Version	URL	License
pyyaml	3.11	*http://pyyaml.org/*	*MIT License*
qdbm	1.8.77	*http://qdbm.sourceforge.net/*	*GNU General Public License, version 2*
qs	4.0.0	*http://registry.npmjs.org/qs/-/qs-4.0.0.tgz*	*The BSD License*
quagga	0.99.16	*http://www.quagga.net*	*GNU General Public License, version 2*
quilt	0.47	*http://savannah.nongnu.org/projects/quilt/*	*GNU General Public License, version 2*
radius	2.2.3	*http://freeradius.org/*	*GNU General Public License, version 2*
range-parser	1.0.2	*http://registry.npmjs.org/range-parser/-/range-parser-1.0.2.tgz*	*MIT License*
raw-body	2.1.2	*http://registry.npmjs.org/raw-body/-/raw-body-2.1.2.tgz*	*MIT License*
redis	3.0.3	*http://redis.io/*	*The BSD License*
redis	0.12.1	*http://registry.npmjs.org/redis/-/redis-0.12.1.tgz*	*MIT License*
regexp-clone	0.0.1	*http://registry.npmjs.org/regexp-clone/-/regexp-clone-0.0.1.tgz*	*MIT License*
report-lab	3.1.44	*http://www.reportlab.com*	*The BSD License*
rp-pppoe	3.1.0	*http://www.roaringpenguin.com/products/pppoe*	*GNU General Public License, version 2*
rsync	3.0.6	*http://rsync.samba.org/*	*GNU General Public License, version 3*
safestr	1.0.3	*http://www.zork.org/*	*The BSD License*
samba	3.5.1	*http://www.samba.org*	*GNU General Public License, version 3*
sed	4.1.2	*http://www.gnu.org/software/sed/*	*GNU General Public License, version 2*
semaphore	1.0.3	*http://registry.npmjs.org/semaphore/-/semaphore-1.0.3.tgz*	*MIT License*
send	0.13.0	*http://registry.npmjs.org/send/-/send-0.13.0.tgz*	*MIT License*
serve-static	1.10.0	*http://registry.npmjs.org/serve-static/-/serve-static-1.10.0.tgz*	*MIT License*
setproctitle	1.1.8	*http://code.google.com/p/py-setproctitle*	*The BSD License*
setuptools	11.3.1	*https://bitbucket.org/pypa/setuptools*	*Python License, Version 2 (Python-2.0)*

Name	Version	URL	License
sliced	1.0.1	*http://registry.npmjs.org/sliced/-/sliced-1.0.1.tgz*	*MIT License*
smarttools	6.2	*http://smartmontools.sourceforge.net*	*GNU General Public License, version 2*
snmpagent	5.0.9	*http://sourceforge.net/*	*The BSD License*
socket.io	1.3.6	*http://registry.npmjs.org/socket.io/-/socket.io-1.3.6.tgz*	*MIT License*
socket.io-adapter	0.3.1	*http://registry.npmjs.org/socket.io-adapter/-/socket.io-adapter-0.3.1.tgz*	*MIT License*
socket.io-adapter-mongo	0.1.4	*http://registry.npmjs.org/socket.io-adapter-mongo/-/socket.io-adapter-mongo-0.1.4.tgz*	*MIT License*
socket.io-client	1.3.6	*http://registry.npmjs.org/socket.io-client/-/socket.io-client-1.3.6.tgz*	*MIT License*
socket.io-parser	2.2.4	*http://registry.npmjs.org/socket.io-parser/-/socket.io-parser-2.2.4.tgz*	*MIT License*
sqlite3	3070900	*http://www.sqlite.org/*	*None*
squashfs	3.0	*http://squashfs.sourceforge.net/*	*GNU General Public License, version 2*
squid	2.7.STABLE9	*http://www.squid-cache.org/*	*GNU General Public License, version 2*
stack-trace	0.0.9	*https://registry.npmjs.org/stack-trace/-/stack-trace-0.0.9.tgz*	*MIT License*
stackless python	2.7.5	*http://www.stackless.com/*	*GNU General Public License, version 2*
sticky-session	0.1.0	*http://registry.npmjs.org/sticky-session/-/sticky-session-0.1.0.tgz*	*MIT License*
strace	4.5.20	*http://sourceforge.net/projects/strace/*	*The BSD License*
stress	1.0.4	*http://people.seas.harvard.edu/~apw/stress/*	*GNU General Public License, version 2*
strongswan	4.4.0	*http://www.strongswan.org*	*GNU General Public License, version 2*
stunnel	4.31	*http://www.stunnel.org/*	*GNU General Public License, version 2*
svg2rlg	0.3	*http://code.google.com/p/svg2rlg/*	*The BSD License*
sysstat	9.0.5	*http://sebastien.godard.pagesperso-orange.fr/*	*GNU General Public License, version 2*
tar	1.17	*http://www.gnu.org/software/tar/*	*GNU General Public License, version 2*
tcpdump	4.0.0	*http://www.tcpdump.org/*	*The BSD License*

Name	Version	URL	License
tinyproxy	1.8.3	*https://banu.com/tinyproxy/*	*GNU General Public License, version 2*
type-is	1.6.4	*http://registry.npmjs.org/type-is/-/type-is-1.6.4.tgz*	*MIT License*
tz	2014b	*http://www.iana.org/time-zones/repository/releases/*	*GNU General Public License, version 2*
u-boot	trunk-2010-03-30	*http://www.denx.de/wiki/U-Boot/*	*GNU General Public License, version 2*
u-boot	trunk-2010-05-10	*http://www.denx.de/wiki/U-Boot/*	*GNU General Public License, version 2*
uClibc	0.9.29	*http://www.uclibc.org/*	*GNU General Public License, version 2*
uClibc	0.9.30.2	*http://www.uclibc.org/*	*GNU General Public License, version 2*
uci	0.7.5	*http://www.openwrt.org/*	*GNU General Public License, version 2*
udev	147	*https://launchpad.net/udev*	*GNU General Public License, version 2*
udev	r147	*http://www.kernel.org/pub/linux/utils/kernel/hotplug/*	*GNU General Public License, version 2*
usbutils	0.73	*http://www.linux-usb.org/*	*GNU General Public License, version 2*
util-linux	2.20	*http://www.kernel.org/pub/linux/utils/util-linux/*	*GNU General Public License, version 2*
utils-merge	1.0.0	*http://registry.npmjs.org/utils-merge/-/utils-merge-1.0.0.tgz*	*MIT License*
valgrind	3.5.0	*http://valgrind.org/*	*GNU General Public License, version 2*
validator	3.41.2	*http://registry.npmjs.org/validator/-/validator-3.41.2.tgz*	*MIT License*
vary	1.0.1	*http://registry.npmjs.org/vary/-/vary-1.0.1.tgz*	*MIT License*
wanpipe	3.5.18	*http://wiki.sangoma.com/wanpipe-linux-drivers*	*GNU General Public License, version 2*
websocket	2.4	*https://github.com/nori0428/mod_websocket*	*MIT License*
wget	1.14	*http://www.gnu.org/software/wget/*	*GNU General Public License, version 3*
winston	1.0.1	*http://registry.npmjs.org/winston/-/winston-1.0.1.tgz*	*MIT License*

Name	Version	URL	License
wireless_tools	r29	*http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html*	*GNU General Public License, version 2*
wpa_supplicant	2.0	*http://hostap.epitest.fi/wpa_supplicant/*	*The BSD License*
ws	0.7.2	*http://registry.npmjs.org/ws/-/ws-0.7.2.tgz*	*MIT License*
wuftpd	1.0.21	*http://wu-ftpd.therockgarden.ca/*	*WU-FTPD Software License*
XenAPI	None	*http://docs.vmd.citrix.com/XenServer/4.0.1/api/client-examples/python/index.html*	*GNU General Public License, version 2*
xen	4.1.5	*http://www.xen.org/*	*GNU General Public License, version 2*
xen-crashdump-analyser	20130505	*http://xenbits.xen.org/people/andrewcoop/*	*GNU General Public License, version 2*
xen-tools	4.2.1	*http://xen-tools.org/software/xen-tools/*	*GNU General Public License, version 2*
xxhashjs	0.1.1	*http://registry.npmjs.org/xxhashjs/-/xxhashjs-0.1.1.tgz*	*MIT License*
z3c-rml	2.7.2	*http://pypi.python.org/pypi/z3c.rml*	*Zope Public License (ZPL) Version 2.0*
zlib	1.2.8	*http://www.zlib.net/*	*zlib License*
zope-event	4.0.3	*http://pypi.python.org/pypi/zope.event*	*Zope Public License (ZPL) Version 2.0*
zope-interface	4.1.1	*http://pypi.python.org/pypi/zope.interface*	*Zope Public License (ZPL) Version 2.1*
zope-schema	4.4.2	*http://pypi.python.org/pypi/zope.schema*	*Zope Public License (ZPL) Version 2.0*
zwave	0.1	*http://code.google.com/p/open-zwave/*	*GNU Lesser General Public License, version 2.1*

A.3 OSS Licenses

A.3.1 Apache License, Version 2.0

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

You must give any other recipients of the Work or Derivative Works a copy of this License; and

You must cause any modified files to carry prominent notices stating that You changed the files; and

You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/

or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

A.3.2 The BSD License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, and the entire permission notice in its entirety, including the disclaimer of warranties.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ”AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ALL OF WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF NOT ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Creative Commons Attribution-ShareAlike License, version 3.0

Creative Commons

Attribution-ShareAlike 3.0 Unported

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS LICENSE DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. REATIVE COMMONS MAKES NO WARRANTIES REGARDING THE INFORMATION PROVIDED, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM ITS USE

License

THE WORK (AS DEFINED BELOW) IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

1. Definitions

"Adaptation" means a work based upon the Work, or upon the Work and other pre-existing works, such as a translation, adaptation, derivative work, arrangement of music or other alterations of a literary or artistic work, or phonogram or performance and includes cinematographic adaptations or any other form in which the Work may be recast, transformed, or adapted including in any form recognizably derived from the original, except that a work that constitutes a Collection will not be considered an Adaptation for the purpose of this License. For the avoidance of doubt, where the Work is a musical work, performance or phonogram, the synchronization of the Work in timed-relation with a moving image ("synching") will be considered an Adaptation for the purpose of this License.

"Collection" means a collection of literary or artistic works, such as encyclopedias and anthologies, or performances, phonograms or broadcasts, or other works or subject matter other than works listed in Section 1(f) below, which, by reason of the selection and arrangement of their contents, constitute intellectual creations, in which the Work is included in its entirety in unmodified form along with one or more other contributions, each constituting separate and independent works in themselves, which together are assembled into a collective whole. A work that constitutes a Collection will not be considered an Adaptation (as defined below) for the purposes of this License.

"Creative Commons Compatible License" means a license that is listed at http://creativecommons.org/compatiblelicenses that has been approved by Creative Commons as being essentially equivalent to this License, including, at a minimum, because that license: (i) contains terms that have the same purpose, meaning and effect as the License Elements of this License; and, (ii) explicitly permits the relicensing of adaptations of works made available under that license under this License or a Creative Commons jurisdiction license with the same License Elements as this License.

4. "Distribute" means to make available to the public the original and copies of the Work or Adaptation, as appropriate, through sale or other transfer of ownership.

5. "License Elements" means the following high-level license attributes as selected by Licensor and indicated in the title of this License: Attribution, ShareAlike.

6. "Licensor" means the individual, individuals, entity or entities that offer(s) the Work under the terms of this License.

7. "Original Author" means, in the case of a literary or artistic work, the individual, individuals, entity or entities who created the Work or if no individual or entity can be identified, the publisher; and in addition (i) in the case of a performance the actors, singers, musicians, dancers, and other persons who act, sing, deliver, declaim, play in, interpret or otherwise perform literary or artistic works or expressions of folklore; (ii) in the case of a phonogram the producer being the person or legal entity who first fixes the sounds of a performance or other sounds; and, (iii) in the case of broadcasts, the organization that transmits the broadcast.

8. "Work" means the literary and/or artistic work offered under the terms of this License including without limitation any production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression including digital form, such as a book, pamphlet and other writing; a lecture, address, sermon or other work of the same nature; a dramatic or dramatico-musical work; a choreographic work or entertainment in dumb show; a musical composition with or without words; a cinematographic work to which are assimilated works

expressed by a process analogous to cinematography; a work of drawing, painting, architecture, sculpture, engraving or lithography; a photographic work to which are assimilated works expressed by a process analogous to photography; a work of applied art; an illustration, map, plan, sketch or three-dimensional work relative to geography, topography, architecture or science; a performance; a broadcast; a phonogram; a compilation of data to the extent it is protected as a copyrightable work; or a work performed by a variety or circus performer to the extent it is not otherwise considered a literary or artistic work.

9. "You" means an individual or entity exercising rights under this License who has not previously violated the terms of this License with respect to the Work, or who has received express permission from the Licensor to exercise rights under this License despite a previous violation.

10. "Publicly Perform" means to perform public recitations of the Work and to communicate to the public those public recitations, by any means or process, including by wire or wireless means or public digital performances; to make available to the public Works in such a way that members of the public may access these Works from a place and at a place individually chosen by them; to perform the Work to the public by any means or process and the communication to the public of the performances of the Work, including by public digital performance; to broadcast and rebroadcast the Work by any means including signs, sounds or images.

11. "Reproduce" means to make copies of the Work by any means including without limitation by sound or visual recordings and the right of fixation and reproducing fixations of the Work, including storage of a protected performance or phonogram in digital form or other electronic medium.

12. Fair Dealing Rights. Nothing in this License is intended to reduce, limit, or restrict any uses free from copyright or rights arising from limitations or exceptions that are provided for in connection with the copyright protection under copyright law or other applicable laws.

13. License Grant. Subject to the terms and conditions of this License, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) license to exercise the rights in the Work as stated below:

a. to Reproduce the Work, to incorporate the Work into one or more Collections, and to Reproduce the Work as incorporated in the Collections;

b. to create and Reproduce Adaptations provided that any such Adaptation, including any translation in any medium, takes reasonable steps to clearly label, demarcate or otherwise identify that changes were made to the original Work. For example, a translation could be marked "The original work was translated from English to Spanish," or a modification could indicate "The original work has been modified.";

c. to Distribute and Publicly Perform the Work including as incorporated in Collections; and,

d. to Distribute and Publicly Perform Adaptations

For the avoidance of doubt:

1. Non-waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme cannot be waived, the Licensor reserves the exclusive right to collect such royalties for any exercise by You of the rights granted under this License;

2. Waivable Compulsory License Schemes. In those jurisdictions in which the right to collect royalties through any statutory or compulsory licensing scheme can be waived, the Licensor waives the exclusive right to collect such royalties for any exercise by You of the rights granted under this License; and,

3. Voluntary License Schemes. The Licensor waives the right to collect royalties, whether individually or, in the event that the Licensor is a member of a collecting society that administers voluntary licensing schemes, via that society, from any exercise by You of the rights granted under this License.

The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. Subject to Section 8(f), all rights not expressly granted by Licensor are hereby reserved.

4. Restrictions. The license granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a. You may Distribute or Publicly Perform the Work only under the terms of this License. You must include a copy of, or the *Uniform Resource Identifier* (URI) for, this License with every copy of the Work You Distribute or Publicly Perform. You may not offer or impose any terms on the Work that restrict the terms of this License or the ability of the recipient of the Work to exercise the rights granted to that recipient under the terms of the License. You may not sublicense the Work. You must keep intact all notices that refer to this License and to the disclaimer of warranties with every copy of the Work You Distribute or Publicly Perform. When You Distribute or Publicly Perform the Work, You may not impose any effective technological measures on the Work that restrict the ability of a recipient of the Work from You to exercise the rights granted to that recipient under the terms of the License. This Section 4(a) applies to the Work as incorporated in a Collection, but this does not require the Collection apart from the Work itself to be made subject to the terms of this License. If You create a Collection, upon notice from any Licensor You must, to the extent practicable, remove from the Collection any credit as required by Section 4(c), as requested. If You create an Adaptation, upon notice from any Licensor You must, to the extent practicable, remove from the Adaptation any credit as required by Section 4(c), as requested.

b. You may Distribute or Publicly Perform an Adaptation only under the terms of: (i) this License; (ii) a later version of this License with the same License Elements as this License; (iii) a Creative Commons jurisdiction license (either this or a later license version) that contains the same License Elements as this License (e.g., Attribution-ShareAlike 3.0 US)); (iv) a Creative Commons Compatible License. If you license the Adaptation under one of the licenses mentioned in (iv), you must comply with the terms of that license. If you license the Adaptation under the terms of any of the licenses mentioned in (i), (ii) or (iii) (the "Applicable License"), you must comply with the terms of the Applicable License generally and the following provisions: (I) You must include a copy of, or the URI for, the Applicable License with every copy of each Adaptation You Distribute or Publicly Perform; (II) You may not offer or impose any terms on the Adaptation that restrict the terms of the Applicable License or the ability of the recipient of the Adaptation to exercise the rights granted to that recipient under the terms of the Applicable License; (III) You must keep intact all notices that refer to the Applicable License and to the disclaimer of warranties with every copy of the ork as included in the Adaptation You Distribute or Publicly Perform; (IV) when You Distribute or Publicly Perform the Adaptation, You may not impose any effective technological measures on the Adaptation that restrict the ability of a recipient of the Adaptation from You to exercise the rights granted to that recipient under the terms of the Applicable License. This Section 4(b) applies to the Adaptation as incorporated in a Collection, but this does not require the Collection apart from the Adaptation itself to be made subject to the terms of the Applicable License.

3. If You Distribute, or Publicly Perform the Work or any Adaptations or Collections, You must, unless a request has been made pursuant to Section 4(a), keep intact all copyright notices for the Work and provide, reasonable to the medium or means You are utilizing: (i) the name of the Original Author (or pseudonym, if applicable) if supplied, and/or if the Original Author and/or Licensor designate another party or parties (e.g., a sponsor institute, publishing entity, journal) for attribution ("Attribution Parties") in Licensor's copyright notice, terms of service or by other reasonable means, the name of such party or parties; (ii) the title of the Work if supplied; (iii) to the extent reasonably practicable, the URI, if any, that Licensor specifies to be associated with the Work, unless such URI does not refer to the copyright notice or licensing information for the Work; and (iv) , consistent with Section 3(b), in the case of an Adaptation, a credit identifying the use of the Work in the Adaptation (e.g., "French translation of

the Work by Original Author," or "Screenplay based on original Work by Original Author"). The credit required by this Section 4(c) may be implemented in any reasonable manner; provided, however, that in the case of a Adaptation or Collection, at a minimum such credit will appear, if a credit for all contributing authors of the Adaptation or Collection appears, then as part of these credits and in a manner at least as prominent as the credits for the other contributing authors. For the avoidance of doubt, You may only use the credit required by this Section for the purpose of attribution in the manner set out above and, by exercising Your rights under this License, You may not implicitly or explicitly assert or imply any connection with, sponsorship or endorsement by the Original Author, Licensor and/or Attribution Parties, as appropriate, of You or Your use of the Work, without the separate, express prior written permission of the Original Author, Licensor and/or Attribution Parties.

4. Except as otherwise agreed in writing by the Licensor or as may be otherwise permitted by applicable law, if You Reproduce, Distribute or Publicly Perform the Work either by itself or as part of any Adaptations or Collections, You must not distort, mutilate, modify or take other derogatory action in relation to the Work which would be prejudicial to the Original Author's honor or reputation. Licensor agrees that in those jurisdictions (e.g. Japan), in which any exercise of the right granted in Section 3(b) of this License (the right to make Adaptations) would be deemed to be a distortion, mutilation, modification or other derogatory action prejudicial to the Original Author's honor and reputation, the Licensor will waive or not assert, as appropriate, this Section, to the fullest extent permitted by the applicable national law, to enable You to reasonably exercise Your right under Section 3(b) of this License (right to make Adaptations) but not otherwise.

5. Representations, Warranties and Disclaimer

UNLESS OTHERWISE MUTUALLY AGREED TO BY THE PARTIES IN WRITING, LICENSOR OFFERS THE WORK AS-IS AND MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND CONCERNING THE WORK, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF TITLE, MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THE ABSENCE OF LATENT OR OTHER DEFECTS, ACCURACY, OR THE PRESENCE OF ABSENCE OF ERRORS, WHETHER OR NOT DISCOVERABLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO SUCH EXCLUSION MAY NOT APPLY TO YOU.

6. Limitation on Liability. EXCEPT TO THE EXTENT REQUIRED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR BE LIABLE TO YOU ON ANY LEGAL THEORY FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF THIS LICENSE OR THE USE OF THE WORK, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. Termination

This License and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this License. Individuals or entities who have received Adaptations or Collections from You under this License, however, will not have their licenses terminated provided such individuals or entities remain in full compliance with those licenses. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this License.

Subject to the above terms and conditions, the license granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different license terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this License (or any other license that has been, or is required to be, granted under the terms of this License), and this License will continue in full force and effect unless terminated as stated above.

8. Miscellaneous

Each time You Distribute or Publicly Perform the Work or a Collection, the Licensor offers to the recipient a license to the Work on the same terms and conditions as the license granted to You under this License.

Each time You Distribute or Publicly Perform an Adaptation, Licensor offers to the recipient a license to the original Work on the same terms and conditions as the license granted to You under this License.

If any provision of this License is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the emainder of the terms of this License, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

No term or provision of this License shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

This License constitutes the entire agreement between the parties with respect to the Work licensed here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This License may not be modified without the mutual written agreement of he Licensor and You.

The rights granted under, and the subject matter referenced, in this License were drafted utilizing the terminology of the Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979), the Rome Convention of 1961, the WIPO Copyright Treaty of 1996, the WIPO Performances and Phonograms Treaty of 1996 and the Universal Copyright Convention (as revised on July 24, 1971). These rights and subject matter take effect in the relevant jurisdiction in which the License terms are sought to be enforced according to the corresponding provisions of the implementation of those treaty provisions in the applicable national law. If the standard suite of rights granted under applicable copyright law includes additional rights not granted under this License, such additional rights are deemed to be included in the License; this License is not intended to restrict the license of any rights under applicable law.

Creative Commons Notice

Creative Commons is not a party to this License, and makes no warranty whatsoever in connection with the Work. Creative Commons will not be liable to You or any party on any legal theory for any damages whatsoever, including without limitation any general, special, incidental or consequential damages arising in connection to this license. Notwithstanding the foregoing two (2) sentences, if Creative Commons has expressly identified itself as the Licensor hereunder, it shall have all rights and obligations of Licensor.

Except for the limited purpose of indicating to the public that the Work is licensed under the CCPL, Creative Commons does not authorize the use by either party of the trademark "Creative Commons" or any related trademark or logo of Creative Commons without the prior written consent of Creative Commons. Any permitted use will be in compliance with Creative Commons' then-current trademark usage guidelines, as may be published on its website or otherwise made available upon request from time to time. For the avoidance of doubt, this trademark restriction does not form part of the License.

Creative Commons may be contacted at http://creativecommons.org/.

DropBear License

Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive.

The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

Copyright (c) 2002-2004 Matt Johnston

Portions copyright (c) 2004 Mihnea Stoenescu

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LibTomCrypt and LibTomMath are written by Tom St Denis, and are .

=====

sshpty.c is taken from OpenSSH 3.5p1,

Copyright (c) 1995 Tatu Ylonen , Espoo, Finland

All rights reserved

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c

loginrec.h

atomicio.h

atomicio.c

and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

A.3.3 GNU General Public License, version 2

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

The modified work must itself be a software library.

You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

IIf a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good

faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is

especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

A.3.4 GNU Lesser General Public License 2.1

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away yourfreedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

Creative Commons Legal Code CC0 1.0 Universal CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL SERVICES. DISTRIBUTION OF THIS DOCUMENT DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER.

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1 You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright

notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

2 You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3 You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a. The modified work must itself be a software library.

b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4 You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

5 You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

6 A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

7 As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the

major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

8 You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

9 You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10 You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

11 Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

12 If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

13 If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

14 The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

15 If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

16 BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

A.3.5 CCO 1.0 Universal

Creative Commons Legal Code

CC0 1.0 Universal

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDELEGAL SERVICES. DISTRIBUTION OF THIS DOCUMENT DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS-IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER, AND DISCLAIMS LIABILITY FOR DAMAGES RESULTING FROM THE USE OF THIS DOCUMENT OR THE INFORMATION OR WORKS PROVIDED HEREUNDER.

Statement of Purpose

The laws of most jurisdictions throughout the world automatically confer exclusive Copyright and Related Rights (defined below) upon the creator and subsequent owner(s) (each and all, an "owner") of an original work of authorship and/or a database (each, a "Work").

Certain owners wish to permanently relinquish those rights to a Work for the purpose of contributing to a commons of creative, cultural and scientific works ("Commons") that the public can reliably and without fear of later claims of infringement build upon, modify, incorporate in other works, reuse and redistribute as freely as possible in any form whatsoever and for any purposes, including without limitation commercial purposes. These owners may contribute to the Commons to promote the ideal of a free culture and the further production of creative, cultural and scientific works, or to gain reputation or greater distribution for their Work in part through the use and efforts of others.

For these and/or other purposes and motivations, and without any expectation of additional consideration or compensation, the person associating CC0 with a Work (the "Affirmer"), to the extent that he or she is an owner of Copyright and Related Rights in the Work, voluntarily elects to apply CC0 to the Work and publicly distribute the Work under its terms, with knowledge of his or her Copyright and Related Rights in the Work and the meaning and intended legal effect of CC0 on those rights.

Copyright and Related Rights. A Work made available under CC0 may be protected by copyright and related or neighboring rights ("Copyright and Related Rights"). Copyright and Related Rights include, but are not limited to, the following:

the right to reproduce, adapt, distribute, perform, display, communicate, and translate a Work;

moral rights retained by the original author(s) and/or performer(s);

publicity and privacy rights pertaining to a person's image or likeness depicted in a Work;

rights protecting against unfair competition in regards to a Work, subject to the limitations in paragraph 4(a), below;

rights protecting the extraction, dissemination, use and reuse of data in a Work;

database rights (such as those arising under Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, and under any national implementation thereof, including any amended or successor version of such directive); and

other similar, equivalent or corresponding rights throughout the world based on applicable law or treaty, and any national implementations thereof.

Waiver. To the greatest extent permitted by, but not in contravention of, applicable law, Affirmer hereby overtly, fully, permanently, irrevocably and unconditionally waives, abandons, and surrenders all of Affirmer's Copyright and Related Rights and associated claims and causes of action, whether now known or unknown (including existing as well as future claims and causes of action), in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the "Waiver"). Affirmer makes the Waiver for the benefit of each member of the public at large and to the detriment of Affirmer's heirs and successors, fully intending that such Waiver shall not be subject to revocation, rescission, cancellation, termination, or any other legal or equitable action to disrupt the quiet enjoyment of the Work by the public as contemplated by Affirmer's express Statement of Purpose.

Public License Fallback. Should any part of the Waiver for any reason be judged legally invalid or ineffective under applicable law, then the Waiver shall be preserved to the maximum extent permitted taking into account Affirmer's express Statement of Purpose. In addition, to the extent the Waiver is so judged Affirmer hereby grants to each affected person a royalty-free, non transferable, non sublicensable, non exclusive, irrevocable and unconditional license to exercise Affirmer's Copyright and Related Rights in the Work (i) in all territories worldwide, (ii) for the maximum duration provided by applicable law or treaty (including future time extensions), (iii) in any current or future medium and for any number of copies, and (iv) for any purpose whatsoever, including without limitation commercial, advertising or promotional purposes (the "License"). The License shall be deemed effective as of the date CC0 was applied by Affirmer to the Work. Should any part of the License for any reason be judged legally invalid or ineffective under applicable law, such partial invalidity or ineffectiveness shall not invalidate the remainder of the License, and in such case Affirmer hereby affirms that he or she will not (i) exercise any of his or her remaining Copyright and Related Rights in the Work or (ii) assert any associated claims and causes of action with respect to the Work, in either case contrary to Affirmer's express Statement of Purpose.

Limitations and Disclaimers.

No trademark or patent rights held by Affirmer are waived, abandoned, surrendered, licensed or otherwise affected by this document.

Affirmer offers the Work as-is and makes no representations or warranties of any kind concerning the Work, express, implied, statutory or otherwise, including without limitation warranties of title, merchantability, fitness for a particular purpose, non infringement, or the absence of latent or other defects, accuracy, or the present or absence of errors, whether or not discoverable, all to the greatest extent permissible under applicable law.

Affirmer disclaims responsibility for clearing rights of other persons that may apply to the Work or any use thereof, including without limitation any person's Copyright and Related Rights in the Work. Further, Affirmer disclaims responsibility for obtaining any necessary consents, permissions or other rights required for any use of the Work.

Affirmer understands and acknowledges that Creative Commons is not a party to this document and has no duty or obligation with respect to this CC0 or use of the Work.

GNU General Public License, version 3

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution andmodification follow.

TERMS AND CONDITIONS

Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case o interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files forthe work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing i not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of echnological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section

7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules andprotocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise ofights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you

(or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OFSUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

ISC License

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OFTHIS SOFTWARE.

A.3.6 GNU Lesser General Public License, version 3.0

GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc.

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General PublicLicense, supplemented by the additional permissions listed below.

Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each ofthe following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

A.3.7 GNU General Public License 2.0

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, thus in effect making the program proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which was designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library,and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public Licensefor libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1 You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright

notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2 You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

The modified work must itself be a software library.

You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

IIf a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3 You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4 You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete

corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5 A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6 As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7 You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8 You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9 You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10 Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11 If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent

application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12 If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13 The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14 If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15 BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

A.3.8 GNU Lesser General Public License, version 2.0

GNU LIBRARY GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the library GPL. It is numbered 2 because it goes with version 2 of the ordinary GPL.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Library General Public License, applies to some specially designated Free Software Foundation software, and to any other libraries whose authors decide to use it. You can use it for your libraries, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library, or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link a program with the library, you must provide complete object files to the recipients so that they can relink them with the library, after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

Our method of protecting your rights has two steps: (1) copyright the library, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the library.

Also, for each distributor's protection, we want to make certain that everyone understands that there is no warranty for this free library. If the library is modified by someone else and passed on, we want its recipients to know that what they have is not the original version, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that companies distributing free software will individually obtain patent licenses, thus in effect transforming the program into proprietary software. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License, which wa designed for utility programs. This license, the GNU Library General Public License, applies to certain designated libraries. This license is quite different from the ordinary one; be sure to read it in full, and don't assume that anything in it is the same as in the ordinary license.

The reason we have a separate public license for some libraries is that they blur the distinction we usually make between modifying or adding to a program and simply using it. Linking a program with a library, without changing the

library, is in some sense simply using the library, and is analogous to running a utility program or application program. However, in a textual and legal sense, the linked executable is a combined work, a derivative of the original library, and the ordinary General Public License treats it as such.

Because of this blurred distinction, using the ordinary General Public License for libraries did not effectively promote software sharing, because most developers did not use the libraries. We concluded that weaker conditions might promote sharing better.

However, unrestricted linking of non-free programs would deprive the users of those programs of all benefit from the free status of the libraries themselves. This Library General Public License is intended to permit developers of non-free programs to use free libraries, while preserving your freedom as a user of such programs to change the free libraries that are incorporated in them. (We have not seen how to achieve this as regards changes in header files, but we have achieved it as regards changes in the actual functions of the Library.) The hope is that this will lead to faster development of free libraries.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, while the latter only works together with the library.

Note that it is possible for a library to be covered by the ordinary General Public License rather than by this special one.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Library General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

* a) The modified work must itself be a software library.

* b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

* c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

* d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other han as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest you rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, s the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete

corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also compile or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

* a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

* b) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

* c) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

* d) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

* a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

* b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose thatchoice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Library General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

A.3.9 GNU Lesser General Public License, version 2.1

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.

Preamble

The licenses for most software are designed to take away yourfreedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the

ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1 You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2 You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. The modified work must itself be a software library.

   b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

   c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

   d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

   (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

   In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3 You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4 You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5 A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6 As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7 You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8 You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9 You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10 Each time you redistribute the Library (or any work based on the library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11 If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12 If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13 The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14 If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15 BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

A.3.10 MIT License

Permission is hereby granted, without written agreement and without icense or royalty fees, to use, copy, modify, and distribute this software and its documentation for any purpose, provided that the above copyright notice and the following two paragraphs appear in all copies of this software.

IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE AND ITS DOCUMENTATION, EVEN IF THE COPYRIGHT HOLDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE COPYRIGHT HOLDER SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE PROVIDED HEREUNDER IS ON AN "AS IS" BASIS, AND THE COPYRIGHT HOLDER HAS NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

A.3.11 Mozilla Public License, version 2

Version 2.0

1. Definitions

1.1. Contributor means each individual or legal entity that creates, contributes to the creation of, or owns Covered Software.

1.2. Contributor Versionâ means the combination of the Contributions of others (if any) used by a Contributor and that particular Contribution.

1.3. Contribution means Covered Software of a particular Contributor.

1.4. Covered Software means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.

1.5. Incompatible With Secondary Licenses means

1. that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or

2. that the Covered Software was made available under the terms of version 1.1 or earlier of the License, but not also under the terms of a Secondary License.

1.6. Executable Form means any form of the work other than Source Code Form.

1.7. Larger Work means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.

1.8. License means this document.

1.9. Licensable means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.

1.10. Modifications means any of the following:

1. any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or

2. any new file in Source Code Form that contains any Covered Software.

1.11. Patent Claims of a Contributor means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the

License, by the making, using, selling, offering for sale, having made, import, or transfer of either its Contributions or its Contributor Version.

1.12. Secondary License means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.

1.13. Source Code Form means the form of the work preferred for making modifications.

1.14. You (orYour) means an individual or a legal entity exercising rights under this License. For legal entities, You includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, control means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants and Conditions

2.1. Grants

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

1. under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and

2. under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

2.2. Effective Date

The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution.

2.3. Limitations on Grant Scope

The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor:

1. for any code that a Contributor has removed from Covered Software; or

2. for infringements caused by: (i) Your and any other third partyâ€™s modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or

3. under Patent Claims infringed by Covered Software in the absence of its Contributions.

This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

2.4. Subsequent Licenses

No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3).

2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

2.6. Fair Use

This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents.

2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

3. Responsibilities

3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipientsâ€™ rights in the Source Code Form.

3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

1. such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and

2. You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipientsâ€™ rights in the Source Code Form under this License.

3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

3.4. Notices

You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies.

3.5. Application of Additional Terms

You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any

Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

4. Inability to Comply Due to Statute or Regulation

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Termination

5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination.

6. Disclaimer of Warranty

Covered Software is provided under this License on an â€œas isâ€?basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer.

7. Limitation of Liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such partyâ€™s

negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You.

8. Litigation

Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party's ability to bring cross-claims or counter-claims.

9. Miscellaneous

This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor.

10. Versions of the License

10.1. New Versions

Mozilla Foundation is the license steward. Except as provided in Section 10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version number.

10.2. Effect of New Versions

You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward.

10.3. Modified Versions

If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such modified license differs from this License).

10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses

If You choose to distribute Source Code Form that is Incompatible With Secondary Licenses under the terms of this version of the License, the notice described in Exhibit B of this License must be attached.

Exhibit A - Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at http://mozilla.org/MPL/2.0/. You may add additional accurate notices of copyright ownership.

Exhibit B - Incompatible With Secondary Licenses Notice

This Source Code Form is Incompatible With Secondary Licenses, as defined by the Mozilla Public License, v. 2.0.

A.3.12 The Open LDAP Public License

The OpenLDAP Public License

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

OpenSSL License

OpenSSL License

Copyright (c) 1998-2000 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org)

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contac openssl-core@openssl.org

5. Products derived from this software may not be called "OpenSSL" nor may OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes oftware written by Tim Hudson (tjh@cryptsoft.com).

WU-FTPD Software License

WU-FTPD SOFTWARE LICENSE

Use, modification, or redistribution (including distribution of any modified or derived work) in any form, or on any medium, is permitted only if all the following conditions are met:

1. Redistributions qualify as "freeware" or "Open Source Software" under the following terms:

a. Redistributions are made at no charge beyond the reasonable cost of materials and delivery. Where redistribution of this software is as part of a larger package or combined work, this restriction applies only to the costs of materials and delivery of this software, not to any other costs associated with the larger package or combined work.

b. Redistributions are accompanied by a copy of the Source Code or by an irrevocable offer to provide a copy of the Source Code for up to three years at the cost of materials and delivery. Such redistributions must allow further use, modification, and redistribution of the Source Code under substantially the same terms as this license. For the purposes of redistribution "Source Code" means all files included in the original distribution, including all modifications or additions, on a medium and in a form allowing fully working executable programs to be produced.

2. Redistributions of Source Code must retain the copyright notices as they appear in each Source Code file and the COPYRIGHT file, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below.

3. Redistributions in binary form must reproduce the Copyright Notice, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below, in the documentation and/or other materials provided with the distribution. For the purposes of binary distribution the"Copyright Notice" refers to the following language:

Copyright (c) 1999,2000,2001 WU-FTPD Development Group.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler

jloup@gzip.org, madler@alumni.caltech.edu

Python License, Version 2 (Python-2.0)

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

------ --

This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.

Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright (c) 2001, 2002, 2003, 2004, 2005, 2006 Python Software Foundation; All Rights Reserved" are retained in Python alone or in any derivative version prepared by Licensee.

In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.

PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON,OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

This License Agreement will automatically terminate upon a material breach of its terms and conditions.

Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSFtrademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

BEOPEN.COM LICENSE AGREEMENT FOR PYTHON 2.0

BEOPEN PYTHON OPEN SOURCE LICENSE AGREEMENT VERSION 1

This LICENSE AGREEMENT is between BeOpen.com ("BeOpen"), having an office at 160 Saratoga Avenue, Santa Clara, CA 95051, and the Individual or Organization ("Licensee") accessing and otherwise using this software in source or binary form and its associated documentation ("the Software").

Subject to the terms and conditions of this BeOpen Python License Agreement, BeOpen hereby grants Licensee a non-exclusive,royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use the Software alone or in any derivative version, provided, however, that the BeOpen Python License is retained in the Software, alone or in any derivative version prepared by Licensee.

BeOpen is making the Software available to Licensee on an "AS IS" basis. BEOPEN MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, BEOPEN MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

BEOPEN SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING THE SOFTWARE, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

This License Agreement will automatically terminate upon a material breach of its terms and conditions.

This License Agreement shall be governed by and interpreted in all respects by the law of the State of California, excluding conflict of law provisions. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between BeOpen and Licensee. This License Agreement does not grant permission to use BeOpen trademarks or trade names in a trademark sense to endorse or promote products or services of Licensee, or any third party. As an exception, the "BeOpen Python" logos available at http://www.pythonlabs.com/logos.html may be used according to the permissions granted on that web page.

By copying, installing or otherwise using the software, Licensee agrees to be bound by the terms and conditions of this License Agreement.

CNRI OPEN SOURCE LICENSE AGREEMENT (for Python 1.6b1)

IMPORTANT: PLEASE READ THE FOLLOWING AGREEMENT CAREFULLY.

BY CLICKING ON "ACCEPT" WHERE INDICATED BELOW, OR BY COPYING, INSTALLING OR OTHERWISE USING PYTHON 1.6, beta 1 SOFTWARE, YOU ARE DEEMED TO HAVE AGREED TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

This LICENSE AGREEMENT is between the Corporation for National Research Initiatives, having an office at 1895 Preston White Drive, Reston, VA 20191 ("CNRI"), and the Individual or Organization ("Licensee") accessing and otherwise using Python 1.6, beta 1 software in source or binary form and its associated documentation,as released at the www.python.org Internet site on August 4, 2000 ("Python 1.6b1").

Subject to the terms and conditions of this License Agreement, CNRI hereby grants Licensee a non-exclusive, royalty-free, world-wide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python 1.6b1 alone or in any derivative version, provided, however, that CNRIs License Agreement is retained in Python 1.6b1, alone or in any derivative version prepared by Licensee.

Alternately, in lieu of CNRIs License Agreement, Licensee may substitute the following text (omitting the quotes): "Python 1.6, beta 1, is made available subject to the terms and conditions in CNR Is License Agreement. This Agreement may be located on the Internet using the following unique, persistent identifier (known as a handle): 1895.22/1011. This Agreement may also be obtained from a proxy server on the Internet using the URL:http://hdl.handle.net/1895.22/1011".

In the event Licensee prepares a derivative work that is based on or incorporates Python 1.6b1 or any part thereof, and wants to make the derivative work available to the public as provided herein, then Licensee hereby agrees to indicate in any such work the nature of the modifications made to Python 1.6b1.

CNRI is making Python 1.6b1 available to Licensee on an "AS IS" basis. CNRI MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, CNRI MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON 1.6b1 WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

CNRI SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF THE SOFTWARE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF USING, MODIFYING OR DISTRIBUTING PYTHON 1.6b1, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

This License Agreement will automatically terminate upon a material breach of its terms and conditions.

This License Agreement shall be governed by and interpreted in all respects by the law of the State of Virginia, excluding conflict of law provisions. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between CNRI and Licensee. This License Agreement does not grant permission to use CNRI trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

By clicking on the "ACCEPT" button where indicated, or by copying, installing or otherwise using Python 1.6b1, Licensee agrees to be bound by the terms and conditions of this License Agreement.

ACCEPT

CWI LICENSE AGREEMENT FOR PYTHON 0.9.0 THROUGH 1.2

Copyright (c) 1991 - 1995, Stichting Mathematisch Centrum Amsterdam, The Netherlands. All rights reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Stichting Mathematisch Centrum or CWI not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

STICHTING MATHEMATISCH CENTRUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL STICHTING MATHEMATISCH CENTRUM BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Zope Public License (ZPL) Version 2.0

Zope Public License (ZPL) Version 2.0

This software is Copyright (c) Zope Corporation (tm) and Contributors. All rights reserved.

This license has been certified as open source. It has also been designated as GPL compatible by the Free Software Foundation (FSF).

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the, following conditions are met:

Redistributions in source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name Zope Corporation (tm) must not be used to endorse or promote products derived from this software without prior written permission from Zope Corporation.

The right to distribute this software or to use it for any purpose does not give you the right to use Servicemarks (sm) orTrademarks (tm) of Zope Corporation. Use of them is covered in a separate agreement (see http://www.zope.com/Marks).

If any files are modified, you must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

Disclaimer

THIS SOFTWARE IS PROVIDED BY ZOPE CORPORATION ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL ZOPE CORPORATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR

OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of contributions made by Zope Corporation and many individuals on behalf of Zope Corporation. Specific attributions are listed in the accompanying credits file.

Zope Public License (ZPL) Version 2.1

Zope Public License (ZPL) Version 2.1

A copyright notice accompanies this license document that identifies the copyright holders.

This license has been certified as open source. It has also been designated as GPL compatible by the Free Software Foundation (FSF).

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the, following conditions are met:

Redistributions in source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

The name Zope Corporation (tm) must not be used to endorse or promote products derived from this software without prior written permission from Zope Corporation.

The right to distribute this software or to use it for any purpose does not give you the right to use Servicemarks (sm) orTrademarks (tm) of Zope Corporation. Use of them is covered in a separate agreement (see http://www.zope.com/Marks).

If any files are modified, you must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

Disclaimer

THIS SOFTWARE IS PROVIDED BY ZOPE CORPORATION ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL ZOPE CORPORATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.