



# WiNG 5.9.2 Wireless Controller and Service Platform

*System Reference Guide*

Copyright © 2018 Extreme Networks, Inc. All rights reserved.

## Legal Notice

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 on Extreme Networks trademarks, please see:

[www.extremenetworks.com/company/legal/trademarks](http://www.extremenetworks.com/company/legal/trademarks)

## Software Licensing

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:

[www.extremenetworks.com/support/policies/software-licensing](http://www.extremenetworks.com/support/policies/software-licensing)

## Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: <http://www.extremenetworks.com/support/contact/>

For product documentation online, visit: <https://www.extremenetworks.com/documentation/>

# Table of Contents

---

<b>Preface.....</b>	<b>6</b>
Text Conventions.....	6
Platform-Dependent Conventions.....	6
Providing Feedback to Us.....	7
Getting Help.....	7
Extreme Networks Documentation.....	8
<b>Chapter 1: About this Guide.....</b>	<b>9</b>
Notational Conventions.....	9
<b>Chapter 2: Overview.....</b>	<b>10</b>
About the WiNG Software.....	10
<b>Chapter 3: Web UI Features.....</b>	<b>13</b>
Accessing the Web UI.....	13
Glossary of Icons Used.....	14
<b>Chapter 4: Dashboard.....</b>	<b>20</b>
Summary.....	20
System Screen.....	22
RF Domain Screen.....	26
Controller Screen.....	30
Access Point Screen.....	34
Network View.....	37
Debug Wireless Clients.....	39
Debug Captive Portal Clients.....	40
<b>Chapter 5: Device Configuration.....</b>	<b>43</b>
Device Configuration.....	44
Auto-Provisioning Policies.....	310
Managing an Event Policy.....	315
Managing MINT Policies.....	316
<b>Chapter 6: Wireless Configuration.....</b>	<b>317</b>
Wireless LAN Policies.....	318
WLAN QoS Policies.....	367
Radio QoS Policies.....	381
Association ACL.....	392
Smart RF Policies.....	395
MeshConnex Policies.....	410
Mesh QoS Policy.....	417
Passpoint Policy.....	424
Sensor Policy.....	435
<b>Chapter 7: Network Configuration.....</b>	<b>438</b>
Policy Based Routing (PBR).....	439
L2TP V3 Configuration.....	444
Crypto CMP Policy.....	447
AAA Policy.....	451
AAA TACACS Policy.....	462

IPv6 Router Advertisement Policy.....	469
Border Gateway Protocol (BGP).....	472
Alias.....	486
Application Policy.....	491
Application.....	495
Application Group.....	497
Schedule Policy.....	500
URL Filtering.....	501
Web Filtering.....	505
Configuring EX3500 QoS Class.....	506
Configuring EX3500 QoS Policy Map.....	510
Network Deployment Considerations.....	515
<b>Chapter 8: Manage Profiles.....</b>	<b>516</b>
General Profile Configuration.....	519
Profile Cluster Configuration (Controllers Only).....	521
Profile Adoption Configuration (Access Points Only).....	523
Profile Adoption Configuration (Controllers Only).....	525
Access Point Radio Power Overrides (AP 7161 Only).....	527
Profile 802.1x Configuration.....	529
Profile Interface Configuration.....	529
Profile Network Configuration.....	572
Profile Security Configuration.....	618
VRRP Configuration.....	654
Critical Resources Configuration.....	658
Profile Services Configuration.....	661
Profile Management Configuration.....	665
Profile Mesh Point Configuration.....	671
Environmental Sensor Configuration (AP 8132 Only).....	678
Advanced Profile Configuration.....	679
<b>Chapter 9: RF Domains.....</b>	<b>689</b>
Managing RF Domains.....	690
<b>Chapter 10: Security Configuration.....</b>	<b>714</b>
Wireless Firewall.....	714
Configuring IP Firewall Rules.....	732
Wireless Client Roles.....	746
Device Fingerprinting.....	754
Intrusion Prevention.....	759
EX3500 Time Range.....	773
<b>Chapter 11: Services Configuration.....</b>	<b>777</b>
Configuring Captive Portal Policies.....	777
Setting the Guest Management Configuration.....	793
Setting the DHCP Configuration.....	803
Setting the Bonjour Gateway Configuration.....	819
Setting the DHCPv6 Server Policy.....	823
Setting the RADIUS Configuration.....	829
Setting the URL List.....	849
Setting the ImagoTag Policy.....	850

<b>Chapter 12: Management Access.....</b>	<b>854</b>
Viewing Management Access Policies.....	855
Adding or Editing a Management Access Policy.....	856
Creating an Administrator Configuration.....	857
Setting an Allowed Location Configuration.....	860
Setting the Access Control Configuration.....	862
Setting the Authentication Configuration.....	866
Setting the SNMP Configuration.....	868
SNMP Trap Configuration.....	868
T5 PowerBroadband SNMP.....	869
EX3500 Management Policies.....	871
Configuring a Hierarchical Tree.....	884
Management Access Deployment Considerations.....	888
<b>Chapter 13: Diagnostics.....</b>	<b>889</b>
Fault Management.....	889
Crash Files.....	893
Advanced.....	894
<b>Chapter 14: Operations.....</b>	<b>899</b>
Device Operations.....	899
Certificates.....	916
Smart RF.....	932
<b>Chapter 15: Statistics.....</b>	<b>936</b>
System Statistics.....	937
RF Domain Statistics.....	950
Controller Statistics.....	1001
EX3500 Interface Extended IF.....	1153
Access Point Statistics.....	1154
Wireless Client Statistics.....	1276
Guest Access Statistics.....	1288
Analytics Developer Interface.....	1298
<b>Chapter 16: WiNG Events.....</b>	<b>1305</b>





# Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks publications.

## Text Conventions

The following tables list text conventions that are used throughout this guide.

**Table 1: Notice Icons**

Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
<b><i>New!</i></b>	New Content	Displayed next to new content. This is searchable text within the PDF.

**Table 2: Text Conventions**

Convention	Description
Screen displays	This typeface indicates command syntax, or represents information as it appears on the screen.
The words <b>enter</b> and <b>type</b>	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
<b>[Key]</b> names	Key names are written with brackets, such as <b>[Return]</b> or <b>[Esc]</b> . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press <b>[Ctrl]+[Alt]+[Del]</b>
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

## Platform-Dependent Conventions

Unless otherwise noted, all information applies to all platforms supported by ExtremeXOS® software, which are the following:

- ExtremeSwitching® switches
- Summit® switches
- SummitStack™

When a feature or feature implementation applies to specific platforms, the specific platform is noted in the heading for the section describing that implementation in the ExtremeXOS command documentation (see the Extreme Documentation page at <http://documentation.extremenetworks.com>). In many cases, although the command is available on all platforms, each platform uses specific keywords. These keywords specific to each platform are shown in the Syntax Description and discussed in the Usage Guidelines sections.

## Providing Feedback to Us

---

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at [documentation@extremenetworks.com](mailto:documentation@extremenetworks.com).

## Getting Help

---

If you require assistance, contact Extreme Networks using one of the following methods:

- **GTAC (Global Technical Assistance Center) for Immediate Support**
  - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: [www.extremenetworks.com/support/contact](http://www.extremenetworks.com/support/contact)
  - **Email:** [support@extremenetworks.com](mailto:support@extremenetworks.com). To expedite your message, enter the product name or model number in the subject line.
- **Extreme Portal** — Search the GTAC knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
- **The Hub** — A forum for Extreme customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

## Extreme Networks Documentation

---

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	<a href="http://www.extremenetworks.com/documentation/">www.extremenetworks.com/documentation/</a>
Archived Documentation (for earlier versions and legacy products)	<a href="http://www.extremenetworks.com/support/documentation-archives/">www.extremenetworks.com/support/documentation-archives/</a>
Release Notes	<a href="http://www.extremenetworks.com/support/release-notes">www.extremenetworks.com/support/release-notes</a>

### Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: [www.extremenetworks.com/support/policies/software-licensing](http://www.extremenetworks.com/support/policies/software-licensing).



# 1 About this Guide

---

## Notational Conventions

This manual supports the following access point, controller and service platform models:

- Wireless Controllers – RFS 4000
- Service Platforms - NX 5500, NX 7510, NX 9500, NX 9510, NX 9600, NX 9610 and VX 9000
- Access Points – AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432 and AP 8533.

---

### Note



In this document ,

- NX 9500 and NX 9510 are collectively referred to as NX 95XX.
  - NX 9600 and NX 9610 are collectively referred to as NX 96XX.
- 

## 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

# 2 Overview

## About the WiNG Software

### About the WiNG Software

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.

**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 large 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 DPI *Deep Packet Inspection* 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.

## 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.

## 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.

## 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.

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

## Network Services, Routing and Switches

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.

## 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.

# 3 Web UI Features

## Accessing the Web UI Glossary of Icons Used

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 GUI Graphical User Interface allows full control of all administration features.

Access points, controllers and service platforms also share a CLI Command Line Interface 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](http://www.extremenetworks.com/support).

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

- [Accessing the Web UI](#) on page 13.
- [Glossary of Icons Used](#) on page 14.

## Accessing the Web UI

Access points, controllers and service platforms use a Graphical User Interface (GUI) that can be accessed using any supported Web browser on a client connected to the subnet the Web UI is configured on.

## 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.

## Connecting to Web UI

Follow the steps below to connect to an *access point's* (AP's), wireless controller or service platform's Web UI for the first time:

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

The Web UI login dialog displays:



**Figure 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.  
When logging in for the first time, you will be prompted to change the password to enhance device security. Set the new password and use it for subsequent logins.
- 6 Click the **Login** button to load the device's (access point, wireless controller or service platform) management interface.

## 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





## Global Icons

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.



## Dialog Box Icons

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.

	<i>Entry Updated</i> – Indicates a value has been modified from its last saved configuration.
	<i>Entry Update</i> – States that an override has been applied to a device profile configuration.
	<i>Mandatory Field</i> – Indicates this control value is a mandatory configuration item. You are not allowed to proceed further without providing all mandatory values in this dialog.
	<i>Error in Entry</i> – Indicates there is an error in a supplied value. A small red popup provides a likely cause of the error.






## Table Icons

The following two override icons are status indicators for transactions:

	<i>Table Row Overridden</i> – 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.
	<i>Table Row Added</i> – 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.












## Status Icons

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

	<i>Fatal Error</i> – States there is an error causing a managed device to stop functioning.
	<i>Error</i> – Indicates an error exists requiring intervention. An action has failed, but the error is not system wide.
	<i>Warning</i> – 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.
	<i>Success</i> – Indicates everything is well within the network or a process has completed successfully without error.
	<i>Information</i> – 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.

## Configurable Object Icons

These icons represent configurable items within the UI.





	<i>Device Configuration</i> – Represents a configuration file supporting a device category (access point, wireless controller etc.).
	<i>Auto Provisioning Policy</i> – 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.
	<i>Critical Resource Policy</i> – 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.
	<i>Wireless LANs</i> – States an action impacting a managed WLAN has occurred.
	<i>WLAN QoS Policy</i> – States a <i>quality of service policy</i> (QoS) configuration has been impacted.
	<i>Radio QoS Policy</i> – Indicates a radio's QoS configuration has been impacted.
	<i>AAA Policy</i> – Indicates an <i>Authentication, Authorization and Accounting</i> (AAA) policy has been impacted. AAA policies define RADIUS authentication and accounting parameters.
	<i>Association ACL</i> – Indicates an <i>Access Control List</i> (ACL) configuration has been impacted. An ACL is a set of configuration parameters either allowing or denying access to network resources.
	<i>Smart RF Policy</i> – 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.
	<i>Profile</i> – States a device profile configuration has been impacted. A profile is a collection of configuration parameters used to configure a device or a feature.
	<i>Bridging Policy</i> – 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.





	<i>RF Domain</i> – States an RF Domain configuration has been impacted.
	<i>Firewall Policy</i> – 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.
	<i>IP Firewall Rules</i> – Indicates an IP firewall rule has been applied. An IP based firewall rule implements restrictions based on the IP address in a received packet.
	<i>MAC Firewall Rules</i> – 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.
	<i>Wireless Client Role</i> – Indicates a wireless client role has been applied to a managed client. The role could be either sensor or client.
	<i>WIPS Policy</i> – 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.
	<i>Device Categorization</i> – 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.
	<i>Captive Portals</i> – 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.
	<i>DNS Whitelist</i> – A DNS whitelist is used in conjunction with captive portal to provide access to requesting wireless clients.
	<i>DHCP Server Policy</i> – 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.
	<i>RADIUS Group</i> – 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.
	<i>RADIUS User Pools</i> – 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.
	<i>RADIUS Server Policy</i> – 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.
	<i>Management Policy</i> – Indicates a management policy has been applied. Management policies configure access control, authentication, traps and administrator permissions.
	<i>BGP – Border Gateway Protocol (BGP)</i> is an inter-ISP routing protocol which establishes routing between ISPs. ISPs use BGP to exchange routing and reachability information between <i>Autonomous Systems (AS)</i> on the Internet. BGP makes routing decisions based on paths, network policies and/or rules configured by network administrators.

## Configuration Object Icons




These configuration icons are used to define the following:

	<i>Configuration</i> – Indicates an item capable of being configured by an interface.
	<i>View Events / Event History</i> – Defines a list of events. Click this icon to view events or view the event history.
	<i>Core Snapshots</i> – 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.
	<i>Panic Snapshots</i> – 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.

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





## Configuration Operation Icons

The following operations icons are used to define configuration operations:

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






## Access Type Icons



The following icons display a user access type:

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

## Administrative Role Icons








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

	<i>Superuser</i> - Indicates superuser privileges. A superuser has complete access to all configuration aspects of the connected device.
	<i>System</i> - States system user privileges. A system user is allowed to configure general settings, such as boot parameters, licenses, auto install, image upgrades etc.
	<i>Network</i> - 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.
	<i>Security</i> - Indicates security user privileges. A security level user is allowed to configure all security related parameters.
	<i>Monitor</i> - Defines a monitor role. This role provides no configuration privileges. A user with this role can view the system configuration but cannot modify it.

	<i>Help Desk</i> - Indicates help desk privileges. A help desk user is allowed to use troubleshooting tools like sniffers, execute service commands, view or retrieve logs. However, help desk personnel <i>are not</i> allowed to conduct controller or service platform reloads.
	<i>Web User</i> - Indicates a web user privilege. A Web user is allowed accessing the device's Web UI.

## Device Icons

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

	<i>System</i> - 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.
	<i>Cluster</i> - 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.
	<i>Service Platform</i> - This icon indicates an NX 5500, NX 7500, or NX 9500 series service platform that's part of the managed network
	<i>Wireless Controller</i> - This icon indicates a wireless controller that's not part of the managed network.
	<i>Wireless Controller</i> - This icon indicates a wireless controller that's part of the managed network.
	<i>Access Point</i> - This icon lists any access point that's part of the managed network.
	<i>Wireless Client</i> - This icon defines any wireless client connection within the network.

# 4 Dashboard

---

Summary  
System Screen  
RF Domain Screen  
Controller Screen  
Access Point Screen  
Network View  
Debug Wireless Clients  
Debug Captive Portal Clients

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

By default, the **Dashboard** screen displays the System Dashboard, which is the top level in the device hierarchy. To view information for access points, RF domains, or controllers/service platforms, select the associated item in the tree.

The dashboard provides the following tools and diagnostics:

- [Summary](#)
- [System Screen](#) on page 22
- [RF Domain Screen](#) on page 26
- [Controller Screen](#) on page 30
- [Access Point Screen](#) on page 34
- [Network View](#)
- [Debug Wireless Clients](#) on page 39
- [Debug Captive Portal Clients](#) on page 40
- [Packet Capture](#)

## Summary

---

The **Dashboard** displays information organized by device association and inter-connectivity between connected access points and wireless clients.

- 1 To review dashboard information, select **Dashboard > Summary**.

The **Dashboard** displays the **Health** tab by default.

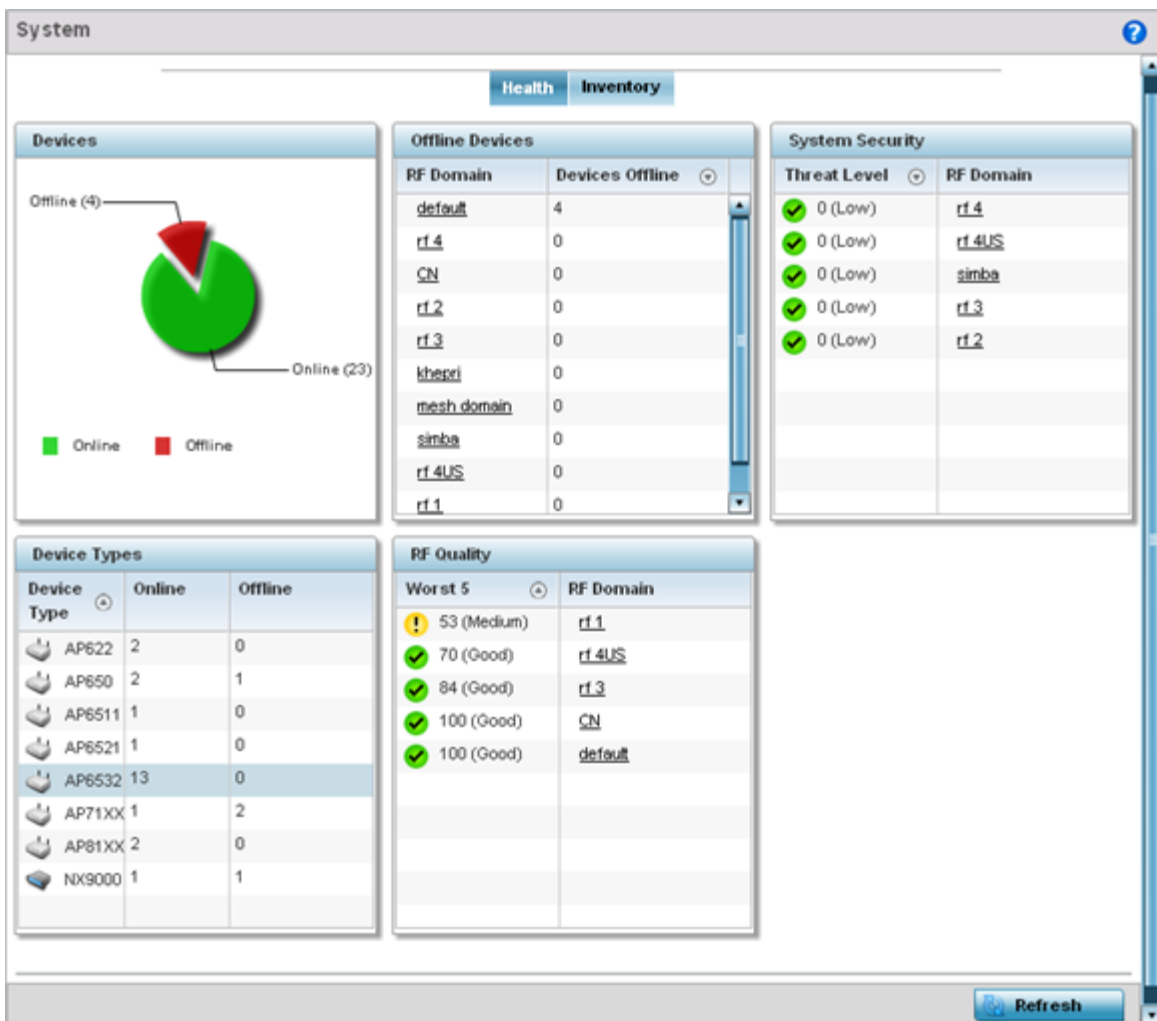
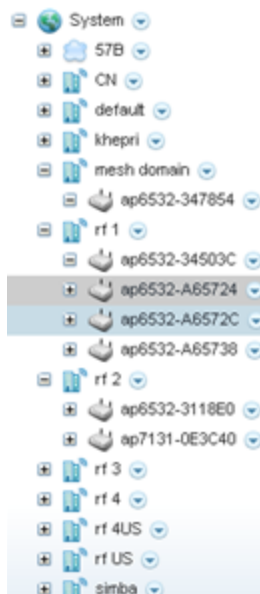


Figure 2: Dashboard Screen - Health Tab

### Device Listing

The device menu displays information as a hierarchical tree, where each node is a RF Domain. Each RF Domain is populated by the specific model access points or controllers.



**Figure 3: Dashboard Menu Tree**

The **Search** option, at the bottom of the screen, enables administrators to filter (search among) RF Domains. The **By** drop-down menu refines the search. 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.

## System Screen

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

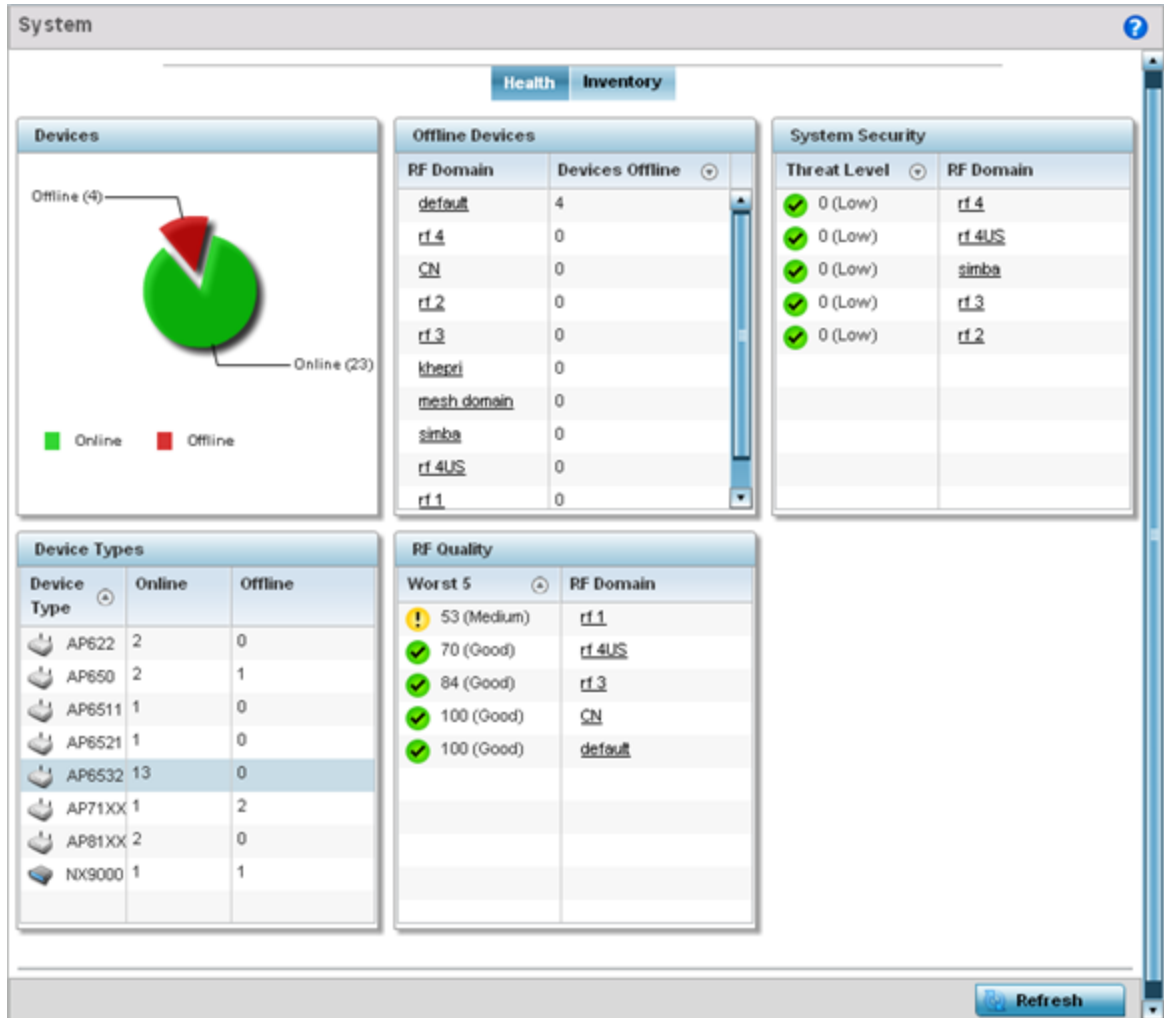
- **Health** – The Health tab displays information about the state of the <WiNG> device managed wireless network.
- **Inventory** – The Inventory tab displays information on the physical devices managed within the <WiNG> wireless network.

### Health

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

To assess system health:

- 1 Select **Dashboard > Summary > System**.
- 2 The **Health** tab displays by default.



**Figure 4: 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** field displays RF quality per RF domain. 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, 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.

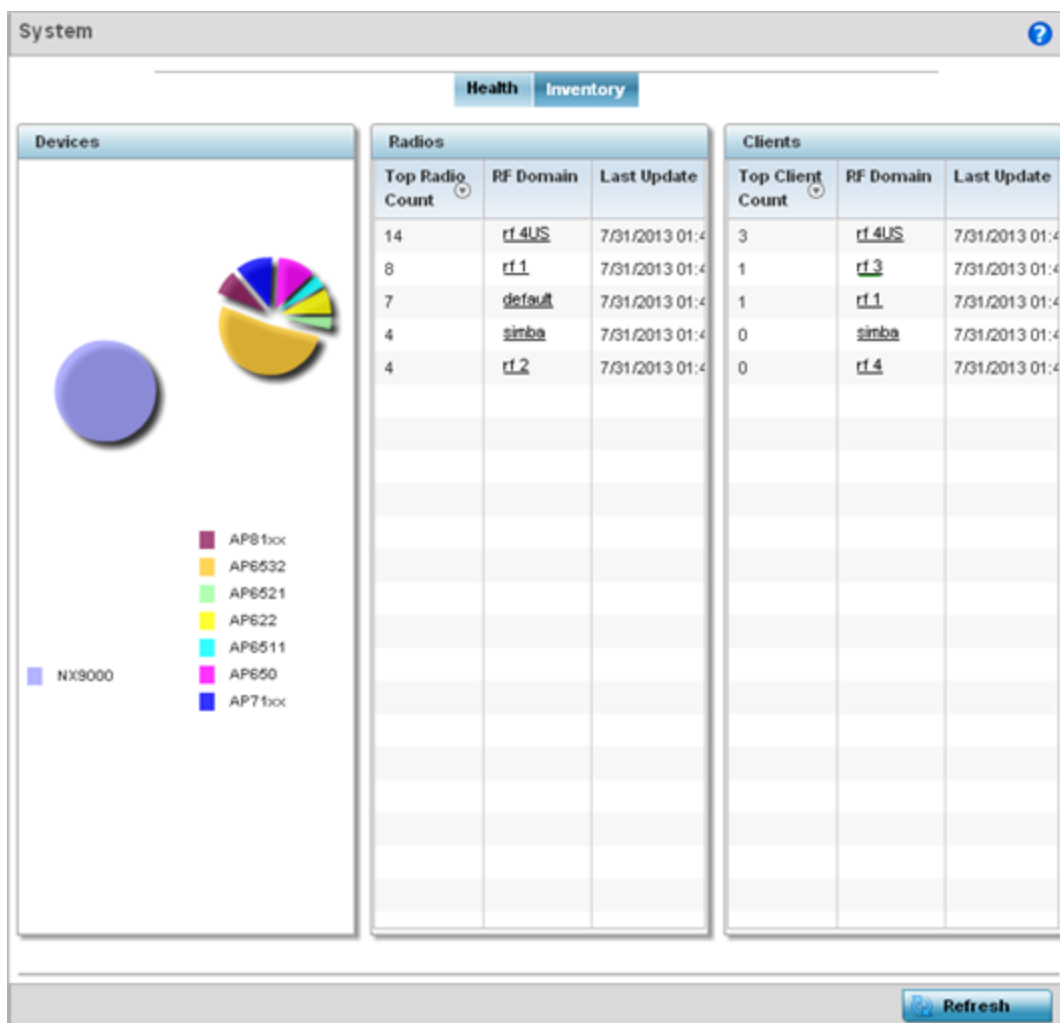
## Inventory

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 of 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** > **Summary** > **System** > **Inventory**.





**Figure 5: 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.
- The wireless **Clients** field lists the top five RF Domains with the highest total number of clients managed by connected devices in this system. Select **Refresh** as needed to update the screen to its latest values.

## 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:

<b>Default RF domain</b>	Automatically assigned to each controller or service platform and associated access point by default.
<b>User Defined RF domains</b>	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:

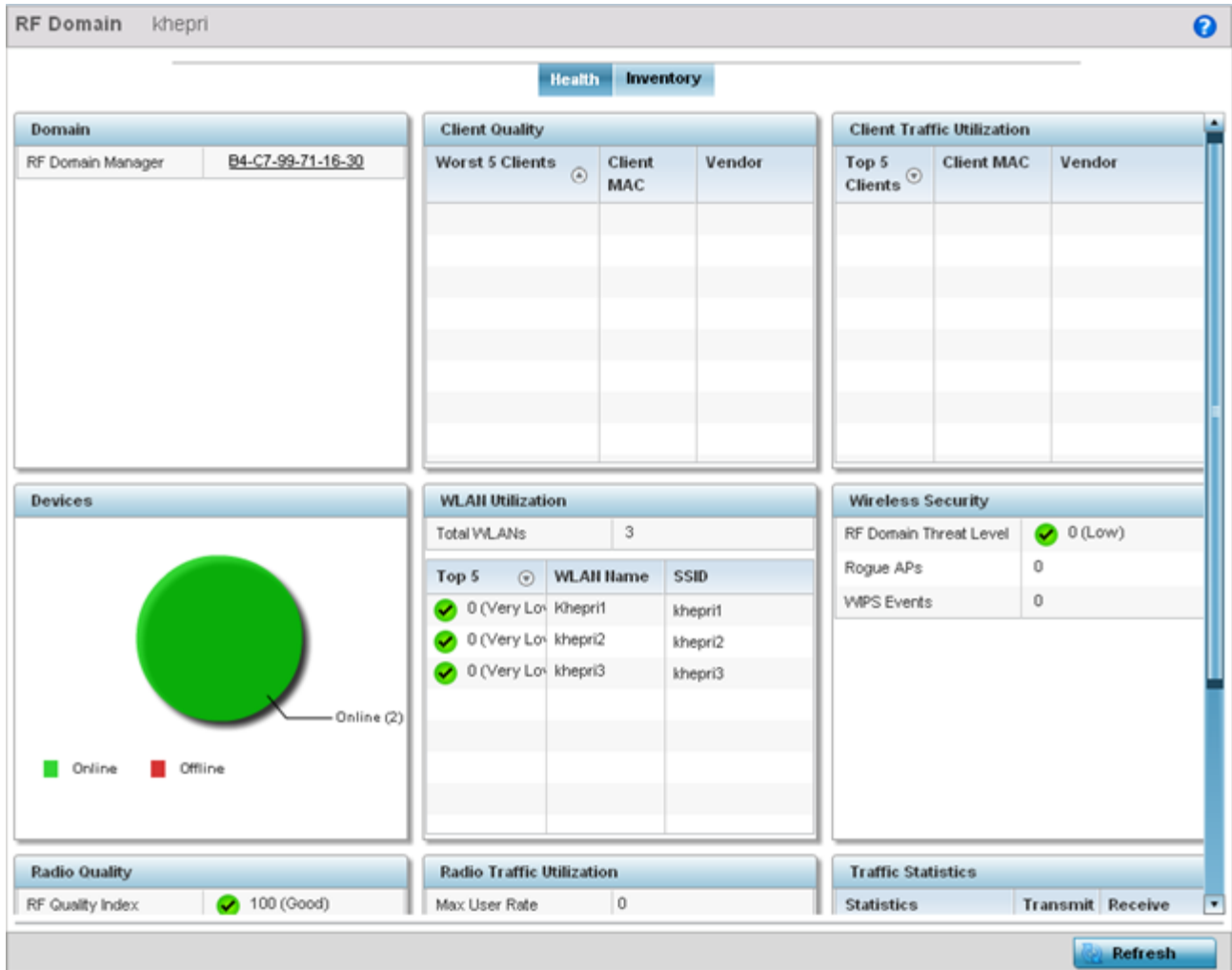
- **RF Domain Health** – The Health tab displays information about the state of the RF domain and network performance as tallied from its collective device members.
- **RF Domain Inventory** – The Inventory tab displays information on the physical devices comprising the RF domain.

## RF Domain Health

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

To assess the RF domain component health:

- 1 Select **Dashboard > Summary**.
- 2 Expand the **System** node to display RF domains.
- 3 Select an RF domain. The **Health** tab displays by default.



**Figure 6: 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.
- 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

- 4 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

- 5 Select a client to view its statistics in greater detail.

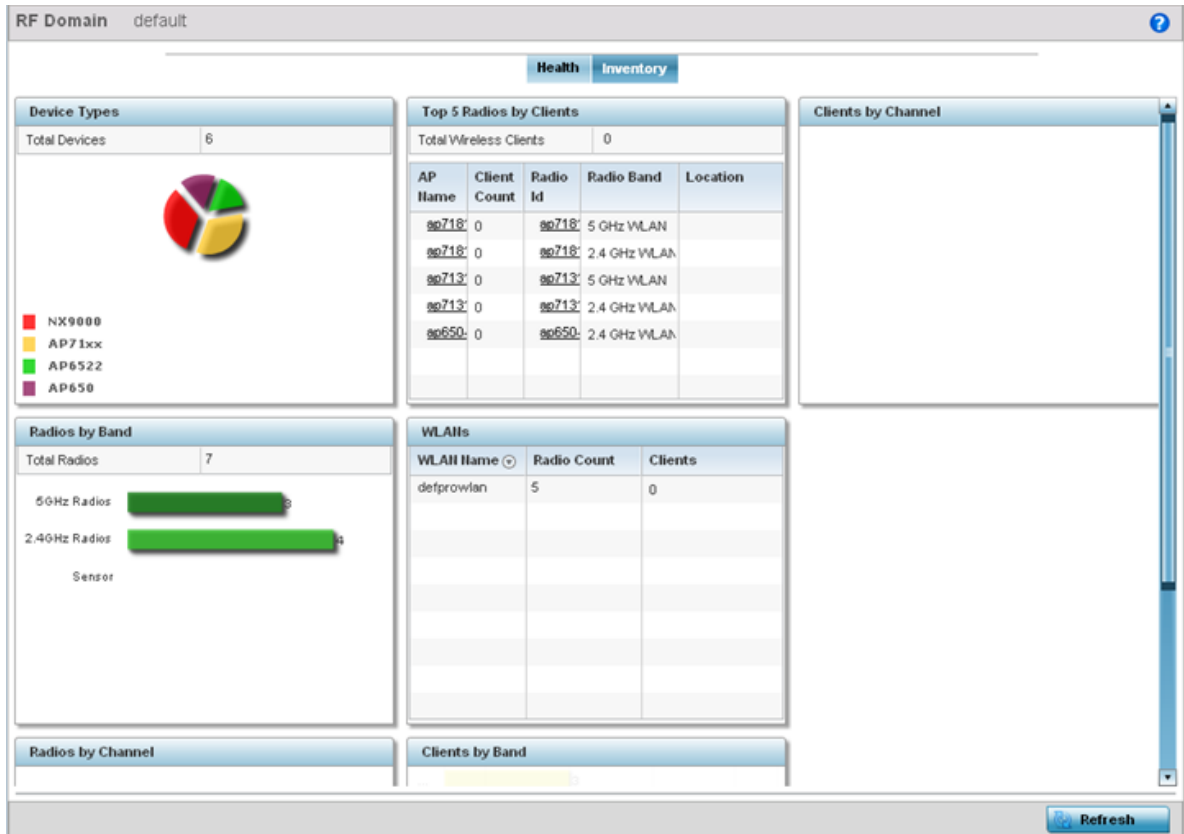
- **WLAN Utilization** displays how efficiently the WLANs are used. Traffic utilization is defined as the percentage of current throughput relative to the maximum possible throughput for the WLAN. The total number of WLANs is displayed above the table. The table displays a list of the top five WLANs 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.

## 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 > Summary**.
- 2 Expand the **System** node to display RF domains.
- 3 Select an RF domain. The **Health** tab displays by default
- 4 Select the **Inventory** tab.



**Figure 7: 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 that have 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 **Client by Channels** 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.

## Controller Screen

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

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

### Note



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 [Controller Adoption Overrides \(Controllers Only\)](#) on page 92.

## Controller Health

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


- 1 Select **Dashboard > Summary**.
- 2 Expand the **System** node to display RF domains.
- 3 Select and expand an RF domain to expose its member controllers or service platforms.
- 4 Select a controller or service platform. The **Health** tab displays by default.

Wireless Controller rfs4000-DD261A (B4-C7-99-DD-26-1A) ?

**Health** **Inventory**

---

**Device Details**

Hostname	rfs4000-DD261A
Device MAC	B4-C7-99-DD-26-1A
Primary IP	172.168.7.198
Type	 RFS4000
RF Domain Name	<a href="#">sitecon</a>
Model Number	RFS-4011-11110-WR
Version	5.5.0.0-069D
Uptime	0 days, 03 hours 20 minutes
CPU	Cavium Networks Octeon CN50XX V0.
RAM	190804 kB
System Clock	2013-08-06 21:05:30 IST

**Radio Utilization**

Parameter	Transmit	Receive
Total Bytes	0	0
Total Packets	0	0
Total Dropped	0	

**Client RF Quality Index**

Worst 5	Client MAC	Retry Rate

**Adopted Devices Health (w/ cluster members)**

Online 26

**Radio RF Quality Index**

RF Quality Index	Radio Id	Radio Type
<input type="checkbox"/> (Off)	<a href="#">rfs4000-DD261A:R2</a>	5 GHz WLAN
<input type="checkbox"/> (Off)	<a href="#">rfs4000-DD261A:R1</a>	2.4 GHz WLAN

[Refresh](#)

**Figure 8: 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.

**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 the 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
- 5 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 the 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
- 6 Select a client MAC to view all the statistics for the selected client in greater detail.

## Controller Inventory

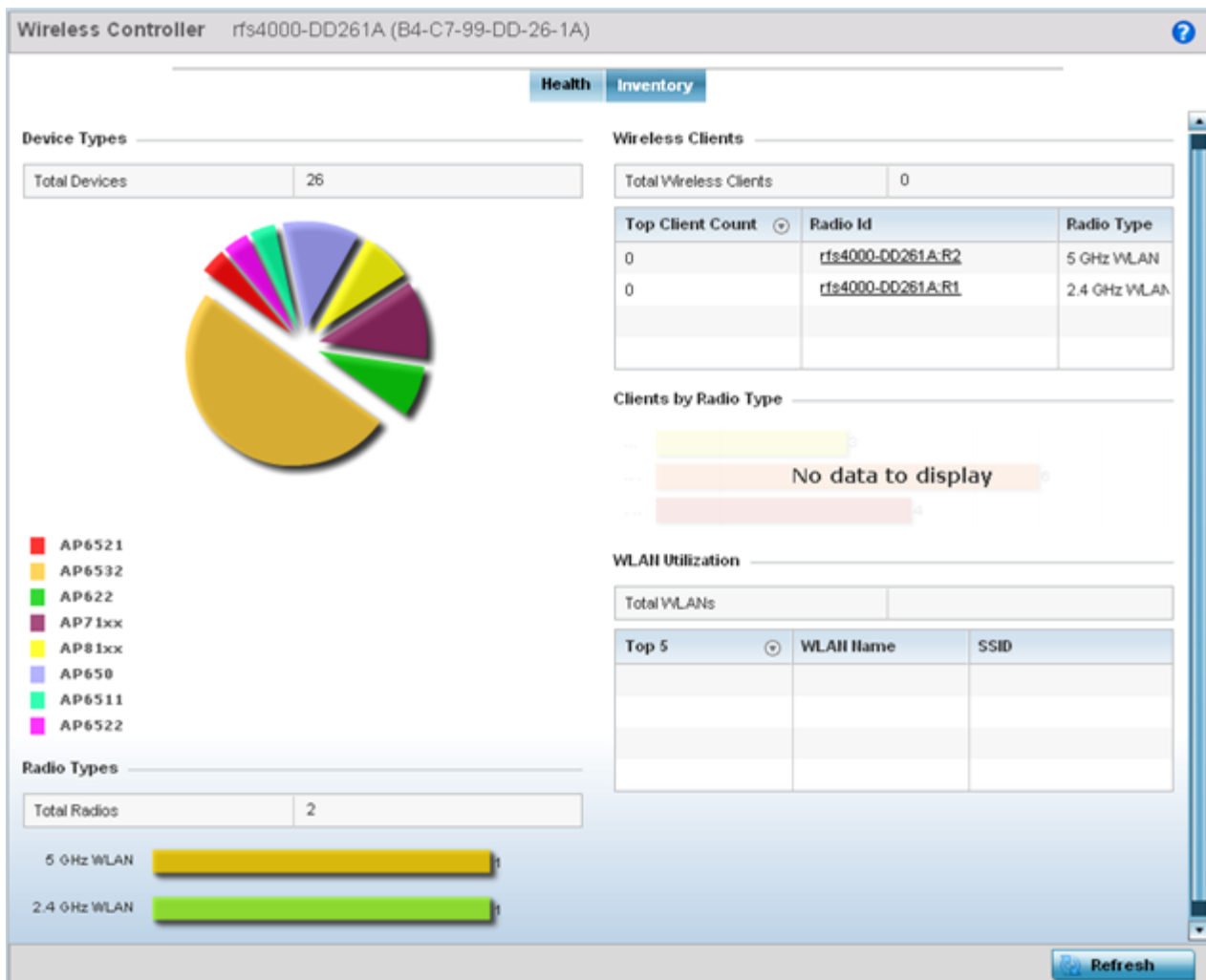
The Inventory tab displays information for the devices managed by the system. This screen enables a system administrator to have a complete overview of the number and state of managed devices. Information is displayed in easy to read tables and graphs. The Inventory screen also provides links for the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

To assess the controller or service platform inventory:

- 1 Select **Dashboard > Summary**.
- 2 Expand the **System** node to display RF domains.
- 3 Select and expand an RF domain to expose its member controllers or service platforms.



- 4 Select a controller or service platform. The **Health** tab displays by default.
- 5 Select the **Inventory** tab.



**Figure 9: 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.

## 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.

## Access Point Health

To assess access point network health:

- 1 Select **Dashboard > Summary**.
- 2 Expand the **System** node to display RF domains.
- 3 Select and expand an RF domain to expose its member controllers or service platforms.
- 4 Select a controller or service platform and expand the menu item to display connected access points.
- 5 Select an access point. The **Health** tab displays by default.

Access Point ap81xx-711630 (B4-C7-99-71-16-30) ?

**Health** **Inventory**

---

**Device Details**

Hostname	ap81xx-711630
Device MAC	B4-C7-99-71-16-30
Primary IP	172.168.6.132
Type	AP81XX
Model Number	AP-8132-66040-WR
RF Domain Name	<a href="#">lhpri</a>
Version	5.5.0.0-069D
Uptime	0 days, 06 hours 28 minutes
CPU	Netlogic XLS V0.1
RAM	172692 kB
System Clock	2013-08-06 18:42:16 UTC

**Radio Utilization**

Parameter	Transmit	Receive
Total Bytes	45,626	46,743
Total Packets	172	229
Total Dropped	0	

**Client RF Quality Index**

Worst 5	Client MAC	Retry Rate
73 (Good)	<a href="#">88-32-9B-6F-C3-7D</a>	0

**Radio RF Quality Index**

RF Quality Index	Radio Id	Radio Type
67 (Good)	<a href="#">ap81xx-711630.R2</a>	5 GHz WLAN
100 (Good)	<a href="#">ap81xx-711630.R1</a>	2.4 GHz WLAN

[Refresh](#)

**Figure 10: 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 the bottom five (5) of the RF quality values by client. The quality is measured as:

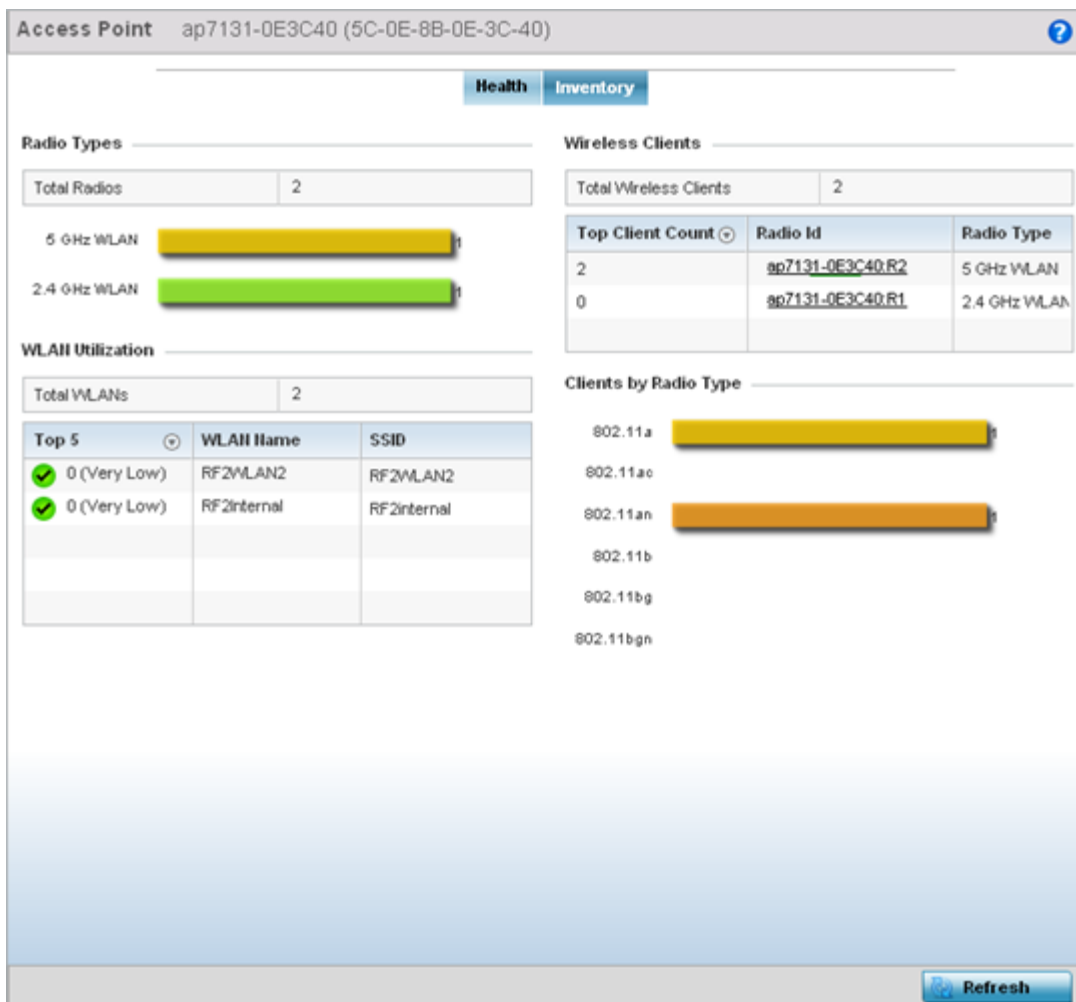
- 0-20 - Very poor quality
- 20-40 - Poor quality
- 40-60 - Average quality
- 60-100 - Good quality

## 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 review the access point's inventory of connected devices:

- 1 Select **Dashboard > Summary**.
- 2 Expand the **System** node to display RF domains.
- 3 Select and expand an RF domain to expose its member controllers or service platforms.
- 4 Select a controller or service platform and expand the menu item to display connected access points.
- 5 Select an access point. The **Health** tab displays by default.
- 6 Select the **Inventory** tab.



**Figure 11: Access Point Screen - Inventory Tab**

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

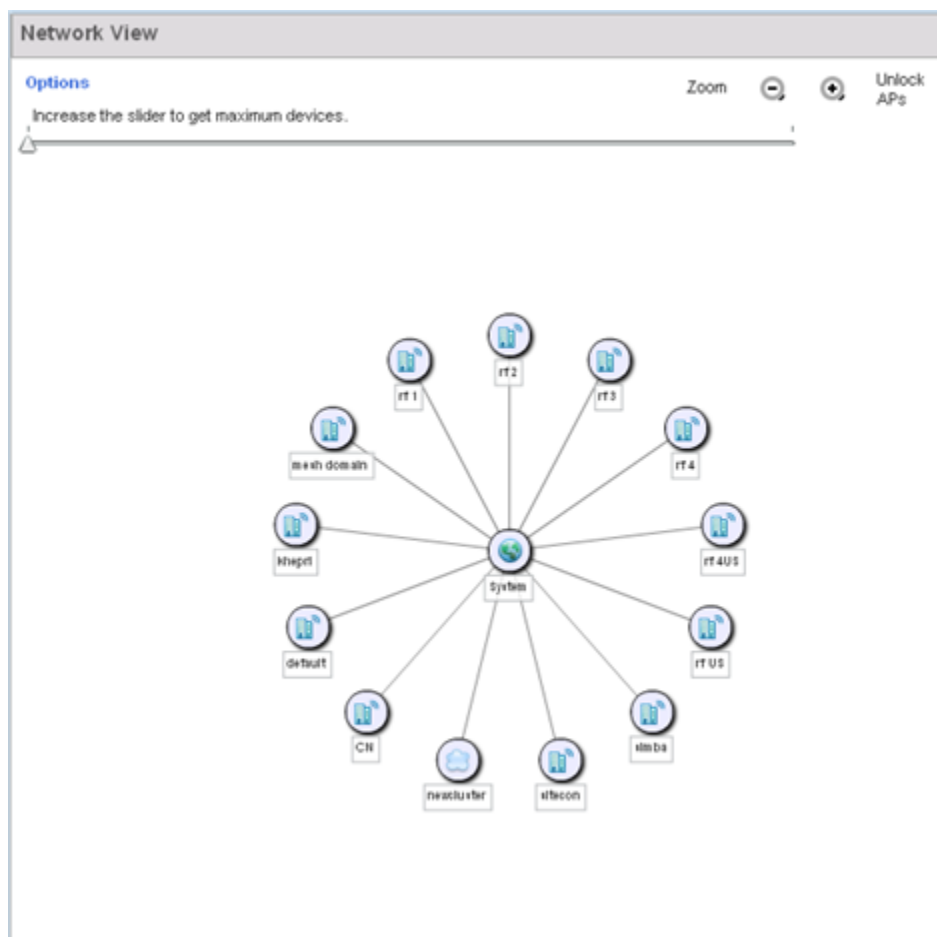
- The **Radios Type** field displays the total number of radios utilized by this access point. The graph lists the number of radios in both the 2.4 GHz and 5 GHz radio bands.
- The **WLAN Utilization** table displays utilization statistics for controller or service platform WLAN configurations. Information 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.

## Network View

The Network View displays device association connectivity among wireless controllers, service platforms, access points, and wireless clients. This association is represented by a number of different

graphs. The Network View is helpful in assessing whether controllers and access point radios are properly deployed in areas where high volumes of client traffic are anticipated.

To review the Network Topology, select **Dashboard > Network View**.



**Figure 12: 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.

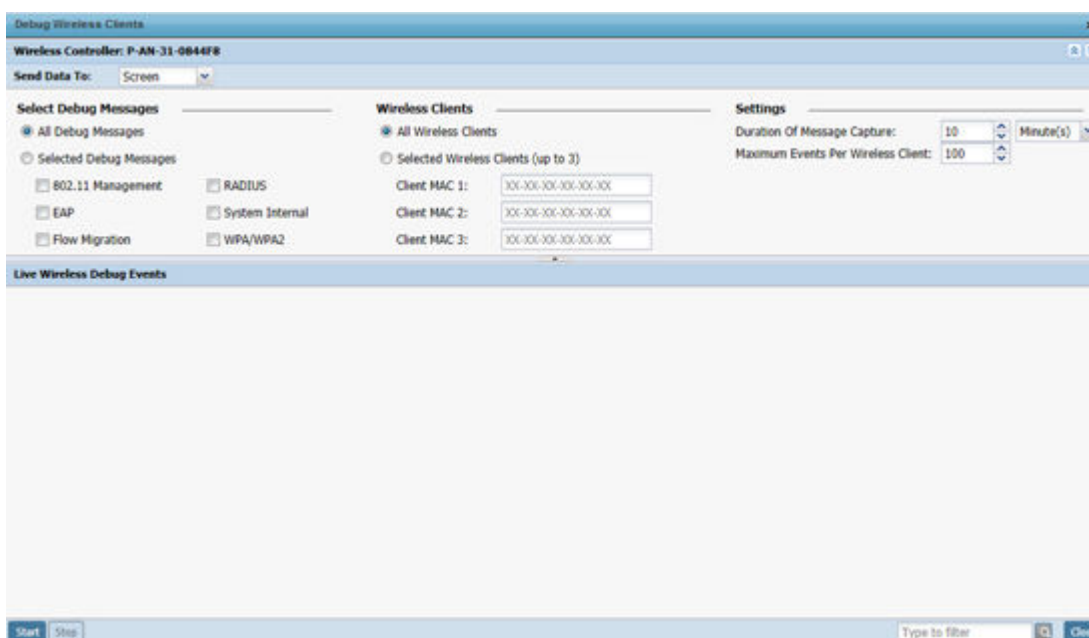
Use the **Lock / Unlock** icon in the upper right of the screen to prevent users from moving APs around within the specified area.

## Debug Wireless Clients

An administrator has the ability to select an 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 realtime.

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 an 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 13: 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 <b>Screen</b> is selected, the wireless client debug information is sent to the <b>Live Wireless Debug Events</b> window at the bottom of the dialog window. If <b>File</b> is selected, the file location must be specified in the File Location section of the window.

Select Debug Messages	Select <b>All Debug Messages</b> to display all wireless client debug information for the selected wireless clients on the current RF domain. Choose <b>Selected Debug Messages</b> to specify which types of wireless client debug messages to display. If the <b>Selected Debug Messages</b> radio button is selected, you can display information for any combination of the following: <ul style="list-style-type: none"> <li>• 802.11 Management</li> <li>• EAP</li> <li>• Flow Migration</li> <li>• RADIUS</li> <li>• System Internal</li> <li>• WPA/WPA2</li> </ul>
Wireless Clients	Select <b>All Wireless Clients</b> to display debug information for all wireless clients currently associated to the current RF domain. Choose <b>Selected Wireless Clients</b> to display information only for specific wireless clients (between 1 and 3). If <b>Selected Wireless Clients</b> 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 <b>Send Data To</b> field is set to <b>File</b> , the <b>File Location</b> configuration displays below the configuration section. If <b>Basic</b> 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 <b>Advanced</b> is selected, configure the Target, Port, Host/IP, User, Password and optionally the path for the wireless client debug log file you want to create.
Live Wireless Debug Events	When the <b>Send Data To</b> field is set to Screen, this area displays live debug information for connected wireless clients in the selected RF domain.

- 7 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 want to end the capture early, select **Stop**.

## Debug Captive Portal Clients

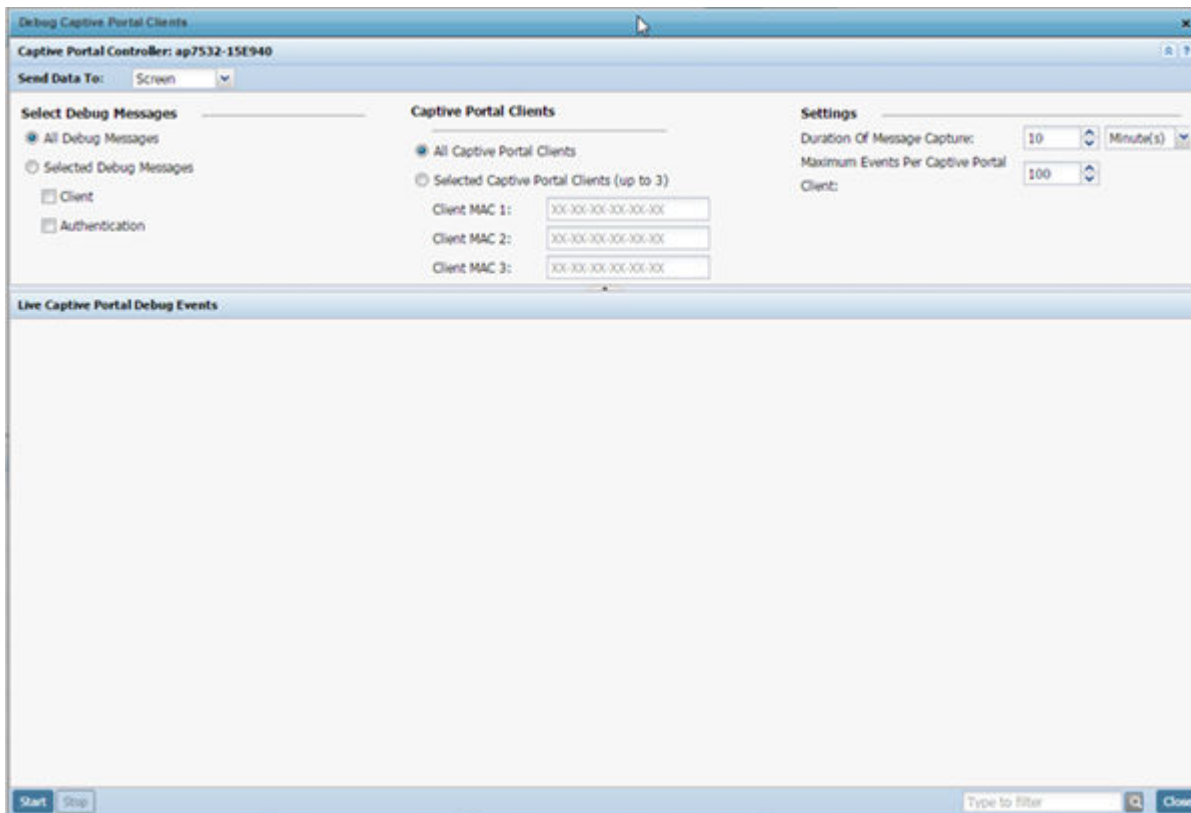
An administrator can select an RF domain and capture captive portal client and authentication debug messages at an administrator assigned interval and location. Captive portal debug information can either be collected historically or in real-time.

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 an 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 14: 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 <b>Selected Debug Messages</b> 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 <b>All Captive Portal Clients</b> 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 want to end the capture early, select **Stop**.

# 5 Device Configuration

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

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.

*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.

*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.

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.

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.

## Device Configuration

When a device is initially managed by an access point, RFS controller or NX series service platform it requires several basic parameters be set (system name, deployment location etc.). Additionally, the number of permitted device licenses needs to be assessed to determine whether additional access points can be adopted under the terms of the existing license. The Basic Configuration screen affords an administrator a means of assessing devices detected by a selected access point, controller or service platform and determining whether they need minor profile or RF Domain re-assignments to be optimally deployed.

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 access points, controllers and service platforms.

Device Configuration								?
System Name	Device	Type	RF Domain Name	Profile Name	Area	Floor	Overrides	
ap650-A65780	5C-0E-8B-A6-57-80	AP650	default	default-ap650			Clear	
ap650-A6ED14	5C-0E-8B-A6-ED-14	AP650	default	default-ap650				
ap7131-4BF364	B4-C7-99-4B-F3-64	AP71XX	default	default-ap71xx				
ap7131-99BB7C	00-23-68-99-BB-7C	AP71XX	TechPubs	default-ap71xx			Clear	
ap7131-9C63D4	00-23-68-9C-63-D4	AP71XX	default	default-ap71xx				
ap71xx-11E6C4	00-23-68-11-E6-C4	AP71XX	TechPubs	default-ap71xx			Clear	
ap7522-8330A4	84-24-8D-83-30-A4	AP7522	default	default-ap7522				
ap7532-1601C4	84-24-8D-16-01-C4	AP7532	default	default-ap7532			Clear	
ap7532-80C2AC	84-24-8D-80-C2-AC	AP7532	TechPubs	default-ap7532			Clear	
ap7562-84A224	84-24-8D-84-A2-24	AP7562	TechPubs	default-ap7562			Clear	
ap8132-711728	B4-C7-99-71-17-28	AP81XX	TechPubs	default-ap81xx			Clear	
ap8132-74B45C	B4-C7-99-74-B4-5C	AP81XX	TechPubs	default-ap81xx			Clear	
nx9500-6C8809	B4-C7-99-6C-88-09	NX9000	TechPubs	default-nx9000			Clear	
rfs4000-880DA7	00-23-68-88-0D-A7	RFS4000	TechPubs	default-rfs4000			Clear	
rfs6000-380649	00-15-70-38-06-49	RFS6000	TechPubs	default-rfs6000			Clear	
rfs6000-6DB5D4	B4-C7-99-6D-B5-D4	RFS6000	TechPubs	default-rfs6000			Clear	
rfs6000-81742D	00-15-70-81-74-2D	RFS6000	TechPubs	default-rfs6000			Clear	
rfs7000-6DCD4B	B4-C7-99-6D-CD-4B	RFS7000	TechPubs	default-rfs7000			Clear	
t5-ED7C6C	B4-C7-99-ED-7C-6C	T5	TechPubs	default-t5			Clear	

Type to search in tables Row Count: 19

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

<b>System Name</b>	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.
<b>Device</b>	Displays the device's factory assigned MAC address used as hardware identifier. The MAC address cannot be revised with the device's configuration.
<b>Type</b>	Displays the device model for the listed access point, controller or service platform.

<b>RF Domain Name</b>	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.
<b>Profile Name</b>	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.
<b>Area</b>	Lists the physical area where the device is deployed. This can be a building, region, campus or other area that describes the deployment location.
<b>Floor</b>	Lists the building Floor name representative of the location within the area or building the device 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.
<b>Overrides</b>	The Overrides column contains an option to clear all profile overrides for any devices that contain overrides. This uniformly restores the device's configuration to that shared by other devices utilizing the same profile. To clear an override, select the clear button to the right of the device.

- 4 Select **Add** to create a new device, select **Edit** to modify an existing device or select **Delete** to remove an existing device.

## Basic 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/adjustments 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 access points, controllers and service platforms. 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. 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 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 peers. The listed devices can either be other access points, controllers or service platforms.

- 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.

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

The screenshot shows the 'Configuration' window with the following sections and fields:

- Configuration:** System Name: nx9500-0C9848
- Location:** Area, Floor, Floor Number (1, range 1 to 4,094), Latitude Coordinate (0.0000, range -90.0000 - 90.0000), Longitude Coordinate (0.0000, range -180.0000 - 180.0000)
- RF Domain:** RF Domain Name: default
- Profile:** Profile Name: default-nx9000
- Device Overrides:** Clear Overrides button
- Set Clock:** Device Time: 2013-03-06 23:31:33 UTC, Refresh button, New Time: 1:00 AM, Update Clock button

A warning message at the bottom states: 'Setting the clock may logout the current session.' Buttons for OK, Reset, and Exit are at the bottom right.

- 5 Set the following **Configuration** settings for the target device:

<b>System Name</b>	Provide the selected device a system name up to 64 characters. This is administrator defined device name appearing within the RF Domain or Profile the device supports.
<b>Area</b>	Assign the device an <i>Area</i> name representative of the location the access point, 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.
<b>Floor</b>	Assign the target a device a building <i>Floor</i> name representative of the location the access point, controller or service platform 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.
<b>Floor Number</b>	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.

<b>Latitude Coordinate</b>	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.
<b>Longitude Coordinate</b>	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.

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

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 [RF Domains](#) on page 689 or [Managing RF Domains](#) on page 690.

- 7 Use the **Profile** drop-down menu to select an existing RF Domain for device membership.
- 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.
- 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 Select **OK** to save the changes made to the device's Basic Configuration. Selecting **Reset** reverts the screen to its last saved configuration.

## License Configuration

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



### Note

The **Licenses** screen is available only to controllers and service platforms capable of sustaining device connections, and thus requires license support to set the maximum number of device connections permitted. The License screen is not available for AP621 and AP650 model access points that are reliant on their connected controller or service platform for their management.

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

**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 <http://support.extremenetworks.com/>.

---

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 **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.



## 3 Select Licenses.

**Device Serial Number**

Serial Number B4C7990C9848

**AP Licenses Details**

AP Licenses

Licenses	Device	Cluster
AP Adoptions	0	0
AP Licenses	48	48
AP Lent Licenses	0	0
AP Borrowed Licenses	0	0
AP Total Licenses	48	48

**AAP Licenses Details**

Adaptive AP Licenses

Licenses	Device	Cluster
AAP Adoptions	21	21
AAP Licenses	10240	20480
AAP Lent Licenses	0	0
AAP Borrowed Licenses	0	0
AAP Total Licenses	10240	20480

**Security Licenses**

Advanced Security

Advanced WPS Licenses

OK Reset Exit

**Figure 15: 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, it is important to distinguish between NOC controllers and site controllers.

NOC controllers are NX 9500 and NX 9510.

The site controller is RFS 4000.

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

AP Adoptions	<p>The <b>Device</b> 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, five 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.</p> <p>The <b>Cluster</b> 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.</p>
AP Licenses	<p>The <b>Device</b> 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.</p> <p>The <b>Cluster</b> column lists the number of APs available for adoption by cluster members under the restrictions of the licenses, as pooled amongst the cluster members.</p>
AP Lent Licenses	<p>Lent licenses are the total number of AP licenses the NOC controller lends (if needed) to its site controllers so that a site controller 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).</p>

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. AP borrowed licenses can be non-zero only on site controllers.
AP Total Licenses	The cumulative number of both <b>Device</b> and <b>Cluster</b> AP licenses supported by the listed controller or service platform.

### Note

The following is a licensing example: Assume there's 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 AP licenses (8 minus 3) to S1, and 6 AP licenses (10 minus 4) 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 plus 6 to S2)
- AP Borrowed Licenses: 0
- AP Total Licenses: 1013 (1024 minus 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 plus 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 plus 6 borrowed)

- 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 <b>Device</b> 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, five 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 <b>Cluster</b> 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 <b>Device</b> 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 <b>Cluster</b> 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 <b>Device</b> and <b>Cluster</b> AAP licenses supported by the listed controller or service platform.

- 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, and NX9000 series service platforms.

- 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.

- Click **OK** to save the changes made to the applied licenses.  
Click **Reset** to revert to the last saved configuration.

## Assigning 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 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 access point locally, while the private portion remains on a secure area of the client.

To configure certificate usage:

- 1 Select **Configuration > Devices** from the Web UI.

The **Device Configuration** screen displays a list of managed devices or peers (other access points, controllers or service platforms).

- 2 Select **Certificates** from the Device menu.

**Figure 16: Device Certificates Screen**

- 3 Set the following **Management Security** certificate configuration:

SSH RSA Key	Either use the <b>default_rsa_key</b> or select <b>Stored</b> to enable a drop-down menu where an existing certificate can be used. To use an existing key, select <b>Launch Manager</b> . For more information, see <a href="#">RSA Key Management</a> on page 65.
-------------	---

**Note**

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

- 4 Set the following **RADIUS Security** certificate configurations:

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

- 5 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 **Stored** to enable a drop-down menu where an existing certificate/trustpoint can be used. To use an existing trustpoint, select **Launch Manager**.

- 6 Click **OK** to save the changes made to the certificate configurations. Click **Reset** to revert the screen to its last saved configuration.

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

- [Certificate Management](#) on page 54
- [RSA Key Management](#) on page 65
- [Certificate Creation](#)
- [Generating a Certificate Signing Request](#)

### *Certificate Management*

A *stored* certificate can be used from a different managed device if you prefer not 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..

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

Certificates Name	RSA Keys	Valid
default-trustpoint	CN=NX9000-B4-C7-99	02:02:2013 18:31:49 UT

**Certificate Details**

Subject Name :

Alternate Subject Name :

Issuer Name :

Serial Number :

RSA Key Used :

Is Self Signed :

RSA Key Used :

CRL Present :

Is CA :

**Validity**

Valid From :  Valid Until :

**Figure 17: Certificate Management - Manage Certificates Screen**

- 2 Select a device from among those displayed to review its certificate information.
- 3 Refer to **All Certificate Details** to review the certificate's properties, self-signed credentials, validity duration, and CA information.

- 4 To optionally import a certificate, click the **Import** button at the bottom of the **Manage Certificates** screen.

The **Import New Trustpoint** screen displays.

**Figure 18: Certificate Management - Import New Trustpoint Screen**

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

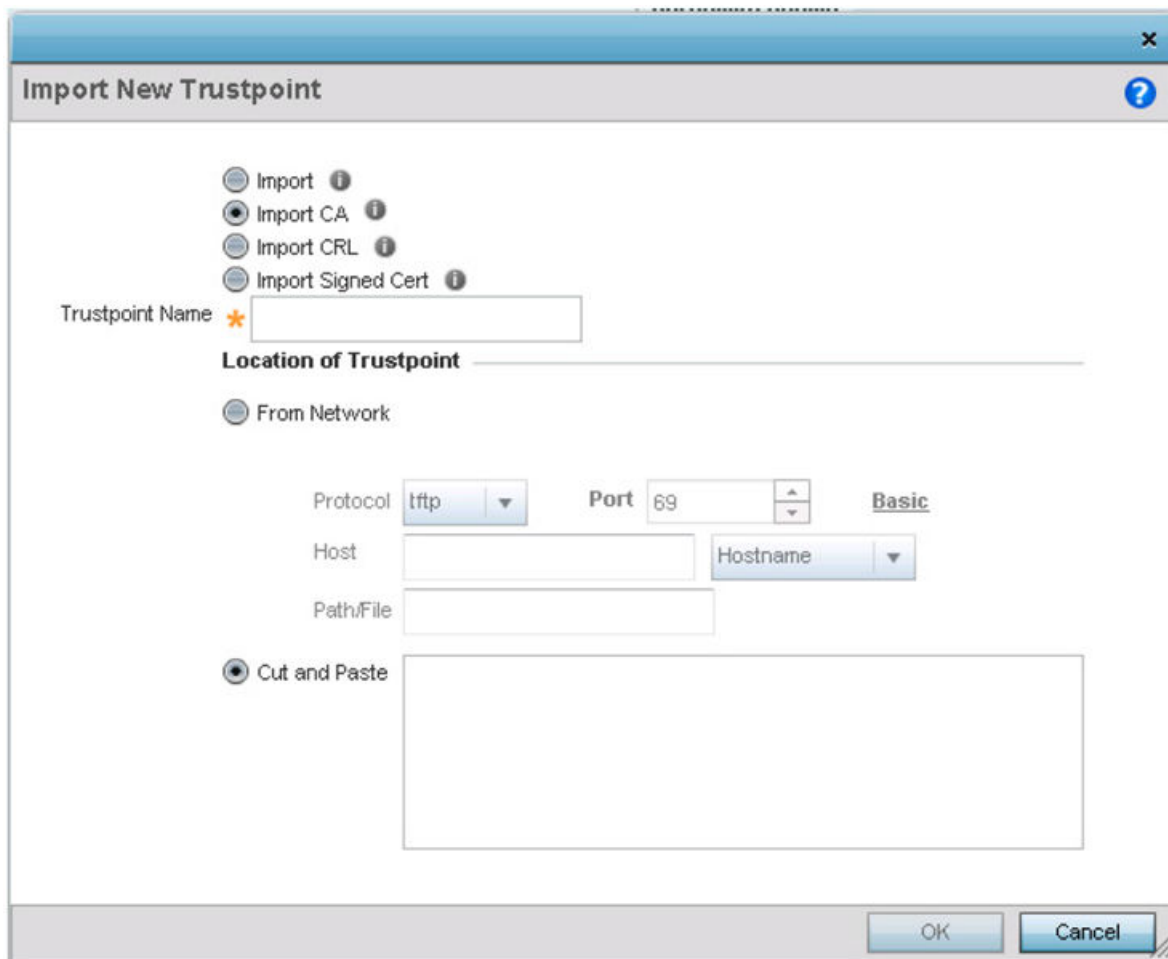
Trustpoint Name	Enter the 32-character maximum name assigned to the target trustpoint. The trustpoint signing the certificate can be a certificate authority, a corporation, or an individual.
URL	Provide the complete URL to the location of the trustpoint. If needed, click <b>Advanced</b> to expand the 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: <ul style="list-style-type: none"> <li>• tftp</li> <li>• ftp</li> <li>• sftp</li> <li>• http</li> <li>• cf</li> <li>• usb1-4</li> </ul>
Port	Set the port. This option is not valid for <b>cf</b> and <b>usb1-4</b> .
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 <b>cf</b> and <b>usb1-4</b> . Select <b>IPv4 Address</b> to use an IPv4 formatted address as the host. Select <b>IPv6 Address</b> 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 Click **OK** to import the defined trustpoint.  
Click **Cancel** to revert to the last saved configuration.

- 7 To optionally import a CA certificate, select **Import CA** 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 19: 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, click <b>Advanced</b> to expand the dialog to display network address information to the location of the target trustpoint. The number of additional fields populating the screen depends on the selected protocol.
Advanced/Basic	Click <b>Advanced</b> or <b>Basic</b> 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: <ul style="list-style-type: none"> <li>• tftp</li> <li>• ftp</li> <li>• sftp</li> <li>• http</li> <li>• cf</li> <li>• usb1-4</li> </ul>
Port	Set the port. This option is not valid for <b>cf</b> and <b>usb1-4</b> .
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 <b>cf</b> and <b>usb1-4</b> . Select <b>IPv4 Address</b> to use an IPv4 formatted address as the host. Select <b>IPv6 Address</b> 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 <b>Cut and Paste</b> to copy an existing CA into the field. When pasting, no additional network address information is required.

- 9 Click **OK** to import the defined CA certificate.  
Click **Cancel** to revert to the last saved configuration.

- 10 To optionally import a a CRL to a controller or service platform, select **Import CRL** in the **Certificate Management** screen.

If a certificate displays in 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 Certificate Revocation List \(CRL\) Configuration](#) on page 620.

**Import New Trustpoint**

Import ⓘ  
 Import CA ⓘ  
 Import CRL ⓘ  
 Import Signed Cert ⓘ

Trustpoint Name \*

**Location of Trustpoint**

From Network

Protocol  Port  **Basic**

Host

Path/File

Cut and Paste

**Figure 20: 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 <b>From Network</b> 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, click <b>Advanced</b> to expand the dialog to display network address information to the location of the CRL. The number of additional fields populating the screen depends on the selected protocol.
Advanced/Basic	Click <b>Advanced</b> or <b>Basic</b> to switch between a basic URL and an advanced location to specify trustpoint location.
Protocol	Select the protocol used for importing the CRL. Available options include: <ul style="list-style-type: none"> <li>• tftp</li> <li>• ftp</li> <li>• sftp</li> <li>• http</li> <li>• cf</li> <li>• usb1-4</li> </ul>
Port	Set the port. This option is not valid for <b>cf</b> and <b>usb1-4</b> .
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 <b>cf</b> and <b>usb1-4</b> . Select <b>IPv4 Address</b> to use an IPv4 formatted address as the host. Select <b>IPv6 Address</b> 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 <b>Cut and Paste</b> to copy an existing CRL into the field. When pasting, no additional network address information is required.

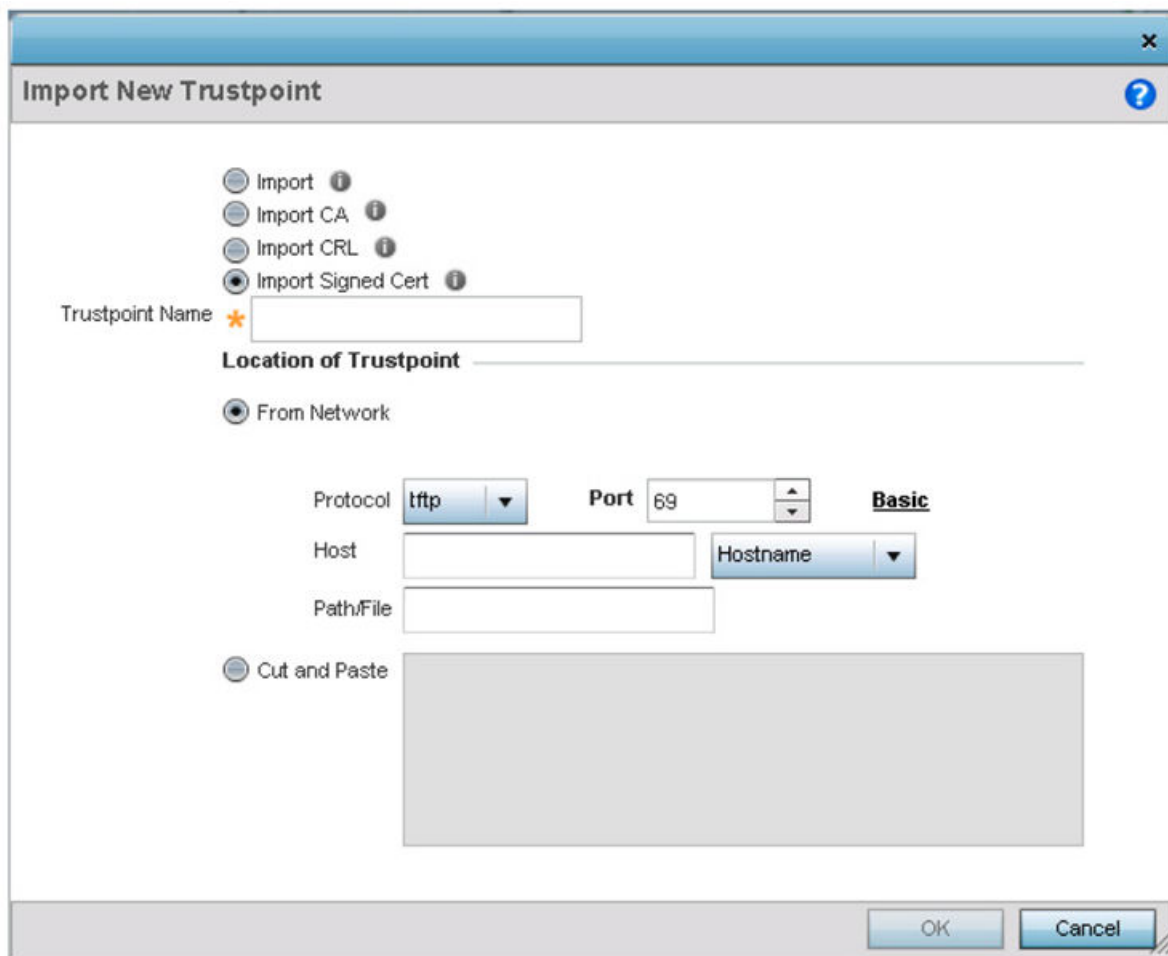
- 12 Click **OK** to import the CRL.

Click **Cancel** to revert to the last saved configuration.

- 13 To import a signed certificate, select **Import Signed Cert** in 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 21: Certificate Management - Import Signed Cert Screen**

- 14 Define the following configuration parameters required for the **Import** of the signed certificate:

Certificate Name	Enter the 32-character maximum trustpoint name with which the certificate should be associated.
From Network	Select <b>From Network</b> to provide network address information to the location of the signed certificate. The number of additional fields that populate the screen is also dependent on the selected protocol. <b>From Network</b> is the default setting.

URL	Provide the complete URL to the location of the signed certificate. If needed, click <b>Advanced</b> to expand the dialog to display network address information to the location of the signed certificate. The number of additional fields populating the screen depends on the selected protocol.
Protocol	Select the protocol used for importing the signed certificate. Available options include: <ul style="list-style-type: none"> <li>• tftp</li> <li>• ftp</li> <li>• sftp</li> <li>• http</li> <li>• cf</li> <li>• usb1-4</li> </ul>
Port	Set the port. This option is not valid for <b>cf</b> and <b>usb1-4</b> .
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 <b>cf</b> and <b>usb1-4</b> . Select <b>IPv4 Address</b> to use an IPv4 formatted address as the host. Select <b>IPv6 Address</b> 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 <b>Cut and Paste</b> to copy an existing certificate into the field. When pasting, no additional network address information is required.

15 Click **OK** to import the signed certificate.

Click **Cancel** to revert to the last saved configuration.

16 To optionally export a trustpoint to a remote location, select **Export** 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 is more than one RADIUS authentication server, export the certificate and do not generate a second key unless you want to deploy two root certificates.

**Figure 22: 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, a corporation, or an individual..
URL	Provide the complete URL to the location of the trustpoint. If needed, click <b>Advanced</b> to expand the dialog to display network address information to the location of the trustpoint. The number of additional fields populating the screen depends on the selected protocol.



Protocol	Select the protocol used for exporting the target trustpoint. Available options include: <ul style="list-style-type: none"> <li>• tftp</li> <li>• ftp</li> <li>• sftp</li> <li>• http</li> <li>• cf</li> <li>• usb1-4</li> </ul>
Port	Set the port. This option is not valid for <b>cf</b> and <b>usb1-4</b> .
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 <b>cf</b> and <b>usb1-4</b> . Select <b>IPv4 Address</b> to use an IPv4 formatted address as the host. Select <b>IPv6 Address</b> 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 <b>Cut and Paste</b> to copy an existing trustpoint into the field. When pasting, no additional network address information is required.

19 Click **OK** to export the defined trustpoint.

Click **Cancel** to revert to the last saved configuration.

20 To optionally delete a trustpoint, click **Delete** in the **Certificate Management** screen.

Provide the trustpoint name in the **Delete Trustpoint** screen and optionally select **Delete RSA Key** to remove the RSA key along with the trustpoint. Click **OK** to proceed with the deletion, or **Cancel** to revert to the **Certificate Management** screen.

### *RSA Key Management*

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. The algorithm 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 In the **Certificate Management** screen, select **Launch Manager** from either the SSH RSA Key, RADIUS Certificate Authority, or RADIUS Server Certificate parameters.

- Click **RSA Keys** from the **Certificate Management** screen.

The screenshot displays the 'RSA Keys' management interface. At the top, there are navigation tabs: 'Manage Certificates', 'RSA Keys' (selected), 'Create Certificate', and 'Create CSR'. Below the tabs is a header 'RSA Keys' with a help icon. The main content is divided into two sections: 'All Certificates Details' and 'Certificate Details'.

**All Certificates Details**

RSA Name	Size (Kb)	RSA Public Key
default_rsa_key	1024	-----BEGIN PUBLIC KEY----- MIGIMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDA5Um7WYz4Mv2Vgsh3qbdMmF3 0v2URptgT3y8ra4eVzCX5QPE2jwq9yM2mpGmYVq3RPVEr+FAA4tkkoXWROsX7Q/ 6pnXBS5evxGfPaq4+LLXvJ+RUlpm7D5P0LYnWCIz+DwZJrOwdeRa09RBVAvocY76 ZgEibeNf8M0pMURWQIDAQAB -----END PUBLIC KEY-----

**Certificate Details**

RSA Name: default\_rsa\_key  
 Size: 1024  
 RSA Public Key: -----BEGIN PUBLIC KEY-----  
 MIGIMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDA5Um7WYz4Mv2Vgsh3qbdMmF3  
 0v2URptgT3y8ra4eVzCX5QPE2jwq9yM2mpGmYVq3RPVEr+FAA4tkkoXWROsX7Q/  
 6pnXBS5evxGfPaq4+LLXvJ+RUlpm7D5P0LYnWCIz+DwZJrOwdeRa09RBVAvocY76  
 ZgEibeNf8M0pMURWQIDAQAB  
 -----END PUBLIC KEY-----

At the bottom of the screen, there are four buttons: 'Generate Key', 'Import', 'Export', and 'Delete'.

**Figure 23: Certificate Management - RSA Keys Screen**

- 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.

- Click **Generate Key** to create a new key with a defined size.

**Figure 24: Certificate Management - Generate RSA Keys Screen**

- 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.

- Click **OK** to generate the RSA key.  
Click **Cancel** to revert to the last saved configuration.

- 7 To optionally import an RSA key, select **Import** from the **Certificate Management > RSA Keys** screen.

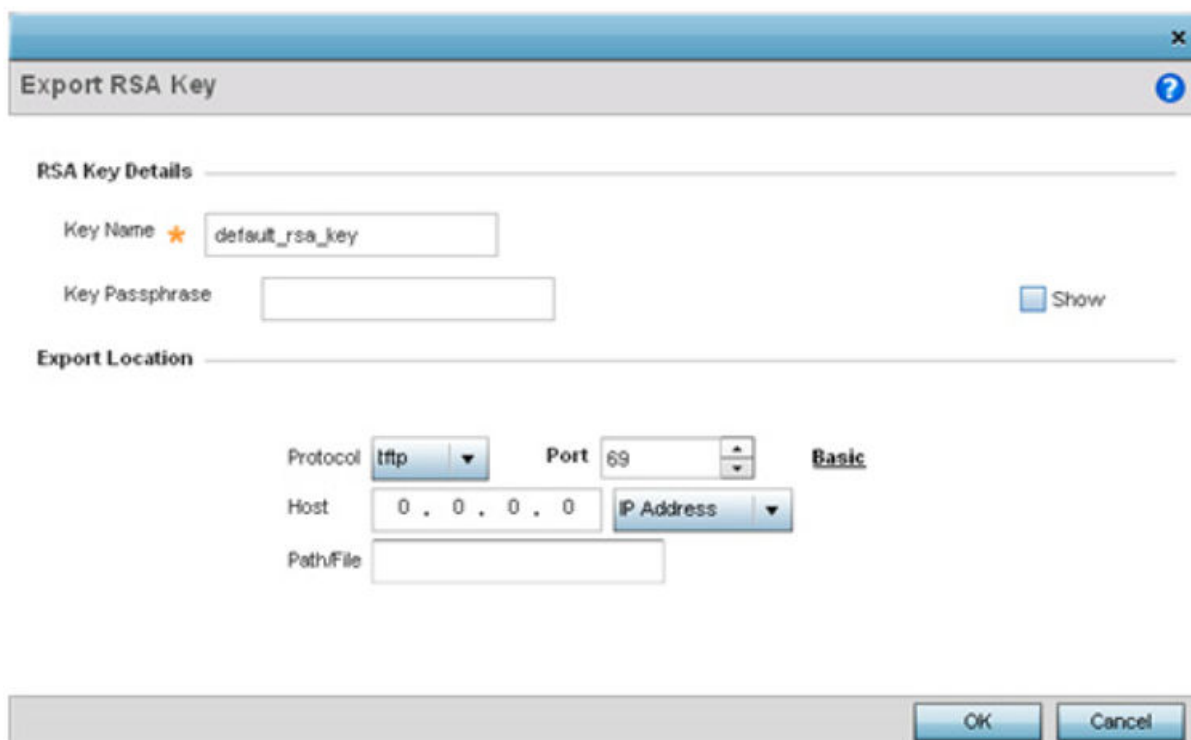
**Figure 25: Certificate Management - Import New RSA Key Screen**

- 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. Click <b>Show</b> expose the actual characters used in the passphrase. When <b>Show</b> is not selected, the passphrase displays as a series of asterisks (****).
URL	Provide the complete URL to the location of the RSA key. If needed, click <b>Advanced</b> 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 <b>Advanced</b> or <b>Basic</b> 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: <ul style="list-style-type: none"> <li>tftp</li> <li>ftp</li> <li>sftp</li> <li>http</li> <li>cf</li> <li>usb1-4</li> </ul>
Port	Set the port. This option is not valid for <b>cf</b> and <b>usb1-4</b> .

Host	Provide the hostname string 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 <b>cf</b> and <b>usb1-4</b> . Select <b>IPv4 Address</b> to use an IPv4 formatted address as the host. Select <b>IPv6 Address</b> 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.

- Click **OK** to import the defined RSA key.  
Click **Cancel** to revert to the last saved configuration.
- To optionally export an RSA key, select **Export** from the **Certificate Management > RSA Keys** screen.



**Figure 26: Certificate Management - Export RSA Key Screen**

- 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 used by both the controller or service platform and the server. Click <b>Show</b> expose the actual characters used in the passphrase. When <b>Show</b> is not selected, the passphrase displays as a series of asterisks (****).
URL	Provide the complete URL to the location of the key. If needed, click <b>Advanced</b> 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: <ul style="list-style-type: none"> <li>tftp</li> <li>ftp</li> <li>sftp</li> <li>http</li> <li>cf</li> <li>usb1-4</li> </ul>
Port	Set the port. This option is not valid for <b>cf</b> and <b>usb1-4</b> .
Host	Provide the hostname string 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 <b>cf</b> and <b>usb1-4</b> . Select <b>IPv4 Address</b> to use an IPv4 formatted address as the host. Select <b>IPv6 Address</b> 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.

- Click **OK** to export the defined RSA key.  
Click **Cancel** to revert to the last saved configuration.
- To optionally delete a key, click **Delete** in the **Certificate Management > RSA Keys** screen.  
Provide the key name in the **Delete RSA Key** screen and select **Delete Certificates** to remove the certificate. Click **OK** to proceed with the deletion, or **Cancel** to revert to the **Certificate Management** screen.

### Certificate Creation

Use the **Certificate Management** screen to create 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:

- In the **Certificate Management** screen, select **Launch Manager** from either the SSH RSA Key, RADIUS Certificate Authority, or RADIUS Server Certificate parameters.
- Select **Create Certificate** from the upper, left-hand, side of the **Certificate Management** screen.

**Figure 27: 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 <b>Use Existing</b> 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 <b>Create New</b> to enter a 32-character maximum name used to identify the RSA key. Set the size of the key to either 1,024 or 2,048 bits. We recommend leaving this value at the default setting of 2,048 to ensure optimum functionality.

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



Certificate Subject Name	Select either <b>auto-generate</b> to automatically create the certificate's subject credentials or <b>user-configured</b> to manually enter the credentials of the self-signed certificate. The default setting is <b>auto-generate</b> .
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 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 the organization represented in the certificate. This is a required field.
Organizational Unit (OU)	Enter the organization unit represented in the certificate. This is a required field.
Common Name (CN)	If there is 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): an unambiguous domain name that absolutely specifies the node's position in the DNS tree hierarchy. To distinguish an FQDN from a regular domain name, a trailing period is added - for example, <i>somehost.example.com</i> . 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. IPv6 formatted addresses are not permitted.

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

### Generating a Certificate Signing Request

A certificate signing request (CSR) is a message from a requestor to a certificate authority to apply for a digital certificate. The CSR is composed of a block of encrypted text generated on the server where the certificate will be used. It contains the organization name, common name (domain name), locality, and country.

An 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 it 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 In the **Certificate Management** screen, select **Launch Manager** from either the SSH RSA Key, RADIUS Certificate Authority, or RADIUS Server Certificate parameters.
- 2 Select **Create CSR** from the upper, left-hand, side of the **Certificate Management** screen.



**Figure 28: Certificate Management - Create CSR Screen**

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

RSA Key	Select <b>Use Existing</b> 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 <b>Create New</b> to enter a 32-character maximum name used to identify the RSA key. Set the size of the key to either 1,024 or 2,048 bits. We recommend leaving this value at the default setting of 2,048 to ensure optimum functionality.
---------	--

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

Certificate Subject Name	Select either <b>auto-generate</b> to automatically create the certificate's subject credentials or <b>user-configured</b> to manually enter the credentials of the self-signed certificate. The default setting is <b>auto-generate</b> .
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 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 organization unit represented in the CSR. This is a required field.
Common Name (CN)	If there is 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): an unambiguous domain name that absolutely specifies the node's position in the DNS tree hierarchy. To distinguish an FQDN from a regular domain name, a trailing period is added – for example, <i>somehost.example.com</i> . 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. IPv6 formatted addresses are not permitted.

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

## Wired 802.1x Configuration

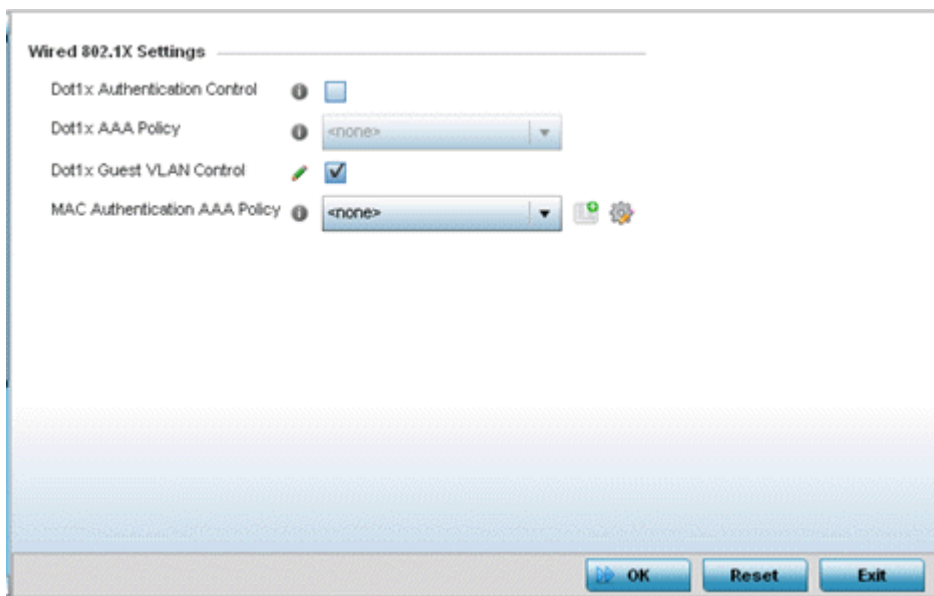
802.1X is an IEEE standard for media-level (Layer 2) access control, providing the capability to permit or deny connectivity based on user or device identity. 802.1X allows port based access using authentication. An 802.1X enabled port can be dynamically enabled or disabled depending on user identity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

To configure a device's wired 802.1x configuration:

- 1 Select **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.

- 3 Select **Wired 802.1x** from the Device menu options.



**Figure 29: Wired 802.1x Screen**

- 4 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	Select a AAA policy to associate with wired 802.1x traffic. If a suitable AAA policy does not exist, click the <b>Create</b> icon to create a new policy or the <b>Edit</b> icon to modify an existing policy.
Dot1x Guest VLAN Control	Select this option to globally enable 802.1x guest VLANs for the selected device.
MAC Authentication AAA Policy	Select a AAA authentication policy for MAC address authentication. If a suitable MAC AAA policy does not exist, click the <b>Create</b> icon to create a new policy or the <b>Edit</b> icon to modify an existing policy.

- 5 Click **OK** to save the changes made to the 802.1x configuration.  
Click **Reset** to revert to the last saved configuration.

## RF Domain Overrides

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, these devices share many configuration attributes because their general client support roles are very similar. However, device configurations may need periodic refinement from their original RF Domain administered design.

A controller's or service platform's configuration contains at least one default RF Domain, but it 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. 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 to a single RF Domain, the greater the likelihood one of the device's configuration requiring an override changing that device's configuration from the original RF Domain assignment shared by other devices of that model type.

To review the RF Domain's original configuration requirements and the options available for a target device, refer to [Managing RF Domains](#) on page 690.

To define a device's RF Domain override configuration, refer to the following sections:

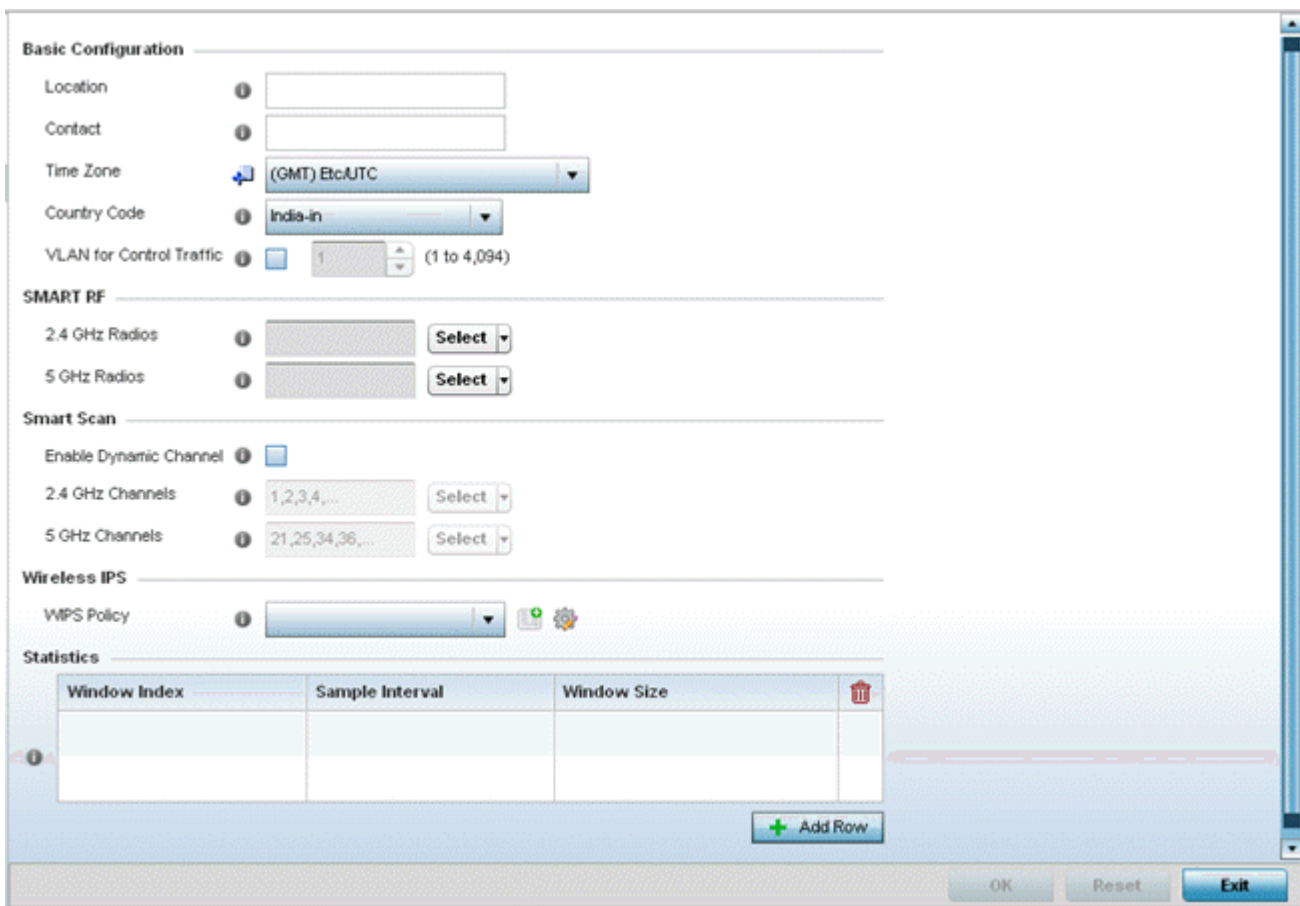
- [Basic RF Domain Configuration](#) on page 76
- [RF Domain Sensor Configuration](#) on page 78
- [RF Domain WLAN Override Configuration](#) on page 81

### *Basic RF Domain Configuration*

To define a device's RF Domain basic override configuration:

- 1 Select **Configuration** > **Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- 3 Expand the **RF Domain Overrides** menu option to display its sub-menu options.

4 Select **RF Domain**.



**Figure 30: 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 **Clear Overrides**. This removes all overrides from the device.

- 5 Refer to the **Basic Configuration** field to review the basic settings defined for the target device's RF Domain configuration, and optionally assign or 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 set for the device as part of its RF Domain configuration.
Country Code	Set the country code set for 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.



- 6 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.

- 7 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 from the drop-down menu for 2.4 GHz Smart RF radios. (Device radios transmit in specific channels unique to their country of operation.)
5 GHz Channels	Select legal channels from the drop-down menu for 5 GHz Smart RF radios. (Device radios transmit in specific channels unique to their country of operation.)

- 8 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.

Click the **Create** icon to define a new WIPS policy that can be applied to the RF Domain, or click 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 759.

- 9 Use the **Licenses** drop-down menu to obtain and leverage feature licenses from RF Domain member devices.
- 10 Click **OK** to save the changes and overrides made to the RF Domain configuration.  
Click **Reset** to revert to the last saved configuration.

### *RF Domain Sensor Configuration*

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.

To define ADSP server credentials for WiNG controller or service platform data exchanges:

- 1 Select **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target device in the left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- 3 Expand the **RF Domain Overrides** menu option to display its sub-menu options.

- 4 Select **Sensor**.

**Sensor Appliance Configuration**

Server Id	IP Address.Hostname	Port
1	lancelot	443

**Note:** The default port used by AirDefense Server is 443 and the default port used by Advanced-WIPS on a Controller is 8443

OK Reset Exit



**Figure 31: RF Domain Overrides - Wireless Controller/ServicePlatform - Sensor Screen**

- 5 Click **+ Add Row** to populate the **Sensor Appliance Configuration** field with up to three rows for WIPS server credentials:

Server Id	Assign a numerical ID for up to three ADSP 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 ADSP sensor server by RF Domain member devices. A hostname cannot exceed 64 characters or contain an underscore.
Port	Specify the port of each ADSP sensor server utilized by RF member devices. The default port is 443.


- 6 If the device selected is an access point, configure the following settings in addition to the **Sensor Appliance Configuration**.

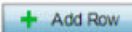
**Sensor Policy**

Sensor Policy   

**Note:** If the sensor is being used by ADSP for WIPS, any policy selected here will be discarded by the sensor. Please use ADSP channel settings instead to configure the sensor

**ExtremeLocation Appliance Configuration**


Server Id	IP Address/Hostname	Port	

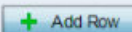


**ExtremeLocation Tenant Account**

Tenant Account

**Sensor Appliance Configuration**

Server Id	IP Address/Hostname	Port	



**NSight Sensor**

Enable NSight Sensor

OK Reset Exit

**Figure 32: RF Domain Overrides - Access Point - Sensor screen**

Sensor Policy	<p>Use the Sensor Policy drop-down menu to select a Sensor policy. If no Sensor policy exists, use the <b>Create</b> icon to create a new Sensor policy. Or, use the <b>Edit</b> icon to edit an existing Sensor policy if required.</p> <p><b>Note:</b> 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.</p>
---------------	--

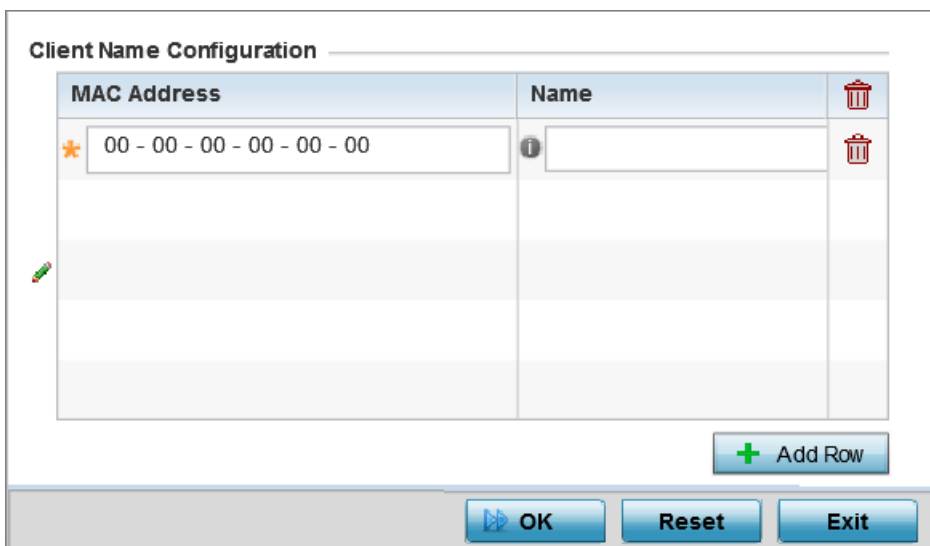
- 7 Enter the ExtremeLocation Tenant's account number in the **Tenant Account** field. Use this field to configure your ExtremeLocation Tenant account number. ExtremeLocation Tenants, at the time of registration, are communicated (via email) an account number uniquely identifying the Tenant. Configure this account number in the RF Domain context. When configured, RF Domain AP reports, pushed to the ExtremeLocation server, include the Tenant's account number along with the reporting AP's MAC address.



- 8 Select the **+ Add Row** button to populate the **ExtremeLocation Appliance Configuration** field with ExtremeLocation server details:

Server Id Policy	Use the spinner control to assign a numerical ID for the ExtremeLocation server resource.  <b>Note:</b> As of now only one server is supported.
IP Address/Hostname	Provide the hostname of the ExtremeLocation server used by RF Domain member devices. A hostname cannot exceed 64 characters or contain an underscore.  <b>Note:</b> Enter the ExtremeLocation server’s hostname and not the IP address, as the IP address is likely to periodically change in order to balance load across multiple Location servers.

- 9 Select the **Enable NSight Sensor** checkbox to enable the NSight module.
- 10 Click **OK** to save the changes to the sensor configuration.  
Click **Reset** to revert to the last saved configuration.
- 11 Select **Client Name** from the expanded list of **RF Domain Overrides**:



**Figure 33: RF Domain Overrides - Client Name screen**

- 12 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.

- 13 Click **OK** to save the changes to the client name configuration.  
Click **Reset** to revert to the last saved configuration.

*RF Domain WLAN Override Configuration*

To define a device’s RF Domain WLAN override configuration:



- 1 Select **Configuration > Devices** from the web UI.

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

- 2 Select a target device in the lower left-hand side of the UI.

You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.

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

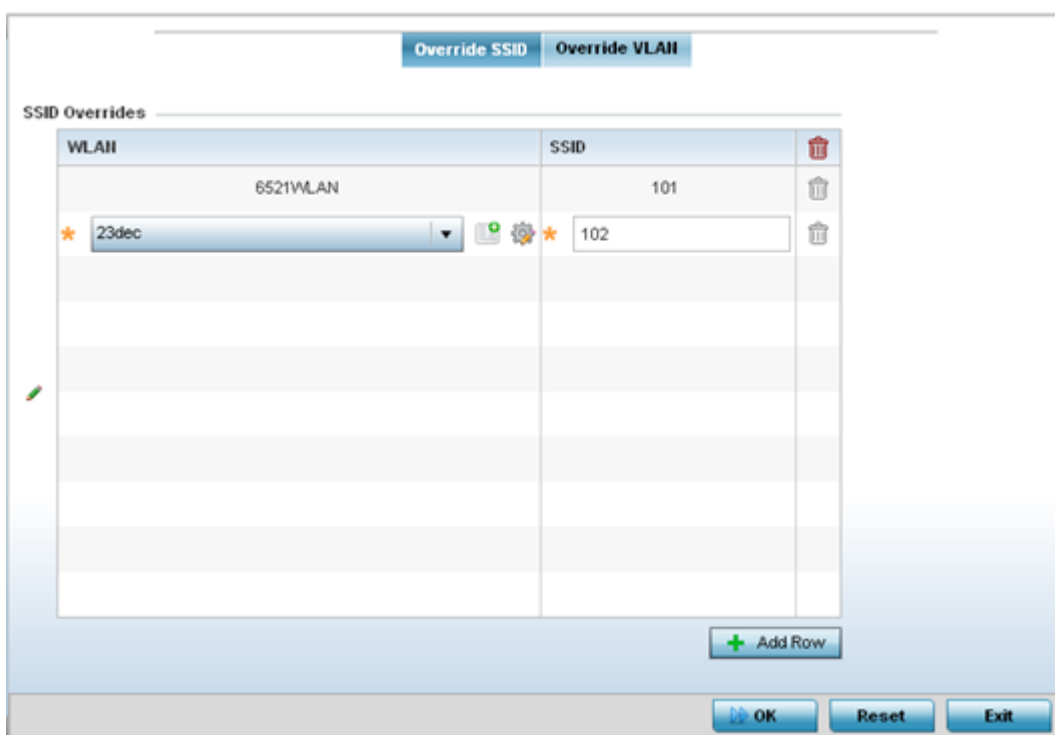
- 4 Select **WLAN Override**.



#### Note

The **WLAN Override** option is available only for access points – not for controllers or service platforms.

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



**Figure 34: WLAN Override screen - Override SSID Tab**

- 5 Optionally, define up to three overrides for the listed WLAN SSID assignment:

WLAN	Optionally use the drop-down menu to change the WLAN assignment for the listed access point. Click the <b>Create</b> icon to define a new WLAN configuration, or click the <b>Edit</b> 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 it is changed (overridden). The maximum number of characters used for the SSID is 32.

- 6 Click **+ Add Row** 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 **Clear Overrides**. This removes all overrides from the device.

- 7 Click **OK** to save the changes and overrides.  
Click **Reset** to revert to the last saved configuration.
- 8 Select the Override VLAN tab to review existing VLAN assignment overrides or to add or edit configurations.

The Override VLAN tab displays VLANs assigned to the access point's WLAN.

WLAN	VLANs
11Dtest	3
23dec	1

**Figure 35: WLAN Override screen - Override VLAN Tab**

- 9 Click **Add** to create a new client limit for a specific WLAN and VLAN, or click **Edit** to modify an existing configuration.

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

VLANS	Set a virtual interface ID (1 - 4094).
Wireless Client Limit	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 **Clear Overrides**. This removes all overrides from the device.

- 11 Click **OK** to save the changes and overrides.  
Click **Reset** to revert to the last saved configuration.

## Profile Overrides

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 within 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 controllers or access points. 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 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.

### General Overrides

To review a profile's original configuration requirements and the options available for a target device, refer to [General Profile Configuration](#) on page 519.

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.

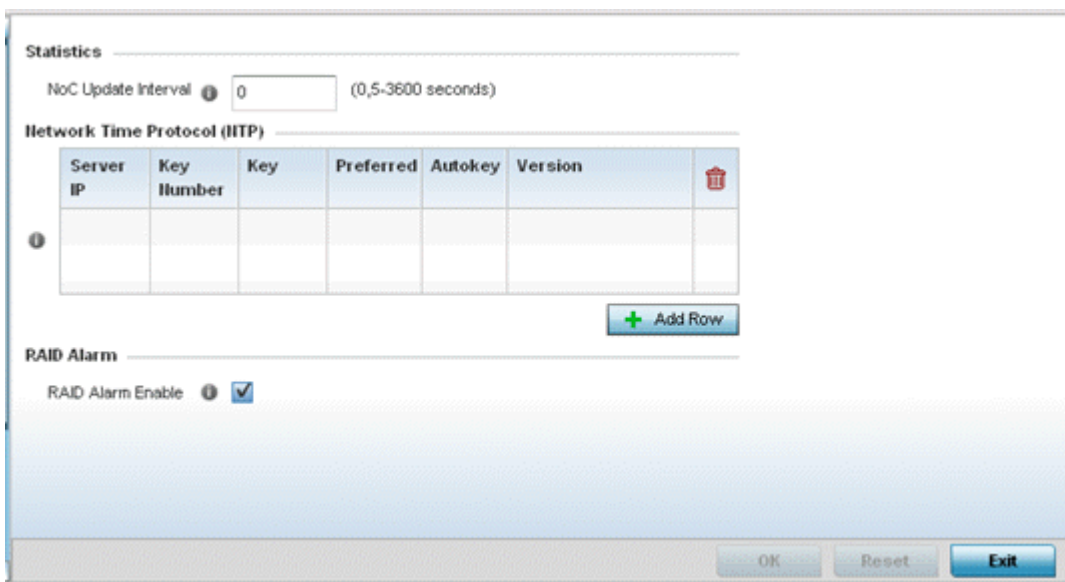
The Device Configuration screen displays a list of managed devices or peer controllers. The listed devices can be other controllers or access points.

- 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 does not display 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.

- 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 5-300 seconds for updates from the RF Domain manager to the controller.
- 8 Select **+ Add Row** below the Network Time Protocol (NTP) table to define (or override) the configurations of NTP server resources the controller uses it obtain its system time. Set the following parameters to define the NTP configuration:

<b>Server IP</b>	Set the IP address of each server as a potential NTP resource.
<b>Key Number</b>	Select the number of the associated <i>Authentication Key</i> for the NTP resource.
<b>Key</b>	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.
<b>Preferred</b>	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 and provide NTP calibration.
<b>AutoKey</b>	Select the radio button to enable an <i>Autokey</i> configuration for the controller and NTP resource. The default setting is disabled.
<b>Version</b>	Use the spinner control to specify the version number used by this NTP server resource. The default setting is 0.

- 9 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 NX 9000series service platform.



RAID controller drive arrays are available within NX 9000 series service platforms (NX 9000, NX 9500 and NX 9510 models) only. However, they can be administrated on behalf of a NX 9000 profile by a different model service platform or controller.

NX 9000 series 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. With the WING 5.5 release, 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.

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

### *Controller Cluster Configuration Overrides (Controllers and Service Platforms Only)*

A redundancy group (cluster) is a group of interactive access points, controllers or service platforms uniquely defined by the profile they share for their unique device type. Within the cluster, members discover and establish connections to other members and provide wireless self-healing support in the event of cluster member failure.

A cluster's AP load balance is typically distributed evenly amongst cluster members. 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.

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



#### **Note**

There is a minimum limit of 2 devices that can be configured as cluster members.

To apply an override (if required) to a profile's 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 access points, controllers or service platforms.

- 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.

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

<b>Cluster Mode</b>	A member can be in either an <i>Active</i> or <i>Standby</i> mode. All active members can adopt access point radios. Standby members only adopt access points when an active member has failed or sees an access point not adopted. The default cluster mode is Active and enabled for use with the profile.
<b>Cluster Name</b>	Define a name for the cluster name unique to its configuration or profile support requirements. The name cannot exceed 64 characters.
<b>Master Priority</b>	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 value is 128.
<b>Handle STP Convergence</b>	Select the radio button to enable <i>Spanning Tree Protocol (STP)</i> convergence for the controller. 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 devices. The spanning tree protocol disables redundant connections and uses the least costly path to maintain a connection between any two devices 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.

<b>Force Configured State</b>	Select the radio button to allow this Access Point, controller or service platform to take over for an active member if it were to fail. A standby cluster member takes the AP adopted by the failed member. If the failed cluster 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 device 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.
<b>Force Configured State Delay</b>	Specify a delay interval in minutes (1 - 1,800). This is the interval a standby cluster member waits before releasing adopted APs and reverts to a monitoring mode once a cluster member becomes active again after a failure. 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 IP Address table.

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

### Access Point Radio Power Overrides (Access Point Only)

A profile can manage the transmit output power of the access point radios.



#### 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, 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 radio 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 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.

**Power Mode Configuration on this AP**

Power Mode Automatic ▼

AP must be restarted for power-management change to take effect.

**802.3af Power Mode**

802.3af Mode Throughput ▼

**802.3at Power Mode**

802.3at Mode Throughput ▼

OK Reset Exit

- 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.

- 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.

- Select **OK** to save the changes and overrides made to the access point power configuration. Select **Reset** to revert to the last saved configuration.

### Access Point Adoption Overrides (Access Points Only)

Adoption is the process an access point uses to discover an available controller or service platform, pick the most desirable one, establish an association and optionally obtain an image upgrade and configuration. Adoption settings are 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 access point adoption requirements and profile settings.

---

#### 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, the auto provisioning policy mapping does not have an impact on subsequent adoptions by the same device.

---

An auto provisioning policy enables an administrator to define adoption rules for access points capable of being adopted by a controller or service platform.

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.

---

**Controller Group**

Preferred Group

**Controller Hello Interval**

Hello Interval   (1 to 120)

Adjacency Hold Time   (2 to 600)

**Controller VLAN**

VLAN   (1 to 4,094)

**Controller Hostnames**

Host	Pool	Routing Level	IPsec Secure	IPsec GW	Force	Remote VPII Client

Auto IPsec Tunnel parameters need to be configured when IPsec Secure is selected

- Define or override the **Preferred Group** used as optimal group of controllers for the access point's adoption. The name of the preferred group cannot exceed 64 characters.
- Set the following **Controller Hello Interval** settings manage message exchanges and connection re-establishments between adopting devices:

<b>Hello Interval</b>	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.
<b>Adjacency Hold Time</b>	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 than the hello interval.

- Select this option to define or override the **VLAN** the access point's associating controller or service platform is reachable on.

VLANs 0 and 4,095 are reserved and cannot be used by a VLAN.

- Enter **Controller Hostnames** as needed to define or override resources for access point adoption.

Select **+ Add Row** as needed to populate the table with IP Addresses or Hostnames of controllers used as access point adoption resources into the managed network.

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

<b>IPSec GW</b>	Select the numerical IP address or administrator defined hostname of the adopting controller resource.
<b>Force</b>	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.
<b>Remote VPN Client</b>	Displays whether a secure controller link has been established using a remote VPN client.

- 9 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.

*Controller Adoption Overrides (Controllers Only)*

Adoption is the process a controller or service platform uses to discover available access points and/or peer controllers/service platforms, establish an association and provision the requesting device. Adoption settings are configurable and supported within a profile and applied to other access points supported by the profile.

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.

- 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 Provision Policy** parameters:

<b>Use NOC Auto-Provisioning Policy</b>	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.
<b>Auto-Provisioning Policy</b>	Select an auto provisioning policy from the drop-down menu. To create a new auto provisioning policy, select the <i>Create</i> icon or modify an existing one by selecting the <i>Edit</i> icon.
<b>Learn and Save Network Configuration</b>	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.

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

<b>Allow Adoption of Devices</b>	Select either <i>access points</i> or <i>Controllers</i> (or both) to refine whether this controller or service platform can adopt networked access points or peer controller devices as well.
<b>Allow Adoption of this Controller</b>	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.
<b>Preferred Group</b>	If <i>Allow Adoption of this Controller</i> 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.
<b>Hello Interval</b>	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.
<b>Adjacency Hold Time</b>	Select this option to set a hold time interval (from 2 - 600 seconds) for the transmission of hello packets.

- 8 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.

<b>Host</b>	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.
<b>Pool</b>	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.
<b>Routing Level</b>	Define a routing level (either 1 or 2) for the link between adopting devices. The default setting is 1.
<b>IPSec Secure</b>	Enable this option to provide IPSec secure peer authentication on the connection (link) between the adopting devices. This option is disabled by default.
<b>IPSec GW</b>	Select the numerical IP address or administrator defined hostname of the adopting controller resource.

<b>Force</b>	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.
<b>Remote VPN Client</b>	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.

### *Overriding a Profile's Interface Configuration*

A profile's interface configuration can be defined to support separate physical Ethernet configurations both unique and specific to RFS 4000 controllers and NX 5500 and NX 7500 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 connected VLAN ID.

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 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 may need careful administration until a profile can be re-applied to the target device. For more information, refer to the following:

- [Ethernet Port Override Configuration](#) on page 94
- [Virtual Interface Override Configuration](#) on page 107
- [Port Channel Override Configuration](#) on page 124
- [VM Interface Override Configuration](#) on page 130
- [Radio Override Configuration](#) on page 136
- [WAN Backhaul Override Configuration](#) on page 153
- [PPPoE Override Configuration](#) on page 155
- [Bluetooth Configuration](#) on page 158

### **Ethernet Port Override Configuration**

Use an Ethernet port override to modify a device's Ethernet port configuration.

The following ports are available on RFS 4000 model controllers: ge1, ge2, ge3, ge4, ge5, up1.

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

- NX 5500: ge1, ge2
- NX 7500: ge1-ge10, xge1-xge2

GE ports are RJ-45 ports supporting 10/100/1000Mbps.

UP ports supports either RJ-45 or fiber. The UP port is the preferred means to connect to the backbone because it has a non-blocking 1gbps connection unlike the GE ports.

The following ports are available on access points:

- AP 6522 and AP6522M: GE1/POE (LAN)
- AP 6532: GE1/POE (LAN)
- AP 6562: GE1/POE (LAN)
- AP 7161: GE1/POE (LAN), GE2 (WAN)
- AP 7502: GE1, fe1, fe2, fe3
- AP 7522: GE1/POE (LAN), GE2 (WAN)
- AP 7532: GE1/POE (LAN), GE2 (WAN)
- AP 7602: GE1/POE (LAN), GE2 (WAN)
- AP 7612: GE1/POE (LAN), GE2 (WAN)
- AP 7622: GE1/POE (LAN)
- AP 7632: GE1/POE (LAN)
- AP 7662: GE1/POE (LAN), GE2 (WAN)
- AP 8132 and AP 8163: GE1/POE (LAN), GE2 (WAN)

T5 controllers have the following Ethernet port designations:

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

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

- 1 Select **Configuration > Devices** from the web UI.

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

- 2 Select a target device in the lower left-hand side of the UI.

You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.

- 3 Select **Profile Overrides > Interface**.

4 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 **Clear Overrides**. This removes all overrides from the device.

Name	Type	Description	Admin Status	Mode	Native VLAN	Tag Native VLAN	Allowed VLANs	Overrides
ge1	Ethernet	test	✓ Enabled	Access	5			
ge2	Ethernet		✓ Enabled	Trunk	4	✗	2-4,10	Clear
xge1	Ethernet		✓ Enabled	Access	1			
xge2	Ethernet		✓ Enabled	Access	1			
xge3	Ethernet		✓ Enabled	Access	1			
xge4	Ethernet		✓ Enabled	Access	1			

Type to search in tables Row Count: 6

Edit Exit

**Figure 36: Device Overrides - Ethernet Ports Screen**

## 5 Refer to the following to review port status and assess whether an override is warranted:

Name	The name of the physical port reporting runtime data and statistics. Supported ports vary by model. <ul style="list-style-type: none"> <li>RFS 4000: ge1, ge2, ge3, ge4, ge5, up1</li> <li>NX 5500: ge1, ge2</li> <li>NX 7500: ge1-ge10, xge1-xge2</li> </ul>
Type	The physical port type. <b>Cooper</b> is used on RJ45 Ethernet ports, and <b>Optical</b> materials are used on fiber optic gigabit Ethernet ports.
Description	An administrator defined description for the port.
Admin Status	A green check mark means the port is active and currently enabled with the profile. A red "X" means the port is currently disabled and not available for use. The interface status can be modified with the port configuration as needed.



Mode	<p>The profile's switching mode: either <b>Access</b> or <b>Trunk</b> (as defined in the <b>Ethernet Port Basic Configuration</b> screen).</p> <p>If <b>Access</b> is selected, the 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.</p> <p>If <b>Trunk</b> is selected, the port allows packets from a list of VLANs added to the trunk. The port supports multiple 802.1Q tagged VLANs and one native VLAN which can be tagged or untagged.</p>
Native VLAN	<p>The 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 over which untagged traffic is directed when using a port in <b>Trunk</b> mode.</p>
Tag Native VLAN	<p>A green check mark means the native VLAN is tagged. A red "X" means the native VLAN is untagged.</p> <p>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.</p>
Allowed VLANs	<p>The VLANs allowed to send packets over the listed port. Allowed VLANs are listed only when the port is in <b>Trunk</b> mode.</p>
Overrides	<p>If overrides have been applied to the port configuration, click <b>Clear</b> to clear the overrides and revert to the configuration originally defined by the administrator for this interface.</p>

- 6 To edit or override the configuration of an existing port, select it from among those displayed and click **Edit**.

The **Ethernet Port Basic Configuration** screen displays.

**Figure 37: Ethernet Ports - Basic Configuration Screen**

- 7 Set or override 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 it simply can be the name of the physical port.
Admin Status	Select <b>Enabled</b> to define this port as active to the profile it supports. Select <b>Disabled</b> to disable this physical port in the profile. It can be activated at any time when needed. Admin status is enabled by default.

Speed	Select the speed at which the port can receive and transmit data, 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 <b>Automatic</b> is selected. Select <b>Automatic</b> 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 <b>Half</b> , <b>Full</b> , or <b>Automatic</b> as the duplex option. Select <b>Half</b> 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 <b>Full</b> 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 <b>Automatic</b> to enable to the controller or service platform to dynamically duplex as port performance needs dictate. <b>Automatic</b> is the default setting.

- 8 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 Cisco discovery protocol for receiving data on this port. If enabled, the port sends out periodic interface updates to a multicast address to advertise its presence to neighbors.
Cisco Discovery Protocol Transmit	Select this option to allow the Cisco discovery protocol for transmitting data 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 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 option 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.

- 9 Set or override the following **Power Over Ethernet (PoE)** parameters (if supported and applicable):

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 RFS 4000 model controllers. 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.
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 <b>Critical</b> , <b>High</b> , or <b>Low</b> . This is the priority assigned to this port versus the power requirements of the other supports available on the controller or service platform.

- 10 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 777.

- 11 Set or override the following **Switching Mode** parameters to apply to the Ethernet port configuration:

Mode	Set the VLAN switching mode over the port: either <b>Access</b> or <b>Trunk</b> . If you select <b>Access</b> , the 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 you select <b>Trunk</b> , the port allows packets from a list of VLANs you add to the trunk. The port supports multiple 802.1Q tagged VLANs and one native VLAN which can be tagged or untagged. <b>Access</b> is the default mode.
Native VLAN	Define a 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 over which untagged traffic is directed when using a port in <b>Trunk</b> 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 to. 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 <b>Trunk</b> as the mode enables the <b>Allowed VLANs</b> parameter. Add VLANs that exclusively send packets over the listed port.

- 12 In the **Dynamic Link Aggregation (LACP)** area, set the following parameters to enable link aggregation on the selected GE port:

Port Channel	Select to configure the selected port as a member of a link aggregation group (LAG). Link aggregation is supported only on the following platforms: AP 7562, AP 7602, AP 7612, AP 8432, AP 8533, NX 5500, NX 75XX, NX 95XX, NX 9600, and VX 9000. 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. It also 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.  <b>Note:</b> if enabling LACP, 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.
Port Mode	Set the port mode as <b>Active</b> or <b>Passive</b> . If setting the port as a LAG member, specify whether the port is an active or passive member within the group. An active member initiates and participates in LACP negotiations. It is the active port that always transmits LACPDU irrespective of the remote device's port mode. The passive port only responds to LACPDU received from its corresponding active port. At least one port within a LAG, on either of the two negotiating peers, should be in the active mode. LACP negotiations are not initiated if all LAG member ports are passive. Further, the peer-to-peer LACP negotiations are always initiated by the peer with the lower system-priority value.
Port Priority	Select the Port Priority check box and set the selected Ethernet Port's priority value, within the LAG, from 1-65535. The selected port's actual priority within the LAG is determined by the port-priority value specified here along with the port's number. Higher the value, lower is the priority. Use this option to manipulate a port's priority. For example, in a LAG having five physical ports, four active and one standby, manually increasing the standby port's priority ensures that if one of the active port fails, the standby port is included in the LAG during re-negotiation.

- 13 Click **+ Add Row** and set or override the **Fabric Attach** parameters. This option enables WiNG devices (access points and controllers) as FA (Fabric Attach) Clients.

**Note**

To enable FA Client feature, the Ethernet port's switching mode should be set to trunk.

VLAN	Set the VLAN from 1 - 4094.
ISID	<p>User the spinner control to specify the ISID from 1 - 16777214. This is the ISID (Individual Service Identifier) associated with the VLAN interface specified above. Configuring a VLAN to ISID assignment, enables FA client operation on the selected Ethernet port.</p> <p>The FA Client requests acceptance of the VLAN to ISID mapping from the FAS within the FC (Fabric Connect) network. Once acceptance is achieved, the FC edge switch applies the ISID to the VLAN traffic from the device (AP or controller), and uses this ISID inside the Fabric.</p> <p><b>Note:</b> A maximum of 94 pairs of I-SID to VLAN mappings can be configured per Ethernet port.</p>

FA-enabled switches, in the FC network, send out LLDP messages with TLV extensions of Organization-specific TLV with OUI, to discover FA clients and advertise capabilities.

The FA-enabled client associates with the FAS (FA Server), and obtains provisioning information (management VLAN interface details, and whether the interface is tagged or not) that allows the client to be configured with parameters that allow traffic to flow through the Fabric to the WLAN controller. Use this option to configure the ISID to VLAN mapping that the FA Client uses to negotiate with the FAS.

You can configure FA Client capability on a device's profile as well as device contexts.

- 14 Optionally select **Port Channel** in 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 Click **OK** to save the changes and overrides made to the Ethernet port's basic configuration. Click **Reset** to revert to the last saved configuration.

16 Select the **Security** tab.

**Ethernet Ports**  
Name: ge1

**Basic Configuration** | **Security** | **Spanning Tree**

**Access Control**

- IPv4 Inbound Firewall Rules: <none>
- Inbound MAC Firewall Rules: <none>
- IPv6 Inbound Firewall Rules: <none>

**Trust**

- Trust ARP Responses:
- Trust DHCP Responses:
- ARP header Mismatch Validation:
- Trust 802.1p COS values:
- Trust IP DSCP:

**IPv6 Settings**

- Trust ND Requests:
- Trust DHCPv6 Responses:
- ND Header Mismatch Validation:
- RA Guard:

**802.1X Settings**

- Host Mode: single-host
- Guest VLAN: 1 (1 to 4,094)
- Port Control: force-authorized
- Re-authenticate:
- Max Re-authenticate Count: 2 (1 to 10)
- Quiet Period: 60 (1 to 65,535)
- Re-authenticate Period: 3600 (1 to 65,535)
- Port MAC Authentication:

**802.1X supplicant (client) feature**

- Enable:
- Username:
- Password:  Show

OK Reset Exit

**Figure 38: 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.
- 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.
  - 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 no firewall rules meet the data protection needs of the target port configuration, select the **Create** icon to define a new firewall rule or the **Edit** icon to modify an existing firewall rule.  
For more information, see [Configuring IP Firewall Rules](#) on page 732 or [Wireless Firewall](#) on page 714.
- 18 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. This option is disabled by default.
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. This option is enabled by default.
ARP Header Mismatch Validation	Select this option to enable a mismatch check for the source MAC in both the ARP and Ethernet header. This option is enabled by default.
Trust 802.1p COS values	Select this option to enable 802.1p COS values on this port. This option is enabled by default.
Trust IP DSCP	Select this option to enable IP DSCP values on this port. This option is enabled by default.



#### 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, even when a conflict exists.



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 Ethernet port. This option is disabled by default.
Trust DHCPv6 Responses	Select this option to 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 option 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 option is disabled by default.
RA Guard	Select this option to enable router advertisements or ICMPv6 redirects from this Ethernet port. This option is disabled by default.

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

Host Mode	Select the port mode for 802.1X authentication. Select <b>single-host</b> to bridge traffic from a single authenticated host. Select <b>multi-host</b> to bridge traffic from any host to this port. The default setting is <b>single-host</b> .
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	Set the way in which the port bridges traffic. Select one of the following options: <ul style="list-style-type: none"> <li>• <b>Automatic</b> - The port is set to the state as received from the authentication server.</li> <li>• <b>force-authorized</b> - Any traffic on the port is considered authenticated and is bridged as configured.</li> <li>• <b>force-unauthorized</b> - Any traffic on the port is considered unauthenticated and is not bridged.</li> </ul> The default setting is <b>force-authorized</b> .
Reauthenticate	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 number of reauthentication attempts (1-10) when a port tries to reauthenticate and fails. Once this count exceeds, the port is considered 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	Set the duration after which a controlled port is forced to reauthenticate. Set a value from 0 - 65535 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 RFS 4000 model controllers. Port MAC authentication may be enabled on ports in conjunction with Wired 802.1x settings for a MAC Authentication AAA policy.

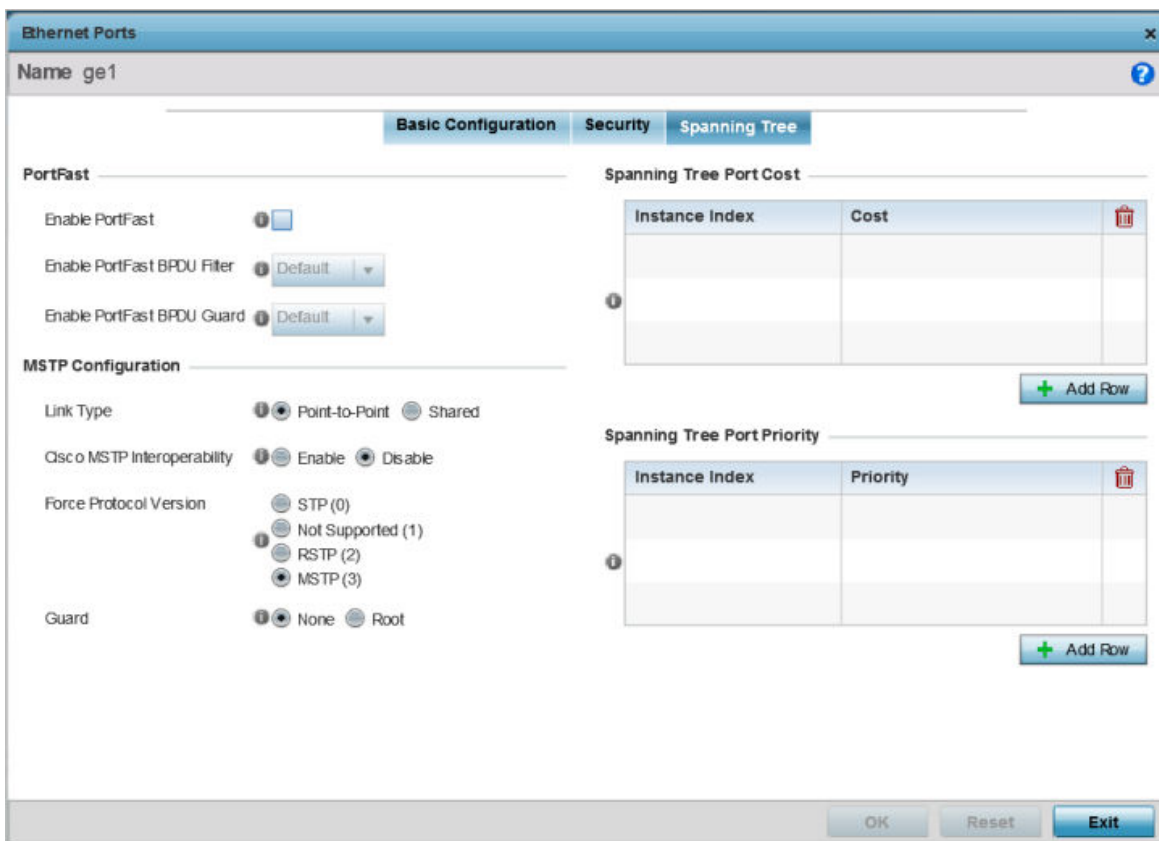
21 In the **802.1x supplicant (client) feature** field, click **Enable** to enable a username and password pair used when authenticating users on this port.

This setting is disabled by default. The password cannot exceed 32 characters.

22 Click **OK** to save the changes and overrides made to the Ethernet port's security configuration.

Click **Reset** to revert to the last saved configuration.

23 Select **Spanning Tree**.



**Figure 39: Ethernet Ports - Spanning Tree Screen**

24 Set the following **MSTP Configuration** settings:

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 <b>Point-to-Point</b> or <b>Shared</b> . When <b>Point-to-Point</b> is selected, the port is treated as connected to a point-to-point link. When <b>Shared</b> is selected, the port is shared between multiple devices. Similarly, an example for a Point-to-Point connection would be when the port is connected to an access point. An example of a <b>Point-to-Point</b> connection is a port that is connected to a controller or service platform. An example of a <b>Shared</b> connection is a port that is connected to a hub.
Cisco MSTP Interoperability	<b>Enable</b> or <b>Disable</b> interoperability with Cisco’s version of MSTP over the port. Cisco’s version of MSTP is incompatible with standard MSTP.
Force Protocol Version	Select <b>STP</b> to use the standard Spanning Tree Protocol. Select <b>RSTP</b> to use Rapid Spanning Tree Protocol. Select <b>MSTP</b> to use Multiple Spanning Tree Protocol.. MSTP is the default setting.
Guard	Select <b>Root</b> radio to ensure that 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. Select <b>None</b> to disable this feature.



Enable PortFast	Select this option to enable drop-down menus for both the <b>Enable PortFast BPDU Filter</b> and <b>Enable PortFast BPDU Guard</b> options for the port.
Enable PortFast BPDU Filter	Select this option 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 this option to invoke a BPDU guard for this PortFast enabled port. Enabling the BPDU guard feature means that this PortFast enabled port will shut down when it receives BPDU messages.

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

Define or override an **Instance Index** using the spinner control, and set its corresponding cost in the **Cost** column.

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.

**Table 3: Spanning Tree Port Cost**

Speed	Default Path Cost
<=100,000 bits/sec	200000000
<=1,000,000 bits/sec	20000000
<=10,000,000 bits/sec	2000000
<=100,000,000 bits/sec	200000
<=1,000,000,000 bits/sec	20000
<=10,000,000,000 bits/sec	2000
<=100,000,000,000 bits/sec	200
<=1,000,000,000,000 bits/sec	20
>1,000,000,000,000 bits/sec	2

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

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

Define or override an **Instance Index** using the spinner control, and set its corresponding priority in the **Priority** column.

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..

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

27 Click **OK** to save the changes and overrides made to the Ethernet port's Spanning Tree configuration.

Click **Reset** to revert to the last saved configuration.

### Virtual Interface Override Configuration

A virtual interface is required for layer 3 (IP) access to a controller or service platform or provide to layer 3 service on a VLAN. The virtual interface defines which IP address is associated with each VLAN ID the

controller or service platform is connected to. 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 for 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 **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- 3 Select **Profile Overrides > Interface**.
- 4 Select **Virtual Interfaces**.



#### Note

A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove overrides from a device, go to the **Basic Configuration** screen for the device and select **Clear Overrides**.

Name	Type	Description	Shutdown	VLAN	IP Address
+ vlan1	VLAN		✓ Enabled	1	10.76.28.131/24

Type to search in tables Row Count: 1

**Figure 40: Profile Overrides - Virtual Interfaces Screen**

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

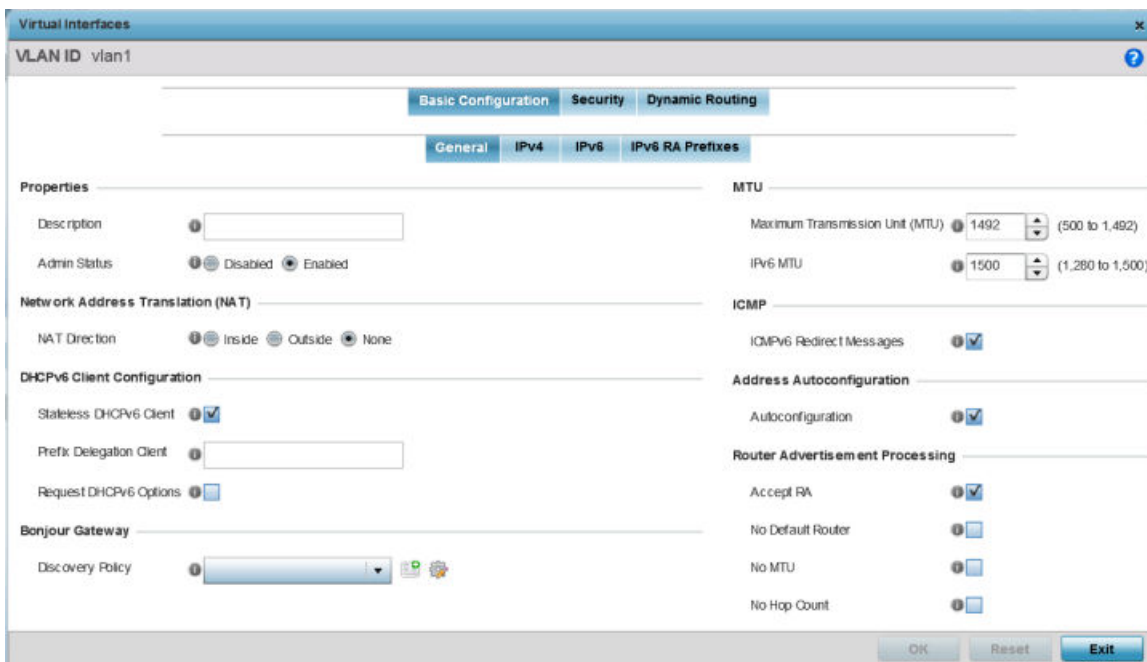
Name	The name of each listed virtual interface assigned when it was created. The name is between 1 - 4094, and cannot be modified as part of a virtual interface edit.
Type	The type of virtual interface for each listed interface.
Description	The description defined for the virtual interface, either when it was created or when it was edited.

Admin Status	A green check mark means the listed virtual interface configuration is active and enabled with its supported profile. A red "X" means the virtual interface is currently shut down. The interface status can be modified when a new virtual interface is created or an existing one modified.
VLAN	The numerical VLAN ID associated with each listed interface.
IP Address	Whether DHCP was used to obtain the primary IP address used by the virtual interface configuration.

After reviewing the configurations of existing virtual interfaces, determine whether a new interface needs to be created, an existing virtual interface needs to be edited (overridden), or an existing virtual interface needs to be deleted.

- 6 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.

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 it is not selected by default..



**Figure 41: Profile Overrides - Virtual Interfaces Basic Configuration Screen**

- 7 If you are creating a new virtual interface, use the **VLAN ID** spinner control to define a numeric VLAN ID from 1 - 4094.
- 8 Define or override the following parameters in 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	Select <b>Disabled</b> or <b>Enabled</b> to define this interface’s current status within the managed network. When set to <b>Enabled</b> , the virtual interface is operational and available to the controller or service platform. The default value is enabled.

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

Select one of the following options:

- 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 640 for instructions on creating a profile's NAT configuration.

- 10 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.

- 11 Define the **Bonjour Gateway** settings.

Bonjour is Apple's implementation of zeroconfiguration 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 works within a single broadcast domain. However, with special DNS configuration, it can be extended to find services across broadcast domains.

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

- 12 Define 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.

- 13 In 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.

- 14 In 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.

- 15 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.

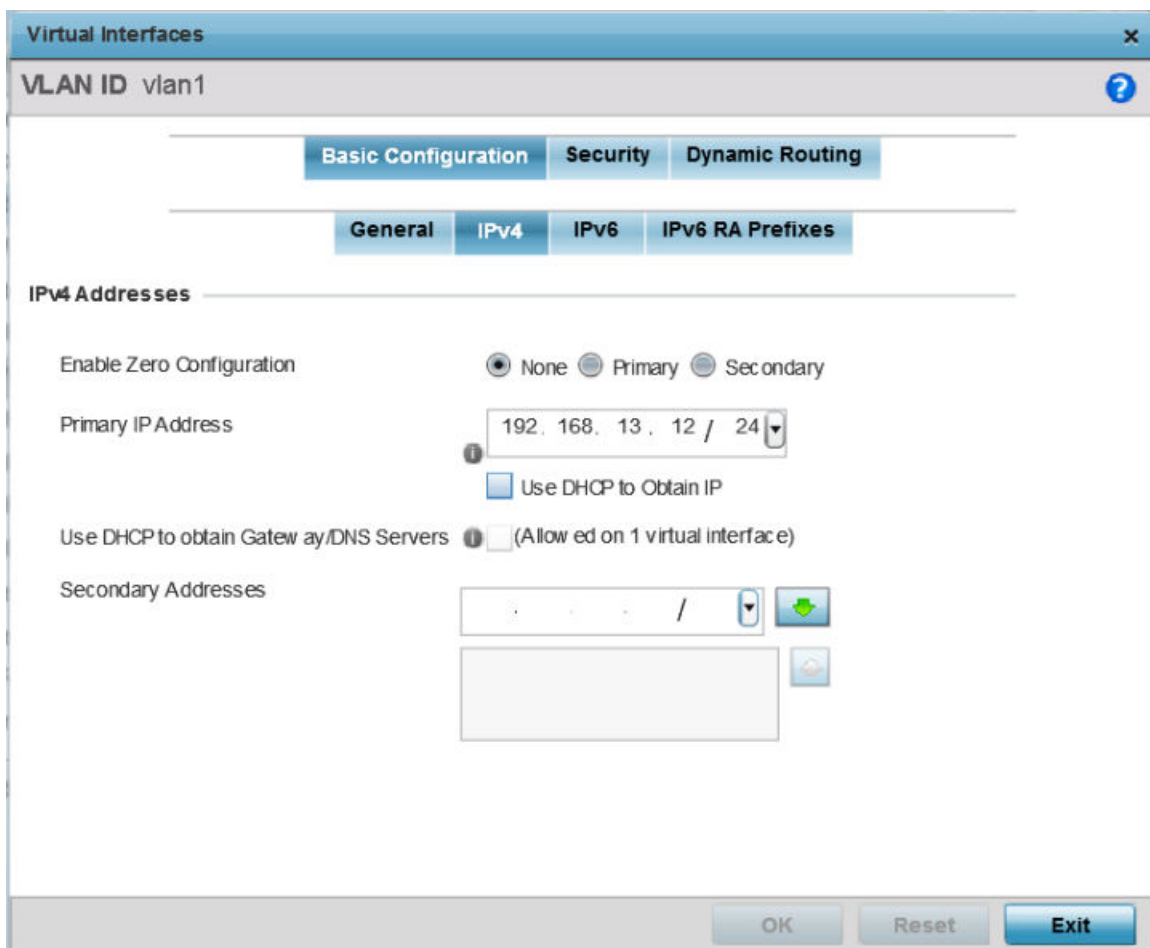
Accept RA	Enable this option to allow router advertisements over this virtual interface. IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the neighbor discovery protocol via ICMPv6 router discovery messages. When first connected to a network, a host sends a link-local 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.

- 16 Click **OK** to save the changes.

Click **Reset** to revert to the last saved configuration.

- 17 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 42: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv4 Tab**

- 18 Set the following network information in 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 <b>None</b> 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 <b>Primary IP Address</b> 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 <b>Use DHCP to Obtain IP</b> option is selected.
Secondary Addresses	Use this 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.

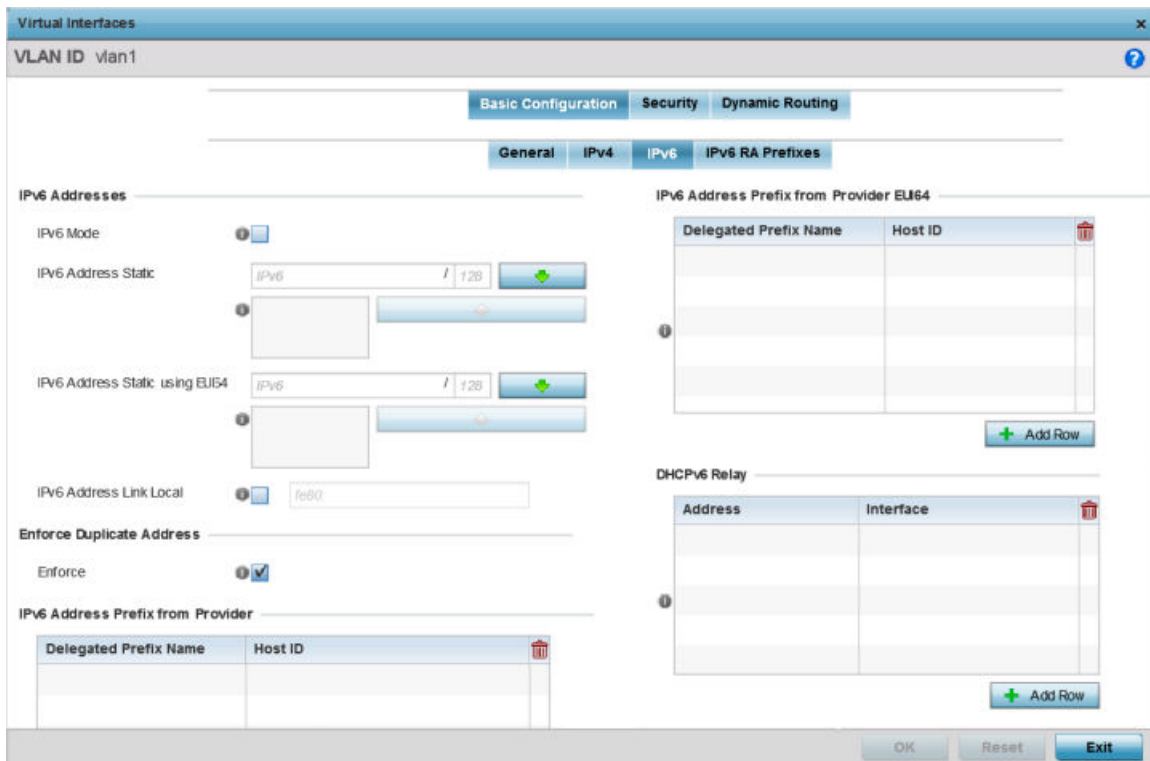
- 19 Refer to the **DHCP Relay** field to set the DHCP relay server configuration used with the virtual interface.

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.

- 20 Click **OK** to save the changes to the IPv4 configuration.  
Click **Reset** to revert to the last saved configuration.

- 21 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 43: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab**

- 22 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 be created statically. IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons.

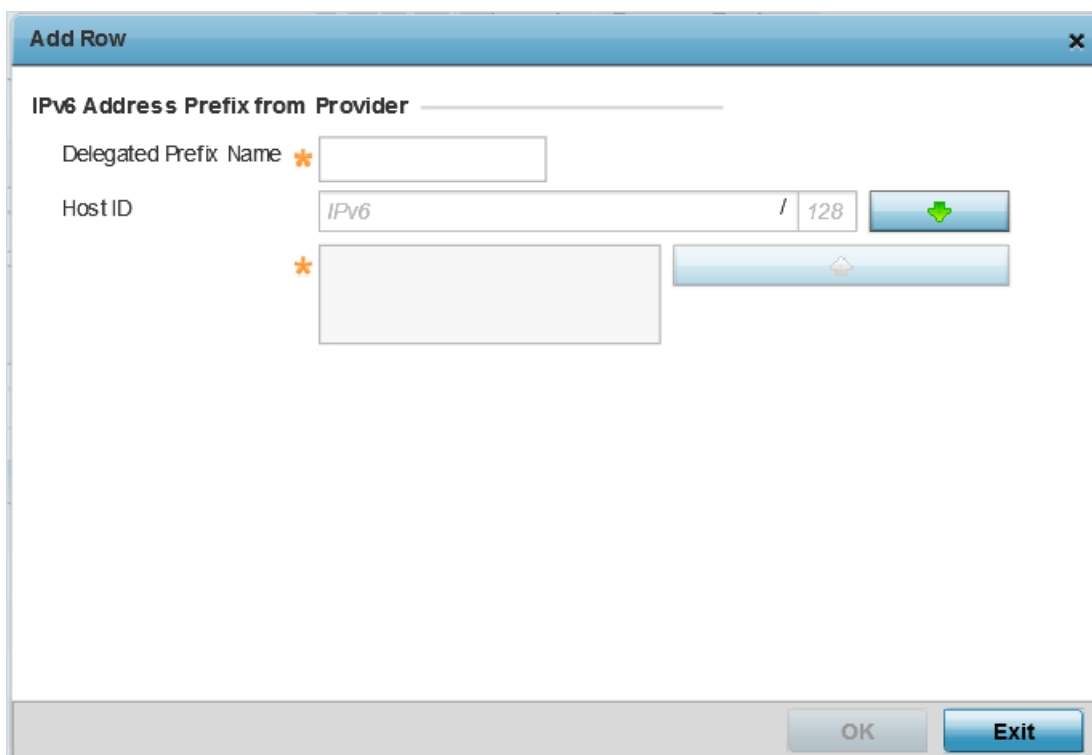
IPv6 Address Static using EUI64	Optionally, set up to 15 global IPv6 IP addresses (in the EUI-64 format) that can be created statically. The IPv6 EUI-64 format address is obtained through a 48-bit MAC address. The MAC is initially separated into two 24-bit segments, with one being an OUI (Organizationally Unique Identifier) and the other being client specific. A 16-bit 0xFFFE is then inserted between the two 24-bit segments 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.

23 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.

24 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 screen in which a new delegated prefix name and host ID can be defined.



**Figure 44: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add Address Prefix from Provider**

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

25 Click **OK** to save the changes to the IPv6 configuration.  
Click **Exit** to close the screen without saving any updates.



26 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 screen in which a new delegated prefix name and host ID can be defined in EUI64 format.

**Figure 45: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 Tab - Add Address Prefix from Provider EUI64**

Designated Prefix Name	Enter a 32-character maximum name for the IPv6 prefix from your 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.

27 Click **OK** to save the changes to the new IPv6 prefix from provider in EUI64 format.

Click **Exit** to close the screen without saving any updates.

28 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.

Select **+ Add Row** to launch a screen in which a new DHCPv6 relay address and interface VLAN ID can be set.

**Figure 46: Profile Overrides - 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.

29 Click **OK** to save the changes to the DHCPv6 relay configuration.

Click **Exit** to close the screen without saving any updates.

30 Select the IPv6 RA Prefixes tab.

Virtual Interfaces x

VLAN ID vlan1 ?

Basic Configuration Security Dynamic Routing

General IPv4 IPv6 IPv6 RA Prefixes

Router Advertisement Policy

Router Advertisement Policy ?

IPv6 RA Prefixes

Prefix Type	Prefix or Id	Site Prefix	Valid Lifetime Type	Valid Lifetime Sec	Valid Lifetime Date	Valid Lifetime Time	Preferred Lifetime Type	Preferred Lifetime Sec	Preferred Lifetime Date	Autoc onfig	Preferred Lifetime Time	On Link	

+ Add Row

OK Reset Exit

**Figure 47: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 RA Prefixes Tab**

31 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.

32 Review the configurations of existing IPv6 advertisement policies.

If necessary, select **+ Add Row** to define the configuration for an additional IPv6 RA prefix.

The screenshot shows the 'Add Row' dialog box for configuring IPv6 RA Prefixes. The settings are as follows:

- Prefix Type:** Prefix
- Prefix or Id:** IPv6 / 128
- Site Prefix:**  IPv6 / 128
- Valid Lifetime Type:** External (Fixed)
- Valid Lifetime Sec:** 30 Days
- Valid Lifetime Date:** [Calendar icon]
- Valid Lifetime Time:** 1 : 0 AM
- Preferred Lifetime Type:** External (Fixed)
- Preferred Lifetime Sec:** 7 Days
- Preferred Lifetime Date:** [Calendar icon]
- Preferred Lifetime Time:** 1 : 0 AM
- Autoc onfig:**
- On Link:**

Buttons: OK, Exit

**Figure 48: Profile Overrides - Virtual Interfaces Basic Configuration Screen - IPv6 RA Prefix**

33 Define the following **IPv6 RA Prefix** settings:

Prefix Type	Set the prefix delegation type used with this configuration. Options include <b>Prefix</b> , and <b>prefix-from-provider</b> . The default setting is <b>Prefix</b> . 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 <b>External</b> (fixed), <b>decrementing</b> , and <b>infinite</b> . If set to <b>External</b> (fixed), only the <b>Valid Lifetime Sec</b> setting is enabled to define the exact time interval for prefix validity. If set to <b>decrementing</b> , use the lifetime date and time settings to refine the prefix expiry period. If set to <b>infinite</b> , no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is <b>External</b> (fixed).
Valid Lifetime Sec	If the lifetime type is set to <b>External</b> (fixed), set the Seconds, Minutes, Hours, or Days values used to measure 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 <b>External</b> (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 <b>decrementing</b> , set the time for the prefix's validity.
Preferred Lifetime Type	Set the administrator preferred lifetime for the prefix's validity. Options include <b>External</b> (fixed), <b>decrementing</b> , and <b>infinite</b> . If set to <b>External</b> (fixed), only the <b>Preferred Lifetime Sec</b> setting is enabled to define the exact time interval for prefix validity. If set to <b>decrementing</b> , use the lifetime date and time settings to refine the prefix expiry period. If set to <b>infinite</b> , no additional date or time settings are required for the prefix and the prefix will not expire. The default setting is <b>External</b> (fixed).
Preferred Lifetime Sec	If the administrator preferred lifetime type is set to <b>External</b> (fixed), set the Seconds, Minutes, Hours, or Days values used to measure 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 <b>External</b> (fixed), set the date in MM/DD/YYYY format for the expiration of the prefix.
Preferred Lifetime Time	If the administrator preferred lifetime type is set to <b>decrementing</b> , 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.

34 Click **OK** to save the changes to the IPv6 RA prefix configuration.

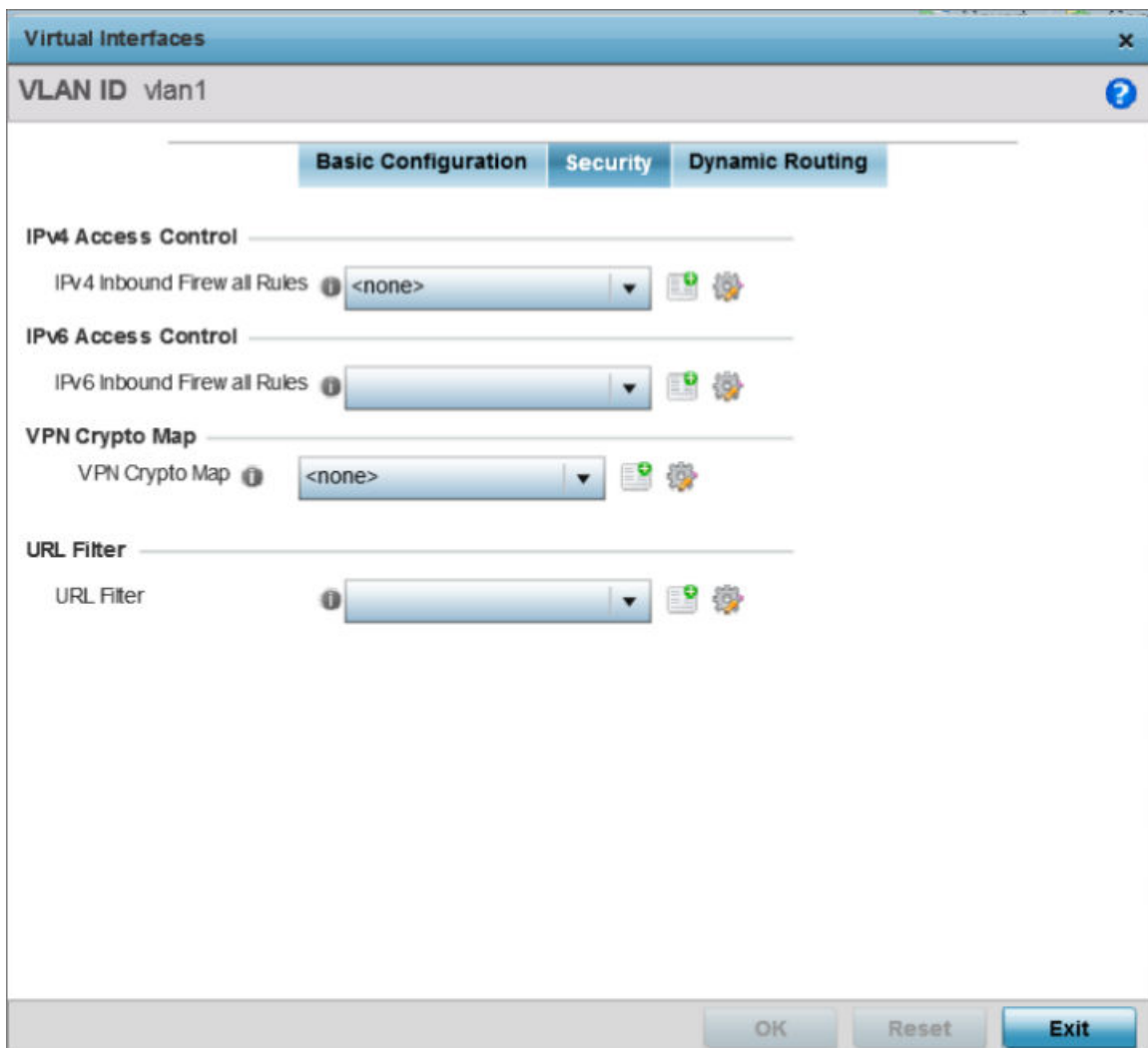
Click **Exit** to close the screen without saving any updates.

35 Click **OK** to save the changes and overrides.

Click **Reset** to revert to the last saved configuration.



36 Select the Security tab.



**Figure 49: Profile Overrides - Virtual Interfaces Security Screen**

37 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.

Click the **Create** icon to define a new IPv4 firewall rule configuration, or click 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.

- 38 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.

Click the **Create** icon to define a new IPv6 firewall rule configuration, or click 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. For more information on creating IPv6 firewall rules, see [Configuring IP Firewall Rules](#) on page 732.

- 39 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 there is no Crypto Map configuration that meets the needs of this virtual interface, click the **Create** icon to define a new Crypto Map configuration or click the **Edit** icon to modify an existing configuration. For more information, see [Overriding a Profile's VPN Configuration](#).

- 40 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.

- 41 Select the Dynamic Routing tab.



#### Note

The Dynamic Routing tab is not available for some controllers or service platforms.

**Figure 50: Profile Overrides - Virtual Interfaces Dynamic Routing Screen**

- 42 Define or override the following parameters in 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 bandwidth from 1 - 10,000,000 KBps.

- 43 From the **Chosen Authentication Type** drop-down list, select the authentication type used to validate credentials within the OSPF dynamic route.

The available options are **None**, **null**, **simple-password**, and **message-digest**. The default value is **None**.

- 44 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**).

- 45 Click **OK** to save the changes and overrides to the **Security** screen.

Click **Reset** to revert to the last saved configuration.

### Port Channel Override Configuration

Profiles can utilize customized port channel configurations as part of their interface settings. Existing port channel profile configurations can be overridden as they become obsolete for specific device deployments.

To define or override a port channel configuration on a profile:

- 1 Select **Configuration > Devices** from the web UI.

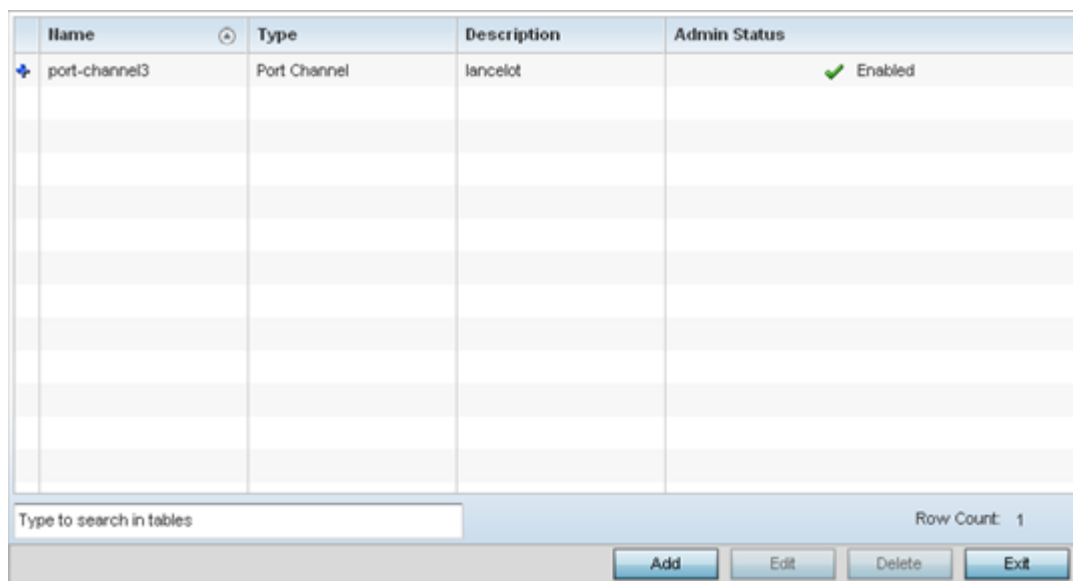
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.

- 2 Select a target device in the lower left-hand side of the UI.

You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.

- 3 Select **Profile Overrides > Interface**.

- 4 Select **Port Channels**.



Name	Type	Description	Admin Status
port-channel3	Port Channel	lancelot	Enabled

Type to search in tables Row Count: 1

Add Edit Delete Exit

**Figure 51: Device Overrides - Port Channels Screen**



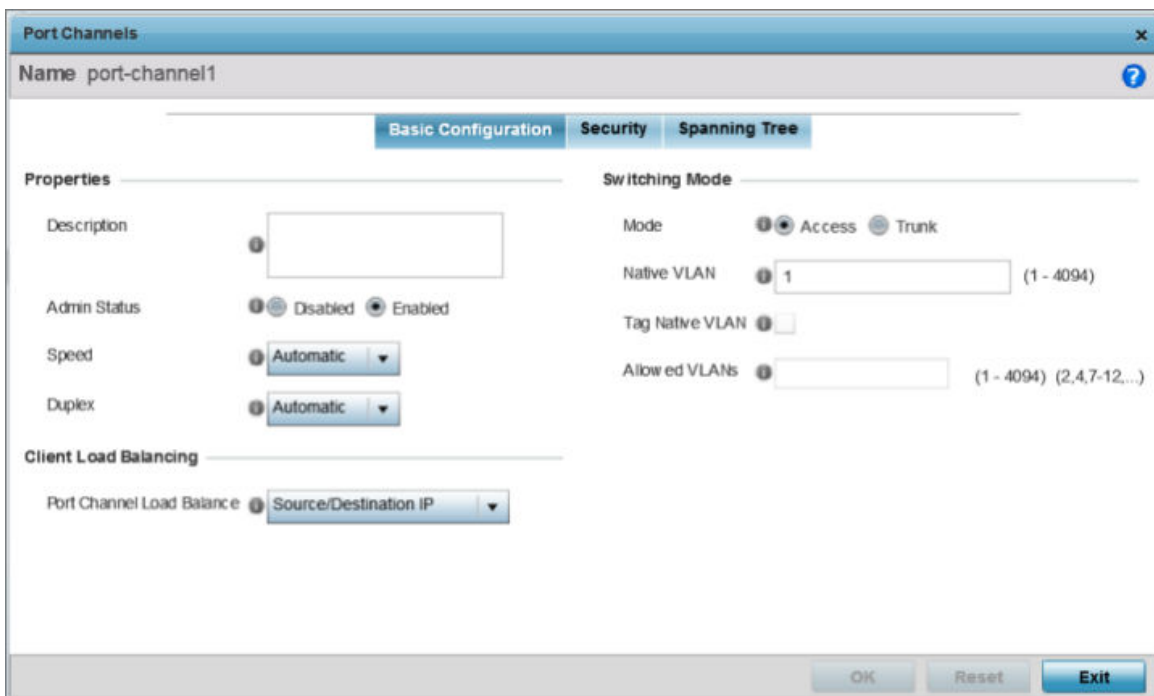
#### Note

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 **Clear Overrides**. This removes all overrides from the device.

- 5 Refer to the following to review existing port channel configurations and their status to determine whether a parameter requires an override:

Name	The port channel's numerical identifier assigned when it was created. The numerical name cannot be modified as part of the edit process.
Type	Whether the type is port channel.
Description	A short description (64 characters maximum) describing the port channel or differentiating it from others with similar configurations.
Admin Status	A green check mark means the listed port channel is active and currently enabled with the profile. A red "X" means the port channel is currently disabled and not available for use. The interface status can be modified with the port channel configuration as required.

- 6 To edit the configuration of an existing port channel, select it from the list and click **Edit**. The **Basic Configuration** screen displays by default.



**Figure 52: Device Overrides - Port Channels - Basic Configuration Screen**

- 7 Set or override the following port channel **Properties**:

Description	Enter a brief description for the port channel (64 characters maximum). The description should reflect the port channel's intended function.
Admin Status	Select <b>Enabled</b> to define this port channel as active to the profile it supports. Select <b>Disabled</b> 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 <b>10 Mbps</b> , <b>100 Mbps</b> , or <b>1000 Mbps</b> 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 <b>Auto</b> is selected. Select <b>Automatic</b> 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. <b>Automatic</b> is the default setting.
Duplex	Select half, full, or automatic. Select <b>Half</b> 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 <b>Full</b> 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 <b>Automatic</b> to enable the controller or service platform to dynamically duplex as port channel performance needs dictate. <b>Automatic</b> is the default setting.

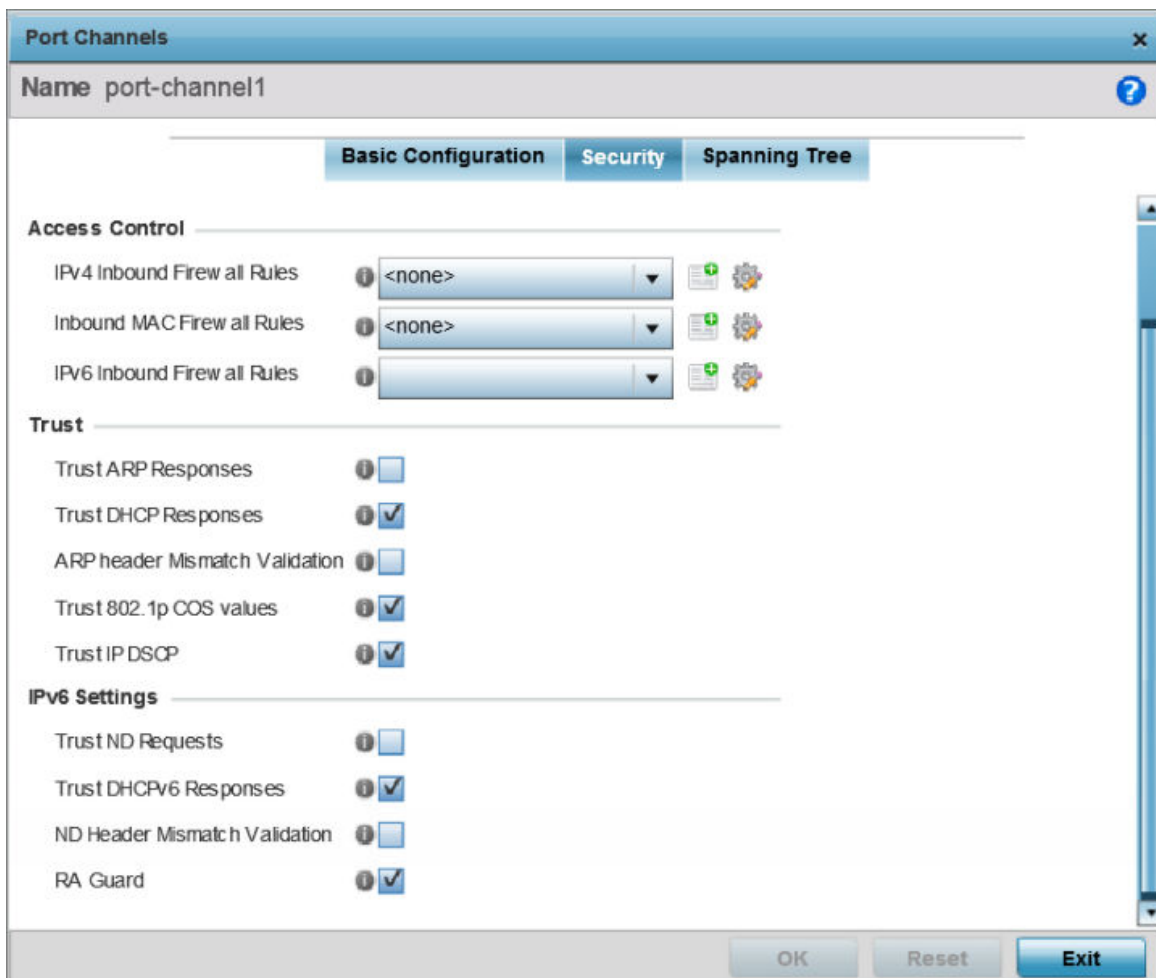
- Use the **Port Channel Load Balance** drop-down menu in the **Client Load Balancing** section to define whether port channel load balancing is conducted using a **Source/Destination IP** or **aSource/Destination MAC**.  
**Source/Destination IP** is the default setting.
- Set or override the following **Switching Mode** parameters to apply to the port channel configuration:

Mode	Select either <b>Access</b> or <b>Trunk</b> to set the VLAN switching mode over the port channel. If <b>Access</b> 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 <b>Trunk</b> , 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. <b>Access</b> 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 <b>Trunk</b> as the mode enables the <b>Allowed VLANs</b> parameter. Add VLANs that exclusively send packets over the port channel.

- Click **OK** to save the changes and overrides to the port channel Basic Configuration.  
Click **Reset** to revert to the last saved configuration.



- 11 Select the Security tab.



**Figure 53: Device Overrides - Port Channels - Security Screen**

- 12 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.

You will 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

- 13 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.

- 14 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.

- 15 If there is no firewall rule that meets the data protection needs of the target port channel configuration, click the **Create** icon to define a new rule configuration, or click the **Edit** icon to modify an existing firewall rule configuration.
- 16 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. This option is disabled by default.
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. This option is enabled by default.
ARP Header Mismatch Validation	Select this option to enable a mismatch check for the source MAC in both the ARP and Ethernet header. This option is enabled by default.
Trust 802.1p COS values	Select this option to enable 802.1p COS values on this port. This option is enabled by default.
Trust IP DSCP	Select this option to enable IP DSCP values on this port. This option is disabled by default.

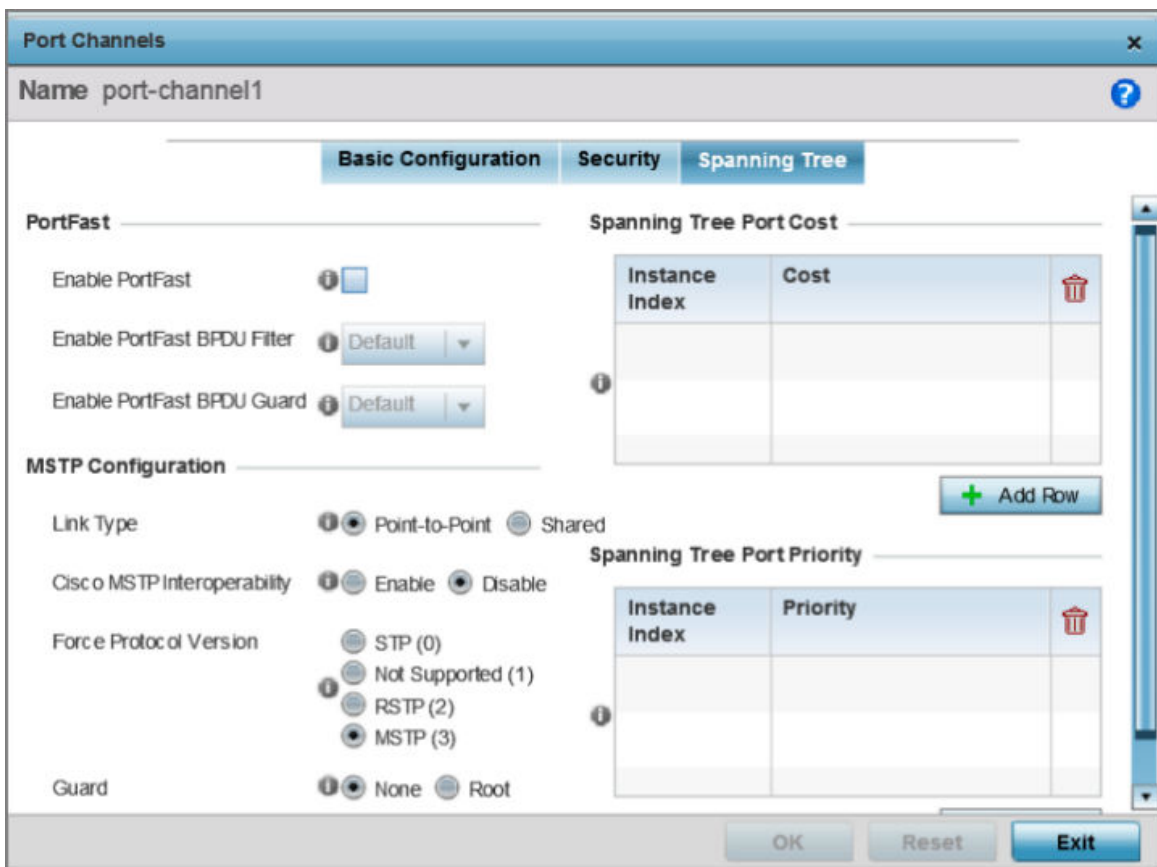
- 17 Set the following **IPv6 Settings**:

Trust ND Requests	Select this option 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 this option 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 this option to enable a mismatch check for the source MAC within the ND header and Link Layer Option. This option 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 sends in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information. This option is disabled by default.

- 18 Click **OK** to save the changes and overrides to the security configuration.  
Click **Reset** to revert to the last saved configuration.



19 Select the Spanning Tree tab.



**Figure 54: Port Channels - Spanning Tree Screen**

20 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 the <b>Enable PortFast BPDU Filter</b> and <b>Enable PortFast BPDU Guard</b> options. 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.

21 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 <b>Point-to-Point</b> or <b>Shared</b> . When <b>Point-to-Point</b> is selected, the port is treated as connected to a point-to-point link. Selecting <b>Shared</b> means this port should be treated as having a shared connection. A port connected to a hub is on a <b>Shared</b> link. A port connected to an access point is a <b>Point-to-Point</b> link. A port connected to a controller or service platform is a <b>Point-to-Point</b> link. <b>Point-to-Point</b> is the default setting.

Cisco MSTP Interoperability	<b>Enable</b> or <b>Disable</b> interoperability with Cisco's version of MSTP over the port. Cisco's version of MSTP is incompatible with standard MSTP. This setting is disabled by default.
Force Protocol Version	Set the protocol version to either <b>STP (0)</b> , <b>Not Supported (1)</b> , <b>RSTP (2)</b> , or <b>MSTP (3)</b> . <b>MSTP (3)</b> 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.

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

Define or override an **Instance Index** using the spinner control, and set its corresponding cost in the **Cost** column. 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.

**Table 4: Spanning Tree Port Cost**

Speed	Default Path Cost
<=100,000 bits/sec	200000000
<=1,000,000 bits/sec	20000000
<=10,000,000 bits/sec	2000000
<=100,000,000 bits/sec	200000
<=1,000,000,000 bits/sec	20000
<=10,000,000,000 bits/sec	2000
<=100,000,000,000 bits/sec	200
<=1,000,000,000,000 bits/sec	20
>1,000,000,000,000 bits/sec	2

23 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.

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

24 Click **OK** to save the changes and overrides made to the Ethernet port's Spanning Tree configuration.

Click **Reset** to revert to the last saved configuration.

### VM 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 enable 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 16 VMF 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, by default, 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.

To define or override a VM interface configuration:

- 1 Select **Configuration > Devices** from the web UI.

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

- 2 Select a target device in the lower left-hand side of the UI.

You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.

- 3 Select **Profile Overrides > Interface**.

- 4 Select **VM Interfaces**.

The **VM Interfaces** screen displays.

Name	Type	Description	Admin Status	Mode	Native VLAN	Tag Native VLAN	Allowed VLANs
vmif1	VM Interface		✓ Enabled	Access	1		
vmif2	VM Interface		✓ Enabled	Access	1		
vmif3	VM Interface		✓ Enabled	Access	1		
vmif4	VM Interface		✓ Enabled	Access	1		
vmif5	VM Interface		✓ Enabled	Access	1		
vmif6	VM Interface		✓ Enabled	Access	1		
vmif7	VM Interface		✓ Enabled	Access	1		
vmif8	VM Interface		✓ Enabled	Access	1		

Type to search in tables Row Count: 8

**Figure 55: Profile Overrides - VM Interfaces Screen**



#### Note

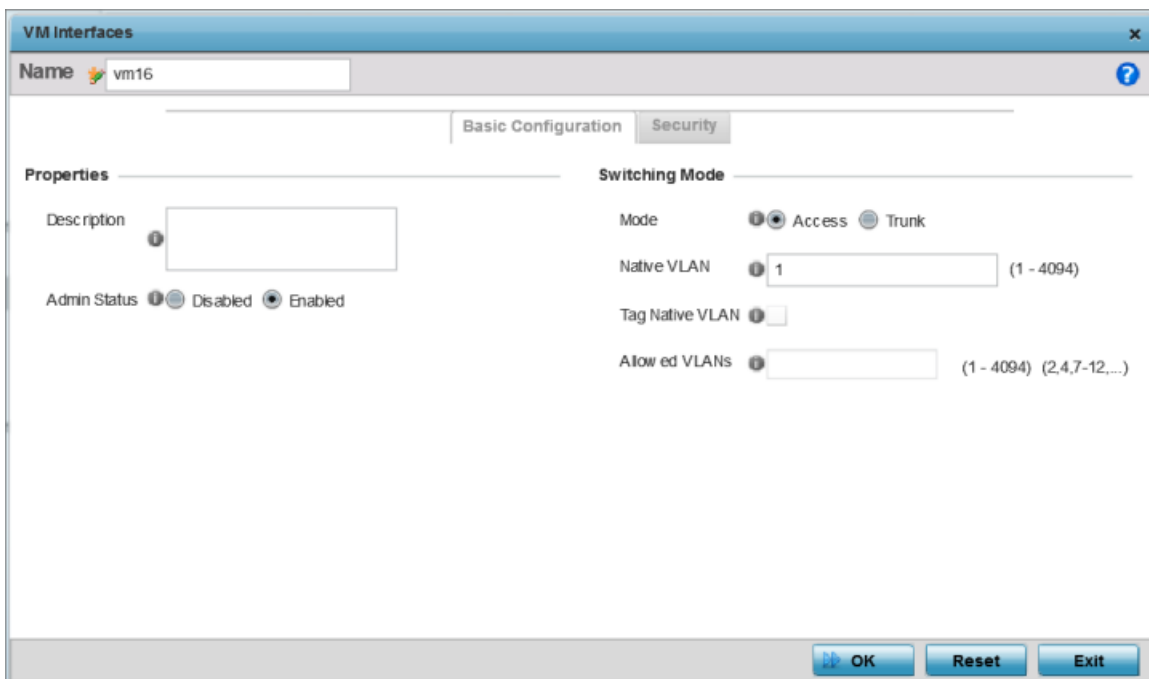
A blue override icon (to the left of a parameter) defines the parameter as having an override applied. To remove an override go to the **Basic Configuration** section of the device and click **Clear Overrides**. This removes all overrides from the device.

- 5 Refer to the following to review existing configurations and status to determine whether a parameter requires an override:

Name	The VM interface numerical identifier assigned when the VM interface was created. The numerical name cannot be modified as part of the edit process.
Type	Whether the type is VM interface.
Description	A short description (64 characters maximum) describing the VM interface or differentiating it from others with similar configurations.
Admin Status	A green check mark means the listed VM interface is active and currently enabled with the profile. A red "X" means the VM interface is currently disabled and not available for use. The interface status can be modified with the <b>VM Interface Basic Configuration</b> screen as required.
Mode	The layer 3 mode of the VM interface: either <b>Access</b> or <b>Trunk</b> (as defined within the <b>VM Interfaces Basic Configuration</b> screen). If <b>Access</b> 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 <b>Trunk</b> , the port allows packets from a list of VLANs added to the trunk. A VM interface configured as <b>Trunk</b> supports multiple 802.1Q tagged VLANs and one native VLAN which can be tagged or untagged.
Native VLAN	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 means the native VLAN is tagged. A red "X" means the native VLAN is 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	The VLANs allowed to send packets over the listed VM interface. Allowed VLANs are listed only when the mode has been set to <b>Trunk</b> .

- To edit or override the configuration of an existing VM interface, select it from among those displayed and click **Edit**.

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



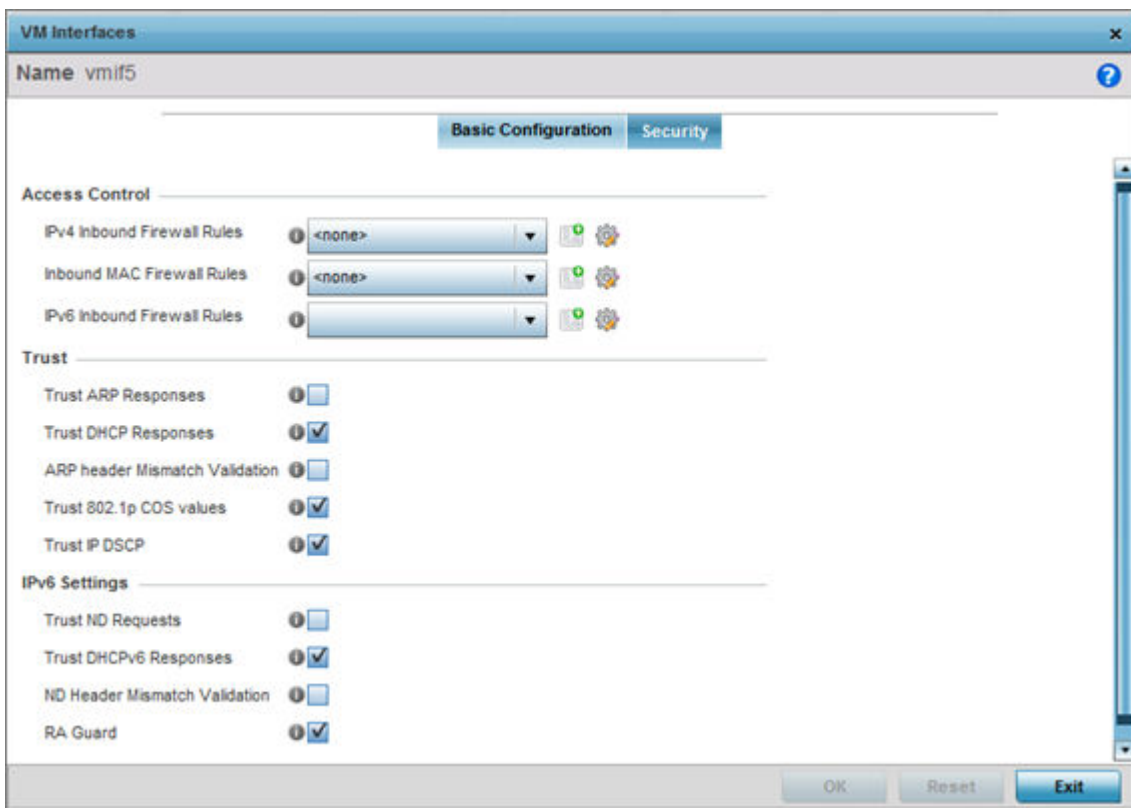
**Figure 56: Profile Overrides - VM Interfaces Basic Configuration Screen**

- 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 <b>Enabled</b> to define this VM interface as active to the profile it supports. Select <b>Disabled</b> to disable this VM interface in the profile. It can be activated at any time when needed. This option is disabled by default.
Mode	Select either <b>Access</b> or <b>Trunk</b> to set the VLAN switching mode over the VM interface. If <b>Access</b> 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 VMF port are expected as untagged and mapped to the native VLAN. If set to <b>Trunk</b> , the port allows packets from a list of VLANs you add to the trunk. A VM interface configured as <b>Trunk</b> supports multiple 802.1Q tagged VLANs and one native VLAN which can be tagged or untagged. <b>Access</b> is the default setting.
Native VLAN	Define the 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 will be directed over when using trunk mode. The default value is 1.

<p>Tag Native VLAN</p>	<p>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.</p>
<p>Allowed VLANs</p>	<p>Selecting <b>Trunk</b> as the mode enables the <b>Allowed VLANs</b> 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.</p>

- 8 Click **OK** to save the changes and overrides made to the VM interface basic configuration.  
Click **Reset** to revert to the last saved configuration.
- 9 Select the Security tab.



**Figure 57: Profile Overrides - 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.

You will 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.

- 11 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.

- 12 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.

- 13 If there is no firewall rule that meets the data protection needs of the target VM interface configuration, click the **Create** icon to define a new rule configuration, or click the **Edit** icon to modify an existing firewall rule configuration.

- 14 Refer to the **Trust** field 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 the information from these packets is used to identify rogue devices. This option is disabled by default.
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 port, and a DHCP server can be connected only to a DHCP trusted port. This option is enabled by default.
ARP Header Mismatch Validation	Select this option to enable a mismatch check for the source MAC in both the ARP and Ethernet header. This option is enabled by default.
Trust 802.1p COS values	Select this option to enable 802.1p COS values on this VM interface. This option is enabled by default.
Trust IP DSCP	Select this option to enable IP DSCP values on this VM interface. This option is disabled by default.

- 15 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 option is disabled by default.
Trust DHCPv6 Responses	Select this option to 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 option 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 option 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 option is disabled by default.







- 16 Click **OK** to save the changes and overrides made to the VM interface configuration.  
Click **Reset** to revert to the last saved configuration.

### Radio Override Configuration

An access point can have its radio profile configuration overridden after its 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 **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- 3 Select **Profile Overrides > Interface**.
- 4 Select **Radios**.

Name	Type	Description	Admin Status	RF Mode	Channel	Transmit Power	Overrides
 radio1	Radio	radio1	 Enabled	2.4 GHz WLAN	smart	smart	 Clear
 radio2	Radio	radio2	 Enabled	5 GHz WLAN	smart	smart	 Clear

Type to search in tables Row Count: 2

Edit Exit

**Figure 58: Device 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 **Clear Overrides**. This removes all overrides from the device.



- 5 Review the following radio configuration data to determine whether a radio configuration needs to be modified or overridden to better support the managed network:

Name	Displays whether the reporting radio is the Access Point's radio1, radio2 or radio3.
Type	Displays whether the radio has been designated as a typical WLAN radio or if the radio has been designated as a sensor.
Description	A brief description provided by the administrator when the radio's configuration was added or modified.
Admin Status	A green check mark means the radio is enabled for client or sensor support. A red "X" means the radio is 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 in the Radio Settings tab.
Channel	Lists the channel setting for the radio. <b>Smart</b> is the default setting. If set to <b>Smart</b> , 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. The column displays <b>smart</b> if set for dynamic Smart RF support.
Transmit Power	Lists the transmit power for each radio displayed as a value in milliwatts. Selecting <b>smart</b> allows the radio to perform power adjustments to compensate for failed neighboring radios.
Overrides	A Clear option appears for each radio configuration that has an override applied to the profile's configuration. Select <b>Clear</b> to revert this specific radio configuration to the profile configuration originally defined by the administrator for this radio.

- 6 If required, select a radio configuration and click **Edit** to modify or override portions of its configuration.

The Radio Settings tab displays by default.

The screenshot shows the 'Radios' configuration window for 'radio1'. The 'Radio Settings' tab is active. The 'Properties' section includes Description (radio1), Admin Status (Enabled), Radio QoS Policy (default), and Association ACL. The 'WLAN Properties' section includes Beacon Interval (100), DTIM Interval BSSID (2), RTS Threshold (65536), Short Preamble, Guard Interval (Any), Probe Response Rate (follow-probe-request), and Probe Response Retry. The 'Radio Settings' section includes RF Mode (2.4GHz-wlan), Lock RF Mode, Channel (smart), DFS Revert Home, DFS Duration (90), Transmit Power (smart), Antenna Gain (0.0), Antenna Mode (2x2), Enable Antenna Diversity, Adaptivity Recovery, and Adaptivity Timeout (90). The 'Radio Share' section includes Feed WLAN Packets to Sensor (Off). Buttons for OK, Reset, and Exit are at the bottom.

**Figure 59: Access Point Radio - Radio Settings Tab**

- 7 Define or override the following radio configuration **Properties**:

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 <b>Enabled</b> or <b>Disabled</b> 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 shut down manually.

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 no existing policy is suitable for this radio's intended operation, select the <b>Create</b> icon to define a new QoS policy. For more information, see <a href="#">Radio QoS Policies</a> on page 381.
Association ACL	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 <b>Create</b> icon to define a new Association ACL that can be applied to this profile.

8 Set or override the following **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 <b>sensor</b> if you are using the radio for rogue device detection. To set a radio as a detector, disable sensor support on the other access point radio. Set the mode to <b>scan-ahead</b> in DFS-aware countries to allow a mesh point's 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 calibration functions for this radio. The default setting is disabled.
Channel	Select the channel of operation for the radio. Only a trained installation professional should define the radio channel. Select <b>Smart</b> for the radio to scan non-overlapping channels to listen for beacons from other access points. After channels are scanned, the radio selects the channel with the fewest access points. In case of multiple access points on the same channel, it selects the channel with the lowest average power level. The default value is <b>Smart</b> . Channels with a "w" appended to them are unique to the 40 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 and 3,600 minutes. This is the duration for which the radio stays in the new channel. The default value is 90 minutes.
Transmit Power	Set the transmit power of the selected access point radio. If the access point has two radios, each radio should be configured with a unique transmit power in respect to its intended client support function. Select the <b>Smart RF</b> 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 <b>dynamic</b> , based on the access point model 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 enable a spinner control for client radio power transmissions in dBm. The available range is 0 - 20 dBm. This option is disabled by default.
Dynamic Chain Selection	Select this option to allow the access point radio to dynamically change the number of transmit chains. This setting is disabled by default.
Rate	Use the <b>Select</b> button to set rate options depending on the 802.11 protocols selected. If the radio band is set to <b>Sensor</b> or <b>Detector</b> , the <b>Data Rates</b> 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 an 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 you are dedicating an AP 81XX model radio to either 2.4 or 5 Ghz support, a <b>Custom Rates</b> option is available to set a modulation and coding scheme (MCS) in respect to the radio’s channel width and guard interval. An 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 <b>Basic</b> is selected within the 802.11n Rates field, the MCS0-7 option is auto selected as a supported rate and that option is grayed out. If <b>Basic</b> 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 AP 81XX model access points and its ability to provide 3x3x3 MIMO support.
Radio Placement	Specify whether the radio is located <b>Indoors</b> or <b>Outdoors</b> . The placement should depend on the country of operation selected and its regulatory domain requirements for radio emissions. The default setting is <b>Indoors</b> .

Max Clients	Set the maximum permissible client connections for this radio. Set a value from 0 - 256. The default value is 256.
Rate Selection Methods	Specify a radio selection method for the radio. The selection methods are:  <b>Standard</b> Standard monotonic radio selection method will be used.  <b>Opportunistic</b> Sets opportunistic radio link adaptation (ORLA) as the radio selection method. This mode uses opportunistic data rate selection to provide the best throughput. The ORLA rate selection mode is supported only on the AP 7161 and AP 8163 model access points.

9 Set or override the following **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 jittersensitive. 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 (from 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 tradeoffs 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 you are using an 802.11bg radio, select this option for the radio to transmit using a short preamble. Short preambles improve throughput. However, some devices (SpectraLink phones) require long preambles. This option is disabled by default.

Guard Interval	Specify a <b>Long</b> or <b>Any</b> 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 <b>Long</b> .
Probe Response Rate	Specify the data rate used for the transmission of probe responses. Options include <b>highest-basic</b> , <b>lowest-basic</b> , and <b>follow-probe-request</b> . The default value is <b>follow-probe-request</b> .
Probe Response Retry	Select this option to retry probe responses if they are not acknowledged by the target wireless client. This option is enabled by default.

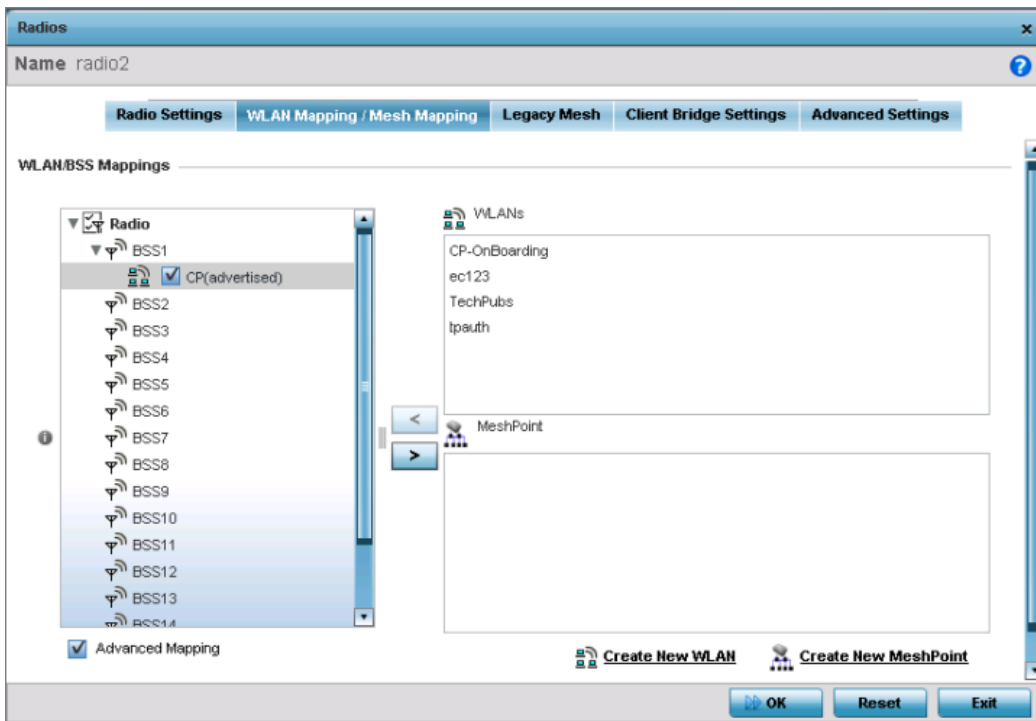
10 Use the **Feed WLAN Packets to Sensor** drop-down menu to allow the radio to send WLAN packets to the sensor radio.

This feature can be enabled in two modes:

- In **Inline** mode, the WIPS sensor receives the packets from the radios with each radio operating in normal mode.
- In **Promiscuous** mode, 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 the packets.

In both **Inline** or **Promiscuous** mode, the packets the radio is switching can also be used by the WIPS analysis module.

11 Select the WLAN Mapping / Mesh Mapping tab.



**Figure 60: Access Point Radio - WLAN Mapping / Mesh Mapping Tab**

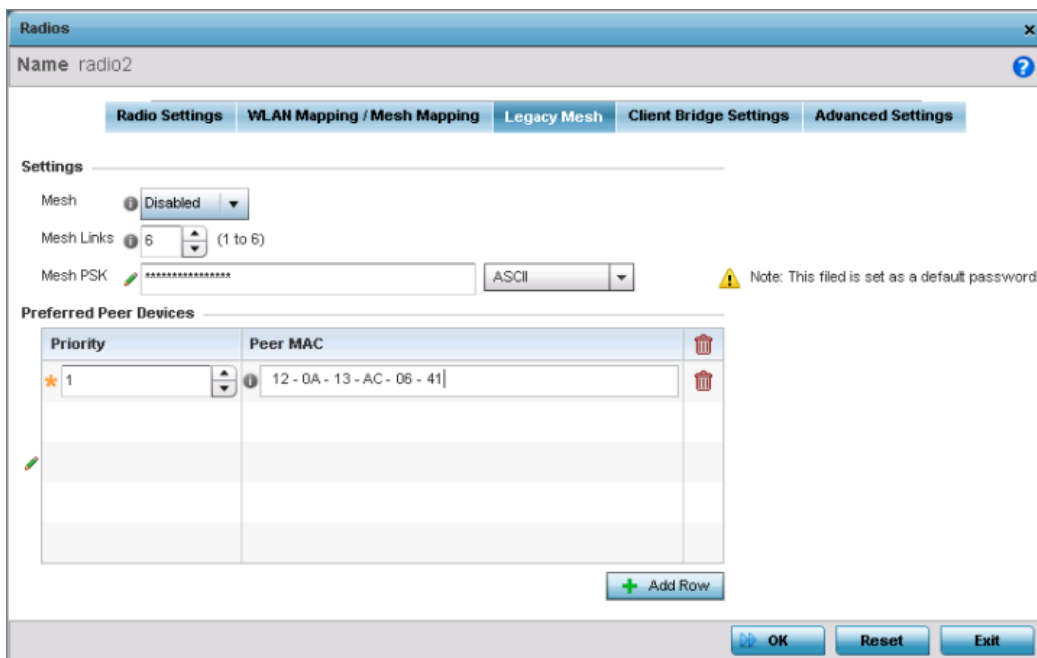
- 12 Refer to the **WLAN/BSS Mappings** field to set or override WLAN BSSID assignments for an existing access point deployment.

Administrators can assign each WLAN its own BSSID. For dual-radio access points, there are eight BSSIDs for the 802.11b/g/n radio and eight BSSIDs for the 802.11a/n radio.

- 13 Select **Advanced Mapping** to enable WLAN mapping to a specific BSS ID.
- 14 Click **OK** to save the changes and overrides to the WLAN mapping.

Click **Reset** to revert to the last saved configuration.

- 15 Select the Legacy Mesh tab.



**Figure 61: Access Point Radio - Legacy Mesh Tab**

- 16 Define the following Mesh Legacy **Settings**:

Mesh	Set the mesh mode for this radio – either <b>Client</b> , <b>Portal</b> , or <b>Disabled</b> . Setting the mesh mode to <b>Client</b> enables the radio to operate as a mesh client that scans and connects to mesh portals or nodes connected to portals. Setting the mesh mode to <b>Portal</b> turns the radio into a mesh portal. This starts the radio beaconing immediately and will accept connections from other mesh nodes. Setting the mesh mode to <b>Disabled</b> deactivates all mesh activity on this radio.
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 that this key is configured on the access point when staged for mesh, added to both the mesh client and the portal access point's configuration on the controller or service platform. Select <b>Show</b> to display the characters used in the PSK.



**Note**  
Only single-hop mesh links are supported at this time.

17 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 the peer is given when it connects to the mesh infrastructure.

Click **+ Add Row** to add preferred peer devices for the radio to connect to in mesh mode.

18 Click **OK** to save the changes and overrides to the Mesh configuration.

Click **Reset** to revert to the last saved configuration.



- 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, thereby providing the clients access to the infrastructure WLAN resources. This feature is supported only on the AP 6522, AP 6562, AP 7532, AP 7562, AP 7602, and AP 7622 model access points.

**Figure 62: Access Point Radio - Client Bridge Settings Tab**

20 Define the following **General** settings:

SSID	Set the infrastructure WLAN's SSID, with which the client-bridge access point associates.
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 64. The default value is 64.
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 <b>None</b> and <b>EAP</b> . If you select <b>EAP</b> , specify the EAP authentication parameters. The default setting is <b>None</b> . For information on WLAN authentication, see <a href="#">Configuring WLAN Security</a> on page 323.
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 <b>None</b> , <b>CCMP</b> , and <b>TKIP</b> . The default setting is <b>None</b> . For information on WLAN encryption, see <a href="#">Configuring WLAN Security</a> on page 323.

21 Refer to the **EAP Parameters** field and define the following EAP authentication parameters:

Type	Select the EAP authentication method used by the supplicant. The options are <b>TLS</b> and <b>PEAP-MS-CHAPv2</b> . The default EAP type is <b>PEAP-MS-CHAPv2</b> .
Username	Set the 32-character maximum user name for an EAP authentication credential exchange.
Password	Set the 32-character maximum password for the specified EAP user name.
Pre-shared Key	Set the pre-shared key (PSK) used with EAP. Note that the authenticating algorithm and PSK should be the same as 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 <b>highest</b> and <b>normal</b> . The default value is <b>highest</b> .
Trustpoint CA	Set the <i>Trustpoint CA</i> name (this is the trustpoint installed on the RADIUS server host). This parameter is applicable to both EAP-TLS and PEAP-MS-CHAPv2 authentication modes. In case of both EAP-TLS and PEAP-MS-CHAPv2 authentication, provide the RADIUS server TP name to enable RADIUS server certificate validation at the client end. This parameter is not mandatory for enabling TP-based authentication of CB (Client-Bridge) AP.

Trustpoint Client	Set the <i>Trustpoint Client</i> name (this is the TP installed on the CB AP). This parameter is applicable only for EAP-TLS authentication mode. When configured, this client certificate is sent across a TLS tunnel and matched for authentication at the RADIUS server host. This configuration is mandatory for enabling TP-based authentication of CB AP.
Trustpoint Expiry	<p>Use the drop-down menu to specify whether the wireless client-bridge is to be continued or discontinued in case of certificate expiry.</p> <p>In EAP-TLS authentication, a CA-signed certificate is used to authenticate the CB AP and RADIUS server host to establish the wireless CB. Use this option to specify whether the wireless CB is to be continued or terminated on expiration of this certificate.</p> <p>continue – Enables continuation of the CB even after the certificate (CA/client) has expired. When selected, this option enables automatic CA certificate deployment as and when new CA certificates are available. This is the default setting.</p> <p>discontinue – Terminates the CB once the certificate (CA/client) has expired.</p> <p><b>Note:</b> Configure this parameter only if the CB AP and the RADIUS server host are using a crypto CMP policy for automatic certificate renewal. For more information, see <a href="#">Crypto CMP Policy</a> on page 447.</p>

- 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 <b>null-data</b> and <b>WNMP</b> packets. The default value is <b>null-data</b> .
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 864,000 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 you enable 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 you are using a DHCP assigned IP address, this option also causes a DHCP renew. This option is enabled by default.

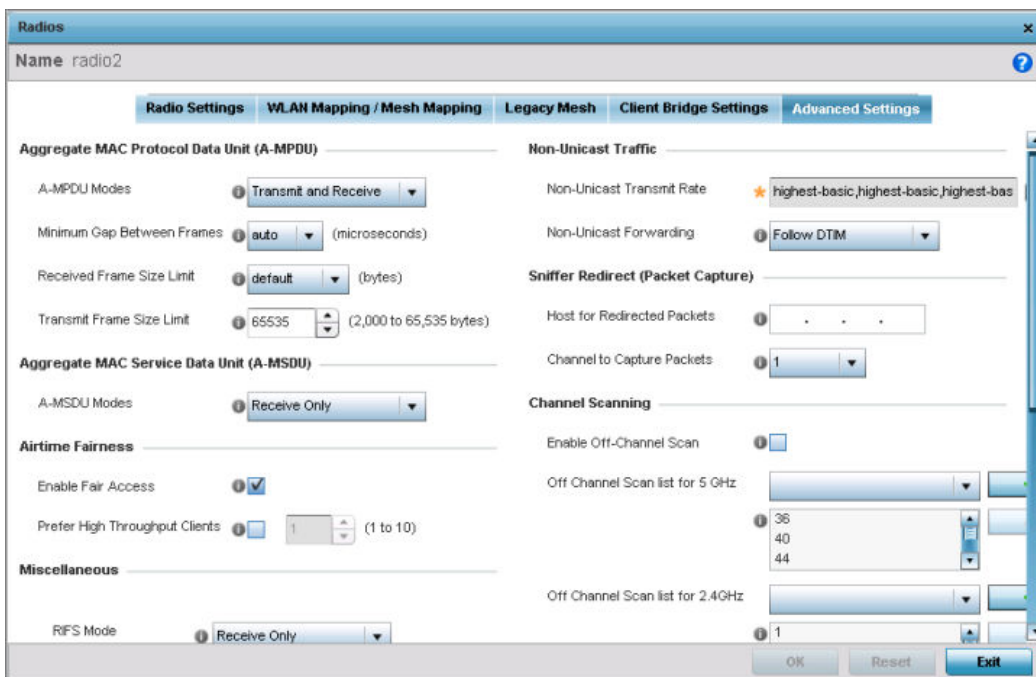
25 Refer to the **Roam Criteria** field and define the following configurations:

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 <b>Seconds for Missed Beacon</b> 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 is 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 Click **OK** to save the changes and overrides to the **Client Bridge Settings** screen.

Click **Reset** to revert to the last saved configuration.

27 Select the **Advanced Settings** tab.



**Figure 63: 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	Specify the A-MPDU mode. Options include <b>Transmit Only</b> , <b>Receive Only</b> , <b>Transmit and Receive</b> , and <b>None</b> . The default value is <b>Transmit and Receive</b> . Using the default value, long frames can be both sent and received (up to 64 KB). When this option is enabled, define a transmit limit, a receive limit, or both.
Minimum Gap Between Frames	Specify the minimum gap between A-MPDU frames (in microseconds). The default value is 4 microseconds. A value of <b>auto</b> means that 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, and 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 2000 to 65535 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 are **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 an RIFS mode to determine whether interframe spacing is applied to access point transmissions or received packets, both, or neither. The default mode is <b>Transmit and Receive</b> . 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 <b>None</b> 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 among 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 only on AP 81XX (AP 8132 and AP 8163) model access points, and it is disabled by default.

32 Set or override the following **Aeroscout Properties** for the selected access point radio.

Forwarding Host	Specify the Aeroscout engine's IP address. When specified, the AP forwards Aeroscout beacons directly to the Aeroscout locationing engine without proxying through the controller or RF Domain manager.  <b>Note:</b> Aeroscout beacon forwarding is supported only on the AP 6532, AP 7502, AP 7522, AP 7532, AP 7562, AP 8432, and AP 8533 model access points.
Forwarding Port	Set the port on which the Aeroscout engine is reachable.
MAC to be forwarded	Specify the MAC address to be forwarded.

33 Set or override the following **Ekahau Properties** for the selected access point radio.

Forwarding 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	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 <b>Select</b> drop-down menu to launch a sub-screen to define the data rate for broadcast and multicast frame transmissions. If you are not using the same rate for each BSSID, seven different rates are available – 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 <b>Follow DTIM</b> .

- 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 redirected from a controller or service platform's connected access point radio, specify the IP address of a resource (additional host system) used to capture the redirected packets. This address is the numerical (non DNS) address of the host used to capture the redirected packets.
Channel to Capture Packets	Specify the channel used to capture redirected 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 toward the channel scan and does not negatively impact client support.
Off Channel Scan list for 5GHz	Select the list of channels for off-channel scans using the access point's 5GHz 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	Select the list of channels for off-channel scans using the access point's 2.4GHz 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) between off-channel scans. The default setting is 20 dtims.
Sniffer Redirect	Specify the IP address of the host to which captured off-channel scan packets are redirected.

- 37 If an AP 7161 access point is deployed, set an **Extended Range** (from 1 - 25 kilometers) to allow AP 7161 access points to transmit and receive with their clients at greater distances without being timed out.
- 38 Click **OK** to save the changes and overrides to the **Advanced Settings** screen.  
Click **Reset** to revert to the last saved configuration.

#### MCS Data Rates

The following tables define **802.11n MCS** rates for with and without *short guard intervals* (SGI):

**Table 5: 802.11n MCS rates: No of Streams 1**

MCS Index	Number of Streams	20 MHz no SGI	20 MHz with SGI	40 MHz no SGI	40 MHz 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: 802.11n MCS rates: No of Streams 2**

MCS Index	Number of Streams	20 MHz no SGI	20 MHz with SGI	40 MHz no SGI	40 MHz 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
6	2	117	130	243	270
7	2	130	144.4	270	300

**Table 7: 802.11n MCS rates: No of Streams 3**

MCS Index	Number of Streams	20 MHz no SGI	20 MHz with SGI	40 MHz no SGI	40 MHz 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	364.7	405
7	3	195	216.7	405	450

The following table defines **802.11ac MCS** rates for both with and without SGI:



**Table 8: 802.11ac MCS rates, with and without SGI**

MCS Index	20 MHz no SGI	20 MHz with SGI	40 MHz no SGI	40 MHz with SGI	80 MHz no SGI	80 MHz 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

### WAN Backhaul 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.

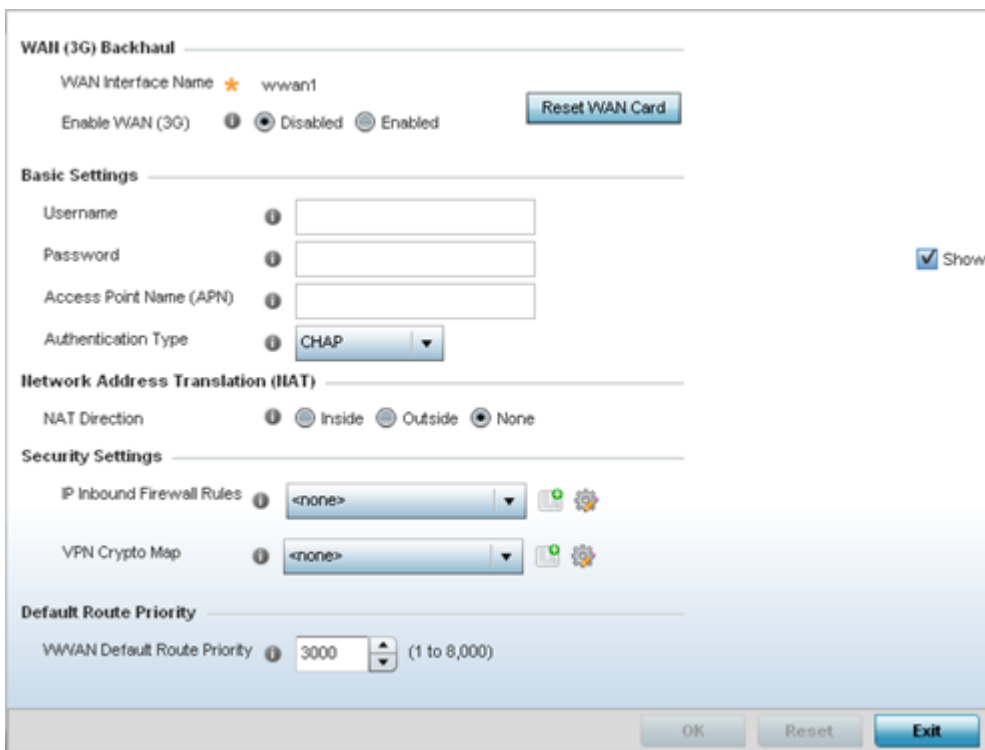
The RFS 4000 controller has a PCI Express card slot that supports 3G WWAN cards.

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.

To define a WAN Backhaul configuration override:

- 1 Select **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- 3 Select **Profile Overrides > Interface**.

4 Select **WAN Backhaul**.



**Figure 64: 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 **Clear Overrides**. This removes all overrides from the device.

5 Refer to the **WAN (3G) Backhaul** configuration to specify WAN card settings:

WAN Interface Name	The WAN Interface name for the WAN 3G Backhaul card.
Reset WAN Card	If the WAN Card becomes unresponsive or experiences other errors, click <b>Reset WAN Card</b> to power cycle and reboot the WAN card.
Enable WAN (3G)	Select 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.

6 Define or override the following authentication parameters in 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	Specify the authentication type used by the cellular data provider. Supported authentication types are <b>None</b> , <b>PAP</b> , <b>CHAP</b> , <b>MSCHAP</b> , and <b>MSCHAP-v2</b> .

- 7 Define or override the following NAT parameter in the **Network Address Translation (NAT)** field:

NAT Direction	<p>Define the Network Address Translation (NAT) direction. Options include:</p> <p><b>Inside</b> 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.</p> <p><b>Outside</b> 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.</p> <p><b>None</b> No NAT activity takes place. This is the default setting.</p>
---------------	--

- 8 Define or override the following security parameters in the **Security Settings** field:

IP Inbound Firewall Rules	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, click <b>Add</b> 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 <b>Create</b> button to configure a new one.

- 9 Define or override the following route parameter in 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 Click **OK** to save the changes and overrides made to the **WAN Backhaul** screen.  
Click **Reset** to revert to the last saved configuration.

### PPPoE 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 failover is available to maintain seamless network access if the access point's Wired WAN should fail.



#### Note

Devices with PPPoE enabled continue to support VPN, NAT, PBR, and 3G failover 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 flow. 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** > **Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- 3 Select **Profile Overrides** > **Interface**.

4 Select **PPPoE**.

**Figure 65: Device 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 **Clear Overrides**. This removes all overrides from the device.

5 Use the **Basic Settings** field to enable PPPoE and define a PPPoE client.

Admin Status	Select <b>Enable</b> 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)	Set the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to the DSL modem. The available range is 1 - 4,094. The default value is 1.
Client IP Address	Provide the numerical (non hostname) IP address of the PPPoE client.

- 6 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. Click <b>Show</b> to display the characters that make up the password.
Authentication Type	Specify the authentication type used by the PPPoE client, and whose credentials must be shared by its peer access point. Supported authentication options include <b>None, PAP, CHAP, MSCHAP, and MSCHAP-v2.</b>

- 7 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 <b>Seconds</b> (1 - 65,535), <b>Minutes</b> (1 - 1,093) or <b>Hours</b> (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 that the point-to-point connection to the PPPoE client is continuously maintained and not timed out. This setting is disabled by default.

- 8 Set the **Network Address Translation (NAT)** direction for the PPPoE configuration.

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 nor outside).

- 9 Define the following **Security Settings** for the PPPoE configuration:

Inbound IP Firewall Rules	Select a firewall (set of IP access connection rules) to apply to the PPPoE client connection. If there is no firewall rule that meets the data protection needs of the PPPoE client connection, select the <b>Create</b> icon to define a new rule configuration or the <b>Edit</b> icon to modify an existing rule. For more information, see <a href="#">Wireless Firewall</a> on page 714.
VPN Crypto Map	Use the drop-down menu to apply an existing crypto map configuration to this PPPoE interface.

- 10 Set the **Default Route Priority** for the default route learned using PPPoE.

Select from 1 - 8,000. The default setting is 2,000.

- 11 Click **OK** to save the changes and overrides made to the **PPPoE** screen.

Click **Reset** to revert to the last saved configuration. Saved configurations are persistent across reloads.

## Bluetooth 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 sensing functionality only, not the Bluetooth 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 they are 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 **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target access point in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- 3 Select **Profile Overrides > Interface**.

4 Select **Bluetooth**.

**Bluetooth Radio Configuration**

Admin Status  Disabled  Enabled

Description

**!** Warning: Enabling Bluetooth may cause interference on 2.4 GHz radio in wlan mode.

**Basic Settings**

Bluetooth Radio Functional Mode

Beacon Transmission Period  (100 to 10,000 milliseconds)

Beacon Transmission Pattern

**Eddystone Settings**

Eddystone Beacon Calibration Signal Strength  (-127 to 127 dBm)

URL-1 to Transmit Eddystone-URL

URL-2 to Transmit Eddystone-URL

**iBeacon Settings**

iBeacon Calibration Signal Strength  (-127 to 127 dBm)

iBeacon Major Number  (0 to 65,535)

iBeacon Minor Number  (0 to 65,535)

iBeacon UUID

OK Reset Exit

**Figure 66: Profile Overrides - Bluetooth Screen**5 Set the following **Bluetooth Radio Configuration** parameters:

Admin Status	<b>Enable</b> or <b>Disable</b> Bluetooth support capabilities for AP 8432 or AP 8533 model access point 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 might be members of the same RF Domain.



6 Set the following **Basic Settings**:

Bluetooth Radio Functional Mode	Set the access point's Bluetooth radio functional mode to either <b>bt-sensor</b> or <b>le-beacon</b> . Use <b>bt-sensor</b> mode for ADSP Bluetooth classic sensing. Use <b>le-beacon</b> mode to have the access point transmit both i beacon and Eddystone-URL low energy beacons. <b>le-beacon</b> 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 <b>le-beacon</b> , use the enabled drop-down menu to set the beacon's emitted transmission pattern to <b>eddytone_url1</b> , <b>eddytone_url2</b> , or <b>ibeacon</b> . An eddytone-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). Apple has made three data fields 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.

7 Define the following **Eddystone Settings** if you have set the **Beacon Transmission Pattern** to either **eddytone\_url1** or **eddytone\_url2**:

Eddystone Beacon Calibration Signal Strength	Set the Eddystone Beacon measured calibration signal strength, from -127 dBm 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 eddytone-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 eddytone-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.

8 Define the following **iBeacon Settings** if you have set the **Beacon Transmission Pattern** to **ibeacon**:

Beacon Calibration Signal Strength	Set the iBeacon measured calibration signal strength, from -127 dBm 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 value 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 Universally Unique Identifier (UUID). The UUID classification contains 32 hexadecimal digits. The UUID distinguishes iBeacons in the network from all other beacons in networks outside of your direct administration.

9 Click **OK** to save the changes made to the Bluetooth configuration.  
Click **Reset** to revert to the last saved configuration.

## Profile Network Configuration

Setting an access point profile's network configuration is a large task comprised of numerous administration activities.

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 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.
- 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 that exist in a network, the more routes need 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 will need a minimum of 81 routes (9 x 9 = 81).

An access point profile network configuration process consists of the following:

- [DNS Configuration](#) on page 162
- [ARP Configuration](#) on page 164
- [L2TPv3 Profile Configuration](#) on page 165
- [IGMP Snooping Configuration](#) on page 181
- [MLD Snooping Configuration](#) on page 182
- [Quality of Service \(QoS\) Configuration](#) on page 184
- [Spanning Tree Configuration](#) on page 189
- [Routing Configuration](#) on page 191
- [Dynamic Routing \(OSPF\) Configuration](#) on page 195
- [Forwarding Database Configuration](#) on page 214
- [Bridge VLAN Configuration](#) on page 215
- [Cisco Discovery Protocol Configuration](#) on page 225
- [Link Layer Discovery Protocol Configuration](#) on page 226
- [Miscellaneous Network Configuration](#) on page 227
- [Alias](#) on page 227
- [IPv6 Neighbor Configuration](#) on page 236

## DNS 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 the **Configuration > Devices > System Profile** tab from the Web UI.
- 2 Expand the **Network** menu and select **DNS**.

**Figure 67: Network - DNS Screen**

- 3 Set the following 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.

- 4 In the **Name Servers** field, provide the IP addresses of up to three DNS server resources available to the access point.

- 5 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.

- 6 Select **OK** to save the changes made to the DNS configuration. Select **Reset** to revert to the last saved configuration.

## ARP 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 the **Configuration > Devices > System Profile** tab from the Web UI.

- Expand the **Network** menu and select **ARP**.

Switch VLAN Interface	IP Address	MAC Address	Device Type	
1	1.2.3.4	10-20-30-40-50-60	Router	

+ Add Row

OK    Reset    Exit

**Figure 68: Network - ARP screen**

- 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.
- Set the following parameters to define the ARP configuration:

Switch VLAN Interface	Use the spinner control to select a virtual interface for an address requiring resolution with the controller, service platform or access point.
IP Address	Define the IP address used to fetch a MAC Address recognized on the wireless network.
MAC Address	Displays 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.
- 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.

### L2TPv3 Profile Configuration

L2TP V3 is an IETF standard used for transporting different types of layer 2 frames in an IP network (and 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 managed devices and 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 pseudowire 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**

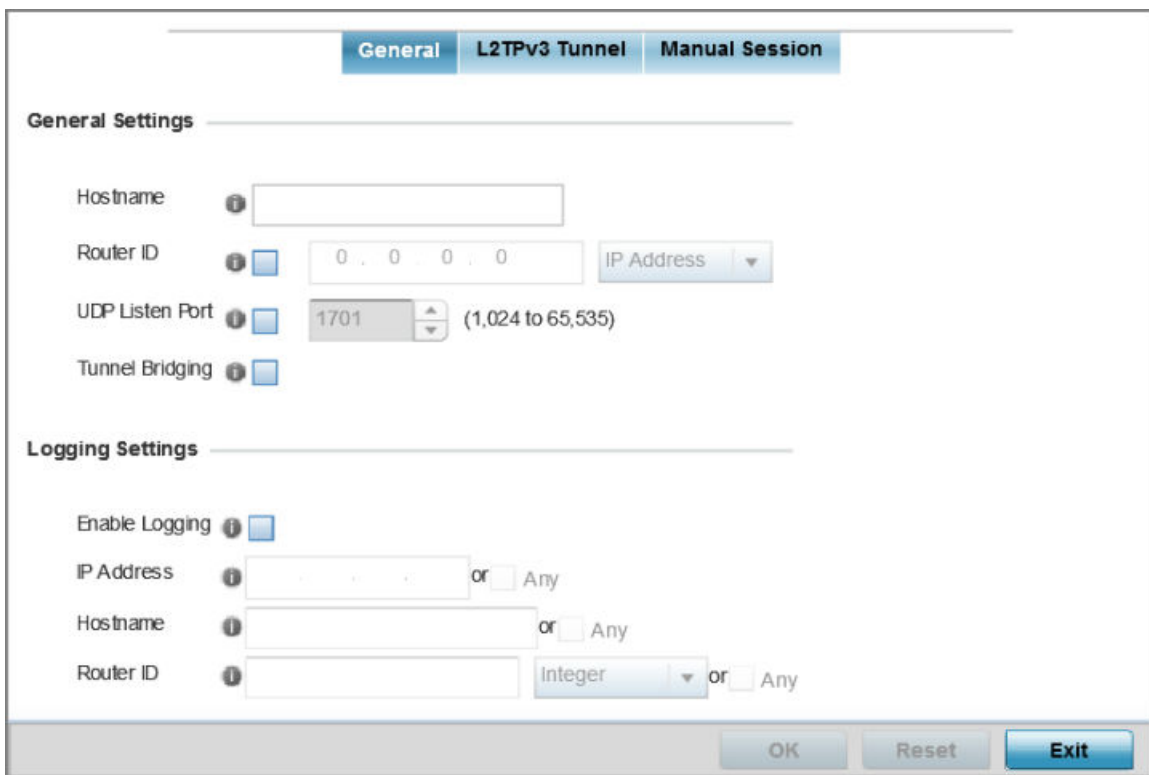
If connecting an Ethernet port to another Ethernet port, the pseudowire type must be *Ethernet port*, if connecting an Ethernet VLAN to another Ethernet VLAN, the pseudowire type must be *Ethernet VLAN*.

---

To define an L2TPV3 configuration for an access point profile:

- 1 Select the **Configuration > Devices > System Profile** tab from the Web UI.

- Expand the **Network** menu and select **L2TPv3**.



**Figure 69: Network - L2TPv3 screen - General tab**

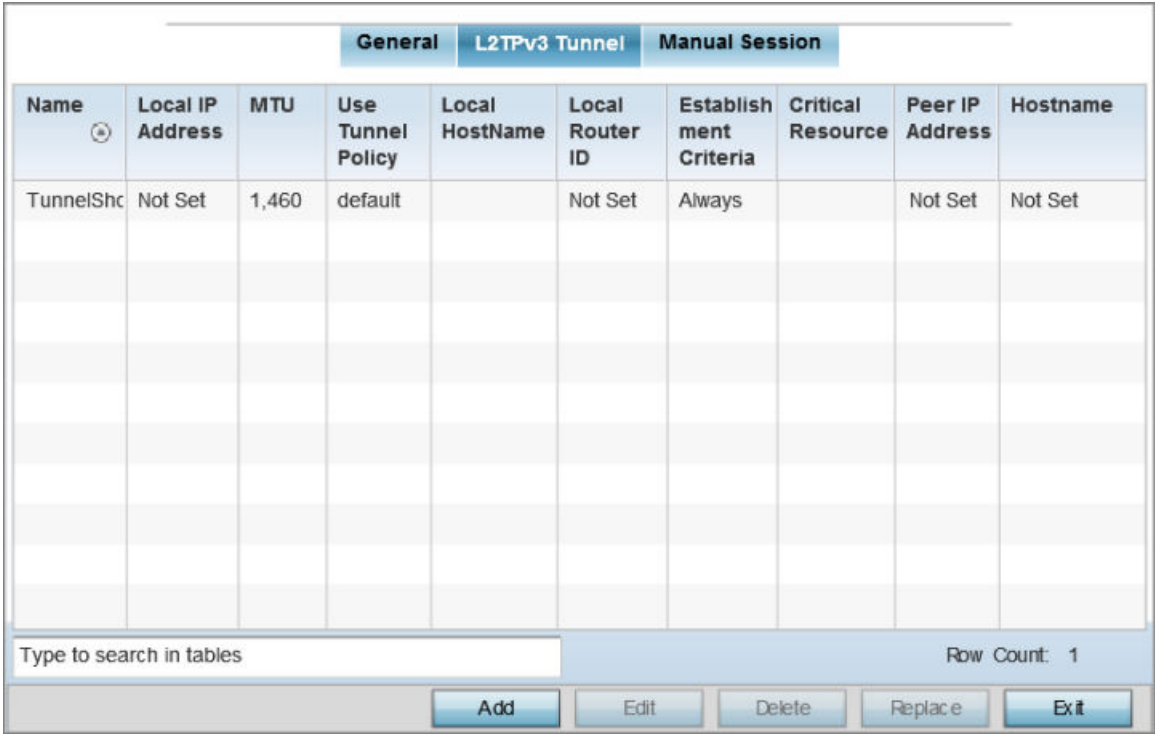
- Set the following **General Settings** for an L2TPv3 profile configuration:

Host Name	Define a 64 character maximum hostname 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. The default port is 1701.
Tunnel Bridging	Select this option to enable or disable bridge packets between two tunnel end points. This setting is disabled by default.

- 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.
Hostname	If not using an IP address for event logging, optionally use a peer tunnel hostname to capture and log L2TPv3 events.
Router ID	If not using an IP address or a hostname for event logging, use a router ID to capture and log L2TPv3 events.

- Select the **L2TPv3 Tunnel** tab.



**Figure 70: Network - L2TPv3 screen - L2TPv3 tunnel tab**

- 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 hostname advertised in tunnel establishment messages.
Local Router ID	Specifies the router ID sent in the tunnel establishment messages.
Establishment Criteria	Specifies tunnel criteria between two peers.
Critical Resource	Specifies the critical resource that should exist for a tunnel between two peers to be created and maintained. Critical resources are device IP addresses or interface destinations interpreted 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.
Peer IP Address	Lists the IP address of the remote peer.
Host Name	Lists the tunnel specific hostname used by the remote peer.

- 7 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.

**L2TPv3 Tunnel**

Name HQSJSAP

Session Settings

Session

Name	Pseudowire ID	Traffic Source Type	Traffic Source Value	Native VLAN	
SQL_01	1	VLAN	496	Not Set	

+ Add Row

OK Reset Exit

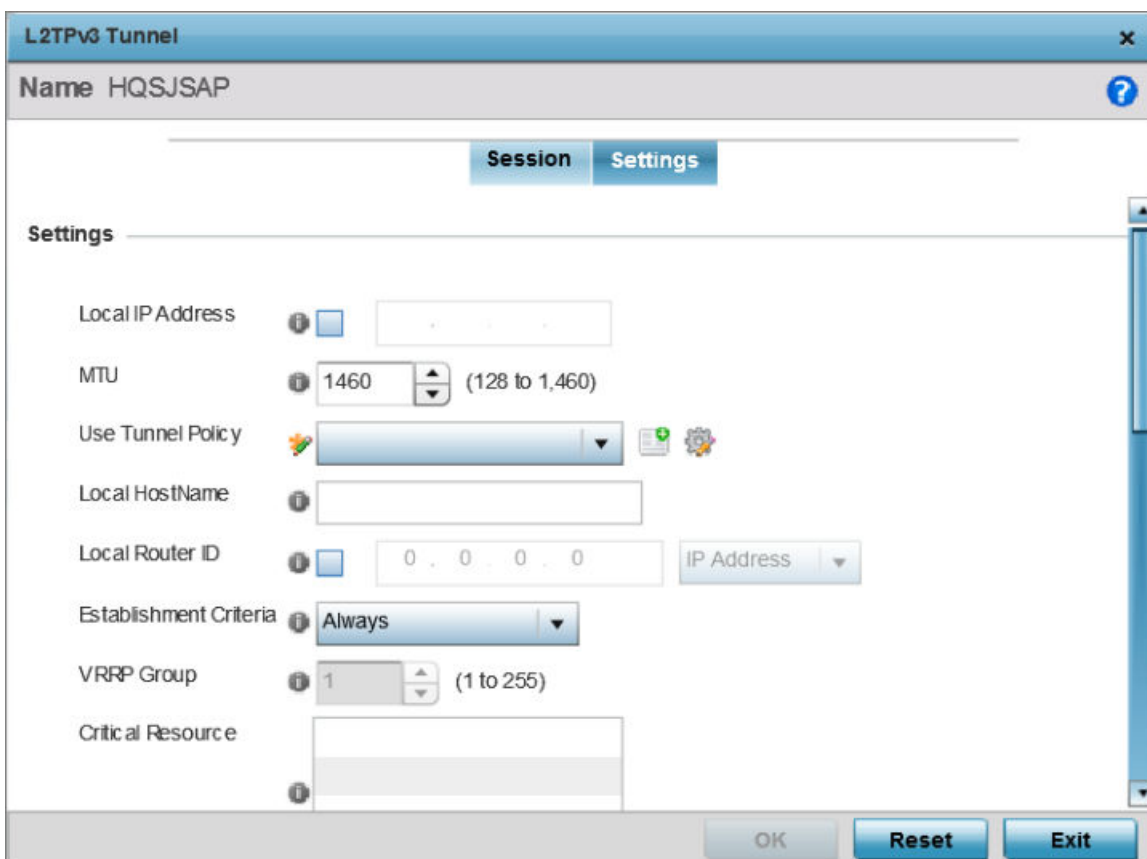
**Figure 71: Network - L2TPv3 screen - Add L2TPv3 Tunnel Configuration**

- 8 If creating a new tunnel configuration, assign it a 31 character maximum **Name**.
- 9 Refer to the **Session** table to review the configurations of the peers available for tunnel connection.
- 10 Select **+ Add Row** to populate the table with configurable session parameters for this tunnel configuration.
- 11 Define the following **Session** parameters:

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 pseudowire 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 VLAN	Select this option to provide a VLAN ID that will not be tagged in tunnel establishment and packet transfer.

12 Select the **Settings** tab.



**Figure 72: Network - L2TPv3 screen - Add L2TPv3 Tunnel Configuration - Settings screen**

13 Define the following Settings required for the L2TP 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 between 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. For more information, refer to <a href="#">L2TP V3 Configuration</a> on page 444.
Local Hostname	Provide the tunnel specific hostname used by this tunnel. This is the hostname advertised in tunnel establishment messages.
Local Router ID	Specify the router ID sent in tunnel establishment messages with a potential peer device.
Establishment Criteria	<p>Configure establishment criteria for creating a tunnel between the device and the NOC. This criteria ensures only one tunnel is created between two sites where the tunnel is established between the vrrp-master/cluster master/rfdomain manager at the remote site and the controller at the NOC. The tunnel is created based on the role of the remote peer.</p> <ul style="list-style-type: none"> <li>• always – The tunnel is always created irrespective of the role of the local device.</li> <li>• vrrp-master – The tunnel is only created when the local device is a VRRP master.</li> <li>• cluster-master – The tunnel is only created when the local device is a cluster master.</li> <li>• rf-domain-manager – The tunnel is only created when the local device is a RF-Domain manager.</li> </ul> <p>In all the above cases, if the local device goes offline for any reason, the tunnel is brought down.</p>
VRRP Group	This field is enabled only when the Establishment Criteria is set to vrrpmaster. Use the spinner to select the VRRP group.
Critical Resource	Enter the critical resources required for creating and maintaining a L2TPV3 tunnel. A tunnel is only established when all critical resources for the tunnel to be operational are available at the time when the tunnel is created. If any one of the listed critical resources goes down, the tunnel is disabled. When a tunnel is established, the listed critical resources are checked for availability. Tunnel establishment is started if the critical resources are available. Similarly, for incoming tunnel termination requests, listed critical resources are checked and tunnel terminations are only allowed when the critical resources are available. For more information on managing critical resources, see <a href="#">Profile Critical Resources</a> .

- 14 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.
Max 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 % for background traffic. Set a value from 1 - 100%. The default is 50%.
Best-Effort	Set the random early detection threshold in % for best-effort traffic. Set a value from 1 - 100%. The default is 50%.
Video	Set the random early detection threshold in % for video traffic. Set a value from 1 - 100%. The default is 25%.
Voice	Set the random early detection threshold in % for voice traffic. Set a value from 1 - 100%. The default is 25%.

- 15 Refer to the **Peer** table to review the configurations of the peers available for tunnel connection. Select **+ Add Row** to populate the table with a maximum of two peer configurations.

**Figure 73: Network - L2TPv3 screen - Add L2TPv3 Peer Configuration**

- 16 Define the following **Peer** parameters:

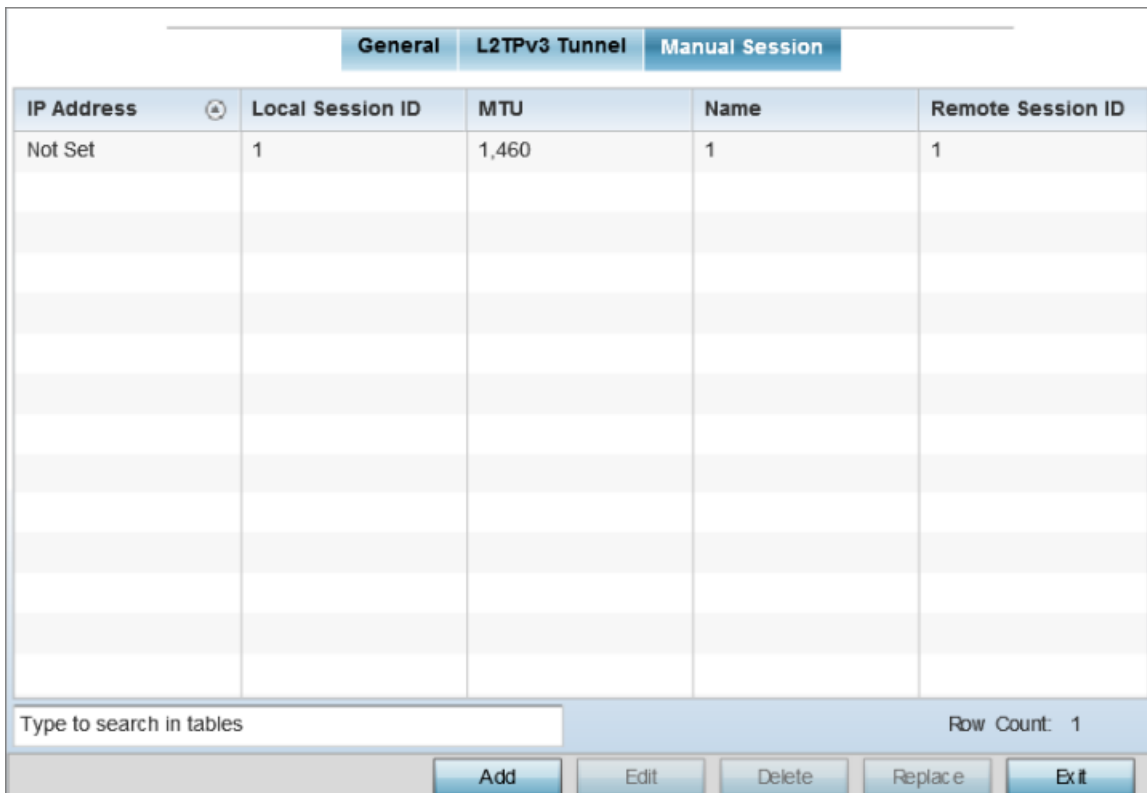
Peer ID	Define the primary peer ID used to set the primary and secondary peer for tunnel fail over. If the peer is not specified, tunnel establishment does not occur. However, if a peer tries to establish a tunnel with this access point, it creates the tunnel if the hostname and/or Router ID matches.
Router ID	Specify the router ID sent in tunnel establishment messages with this specific peer.
Hostname	Assign the peer a hostname that can be used as matching criteria in the tunnel establishment process.
Encapsulation	Select either <i>IP</i> or <i>UDP</i> as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes.
Peer IP Address	Select this option to enter the numeric IP address used as the destination peer address for tunnel establishment.
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.
IPSec Gateway	Specify the IP Address of the IPSec Secure Gateway.

- 17 Select **OK** to save the peer configuration.
- 18 From the **L2TPv3 Tunnel** screen's **Settings** tab, configure the **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 tunnel is defined as active and the other as 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.

- 19 Select **OK** to save the changes within the L2TPv3 Tunnel screen. Select **Reset** to revert the screen to its last saved configuration.
- 20 Select the **Manual Session** tab.

After 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.



IP Address	Local Session ID	MTU	Name	Remote Session ID
Not Set	1	1,460	1	1

**Figure 74: Network - L2TPv3 screen - Manual Session tab**

- 21 Refer to the following manual session configurations to determine whether a session 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 <i>maximum transmission unit</i> (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.



- 22 Select **Add** to create a new manual session, **Edit** to modify an existing session configuration or **Delete** to remove a selected manual session.

**Manual Session**

Name ★

**Settings**

IP Address i

IP ★

Local Session ID ★ 1 (1 to 15)

MTU i 1460 (128 to 1,460)

Remote Session ID ★ 1 (1 to 4,294,967,295)

Encapsulation i IP

UDP Port i 1701 (1,024 to 65,535)

Source Type ★ VLAN

Source Value ★  (1 - 4094) (2,4,7-12,...)

Native VLAN i  1 (1 to 4,094)

Cookie

Cookie Size	Value 1	Value 2	End Point	
<span style="color: grey;">i</span>				

+ Add Row

OK Reset Exit

**Figure 75: Network - L2TPv3 screen, Add L2TPv3 Manual Session Configuration**

23 Set the following session parameters:

Name	Define a 31 character maximum name for this tunnel session. Each session name represents a single data stream.
IP Address	Specify the IP address used as a 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, the tunnel would use the IP address received in the tunnel create 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 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 will not be tagged.

24 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.

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

## GRE

GRE tunneling can be configured to bridge Ethernet packets between WLANs and a remote WLAN gateway over an IPv4 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 server using IPv4.

To review a profile's GRE settings:

- 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.

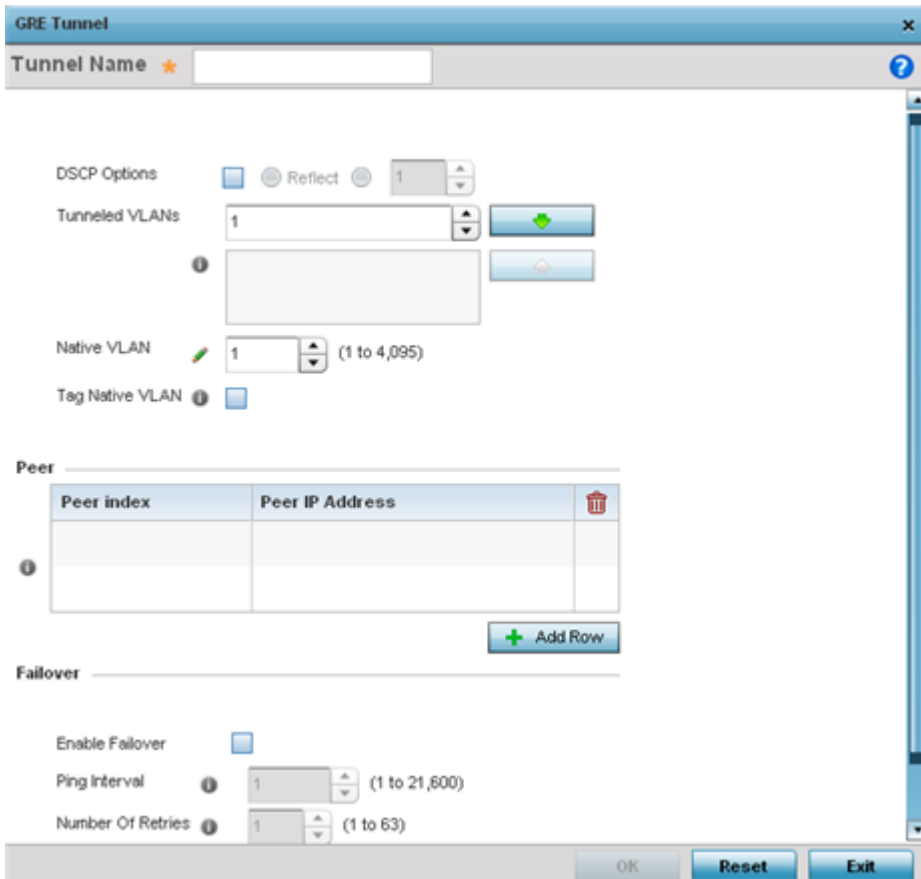
### GRE Configuration

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.



- 5 If creating a new GRE configuration, assign it a name to distinguish its configuration.
- 6 Define the following settings for the GRE configuration:

<b>DSCP Options</b>	Use the spinner control to set the tunnel DSCP / 802.1q priority value from encapsulated packets to the outer packet IPv4 header.
<b>Tunneled VLANs</b>	Define the VLAN connected clients use to route GRE tunneled traffic within their respective VLANs.
<b>Native VLAN</b>	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.
<b>Tag Native VLAN</b>	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.

- 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.

- Define the following **Peer** parameters:

<b>Peer Index</b>	Assign a numeric index to each peer to help differentiate tunnel end points.
<b>Peer IP Address</b>	Define the IP address of the added GRE peer to serve as a network address identifier.

- Define the following **Failover** parameters to apply to the GRE tunnel configuration:

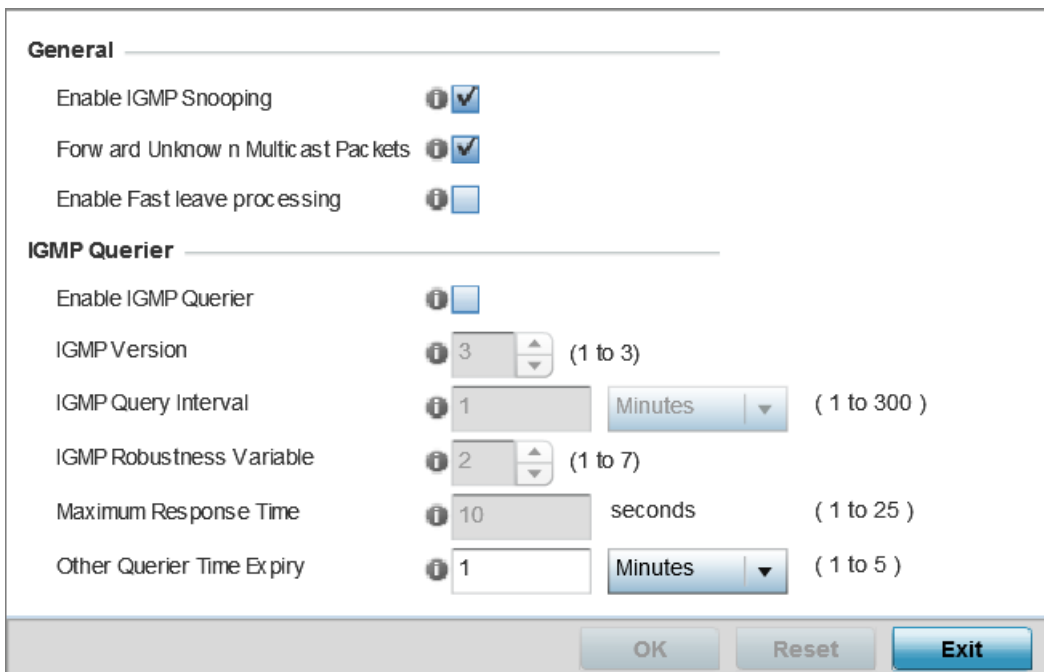
<b>Enable Failover</b>	Select this option to periodically ping the primary gateway to assess its availability for failover support.
<b>Ping Interval</b>	Set the duration between two successive pings to the gateway. Define this value in seconds from 0 - 86,400.
<b>Number of Retries</b>	Set the number of retry ping opportunities before the session is terminated.

- Select the **OK** button located to save the changes. Select **Reset** to revert to the last saved configuration.

### IGMP Snooping Configuration

The *Internet Group Management Protocol* (IGMP) is used for managing IP multicast group members. Controllers 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 controller or service platform floods all the wired interfaces. This feature reduces unnecessary flooding of multicast traffic in the network.

- Select the **Configuration > Devices > System Profile** tab from the Web UI.
- Expand the **Network** menu and select **IGMP Snooping**.



**Figure 76: IGMP Snooping Screen**

- 3 Set the following parameters to configure **General IGMP Snooping** values:

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..

- 4 Set the following for **IGMP Querier** 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. This parameter is used only when the querier functionality is enabled. Define an interval value in <i>Seconds</i> (1 - 18,000), <i>Minutes</i> (1 - 300) and <i>Hours</i> (1 - 5). The default setting is one minute.
IGMP Robustness Variable	Sets the IGMP robustness variable. The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. Define a robustness variable from 1 - 7. The default robustness value 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. Only multicast packets are forwarded 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 <i>Seconds</i> (60 - 300) or <i>Minutes</i> (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute.

- 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.

### MLD Snooping 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.

- 1 Select the **Configuration > Devices > System Profile** tab from the Web UI.
- 2 Expand the **Network** menu and select **MLD Snooping**.

**Figure 77: Profile - Network MLD Snooping screen**

- 3 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.

- 4 Define the following **MLD Querier** settings for the MLD snooping configuration:

Enable MLD Querier	Select this 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.

- 5 Select the **OK** button located to save the changes. Select **Reset** to revert to the last saved configuration.

### Quality of Service (QoS) Configuration

The uses different Quality of Service (QoS) screens to define WLAN and device radio QoS configurations. The **System Profiles > Network > QoS** facility is separate from WLAN and radio QoS configurations, and is used to configure the priority of the different DSCP packet types.

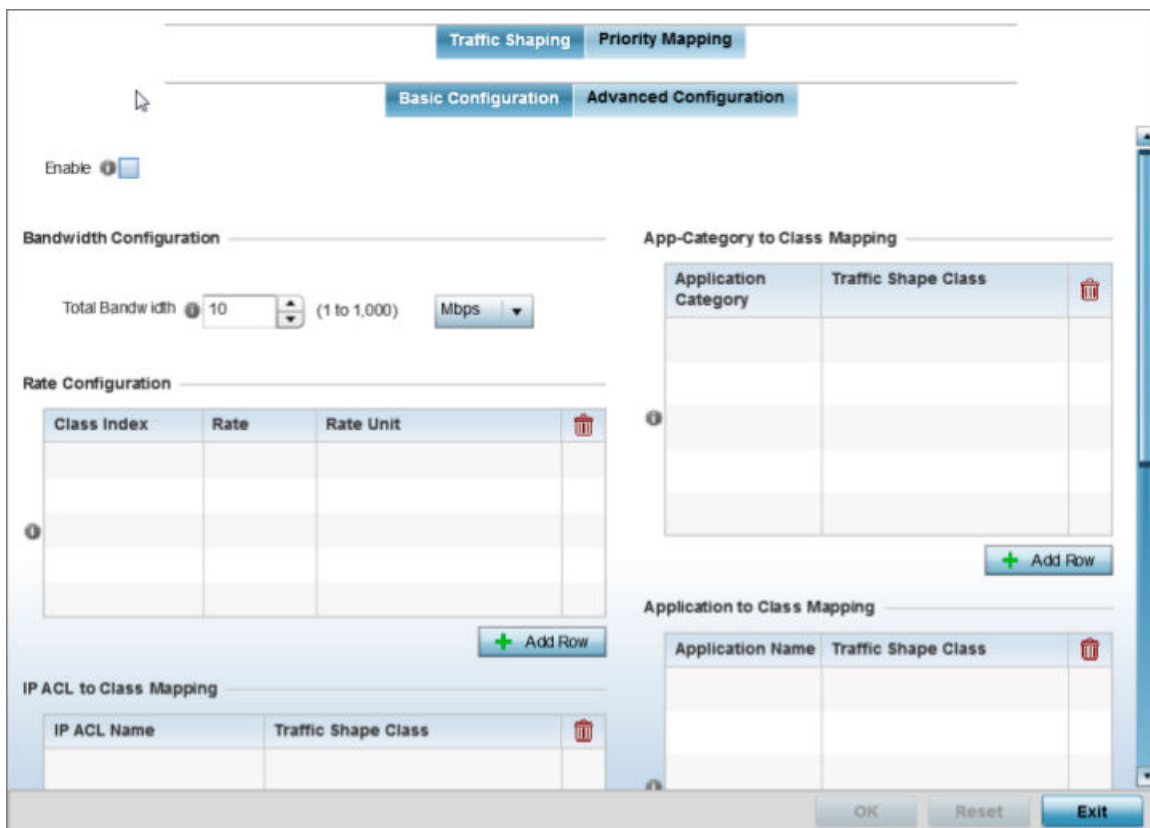
QoS values are required to provide priority of service to some packets over others. For example, VoIP packets get higher priority than data packets to provide a better quality of service for high priority voice traffic.

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 applied to a packet.

To define an QoS configuration for DSCP mappings:

- 1 Select the **Configuration > Devices > System Profile** tab from the Web UI.
- 2 Expand the **Network** menu and select **Quality of Service (QoS)**

The **Traffic Shaping** screen displays with the **Basic Configuration** tab displayed by default.



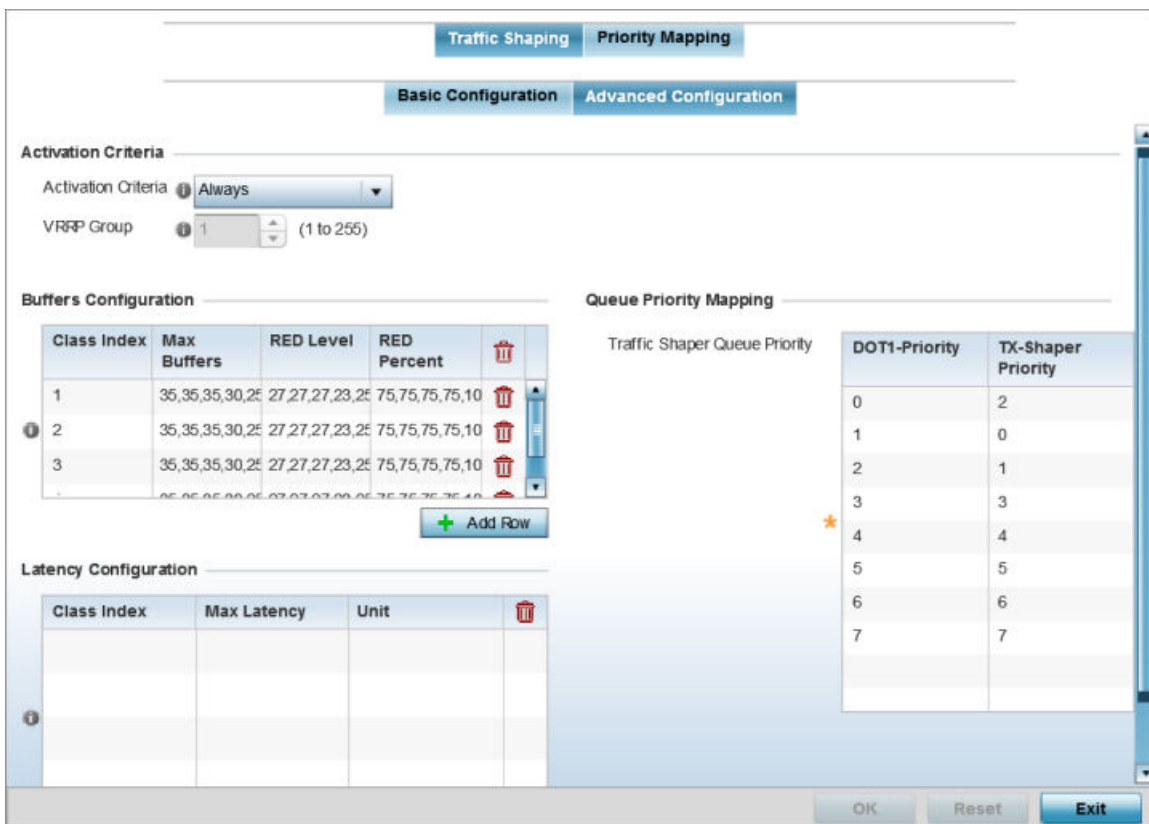
**Figure 78: Profile Overrides - Network QoS Traffic Shaping Basic Configuration Screen**

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.



- 3 Select **Enable** to provide traffic shaping using the defined bandwidth, rate and class mappings.
- 4 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.
- 5 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.
- 6 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 732 and [Setting an IPv4 or IPv6 Firewall Policy](#) on page 732.
- 7 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 732 and [Setting an IPv4 or IPv6 Firewall Policy](#).
- 8 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 495.
- 9 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 495.
- 10 Select the **OK** button located to save the changes to the traffic shaping basic configuration. Select **Reset** to revert to the last saved configuration.

- 11 Select the **Advanced Configuration** tab.



**Figure 79: Profile Overrides - Network QoS Traffic Shaping Advanced Configuration Screen**

- 12 Set the following **Activation Criteria** for traffic shaper activation:

<p>Activation Criteria</p>	<p>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.</p>
<p>VRRP Group</p>	<p>Set the VRRP group ID from 1 - 255. VRRP groups is only enabled when the Establishment Criteria is set to vrrp-master.</p>

- 13 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.

- 14 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 is dropped. By default latency is not set, so packets remain in queue for long time.

- 15 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.
- 16 Select the **OK** button located to save the changes to the traffic shaping advanced configuration. Select **Reset** to revert to the last saved configuration.

- 17 Select the **Priority Mapping** tab.

**Priority Mapping**

**DSCP Mapping**

DSCP	802.1p Priority
0	0
1	0
2	0
3	0
* 4	0
5	0
6	0
7	0
8	1
9	1

**IPv6 Traffic Class Mapping**

Traffic Class	802.1p Priority
0	0
1	0
2	0
3	0
* 4	0
5	0
6	0
7	0
8	1
9	1

OK Reset Exit

**Figure 80: Network - Quality of Service (QoS) Screen**

- 18 Set 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 - <i>Best Effort</i> 1 - <i>Background</i> 2 - <i>Spare</i> 3 - <i>Excellent Effort</i> 4 - <i>Controlled Load</i> 5 - <i>Video</i> 6 - <i>Voice</i> 7 - <i>Network Control</i>

Use the spinner controls within the **802.1p Priority** field for each DSCP row to change its priority value.

19 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 - <i>Best Effort</i> 1 - <i>Background</i> 2 - <i>Spare</i> 3 - <i>Excellent Effort</i> 4 - <i>Controlled Load</i> 5 - <i>Video</i> 6 - <i>Voice</i> 7 - <i>Network Control</i>

20 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.

### Spanning Tree 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.

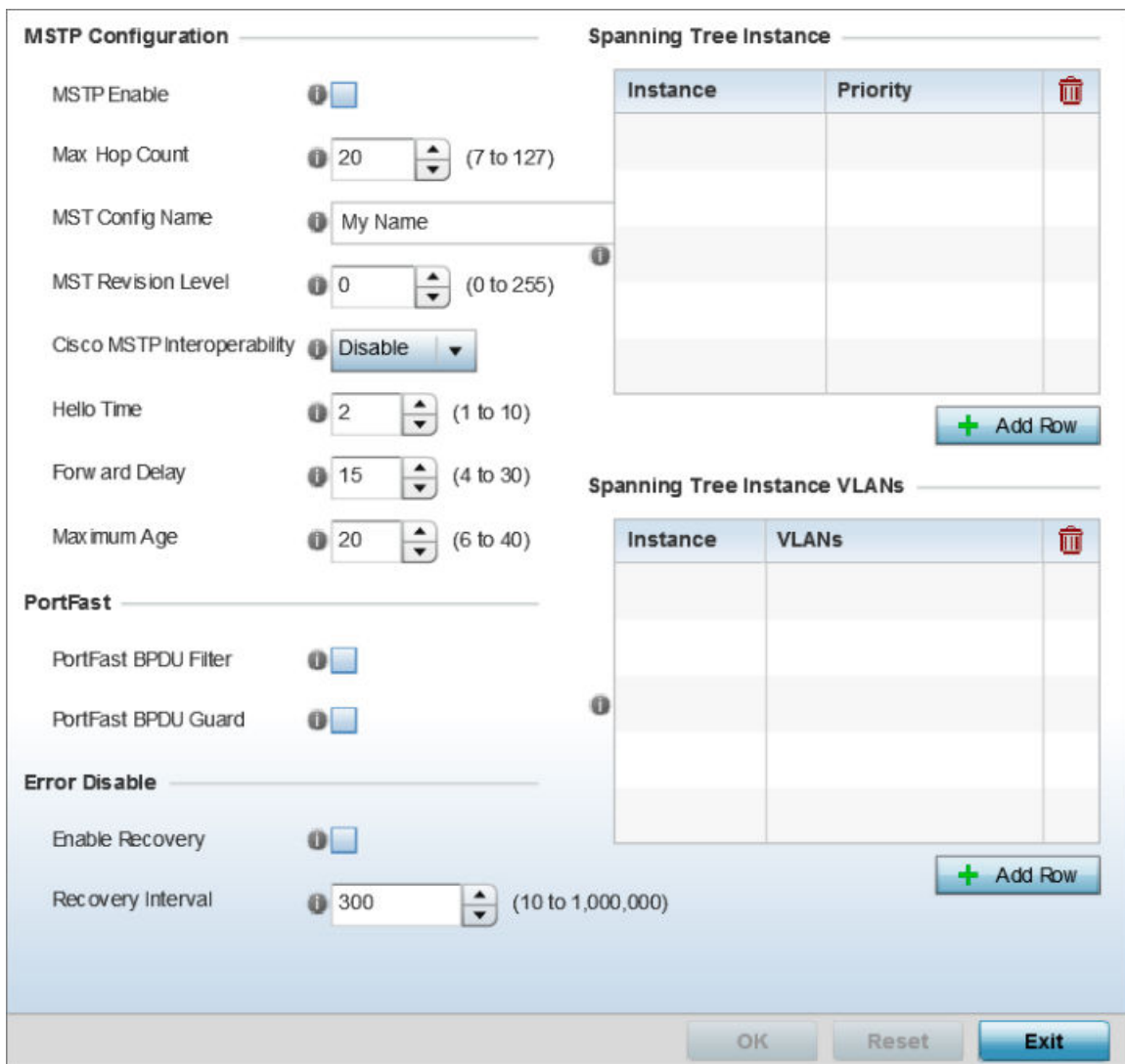
If there is just one VLAN in the access point managed network, a single spanning tree works fine. However, if the network contains more than one VLAN, the network topology defined by single STP would work, but it is possible to make better use of the alternate paths available by using an alternate spanning 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 define the spanning tree configuration:

- 1 Select the **Configuration > Devices > System Profile** tab from the Web UI.

- Expand the **Network** menu and select **Spanning Tree**.



**Figure 81: Network - Spanning Tree Screen**

- 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.

- 4 Define the following **Port Fast** 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 setting is disabled.

- 5 Define the following **Error Disable** settings:

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.

- 6 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.
- 7 Use the **Spanning Tree Instance** VLANs table to add VLAN instance indexes (by numeric ID) and VLANs to the spanning tree topology.
- 8 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.

## Routing Configuration

Routing is the process of selecting IP paths to send access point managed network traffic. Use the Routing screen to set destination IP and gateway addresses enabling 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 static routes:

- 1 Select the **Configuration > Devices > System Profile** tab from the Web UI.
- 2 Expand the **Network** menu and select **Routing**.  
The **IPv4 Routing** tab displays by default.

The screenshot shows the 'IPv4 Routing' configuration page. It includes the following elements:

- IP Routing:** A section with a checked checkbox for 'IP Routing'.
- Policy Based Routing:** A section with a dropdown menu for selecting a policy.
- Static Routes:** A table with the following structure:
 

Network Address	Gateway	Default Gateway	

 Below the table is an '+ Add Row' button.
- Default Route Priority:** A section with:
  - Static Default Route Priority: 100 (range 1 to 8,000)
  - DHCP Client Default Route Priority: 1000 (range 1 to 8,000)
  - Enable Routing Failure: checked checkbox
- Footer:** A checkbox 'Use Network Address of 0.0.0.0/0 to Set Default Gateway' and buttons for 'OK', 'Reset', and 'Exit'.

**Figure 82: Network - Routing screen**

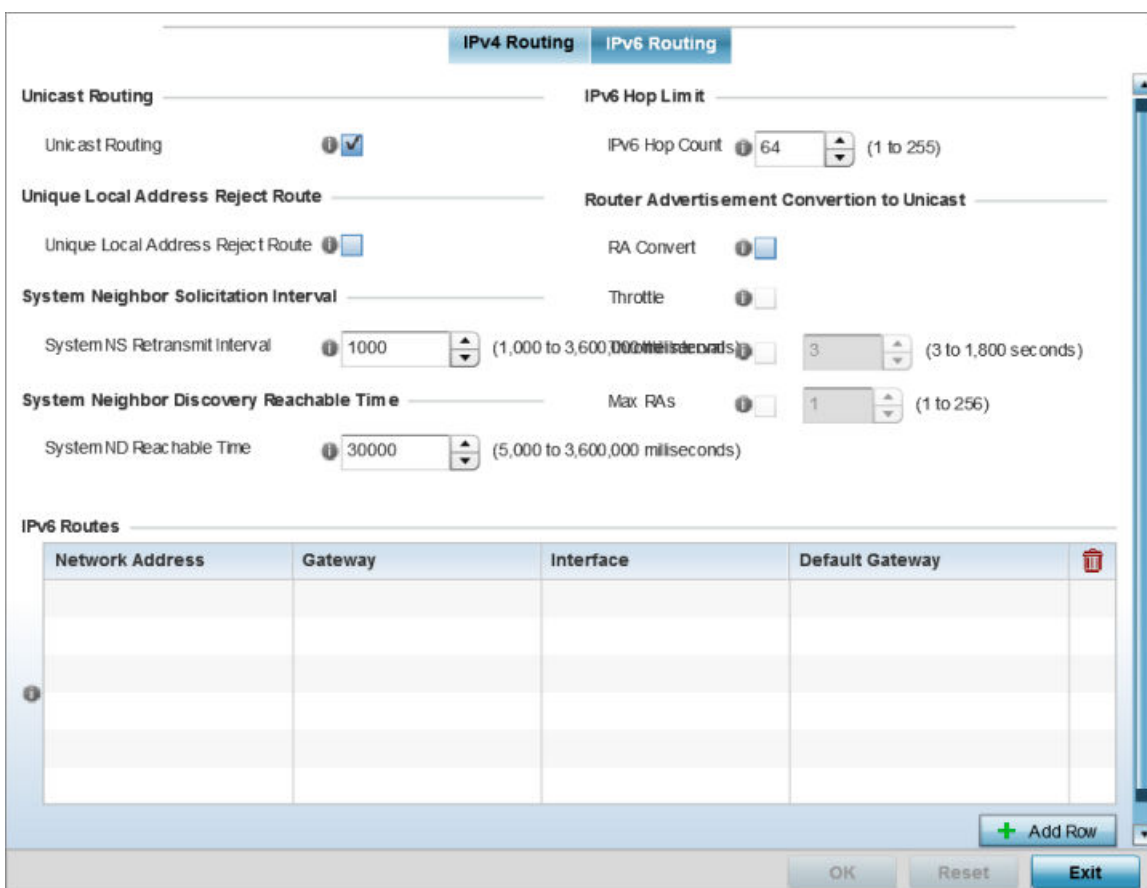
- 3 Select **IP Routing** to enable static routes using IPv4 addresses. This option is enabled by default.
- 4 Select the **Policy Based Routing** policy to apply to this profile. Select the **Create** icon to create a policy based route or select the **Edit** icon to edit an existing policy after selecting it in the drop-down list. For more information on creating a Policy Based Routing Policy, see [Policy Based Routing \(PBR\)](#) on page 439.
- 5 Select **Add Row +** as needed to include single rows with in the static IPv4 route table.
- 6 Add IP addresses and network masks in the **Network Address** column of the **Static Routes** table.
- 7 Provide the **Gateway** used to route traffic.



- 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 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 **IPv6 Routing** tab. IPv6 networks are connected by IPv6 routers. IPv6 routers pass IPv6 packets from one network segment to another.



**Figure 83: Static Routes Screen - IPv6 Routing Tab**

- 10 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.
- 11 Select **Unique Local Address Reject Route** to enable rejecting local routes in the format FC00::/7.

- 12 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.
- 13 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.
- 14 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.
- 15 Set the **Router Advertisement Conversion to Unicast** settings:

RA Convert (milliseconds)	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.

- 16 Select **+ Add Row** as needed within the IPv6 Routes table to add an additional 256 IPv6 route resources.

**Figure 84: 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.
Default Gateway	Use a network address of ::/0 to set the default gateway.

- 17 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.

### Dynamic Routing (OSPF) 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 be 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 is 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 sends 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-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.



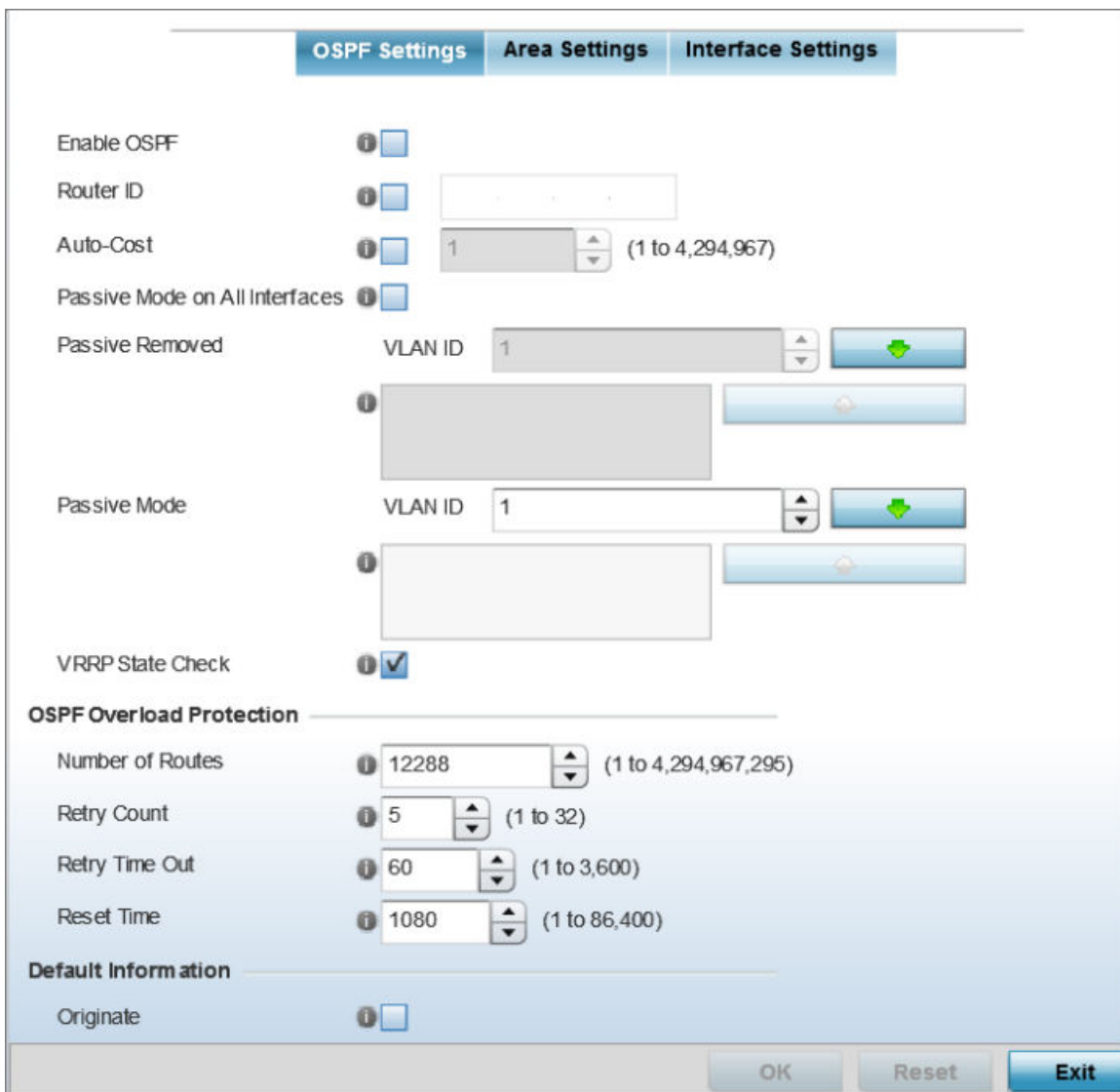
#### Note

OSPF is available on the following access points: AP8432, AP8533, AP7522, AP7532, AP7562, AP82XX, AP81XX.

To define a dynamic routing configuration:

- 1 Select the **Configuration > Devices > System Profile** tab from the Web UI.

- Expand the **Network** menu and select **OSPF**.



**Figure 85: Network - OSPF Settings tab**

- 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). 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 <i>enabling</i> Passive Mode on All Interfaces, use the spinner control to select VLANs (by numeric ID) as OSPF <i>non</i> passive interfaces. Multiple VLANs can be added to the list.

Passive Mode	If <i>disabling</i> 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 enable checking VRRP state. If the interface's VRRP state is not Backup, then the interface is published via OSPF.

- 4 Set the following **OSPF Overload Protection** settings:

Number of Routes	Use the spinner controller 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.

- 5 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.

- 6 Refer to the **Route Redistribution** table to set the types of routes that can be used by OSPF.
- 7 Select the **+ Add Row** button to populate the table. Set the **Route Type** used to define the redistributed route. Options include connected, kernel 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 priority is 7000.

- 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.

Area ID	Authentication Type	Type
0.0.0.1	simple-password	non-stub

Type to search in tables Row Count: 1

**Figure 86: Network - Area Settings tab**

- 13 Review existing **Area Settings** configurations using:

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.

- 14 Select **Add** to create a new OSPF configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.

**Figure 87: Network - 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 translatecandidate.
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.

<span>OSPF Settings</span> <span>Area Settings</span> <span><b>Interface Settings</b></span>					
Name	Type	Description	Admin Status	VLAN	IP Address
vlan1	VLAN		Enabled	1	dhcp

Type to search in tables Row Count: 1

Add
Edit
Delete
Replace
Exit

**Figure 88: Network - Interface Settings tab**

18 Review existing **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	A green check mark defines the interface as active and currently enabled with the profile. A red "X" defines the interface as currently disabled and not available for use.
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.

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.

The screenshot shows the 'Virtual Interfaces' configuration window for 'VLAN ID vlan2'. The 'Basic Configuration' section is active, with the 'General' sub-tab selected. The configuration is organized into several sections:

- Properties:** Includes a 'Description' text field, 'Admin Status' with 'Disabled' and 'Enabled' radio buttons, and 'MTU' settings for 'Maximum Transmission Unit (MTU)' (1492) and 'IPv6 MTU' (1500).
- Network Address Translation (NAT):** Includes 'NAT Direction' with 'Inside', 'Outside', and 'None' radio buttons.
- DHCPv6 Client Configuration:** Includes 'Stateless DHCPv6 Client' (checkbox), 'Prefix Delegation Client' (text field), and 'Request DHCPv6 Options' (checkbox).
- Bonjour Gateway:** Includes a 'Discovery Policy' dropdown menu.
- ICMP:** Includes 'ICMPv6 Redirect Messages' (checkbox).
- Address Autoconfiguration:** Includes 'Autoconfiguration' (checkbox).
- Router Advertisement Processing:** Includes 'Accept RA' (checkbox), 'No Default Router' (checkbox), 'No MTU' (checkbox), and 'No Hop Count' (checkbox).

Buttons for 'OK', 'Reset', and 'Exit' are located at the bottom right of the window.

**Figure 89: Network - OSPF Virtual Interfaces - Basic Configuration - General tab**

- 20 If creating a new Virtual Interface, use the **Name** spinner control to define a numeric ID from 1 - 4094.
- 21 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 the Disabled or Enabled radio button to define this interface's current status within the network. When set to Enabled, the Virtual Interface is operational and available. The default value is Disabled.

22 Define 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 to 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 LAN are searched against 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.

23 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.

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. Router advertisements contain prefixes used for link determination, address configuration and maximum hop limits. This setting is enabled by default.



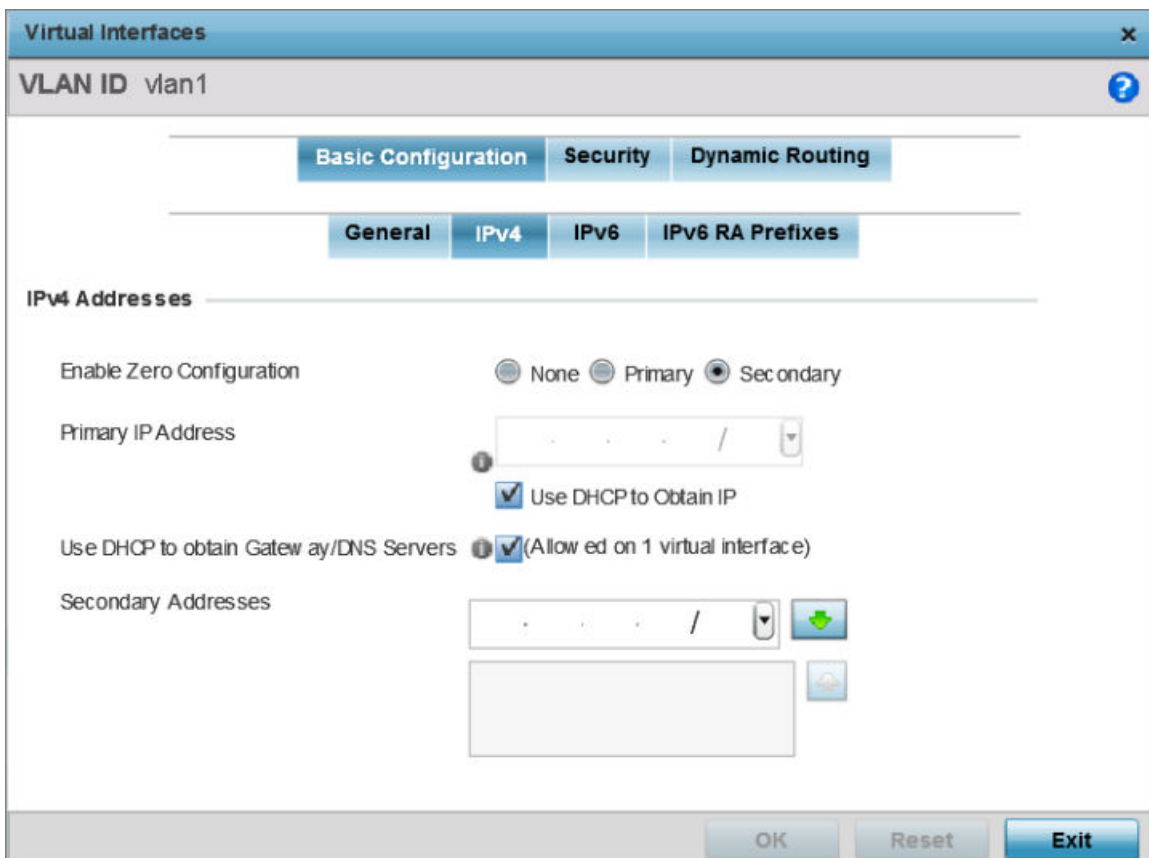
- 27 Set the following **Router Advertisement Processing** settings for the virtual interface. Router advertisements are periodically sent to hosts or sent in response to solicitation requests. The advertisement includes IPv6 prefixes and other subnet and host information.

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 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.

- 28 Use the drop-down menu to define the **Bonjour Gateway Discovery Policy**. Bonjour is Apple's service discovery protocol.
- 29 Select **OK** to save the changes to the basic configuration. Select Reset to revert to the last saved configuration.

30 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 90: Network - OSPF Virtual Interfaces - Basic Configuration screen - IPv4 tab**

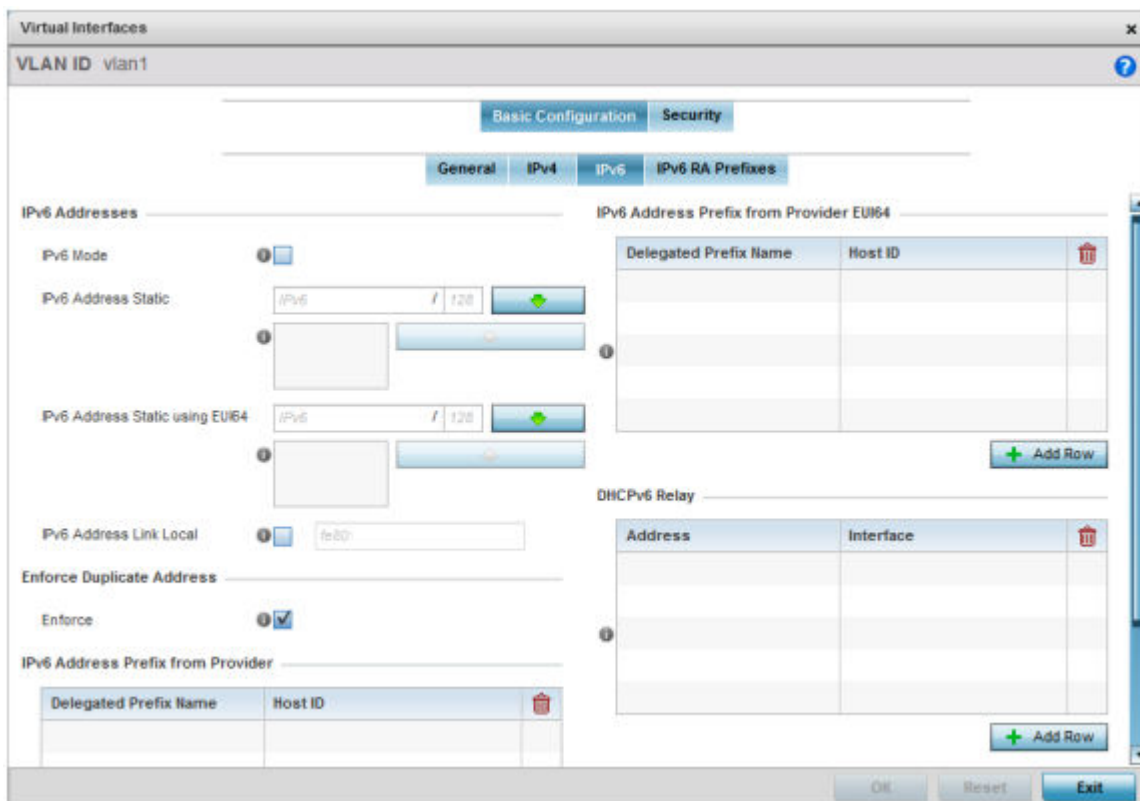
31 Set the following network information from within the **IPv4 Addresses** field:

Enable Zero Configuration	Zero configuration can provide 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.

- 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 91: Network - OSPF Virtual Interfaces - Basic Configuration screen - IPv6 tab**

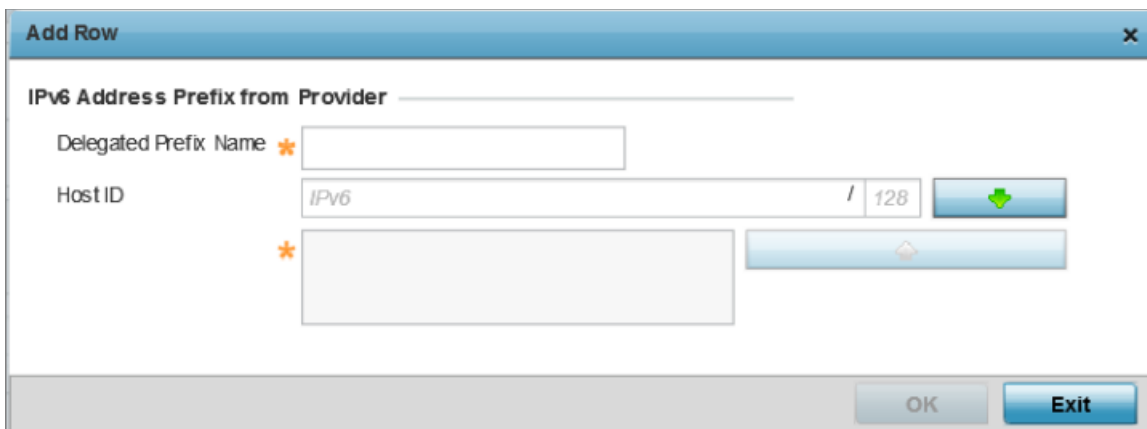
34 Refer to the **IPv6 Addresses** field to define how IPv6 addresses are created and utilized.

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 be 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 be 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 to create IPv6 format prefix shortcuts as supplied by an ISP.

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

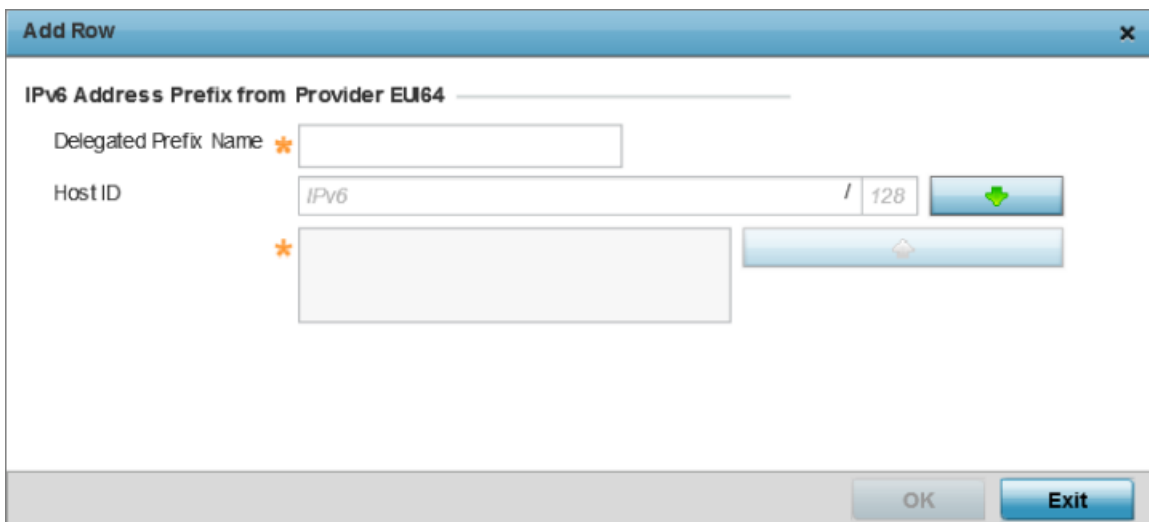


**Figure 92: Network - OSPF Virtual Interfaces - Basic Configuration screen - IPv6 tab - Add Address Prefix from Provider**

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 set an (abbreviated) IP address prefix in EUI64 format.
- 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 93: Network - OSPF 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.

- 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 94: Network - OSPF 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.

- 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.

Virtual Interfaces

VLAN ID vlan2

Basic Configuration Security Dynamic Routing

General IPv4 IPv6 IPv6 RA Prefixes

Router Advertisement Policy

Router Advertisement Policy

IPv6 RA Prefixes

Prefix Type	Prefix or Id	Site Prefix	Valid Lifetime Type	Valid Lifetime Sec	Valid Lifetime Date	Valid Lifetime Time	Preferred Lifetime Type	Preferred Lifetime Sec	Preferred Lifetime Date	Autoconfig	Preferred Lifetime Time	On Link	

+ Add Row

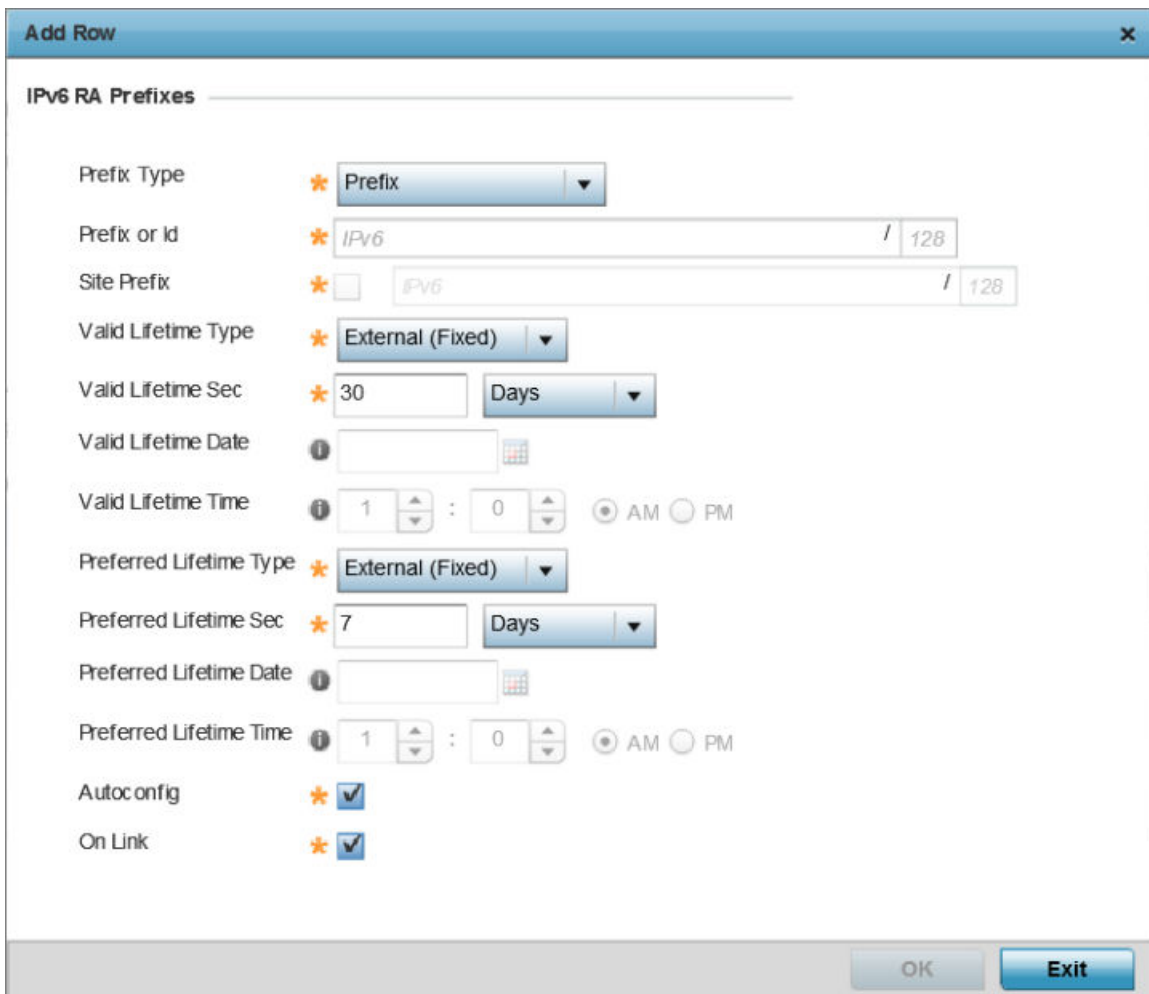
OK Reset Exit

**Figure 95: Network - OSPF 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. For more information on Router Advertisement Policy, see [IPv6 Router Advertisement Policy](#) on page 469.

47 Review the configurations of existing IPv6 advertisement policies. If needed select **+ Add Row** to define the configuration of an additional IPv6 RA prefix.



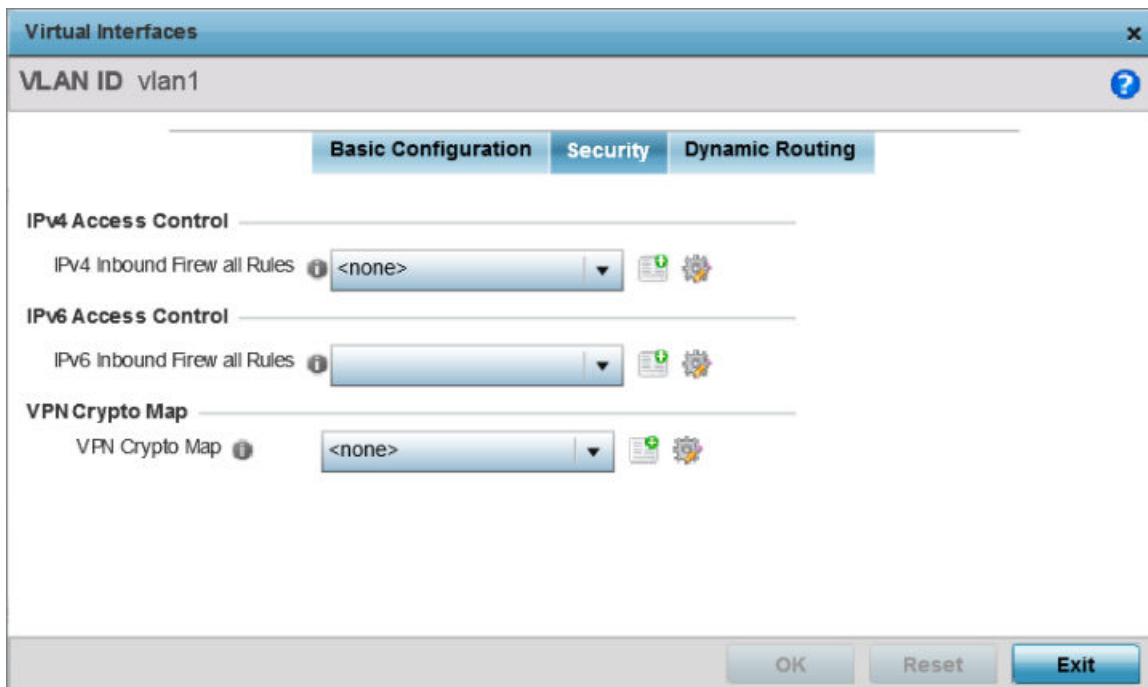
**Figure 96: Network - OSPF Virtual Interfaces - Basic Configuration screen - Add IPv6 RA Prefix**

48 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 decrementing, 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. Use the spinner controls to set the time in hours and minutes. Use the AM PM radio buttons to set the appropriate hour.
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 decrementing, 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. Use the spinner controls to set the time in hours and minutes. Use the AM PM radio buttons to set the appropriate hour.
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.

- 49 Select **OK** to save the changes to the IPv6 RA prefix configuration. Select **Exit** to close the screen without saving the updates.
- 50 Select the **OK** button to save the changes and overrides to the basic configuration. Select **Reset** to revert to the last saved configuration.
- 51 Select the **Security** tab.



**Figure 97: Network - OSPF Virtual Interface - Security tab**

- 52 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. For more information on IPv4 firewall rules, see [Configuring IP Firewall Rules](#) on page 732. "Configuring IP Firewall Rules" on page 724.

- 53 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. For more information on IPv6 firewall rules, see [Configuring IP Firewall Rules](#) on page 732. see "Configuring IP Firewall Rules" on page 724.

- 54 Use the **VPN Crypto Map** drop-down menu to select and apply a VPN crypto map entry to apply to the OSPF dynamic route.

Crypto Map entries are sets of configuration parameters for encrypting packets passing 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.

- 55 Select **OK** to save the changes to the OSPF route security configuration. Select **Reset** to revert to the last saved configuration.

### Forwarding Database 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.

To define a forwarding database configuration:

- 1 Select the **Configuration > Devices > System Profile** tab from the Web UI.
- 2 Expand the **Network** menu and select **Forwarding Database**.

**Aging Time**

Bridge Aging Time  (0,10-1000000 seconds)

**Static Forwarding Table**

MAC Address	VLAN Id	Interface Name	
02-03-04-05-06-07	1	FI123	
0A-0B-0C-0D-0E-0F	4	FI345	

**Figure 98: Network - Forwarding Database screen**

- 3 Define a **Bridge Aging Time** from 0, 10-1,000,000 seconds.  
The aging time defines the length of time an entry will remain in the bridge's forwarding table before it is deleted due to lack of activity. If an entry replenishes 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.
- 4 Use the **+Add Row** button to create a new row within the **Static Forwarding Table**.
- 5 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).
- 6 Define the target **VLAN ID** if the destination MAC is on a different network segment.
- 7 Provide an **Interface Name** used as the target destination interface for the target MAC address.
- 8 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

### Bridge VLAN Configuration

A *Virtual LAN* (VLAN) is separately administrated virtual network within the same physical network. VLANs are broadcast domains defined within switches to allow control of broadcast, multicast, unicast, and unknown unicast within a Layer 2 device.

For example, say several computers are used in conference room X and some in conference Y. The systems in conference room X can communicate with one another, but not with the systems in conference room Y. The creation of a VLAN enables the systems in conference rooms X and Y to communicate with one another even though they are on separate physical subnets. The systems in conference rooms X and Y are managed by the same single device, but ignore the systems that aren't using same VLAN ID.

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). VLANs are useful to set separate networks to isolate some computers from others, without actually having to have separate cabling and Ethernet switches. Another common use is to put specialized devices like VoIP Phones on a separate network for easier configuration, administration, security, or quality of service.

To define a Bridge VLAN configuration:

- 1 Select the **Configuration > Devices > System Profile** tab from the Web UI.

- 2 Expand the **Network** menu and select **Bridge VLAN**.

VLAN	Description	Edge VLAN Mode	Trust ARP Responses	Trust DHCP Responses	IPv6 Firewall	DHCPv6 Trust	RA Guard
1	Test Bridge VLAN	✓	✗	✓	✓	✓	✓
Type to search in tables			Row Count: 1				
		Add	Edit	Delete	Replace	Exit	

**Figure 99: Network - Bridge VLAN screen**

VLAN	Lists the numerical identifier defined for the Bridge VLAN when it was initially created. The available range is from 1 - 4095. 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. 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 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 Response	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.

- 3 Select **Add** to define a new Bridge VLAN configuration, **Edit** to modify the configuration of an existing Bridge VLAN configuration or **Delete** to remove a VLAN configuration.

The screenshot displays the 'Bridge VLAN' configuration window for 'VLAN 1'. The 'General' tab is active, showing the following settings:

- Description:** Test Bridge VLAN
- Per VLAN Firewall:**
- URL Filter:** (Dropdown menu)
- Application Policy:** (Dropdown menu)
- Extended VLAN Tunnel:**
  - Bridging Mode:** Automatic
  - IP Outbound Tunnel ACL:** <none>
  - IPv6 Outbound Tunnel ACL:** (Dropdown menu)
  - MAC Outbound Tunnel ACL:** <none>
  - Tunnel Over Level 2:**
- Tunnel Rate Limit:** A table with columns: Mint Link Level, Rate, Max Burst Size, Background, Best-Effort, Video, Voice, and a delete icon. An 'Add Row' button is located below the table.
- Layer 2 Firewall:**
  - Trust ARP Responses:**
  - Trust DHCP Responses:**

Buttons at the bottom include 'OK', 'Reset', and 'Exit'.

**Figure 100: Network - Bridge VLAN - General Configuration screen**

- 4 If adding a new Bridge VLAN configuration, use the spinner control to define a **VLAN ID** from 1 - 4095. This value must be defined and saved before the **General** tab can become enabled and the remainder of the settings defined.
- 5 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.

- 6 Select the **Per VLAN Firewall** option to enable firewall on this interface.

Firewalls, generally, are configured for all interfaces on a device. When configured, firewalls generate flow tables that store information on the traffic allowed to traverse through the firewall. These flow tables occupy a large portion of the limited memory that could be used for other critical purposes. With the per VLAN firewall feature enabled on an interface, flow tables are only generated for that interface. Flow tables are not generated for those interfaces where this feature is not enabled. This frees up memory which can be used for other purposes. Firewalls can be switched off for those interfaces which are known to carry trusted traffic and only enabled on the interfaces that can provide a vector for an attack on the network.

- 7 Set or override the following **Web 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.
------------	---

- 8 Set or override the following **Extended VLAN Tunnel** parameters:

Bridging Mode	Specify one of the following bridging modes for the VLAN. <ul style="list-style-type: none"> <li>• <i>Automatic</i>: Select automatic to let the controller, service platform or access point determine the best bridging mode for the VLAN.</li> <li>• <i>Local</i>: Select Local to use local bridging mode for bridging traffic on the VLAN.</li> <li>• <i>Tunnel</i>: Select Tunnel to use a shared tunnel for bridging traffic on the VLAN.</li> <li>• <i>isolated-tunnel</i>: Select isolated-tunnel to use a dedicated tunnel for bridging VLAN traffic.</li> </ul>
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 <i>Create</i> 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 <i>Create</i> 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.
IPv6 Outbound Tunnel ACL	Select an IPv6 Outbound Tunnel ACL for outbound traffic from the drop-down menu. If an appropriate outbound IPv6 ACL is not available, select the <i>Create</i> button.

- 9 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.
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 background traffic. Set a value from 1 - 100%. The default is 50%.



Best Effort	Set the random early detection threshold in % for best-effort traffic. Set a value from 1 - 100%. The default is 50%.
Video	Set the random early detection threshold in % for video traffic. Set a value from 1 - 100%. The default is 25%.
Voice	Set the random early detection threshold in % for voice traffic. Set a value from 1 - 100%. The default is 25%.

- 10 Define 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.
Edge VLAN Mode	Select this option to enable edge VLAN mode. When selected, the edge controller'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.

- 11 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.

- 12 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 777.

- 13 Select the IGMP Snooping tab.

**Bridge VLAN** x

VLAN 1 ?

General IGMP Snooping MLD Snooping

**General**

Enable IGMP Snooping

Forward Unknown Multicast Packets

Enable Fast leave processing

Last Member Query Count  (1 to 7)

**Multicast Router**

Interface Names

- ge1
- ge2
- radio1
- radio2

Multicast Router Learn Mode

**IGMP Querier**

Enable IGMP Querier

Source IP Address

IGMP Version  (1 to 3)

Maximum Response Time  (1 to 25 seconds)

Other Querier Timer Expiry  (60 to 300 seconds)

OK Reset Exit

**Figure 101: Network - Bridge VLAN - IGMP Snooping screen**

- 14 Define the following IGMP **General** parameters.

Enable IGMP Snooping	Select this option to enable IGMP snooping. If disabled, snooping on this Bridge VLAN is disabled. This feature is enabled by default. If disabled, the settings under bridge configuration are overridden.
Forward Unknown Unicast Packets	Select this option to enable forwarding of multicast packets from unregistered multicast groups. If disabled, the unknown multicast forward feature is also disabled for this Bridge VLAN. 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 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 setting is 2.

15 Define the following **Multicast Router** settings:

Interface Names	Select the interface used for IGMP snooping over a multicast router. Multiple interfaces can be selected.
Multicast Router Learn Mode	Select static or pim-dvmrp as the mode used to determine client multicast traffic levels on specific routes.

16 Set the following **IGMP Querier** parameters for the Bridge VLAN configuration:

Enable IGMP Snooping	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 <i>Seconds</i> (60 - 300) or <i>Minutes</i> (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute.

17 Select the MLD Snooping tab.

The screenshot shows the 'Bridge VLAN' configuration window for 'VLAN 1'. The 'MLD Snooping' tab is selected. The configuration is organized into three sections: General, Multicast Router, and MLD Querier.

- General:**
  - Enable MLD Snooping:
  - Forward Unknown Multicast Packets:
- Multicast Router:**
  - Interface Names: A list box containing 'ge1', 'ge2', 'radio1', and 'radio2'. 'ge2' is selected.
  - Multicast Router Learn Mode: A dropdown menu set to 'pim-dvmrp'.
- MLD Querier:**
  - Enable MLD Querier:
  - MLD Version:  1 (range: 1 to 2)
  - Maximum Response Time:  1 (range: 1 to 25,000 milliseconds)
  - Other Querier Timer Expiry:  60 (range: 60 to 300 seconds)

At the bottom of the window are three buttons: 'OK', 'Reset', and 'Exit'.

Figure 102: Network Bridge VLAN screen, MLD Snooping tab

- 18 Define the following **General** MLD snooping parameters for the Bridge VLAN configuration:

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 Packets	Use this option to either enable or disable IPv6 unknown multicast forwarding. This setting is enabled by default.

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.

- 19 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.

- 20 Set the following **MLD Querier** parameters for the profile's Bridge VLAN configuration:

Enable MLD Querier	Select this 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

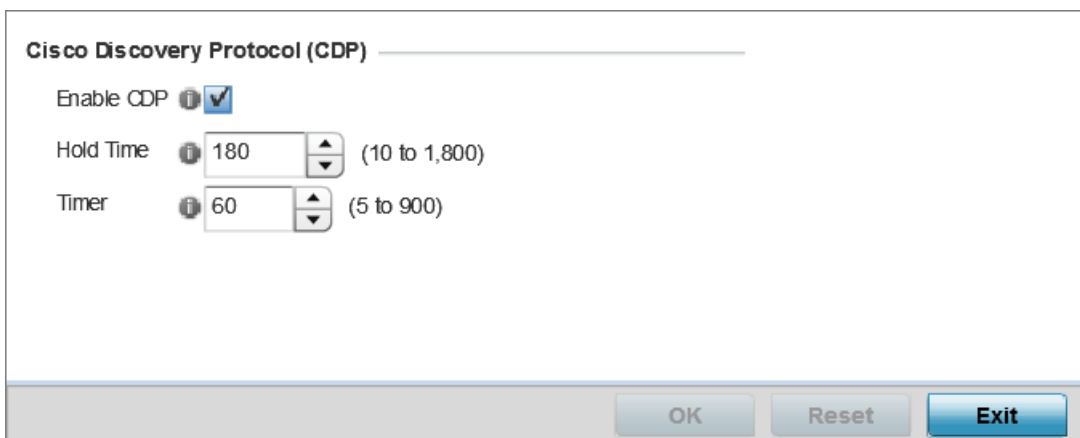
- 21 Select the **OK** button located at the bottom right of the screen to save the changes. Select **Reset** to revert to the last saved configuration.

### Cisco Discovery Protocol Configuration

The Cisco Discovery Protocol (CDP) is a proprietary Data Link Layer protocol implemented in Cisco networking equipment. It's primarily used to obtain IP addresses of neighboring devices and discover their platform information. CDP is also used to obtain information about the interfaces the access point uses. CDP runs only over the data link layer enabling two systems that support different network-layer protocols to learn about each other.

To define the profile's CDP configuration:

- 1 Select the **Configuration > Devices > System Profile** tab from the Web UI.
- 2 Expand the **Network** menu and select **Cisco Discovery Protocol**.



**Figure 103: Network - Cisco Discovery Protocol (CDP) screen**

- 3 Enable/disable CDP and set the following settings:

Enable CDP	Select this option to enable CDP and allow for network address discovery of Cisco supported devices and operating system version. This setting is enabled by default.
Hold Time	Set a hold time (in seconds) for the transmission of CDP packets. Set a value from 10 - 1,800. The default setting is 1,800 seconds.
Timer	Use the spinner control to set the interval for CDP packet transmissions. The default setting is 60 seconds.

- 4 Select the **OK** button located at the bottom right of the screen to save the changes to the CDP configuration. Select **Reset** to revert to the last saved configuration.

### Link Layer Discovery Protocol Configuration

The Link Layer Discovery Protocol (LLDP) provides a standard way for a controller or access point to advertise information about themselves to networked neighbors and store information they discover from their peers.

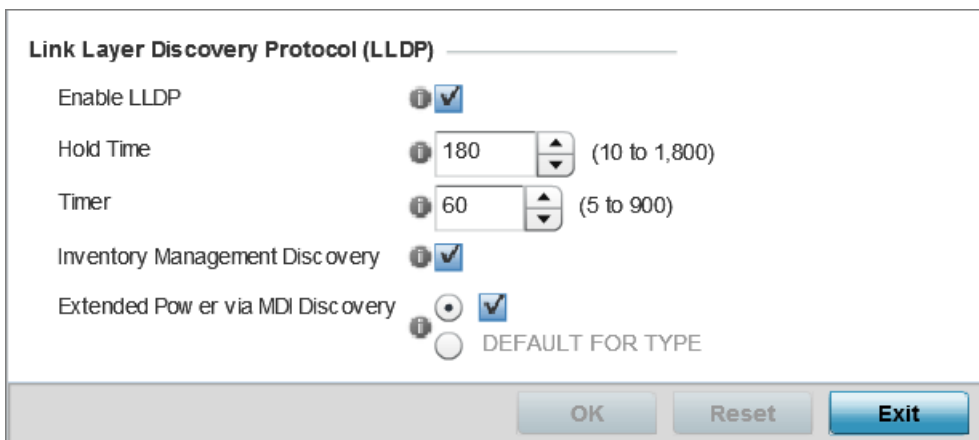
LLDP is neighbor discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise information about them to peer devices on the same physical LAN and store information about the network. It allows a device to learn higher layer management and connection endpoint information from adjacent devices.

Using LLDP, an access point is able to advertise its own identification, capabilities and media-specific configuration information and learn the same information from connected peer devices.

LLDP information is sent in an Ethernet frame at a fixed interval. Each frame contains one Link Layer Discovery Protocol Data Unit (LLDP PDU). A single LLDP PDU is transmitted in a single 802.3 Ethernet frame.

To set the LLDP configuration:

- 1 Select the **Configuration > Devices > System Profile** tab from the Web UI.
- 2 Expand the **Network** menu and select **Link Layer Discovery Protocol**.



**Figure 104: Network - Link Layer Discovery Protocol (LLDP) screen**

- 3 Set the following LLDP parameters for the profile configuration:

Enable LLDP	Select this option to enable LLDP on the access point. LLDP is enabled by default. When enabled, an access point advertises its identity, capabilities and configuration information to connected peers and learns the same from them.
Hold Time	Use the spinner control to set the hold time (in seconds) for transmitted LLDP PDUs. Set a value from 10 - 1,800. The default hold time is 180 seconds.

Timer	Set the interval used to transmit LLDP PDUs. Define an interval from 5 - 900 seconds. The default setting is 60 seconds.
Inventory Management Discovery	Select this option to include LLDP-MED inventory management discovery TLV in LLDP PDUs. This setting is enabled by default.
Extended Power via MDI Discovery	Select this option to include LLDP-MED extended power via MDI discovery TLV in LLDP PDUs. This setting is disabled by default.

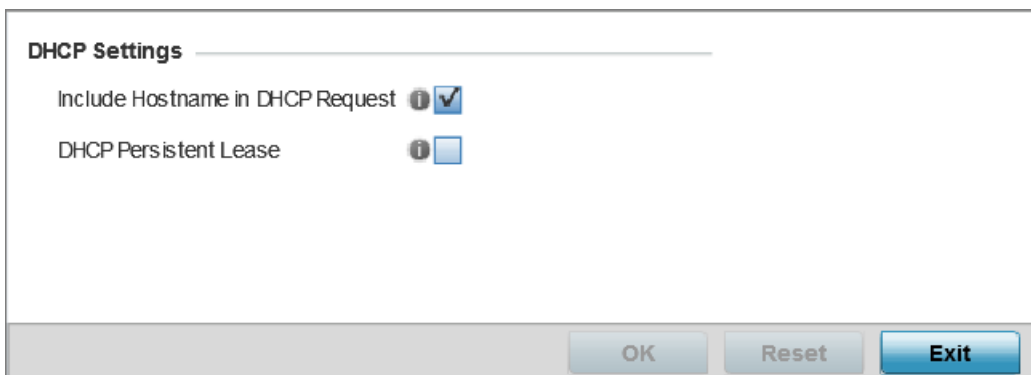
- 4 Select the **OK** button to save the changes to the LLDP configuration. Select **Reset** to revert to the last saved configuration.

### Miscellaneous 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 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 hostnames in DHCP requests:

- 1 Select the **Configuration > Devices > System Profile** tab from the Web UI.
- 2 Expand the **Network** menu and select **Miscellaneous**.



**Figure 105: Network - Miscellaneous screen**

- 3 Select the **Include Hostname in DHCP Request** option to include a hostname in a DHCP lease for a requesting device. This feature is enabled by default.
- 4 Select the **DHCP Persistent Lease** option to retain the lease that was last used by the access point if the access point's DHCP server resource were to become unavailable. This feature is enabled by default.
- 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.

### 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 **Configuration > Devices > System Profile > Network > Alias**. These aliases are available for use to a specific group of wireless controllers Device Configuration WiNG 5.9.0 Access Point System Reference Guide 208 or access points. Alias values defined in this profile override alias values defined within global aliases.
- RF Domain aliases are defined from **Configuration > Devices > RF Domain > Alias** screen. These 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 **Configuration > Devices > Device Overrides > Network > Alias** screen. Device alias are utilized by a single device only. Device alias values override alias values defined in a global alias, profiles alias or RF Domain alias configuration.

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 works 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.

Alias can be classified as:

- [Network Basic Alias](#) on page 228
- [Network Group Alias](#) on page 231
- [Network Service Alias](#) on page 233

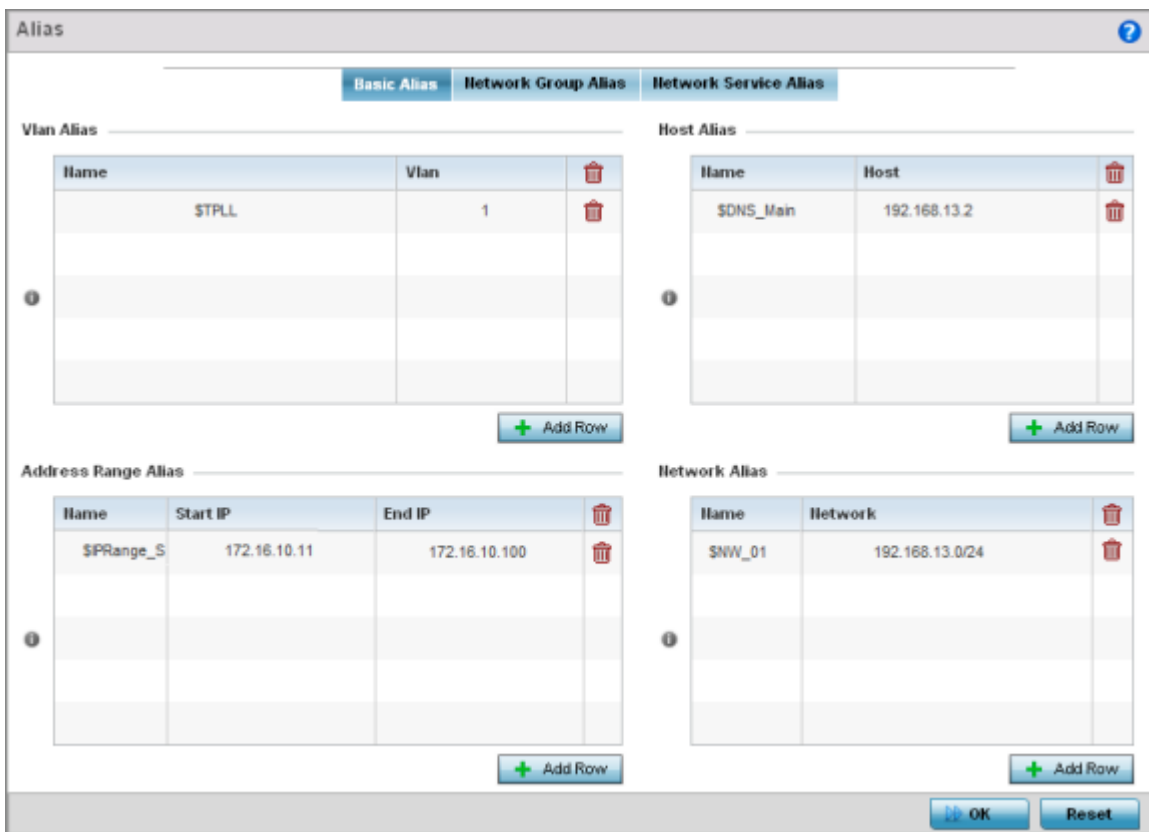
## Network Basic Alias

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 > System Profiles > Network > Alias**.

The **Basic Alias** screen displays.



**Figure 106: Network - Basic Alias Screen**

- 2 Select **+ Add Row** to define **VLAN Alias** settings:
- 3 Use the **VLAN Alias** field to create unique aliases for VLANs that can be used at different deployments. For example, if a named VLAN is defined as 10 for the central network, and the VLAN is set at 26 at a remote location, the VLAN can be overridden at the deployment location with an alias. At the remote deployment location, the network is functional with a VLAN ID of 26 but utilizes the name defined at the centrally managed network. A new VLAN need not be created specifically for the remote deployment.

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.

A VLAN alias is used to replace VLANs in the following locations:

- Bridge VLAN
- IP Firewall Rules
- L2TPv3
- Switchport
- Wireless LANs



- 4 Select **+ Add Row** to define **Address Range Alias** settings:
- 5 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 a ending IP address used with a range of addresses utilized with the address range alias.

An address range alias can be used to replace an IP address range in IP firewall rules.

- 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.

A host alias can be used to replace hostnames in the following locations:

- IP Firewall Rules
- DHCP

- 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.

A network alias can be used to replace network declarations in the following locations:

- IP Firewall Rules

- DHCP

8 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 string value to use in the alias.

A string alias can be used to replace domain name strings in DHCP.

9 Select **OK** when completed to update the basic alias rules. Select **Reset** to revert the screen back to its last saved configuration.

#### 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.

A network group alias can be used in IP firewall rules to substitute hosts, subnets and IP address ranges.

To edit or delete a network alias configuration:

1 Select **Configuration > System Profiles > Network > Alias**.

The **Basic Alias** screen displays.

2 Select the Network Group Alias tab.

Basic Alias <b>Network Group Alias</b> Network Service Alias		
Name	Host	Network
\$test		1.2.3.0/24,2.3.4.0/24

Type to search in tables  Row Count: 1

**Figure 107: Network Alias - 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.

**Figure 108: Network Alias - Network Group Alias Add Screen**

If you are adding a new network alias rule, provide a name up to 32 characters. The network group alias name always starts with a dollar sign (\$).

- 4 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.

- 5 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 alias range entry to edit it.
- 6 Select **OK** when completed to update the network group alias settings.  
Select **Reset** to revert the screen to its last saved configuration.

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 two source port ranges and up to two destination port ranges can be configured. A maximum of four 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.

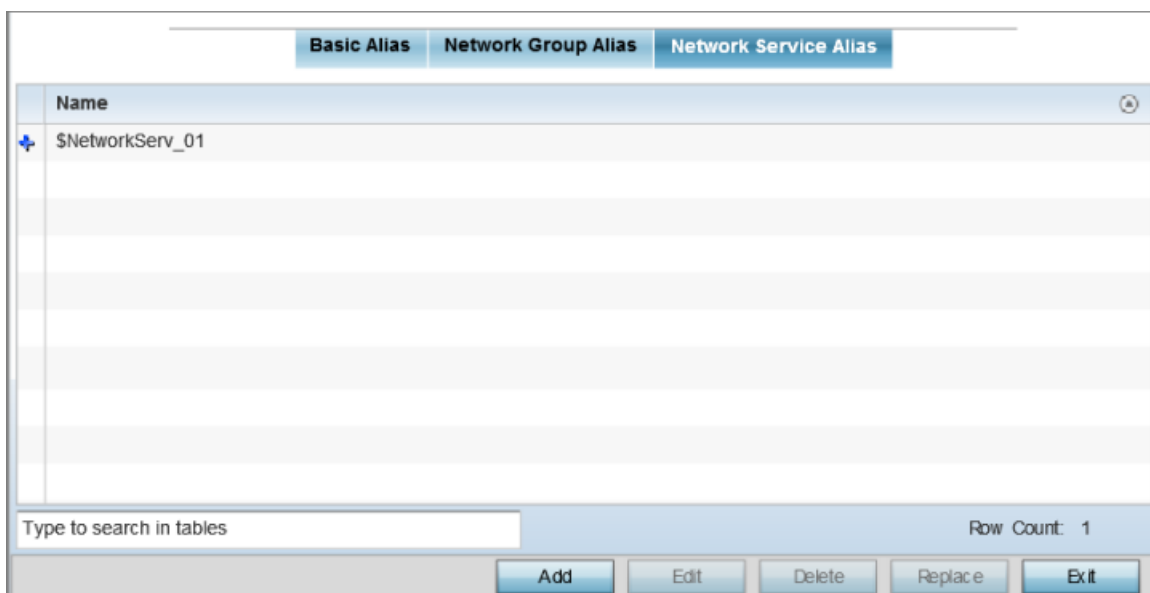
A network service alias can be used to substitute protocols and ports in IP firewall rules.

To edit or delete a network service alias configuration:

- 1 Select **Configuration > System Profiles > Network > Alias**.

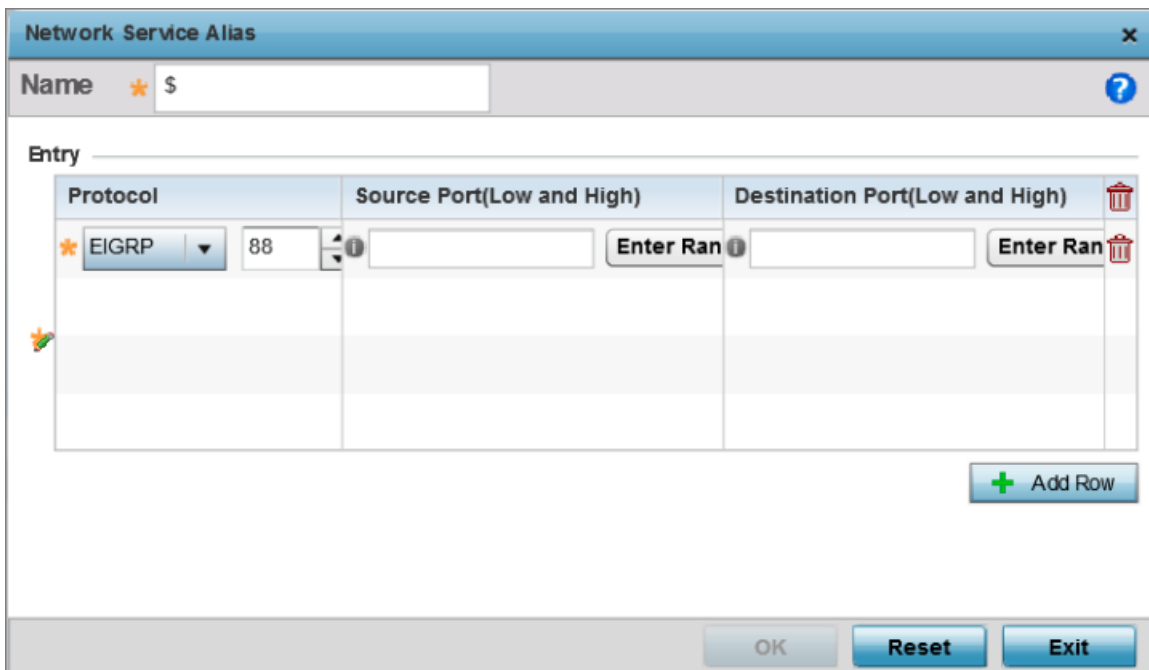
The **Basic Alias** screen displays.

- 2 Select the **Network Service Alias** tab.



**Figure 109: Network Alias - Network Service Alias Screen**

- 3 Select **Add** to create a new network service alias.  
 Select an existing network service alias and click **Edit** to modify it. Select **Delete** to remove an existing network service alias from those available in the list.  
  
 Use **Copy** to create a copy of the selected policy and modify it for further use. Use **Rename** to rename the selected policy.



**Figure 110: Network Alias - Network Service Alias Add screen**

- 4 If you are adding a new **Network Service Alias**, give it a **Name** up to 32 characters to distinguish this alias configuration from others with similar attributes.



**Note**  
 The Network Service Alias Name always starts with a dollar sign (\$).

- 5 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.

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 <b>other</b> 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 relevant only if the protocol is tcp or udp. Specify the source ports for this protocol entry. A range of ports can be specified. Select the <b>Enter Ranges</b> 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 relevant only if the protocol is tcp or udp. Specify the destination ports for this protocol entry. A range of ports can be specified. Select the <b>Enter Ranges</b> button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

- 6 Select **OK** when completed to update the network service alias rules. Select **Reset** to revert the screen back to its last saved configuration.



## IPv6 Neighbor 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 **Devices > Device Overrides**
- 2 Select a target device from the device browser in the lower, left-hand side of the UI.
- 3 Select **Network** to expand it and display its sub menus.
- 4 Select **IPv6 Neighbor**.

IPv6 Address	MAC Address	Switch VLAN Interface	Device Type	

**Figure 111: IPv6 Neighbor screen**

- 5 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.
- 6 Select **+ Add Row** to define the configuration of **IPv6 Neighbor Discovery** configurations. A maximum of 256 neighbor entries can be defined.

<b>IPv6 Address</b>	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.
<b>MAC Address</b>	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.
<b>Switch VLAN Interface</b>	Use the spinner control to set the virtual interface (from 1 - 4094) used for neighbor advertisements and solicitation messages.
<b>Device Type</b>	Specify the device type for this neighbor solicitation is for. Options include Host, Router and DHCP Server. The default setting is Host.

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

### Overriding a Profile's Security Configuration

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** portion of the UI to the **Configuration > Security** portion 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. When this is done, however, 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:

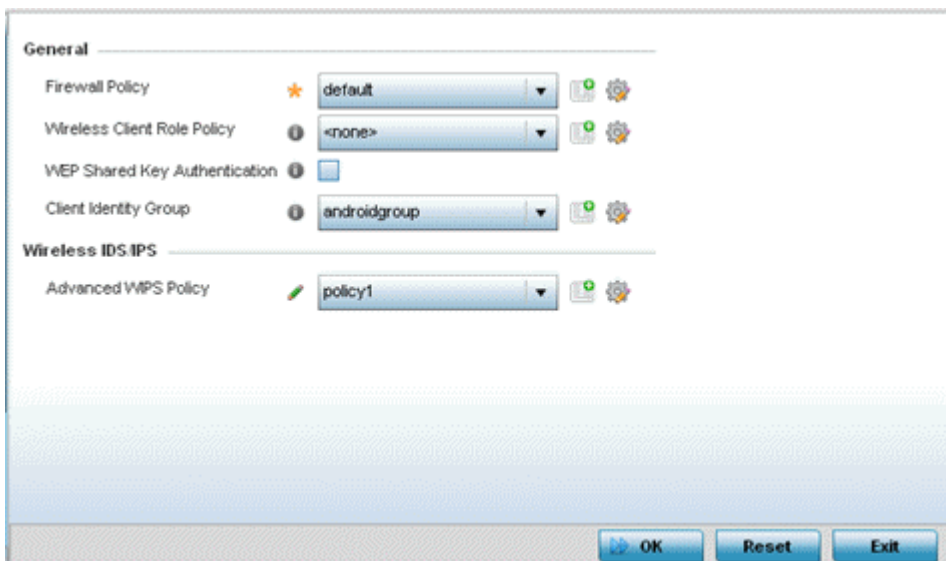
- [Overriding General Security Settings](#) on page 237
- [Overriding a Certificate Revocation List \(CRL\) Configuration](#) on page 239
- [Overriding RADIUS Trustpoint Configuration](#) on page 240
- [Overriding VPN Configuration](#) on page 242
- [Overriding Auto IPsec Tunnel Settings](#) on page 250
- [Overriding NAT Configuration](#) on page 253
- [Overriding a Bridge NAT Configuration](#) on page 261
- [Overriding Application Visibility Settings](#) on page 264

### Overriding General Security Settings

A profile can make use of 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 for best meeting the data protection requirements of the profile it 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 **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- 3 Select **Profile Overrides > Security**.
- 4 Select **Settings**.



**Figure 112: Device Overrides - Security 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 **Clear Overrides**. This removes all overrides from the device.

- 5 Refer to the **General** field to assign or override the following:

Firewall Policy	Select an existing Firewall policy to use as an additional security mechanism with a 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 that both block and permit data traffic within the network. If an existing firewall policy does not meet your requirements, click the <b>Create</b> icon to create a new firewall policy that can be applied to this profile. An existing policy can also be selected and overridden as needed using the <b>Edit</b> icon.
Wireless Client Role Policy	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, click the <b>Create</b> icon to create a new firewall policy that can be applied to this profile. An existing policy can also be selected and overridden as needed using the <b>Edit</b> 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 uses 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.

- 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.

- Click **OK** to save the changes or overrides.

Click **Reset** to revert to the last saved configuration.

### Overriding a Certificate Revocation List (CRL) 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) has improperly issued a certificate, or if a private key is compromised. The most common reason for revocation is that the user is no longer in sole possession of the private key.

To define a certificate revocation configuration or override:

- Select **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- Select **Profile Overrides > Security**.

4 Select **Certificate Revocation**.

Trustpoint Name	URL	Hours	
★ trustpoint1	www.trutpoint.com	1	

+ Add Row

OK Reset Exit

**Figure 113: Device Overrides - Certificate Revocation 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 **Clear Overrides**. This removes all overrides from the device.

- 5 Click **+ Add Row** to add a column in 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 user defined period. If, for instance, a private key was found and nobody had access to it, its status could be reinstated.

  - a In the **Trustpoint Name** field, provide the name of the trustpoint in question.
 

The name cannot exceed 32 characters.
  - b In the **URL** field, enter the third-party resource ensuring the trustpoint's legitimacy.
  - 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.
- 6 Click **OK** to save the changes or overrides to the **Certificate Revocation** screen.
 

Click **Reset** to revert to the last saved configuration.

### Overriding RADIUS Trustpoint 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 **Configuration > Devices** from the web UI.

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

- 2 Select a target device in the lower left-hand side of the UI.

You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.

- 3 Select **Profile Overrides > Security**.
- 4 Select **Trustpoints**.

**RADIUS Security**

RADIUS Certificate Authority Pending  Stored  default-trustpoint Launch Manager

RADIUS Server Certificate Pending  Stored  default-trustpoint Launch Manager

**HTTPS Trustpoints**

HTTPS Trustpoint Pending  Stored  default-trustpoint Launch Manager

OK Reset Exit

**Figure 114: Profile Overrides - Trustpoints Screen**

- 5 Set the following RADIUS Security certificate settings:

RADIUS Certificate Authority	Either use the <b>default-trustpoint</b> or click <b>Stored</b> to enable a drop-down menu where an existing certificate can be used. To make use of an existing certificate, click <b>Launch Manager</b> .
RADIUS Server Certificate	Either use the <b>default-trustpoint</b> or click <b>Stored</b> to enable a drop-down menu where an existing certificate/trustpoint can be used. To make use of an existing trustpoint, click <b>Launch Manager</b> .

- 6 Set the following **HTTPS Trustpoints** certificate settings:

HTTPS Trustpoint	Either use the <b>default-trustpoint</b> or click <b>Stored</b> to enable a drop-down menu where an existing certificate/trustpoint can be used. To use an existing certificate for this device, click <b>Launch Manager</b> . For more information, see <a href="#">Certificate Management</a> on page 917.
------------------	--

- 7 Click **OK** to save the changes made in the **RADIUS Trustpoints** screen.

Click **Reset** to revert to the last saved configuration.

### Overriding VPN 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 tunneled 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 (SAs) between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunneled 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.

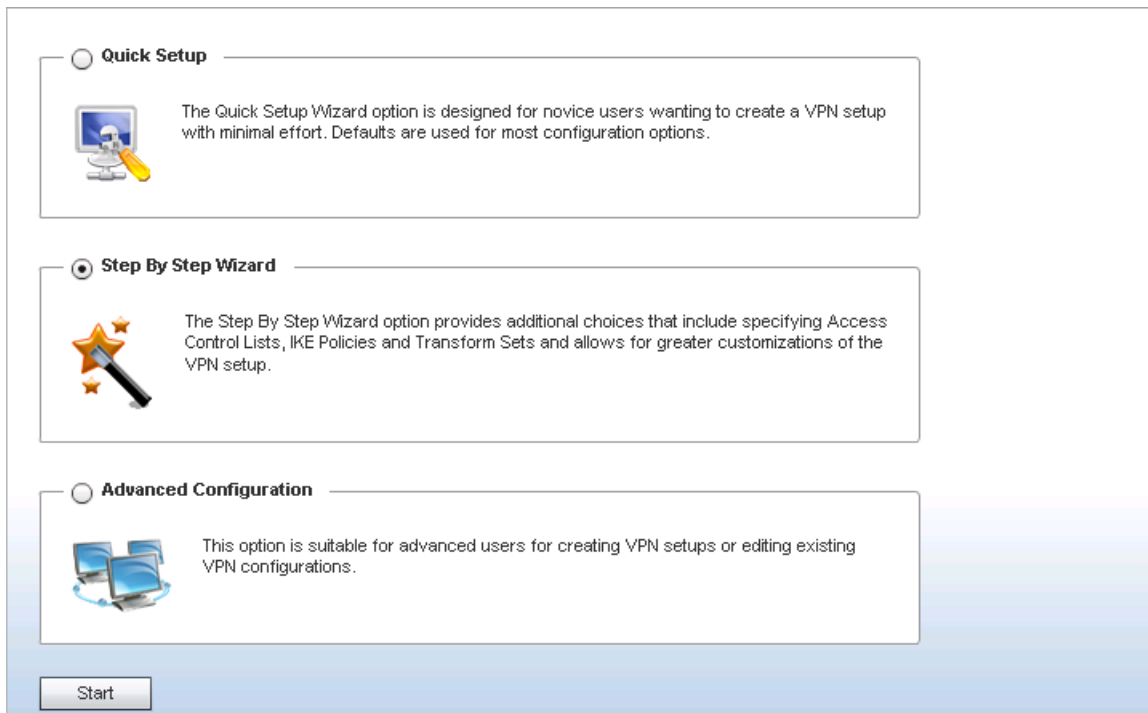
Internet Key Exchange (IKE) protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs, and enables secure communications without time consuming manual pre-configuration.

To define a profile's VPN settings:

- 1 Select **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- 3 Select **Profile Overrides > Security**.

#### 4 Select VPN.

The VPN configuration can be overridden either by using a built-in wizard or by manually configuring the required parameters. This section describes how to use the inbuilt wizards to override the VPN parameters. The user interface provides two wizards that provide either basic or more thorough administration.



**Figure 115: VPN Setup Wizard**

- **Quick Setup Wizard**: Use this 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 this wizard to create a VPN tunnel using settings updated from their minimum default values. This wizard is designed for intermediate users who require the ability to customize some of the parameters.
- **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 [Profile Security Configuration](#) on page 618.

#### Overriding VPN Configuration: Quick Setup Wizard

The Quick Setup Wizard creates a VPN connection with minimum manual configuration. Default values are retained for most of the parameters.

- 1 In the **Security Configuration Wizard** screen, click **Quick Setup**.

**Figure 116: VPN Quick Setup Wizard**

- 2 Provide the following information to configure a VPN tunnel:

Tunnel Name	Provide a name for the tunnel. The name should identify the tunnel uniquely.
Tunnel Type	Configure the tunnel type as one of the following: <ul style="list-style-type: none"> <li>• Site-to-Site – The tunnel provides a secured connection between two sites. This is the default setting.</li> <li>• Remote Access – The tunnel provides access to a network to remote devices.</li> </ul>
Select Interface	Configure the interface to use for creating the tunnel. The following options are available: <ul style="list-style-type: none"> <li>• VLAN – Configure the tunnel over a Virtual LAN interface. Use the spinner to configure the VLAN number.</li> <li>• WWAN – Configure the tunnel over the WAN interface.</li> <li>• PPPoE – Configure the tunnel over the PPPoE interface.</li> </ul>

Traffic Selector (ACL)	Configure ACLs that manage the traffic passing through the VPN tunnel. The following options are available: <ul style="list-style-type: none"> <li>• Source – Provide the source network along with its mask.</li> <li>• Destination – Provide the destination network along with its mask.</li> </ul>
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 on opposite ends of the VPN tunnel connection. The following can be configured: <ul style="list-style-type: none"> <li>• Certificate – Use a certificate to authenticate. This is the default setting.</li> <li>• Pre-Shared Key – Use a pre-shared key to authenticate. Enter the secret key in the space provided.</li> </ul>
Local Identity	Configure the local identity used with this peer configuration for an IKE exchange with the target VPN IPsec peer. Options include <b>IP Address</b> , <b>Distinguished Name</b> , <b>FQDN</b> , <b>email</b> , and <b>string</b> . The default setting is <b>string</b> .
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 <b>IP Address</b> , <b>Distinguished Name</b> , <b>FQDN</b> , <b>email</b> , and <b>string</b> . The default setting is <b>string</b> .
IKE Policy	Configure the Internet Key Exchange (IKE) policy to use. IKE is used to exchange authentication keys. Select from one of the following: <ul style="list-style-type: none"> <li>• All – Use any IKE policy. This is the default setting.</li> <li>• IKE1 – Use IKE 1 only.</li> <li>• IKE2 – Use IKE 2 only.</li> </ul>
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 Click **Save** to save the VPN tunnel configuration.

To exit without saving, click **Cancel**.

#### Overriding VPN Configuration: 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 In the **Security Configuration Wizard** screen, click **Step-By-Step Wizard**.

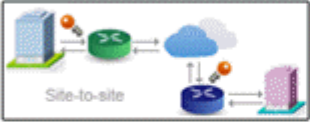

2 Click **Start**

VPN Basic Configuration Step 1/4

The Quick Setup Wizard option is designed for novice users wanting to create a VPN setup with minimal effort. Defaults are used for most configuration options.

Tunnel Name \* tunnel1 ?

**Tunnel Type**


Site-to-site
 Site-to-Site
 
Remote Access
 Remote Access

**Interface**

Select Interface \*  VLAN 1  WWAN  PPPoE ?

**Traffic Selector (ACL)**

Source \* . . . / Destination \* . . . /  ?

Source	Destination

**Figure 117: VPN Step-By-Step Wizard - Step 1**

3 Set the following VPN values in the **Step 1** screen.

Tunnel Name	Provide a name for the tunnel.
Tunnel Type	Select the tunnel type being created. Two types of tunnels can be created. Use <b>Site to Site</b> to create a tunnel between two remote sites. Use <b>Remote Access</b> to create a tunnel between a user device and a network. <b>Site to Site</b> is the default setting.
Interface	Configure the interface to use for creating the tunnel - either Virtual LAN ( <b>VLAN</b> ), <b>WWAN</b> , or <b>PPPoE</b> depending on the interfaces available on the device.
Traffic Selector (ACL)	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 <b>Add Rule</b> to add the rule into the ACL.

- 4 Click **Next**.

Remote Configuration Site Step 24

**Peer Definition**

Peer \*  IP Address  Host Name  
 .  .  ?

Authentication \*  Certificate  Pre-Shared Key

Local Identity  IP Address  FQDN  Email  
 .  .  ?

Remote Identity  IP Address  FQDN  Email  
 .  .  ?

IKE Policy \*  Use Default  Create new Policy  
ikev1-default ▼

Add Peer

**Peer(s)**

Peer	Authentication	Local ID	IKE Policy

Next Close

**Figure 118: VPN Step-By-Step Wizard - Step 2**

- 5 Set the following VPN values in the **Step 2** screen.

If any of the required values in the **Step 1** screen are not set properly, the **Step 2** screen will not display until they are properly set.

Peer	Select the type of peer for this device when forming a tunnel. Peer information can be either an <b>IP Address</b> (default value) or <b>Host Name</b> . Provide the IP address or the host name of the peer device.
Authentication	Configure how devices authenticate on opposite ends of the tunnel connection. The following can be configured: <ul style="list-style-type: none"> <li>• Certificate – The devices use a certificate to authenticate. This is the default setting.</li> <li>• Pre-Shared Key – The devices use a pre-shared key to authenticate.</li> </ul>
Local Identity	Configure the local identity for the VPN tunnel. <ul style="list-style-type: none"> <li>• P Address – The local identity is an IP address. This is the default setting.</li> <li>• FQDN – The local identity is a Fully Qualified Domain Name (FQDN).</li> <li>• Email – The local identity is an E-mail address.</li> </ul>

Remote Identity	Configure the remote identity for the VPN tunnel. <ul style="list-style-type: none"> <li>• P Address – The remote identity is an IP address. This is the default setting.</li> <li>• FQDN – The remote identity is a Fully Qualified Domain Name (FQDN).</li> <li>• Email – The remote identity is an E-mail address.</li> </ul>
IKE Policy	Configure the Internet Key Exchange (IKE) policy to use when creating this VPN tunnel. The following options are available: <ul style="list-style-type: none"> <li>• Use Default – Use the default IKE profiles.</li> <li>• Create new Policy – Create a new IKE policy.</li> </ul>

- 6 Click **Add Peer** to add the tunnel peer information into the **Peer(s)** table.

This table lists all of the peers that are set for the VPN tunnel.

- 7 Click **Next** to proceed to the **Step 3** screen.

Use the **Back** button to go to the previous step. If any of the required values in the **Step 2** screen are not set properly, the **Step 3** screen will not display until they are properly set.

IPsec Configuration Step 3/4

Transform Set: default

Encryption: esp-null

Authentication: md5-hmac

Mode:  Tunnel  Transport

Security Association:  Lifetime: 3600 (Seconds 500 to 2147483646)

Data: 4608000 (Data-based IPsec security association lifetime. 500 to 2147483646)

Next Close

**Figure 119: VPN Step-By-Step Wizard - Step 3**



8 Set the following IPSec VPN values in the **Step 3** screen.

Transform Set	<p>Transform set is a set of configurations exchanged for creating the VPN tunnel and imposing a security policy. The transform set consists of the following:</p> <ul style="list-style-type: none"> <li>• Encryption – The encryption to use for creating the tunnel.</li> <li>• Authentication – The authentication used to identify tunnel peers.</li> <li>• Mode – The mode of the tunnel. This is how the tunnel will operate.</li> </ul> <p>From the drop-down list, select any pre-configured transform set, or click <b>Create New Policy</b> to create a new transform set.</p>
Encryption	<p>This field is enabled when <b>Create New Policy</b> is selected in the <b>Transform Set</b> field. This is the encryption that is used on data traversing through the tunnel. Select from the following algorithms: <b>esp-null</b>, <b>des</b>, <b>3des</b>, <b>aes</b>, <b>aes-192</b>, or <b>aes-256</b>.</p>
Authentication	<p>This field is enabled when <b>Create New Policy</b> is selected in the <b>Transform Set</b> field. This is the method peers authenticate as the source of the packet to other peers after a VPN tunnel has been created. Select from the following: <b>MD5</b>, <b>SHA</b>, <b>SHA256</b>, or <b>AES-XCBC-HMAC-128</b>.</p>
Mode	<p>This field is enabled when <b>Create New Policy</b> is selected in the <b>Transform Set</b> field. The mode indicates how packets are transported through the tunnel.</p> <ul style="list-style-type: none"> <li>• Tunnel – The tunnel is between two routers or servers.</li> <li>• Transport – The tunnel is between a client and a server.</li> </ul>
Security Association	<p>Configures the lifetime of a security association (SA). Keys and SAs should be renewed periodically to maintain the security of the tunnel.</p> <ul style="list-style-type: none"> <li>• Lifetime – Duration in seconds after which the keys should be changed. Set a value from 500 - 2,147,483,646 seconds.</li> <li>• Data – The key is changed after this quantity of data has been encrypted/decrypted. Set a value from 500 - 2,147,483,646 KB.</li> </ul>

- 9 Click **Next** to proceed to the **Step 4** screen.

Use the **Back** button to go to the previous step. If any of the required values in the **Step 3** screen are not set properly, the **Step 4** screen will not display until they are properly set.

Summary Step 4/4

**VPII Basic Configuration:**

Tunnel Name: test

Tunnel Type: Site-to-Site

Interface: VLAN1

**Remote Site Specification:**

Type: IKE V1

Peer: 1.2.2.1

Authentication: rsa

Local ID: 1.2.2.1

Remote ID: 2.2.2.1

IKE Policy: ikev1-default

**IPSec Configuration:**

Security Association:

Transform Set: default

Done Back Close

**Figure 120: VPN Step-By-Step Wizard - Step 4**

- 10 Review the configuration and click **Done** to create the VPN tunnel.

Use the **Back** button to go back to a previous screen and modify the configuration. Click **Close** to close the wizard without creating a VPN tunnel.

#### Advanced VPN Configuration

The advanced VPN configuration option does not utilize a setup wizard. Rather, it utilizes its own screen flow where most facets of a VPN tunnel configuration can be set by a qualified network administrator.

For detailed information on creating a VPN tunnel configuration, refer to [Defining Profile VPN Settings](#).

#### Overriding Auto IPSec Tunnel Settings

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 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 or associated access point.

Tunnels are sets of security associations (SAs) 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 **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- 3 Select **Profile Overrides > Security**.


4 Select **Auto IPSec Tunnel**.


**Settings**


Group ID  test


Authentication Type  rsa


Authentication Key   Confirm

IKE Version  ikev2

Enable NAT after IPSec 

Use Unique ID 

Re-Authentication 

IKE Life Time  8600 Seconds ( 600 to 86,400 )

OK Reset Exit

**Figure 121: Device Overrides - Security - 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 **Clear Overrides**. This removes all overrides from the device.

## 5 Refer to the following table to override the Auto IPSec tunnel settings:

Group ID	Define a 1 - 64 character identifier for an IKE exchange supporting auto IPSec tunnel secure peers.
Authentication Type	Select either <b>RSA</b> or <b>PSK</b> (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 is the first algorithm known to be suitable for signing, as well as encryption. The default setting is <b>RSA</b> .
Authentication Key	Enter the 8 - 21 character shared key (password) used for auto IPSec tunnel secure peer authentication.
IKE Version	Select the IKE version used for auto IPSec tunnel secure authentication with the IPSec gateway. <b>IKEv2</b> is the default setting.
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 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.

- Click **OK** to save the changes made in the **Auto IPSec Tunnel** screen.  
Click **Reset** to revert to the last saved configuration.

### Overriding NAT 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, service platform or Access Point 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 a controller, service platform or Access Point. Many-to-one NAT is the most common NAT technique for outbound internet access. Many-to-one NAT allows a controller, service platform or Access Point 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 or override a NAT configuration that can be applied to a profile:

- Select **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- Select **Profile Overrides > Security**.

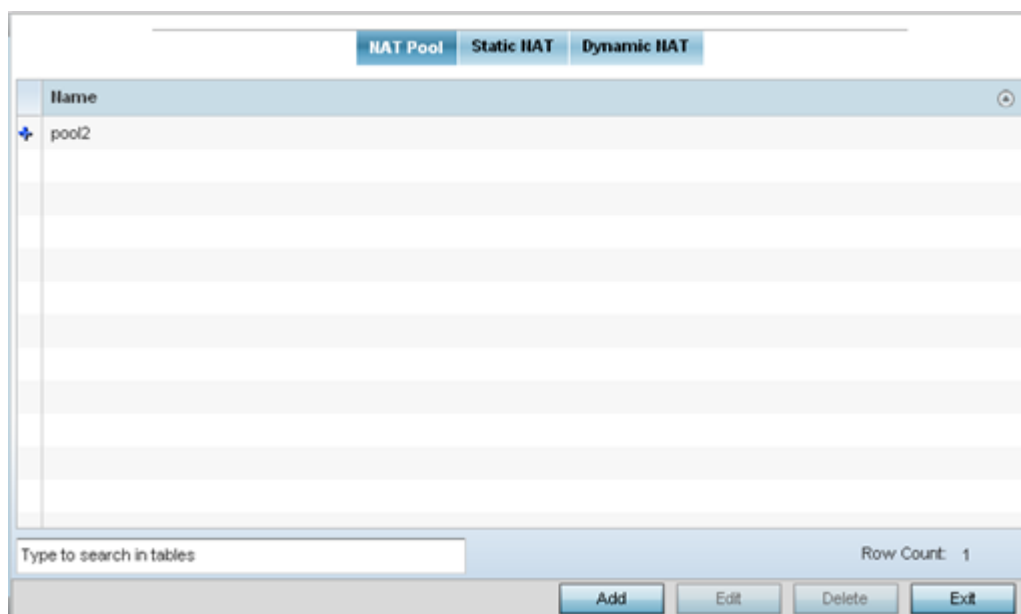
4. Select **NAT**.

The **NAT Pool** screen displays by default. The **NAT Pool** screen lists the NAT policies that have been 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 **Clear Overrides**. This removes all overrides from the device.



**Figure 122: Device Overrides - NAT Pool Screen**

- 5 Click **Add** to create a new NAT policy that can be applied to a profile.  
Click **Edit** to modify or override the attributes of an existing policy, or click **Delete** to remove obsolete NAT policies from the list of those available to a profile.

**Figure 123: Device Overrides - Security - NAT Pool Screen**

- 6 If you are adding a new NAT policy or editing the configuration of an existing policy, define the following parameters:

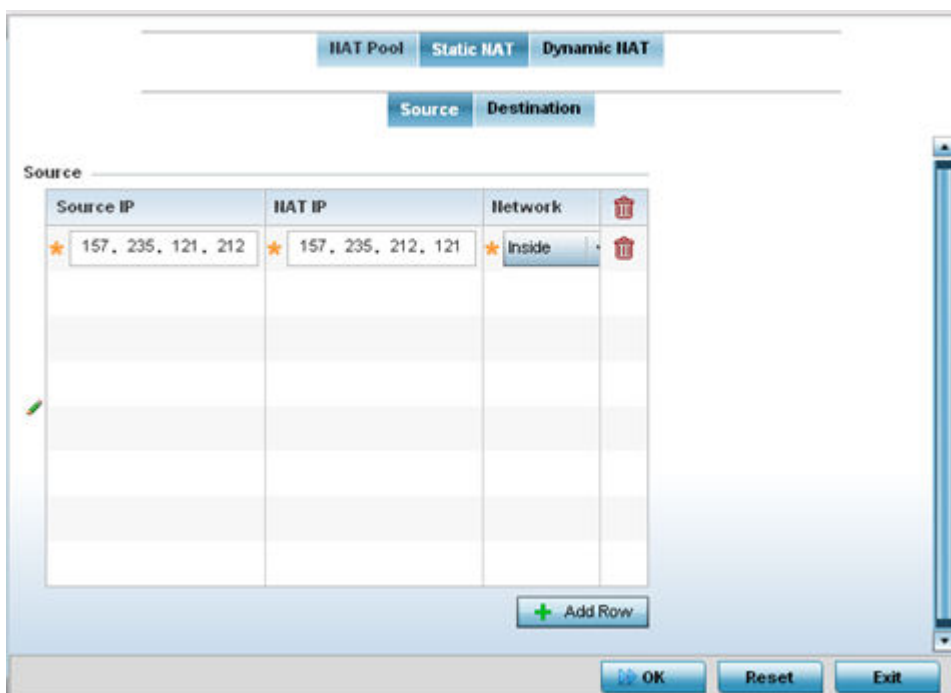
Name	If you are adding a new NAT policy, provide a name to help distinguish it from others with similar configurations. The length cannot exceed 64 characters.
IP Address Range	Define a range of IP addresses that are hidden from the public internet. NAT modifies network address information in the defined 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 potentially being routed through a NAT device. Consequently, NAT should be deployed with a stateful firewall.

- 7 Click **+ Add Row** as needed to append additional rows to the **IP Address Range** table.  
8 Click **OK** to save the changes made to the profile's NAT pool configuration.  
Click **Reset** to revert to the last saved configuration.

- 9 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 124: Device Overrides - Static NAT Screen**

- 10 Select **+ Add Row** to create a new static NAT configuration.

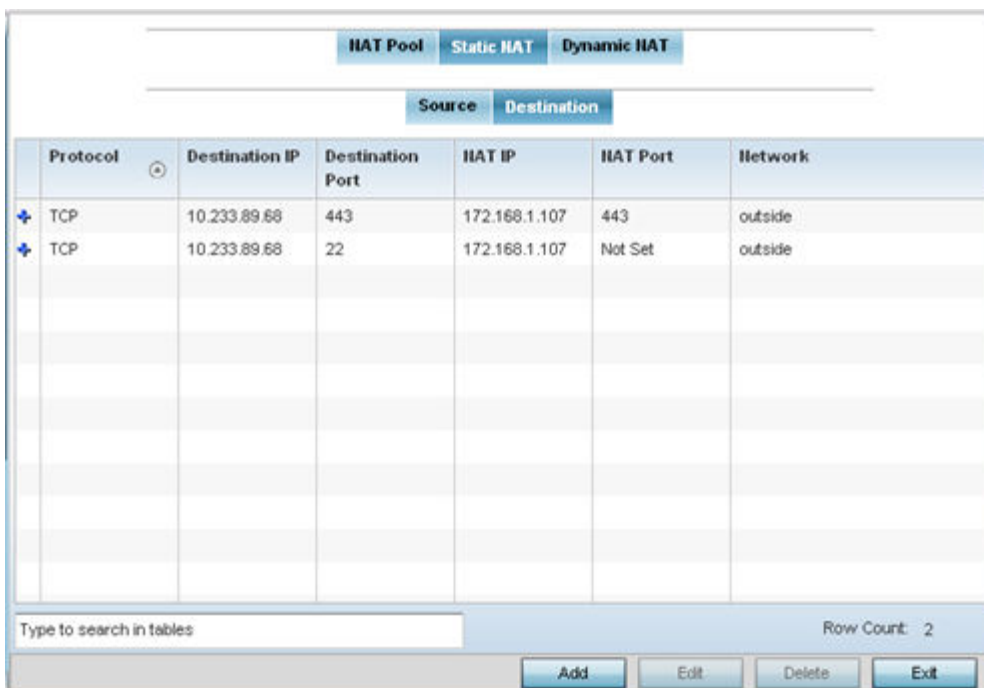


- 11 Define the following **Source NAT** parameters:

Source IP	Enter the address used at the (internal) end of the static NAT configuration. This address (once translated) will not be 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 <b>source</b> or <b>destination</b> based on the direction specified.
Network	Select <b>Inside</b> or <b>Outside</b> NAT as the network direction. <b>Inside</b> NAT is the default setting. Select <b>Inside</b> 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.

- 12 Select the Destination tab to view destination NAT configurations and to define the way in which packets passing through the NAT on the way back to the LAN are searched against the records kept by the NAT engine.

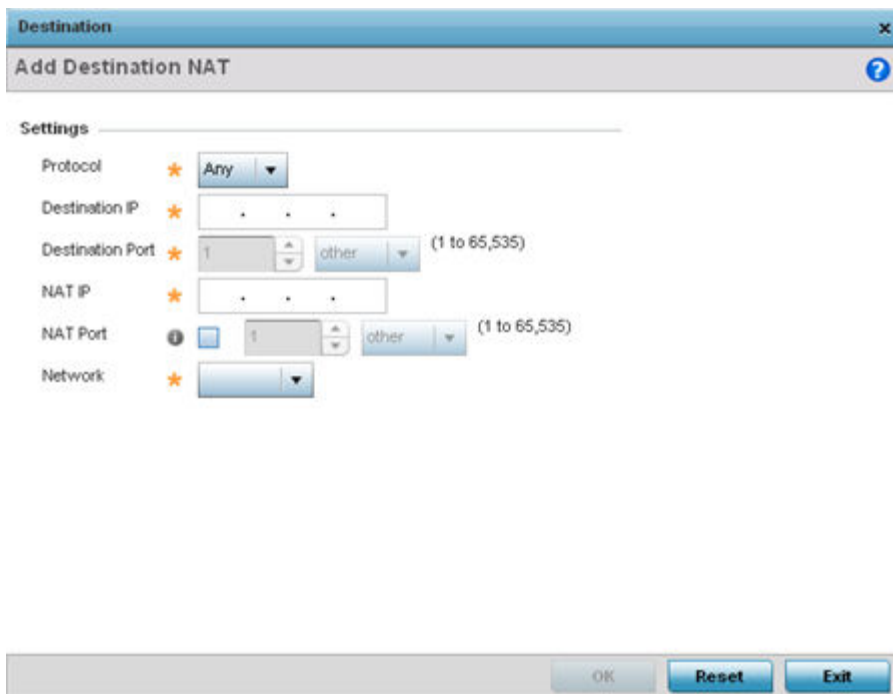
The destination IP address is changed back to the specific internal private class IP address to reach the LAN over the network.



**Figure 125: Device Overrides - NAT Destination Screen**

- Click **Add** to create a new NAT destination configuration, or click **Delete** to permanently remove a NAT destination.

Existing NAT destination configurations cannot be edited.



**Figure 126: NAT Destination - Add Screen**

- 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. Available options are <b>TCP</b> , <b>UDP</b> , and <b>Any</b> . The default setting is <b>Any</b> . TCP is a transport layer protocol used by applications requiring guaranteed delivery. It is 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.
Destination IP	Enter the local address used at the (source) end of the static NAT configuration. This address (once translated) will not be exposed to the outside world when the translation address is used to interact with the remote destination
Destination Port	Set the local port number used at the (source) end of the static NAT configuration. The default value is port 1.



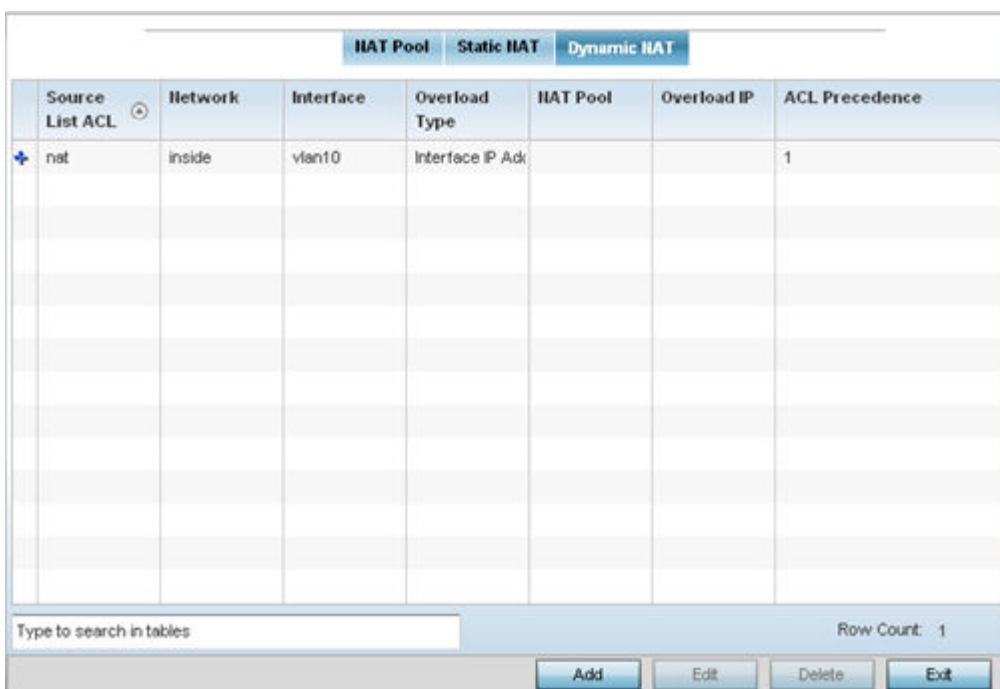
NAT IP	Enter the IP address of the matching packet to the specified value. The IP address modified can be either source or destination based on the direction specified.
NAT Port	Enter the port number of the matching packet to the specified value. This option is valid only if the direction specified is <b>destination</b> .
Network	Select <b>Inside</b> or <b>Outside</b> NAT as the network direction. <b>Inside</b> is the default setting.

15 Click **OK** to save the changes made to the static NAT configuration.

Click **Reset** to revert to the last saved configuration.

16 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.



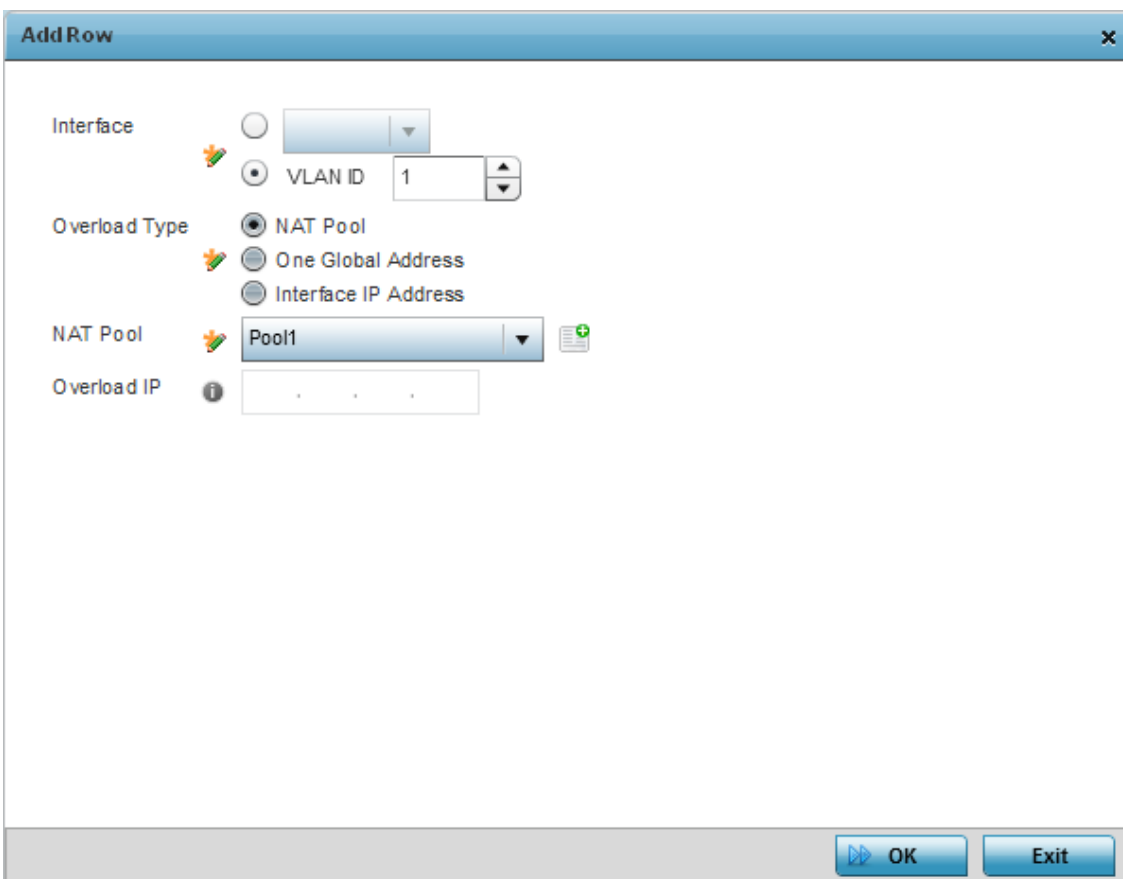
**Figure 127: Device Overrides - Dynamic NAT Screen**

17 Refer to the following to determine whether a new dynamic NAT configuration needs to be created, or whether an existing one can be edited or deleted:

Source List ACL	Lists an ACL 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 <b>Inside</b> or <b>Outside</b> 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 used when several internal addresses are NATed to only one or a few external addresses. Options include <b>NAT Pool</b> , <b>One Global Address</b> , and <b>Interface IP Address</b> . <b>Interface IP Address</b> is the default setting.
NAT Pool	Displays the name of an existing NAT pool used with the dynamic NAT configuration.
Overload IP	If <b>One Global IP Address</b> is selected as the <b>Overload Type</b> , define an IP address to use as 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 this ACL rule.

18 Click **Add** to create a new dynamic NAT configuration, **Edit** to modify or override an existing configuration, or **Delete** to permanently remove a configuration.



**Figure 128: Device Overrides - Dynamic NAT Add Screen**

19 Set or override the following to define the **Dynamic NAT** configuration:

Source List ACL	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) will not be exposed to the outside world when the translation address is used to interact with the remote destination.
Network	Select <b>Inside</b> or <b>Outside</b> NAT as the network direction for the dynamic NAT configuration. <b>Inside</b> 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 the ACL rule.
Interface	Select the VLAN (from 1 - 4094) or WWAN used as the communication medium between the source and destination points within the NAT configuration. Ensure that the VLAN selected adequately supports the intended network traffic within the NAT supported configuration. VLAN1 is available by default.
Overload Type	Define the overload type used when several internal addresses are NATed to only one or a few external addresses. Options include <b>NAT Pool</b> , <b>One Global Address</b> , and <b>Interface IP Address</b> . <b>Interface IP Address</b> is the default setting.
NAT Pool	Provide the name of an existing NAT pool for use with the dynamic NAT configuration.
Overload IP	If <b>One Global IP Address</b> is selected as the <b>Overload Type</b> , define an IP address to use as a filter address for the IP ACL rule.

20 Click **OK** to save the changes made to the dynamic NAT configuration.

Click **Reset** to revert to the last saved configuration.

### Overriding a Bridge NAT 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.

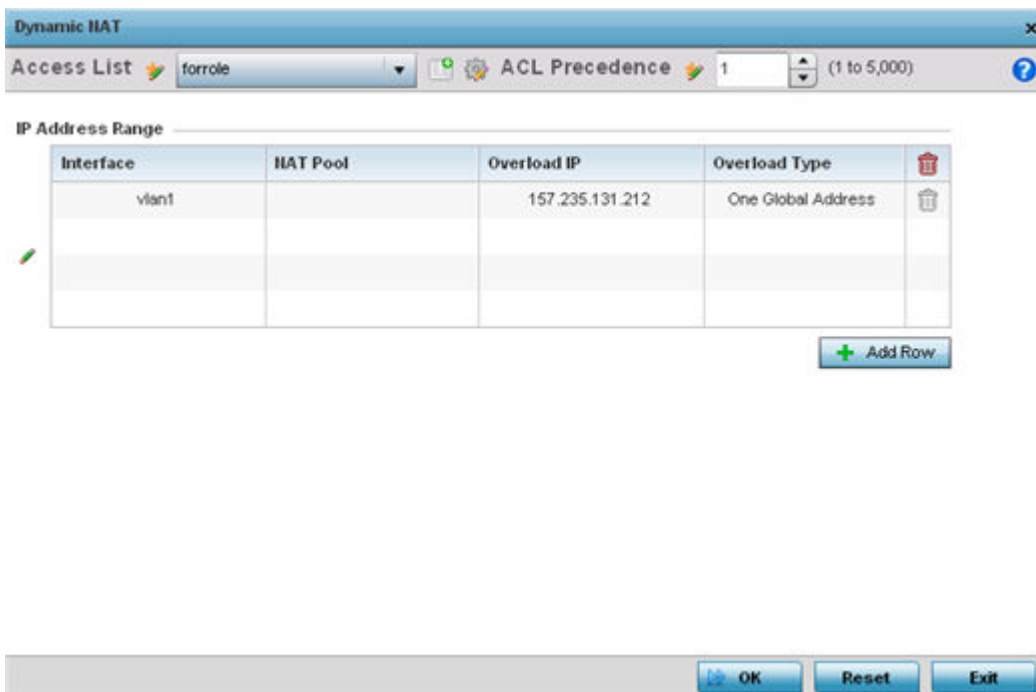
To resolve latency issues, Bridge NAT identifies and segregates traffic heading towards the NoC and outwards towards the internet. Traffic towards the NoC is allowed over the secure tunnel. Traffic towards the internet is switched to a local WLAN link with access to the internet.

To define a NAT configuration or override that can be applied to a profile:

- 1 Select **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- 3 Select **Profile Overrides > Security**.



- Click **Add** to create a new bridge VLAN configuration, **Edit** to modify or override an existing configuration, or **Delete** to permanently remove a configuration.



**Figure 130: Profile Security - Dynamic NAT - Screen**

- Select the **ACL** whose IP rules are applied to the policy based forwarding rule.  
You can define a new ACL by clicking the **Create** icon, or you can modify an existing set of IP ACL rules by clicking the **Edit** icon.
- 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	Select the outgoing Layer 3 interface on which traffic is redirected. The interface can be an access point <b>wwan</b> or <b>pppoe</b> 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 <b>Overload Type</b> has been set to <b>NAT Pool</b> .
Overload IP	Lists the IP address used to represent a large number of local addresses for this configuration.
Overload Type	Define the overload type utilized when several internal addresses are NATed to only one or a few external addresses. Select <b>NAT Pool</b> , <b>One Global Address</b> , or <b>Interface IP Address</b> . <b>Interface IP Address</b> is the default setting.

- Click **+ Add Row** to set the interface, overload, and NAT pool settings for the bridge NAT configuration.

**Figure 131: Security Source Dynamic NAT Screen**

- Click **OK** to save the changes made in the **Add Row** and **Source Dynamic NAT** screens.  
Click **Reset** to revert to the last saved configuration.

### Overriding Application Visibility Settings

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:

- Select **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- Select **Profile Overrides > Security**.

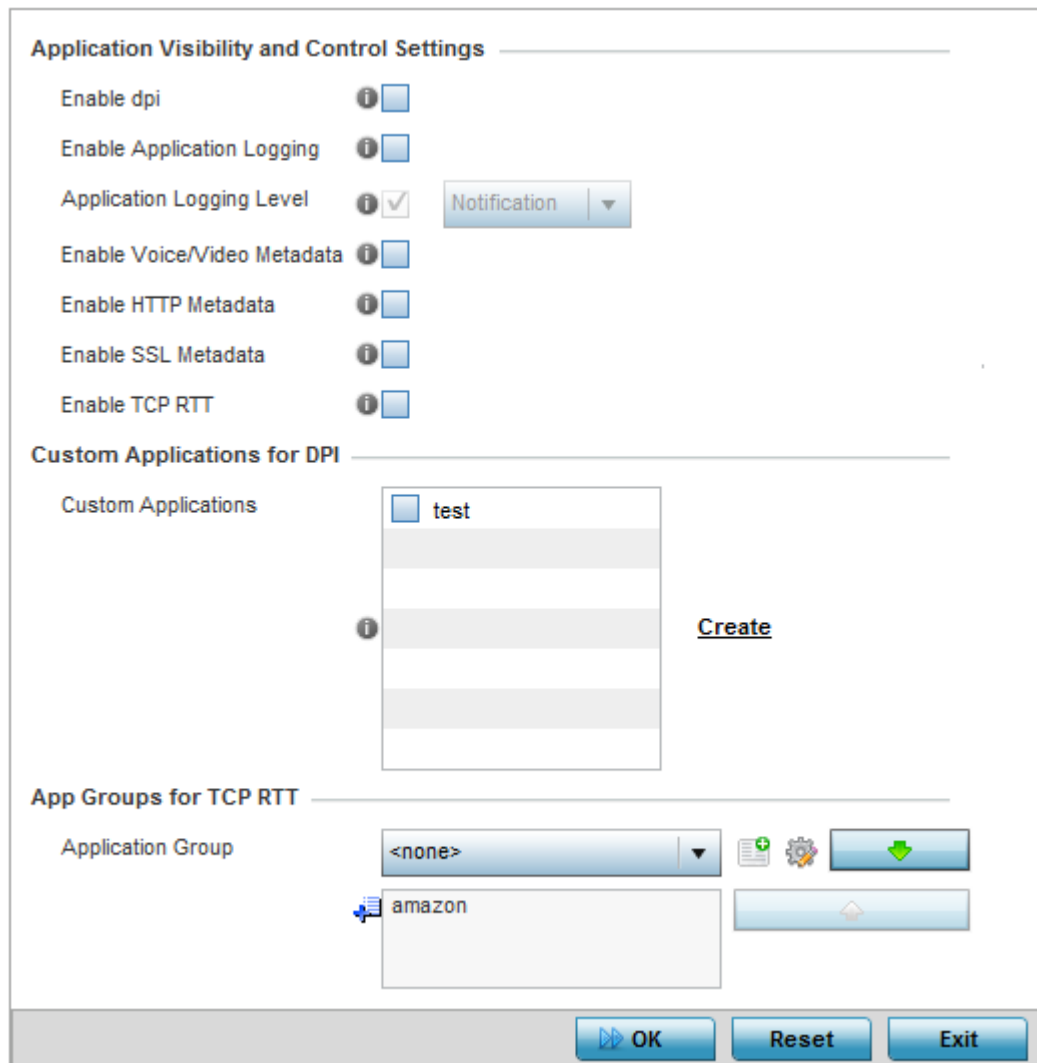


4 Select **Application Visibility**.



**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 **Clear Overrides**. This removes all overrides from the device.



**Figure 132: Profile Security - Application Visibility screen**

5 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.

Applications Logging Level	If enabling DPI application recognition event logging, set the logging level. Severity levels include <b>Emergency, Alert, Critical, Errors, Warning, Notice, Info</b> , and <b>Debug</b> . The default logging level is <b>Notification</b> .
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 extraction of metadata from HTTP application data flows. The default setting is disabled.
Enable SSL Metadata	Select this option to enable extraction of metadata from SSL application data 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.

- 6 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.”

- 7 If you are enabling TCP-RTT metadata collection, use the **App Groups for TCP RTT** field to 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. You can add a maximum of 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.”

- 8 Click **OK** to save the changes or overrides.  
Click **Reset** to revert to the last saved configuration.

### Overriding 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 by the Access Point. If WAN backhaul is available, and a router failure occurs, then an 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 that lose the election process enter a backup state where they monitor the master for any failures. In case of a failure, one of the backups 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 > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- 3 Select **Profile Overrides**.
- 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 **Clear Overrides**. This removes all overrides from the device.

Virtual Router ID	Description	Virtual IP Addresses	Interface	Priority
1	router1	157.235.232.32	vlan1	100

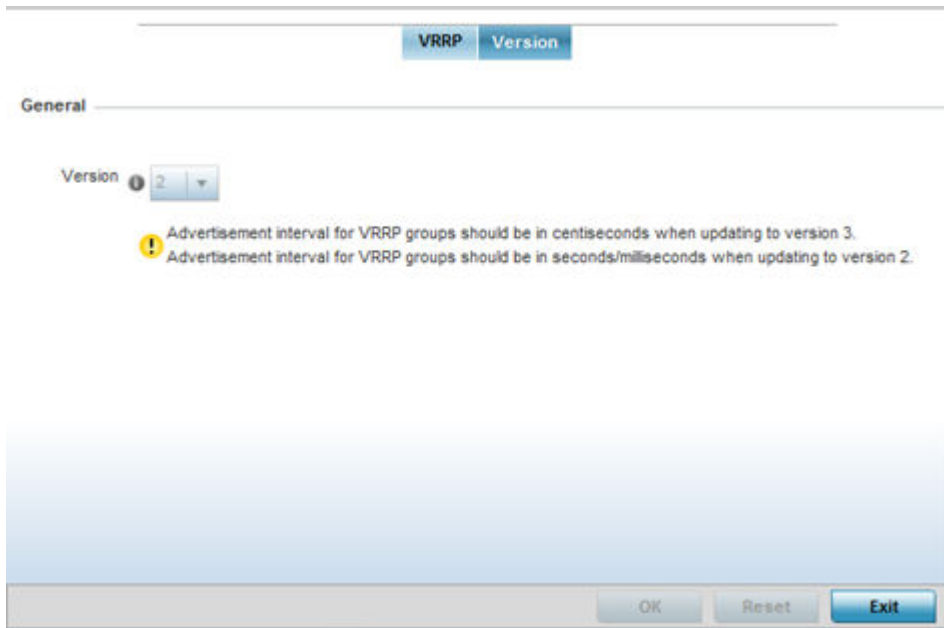
**Figure 133: Device Overrides - VRRP Screen**

- 5 Review the following VRRP configuration data to assess whether a new VRRP configuration is required or whether an existing VRRP configuration can be modified or removed:

Virtual Router ID	A numerical index (from 1 - 255) used to differentiate VRRP configurations. The index is assigned when a VRRP configuration is initially defined. This ID identifies the virtual router for which a packet is reporting status.
Description	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	The virtual interface IP address used as the redundant gateway address for the virtual route.

Interface	The interfaces selected on the access point to supply VRRP redundancy failover support.
Priority	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 134: Device Overrides - 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 Click **Add** to create a new VRRP configuration.

Click **Edit** to modify or override the attributes of an existing VRRP configuration. If necessary, existing VRRP configurations can be selected and permanently removed by clicking **Delete**.

The screenshot shows the VRRP configuration interface for Virtual Router ID 1. The 'General' tab is selected. The configuration parameters are as follows:

- Description:** router1
- Priority:** 100 (range 1 to 254)
- Virtual IP Addresses:** A list of four IP addresses: 157.235.232.32, 0.0.0.0, 0.0.0.0, and 0.0.0.0. Each address has a 'Clear' button next to it.
- Advertisement Interval Unit:** seconds
- Advertisement Interval:** 1 (range 1 to 255). There are also options for milliseconds (250 to 999) and centiseconds (25 to 4,095).
- Preempt:** checked
- Preempt Delay:** 1 (range 1 to 65,535 seconds)
- Interface:** VLAN ID 1 (range 1 to 4,094)

Buttons for 'OK', 'Reset', and 'Exit' are visible at the bottom right of the window.

**Figure 135: Device Overrides - VRRP - Virtual Router Screen**

- 8 If you are 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 for which a packet is reporting status.
- 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 eight IP addresses representing the Ethernet switches, routers, or security appliances defined as virtual router resources.
Advertisement Interval Unit	Select either <b>seconds</b> , <b>milliseconds</b> , or <b>centiseconds</b> as the unit used to define VRRP advertisements. After an option is selected, the spinner control becomes enabled for that Advertisement Interval option. The default interval unit is seconds. If you are changing the VRRP group version from 2 to 3, the advertisement interval must be in centiseconds. Use VRRP group version 2 when the advertisement interval is either in seconds or milliseconds.
Advertisement Interval	After an <b>Advertisement Interval Unit</b> is 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 <b>Preempt Delay</b> 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 <b>Preempt</b> option is selected, use the spinner control to set the delay interval (in seconds) for preemption.
Interface	Select this value to enable or 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 by 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 in 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 <b>None</b> , <b>increment-priority</b> , and <b>decrement priority</b> .
Network Monitoring: Critical Resource Name	Select each critical resource needed for monitoring. The action specified in the <b>Critical Resource</b> 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 is enabled, the value is incremented by the setting defined.

11 Click **OK** to save the changes made to the VRRP configuration.

Click **Reset** to revert to the last saved configuration.

### Overriding a Critical Resource Configuration

Critical resources are device IP addresses or interface destinations on the network interoperated 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, a AAA server, a WAN interface, or any hardware or service on which the stability of the network depends. Critical resources are pinged regularly by the access point. If there is a connectivity issue, an event is generated stating a critical resource is unavailable. By default, no critical resource policy is enabled, 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 be 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 > Devices** from the web UI.

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

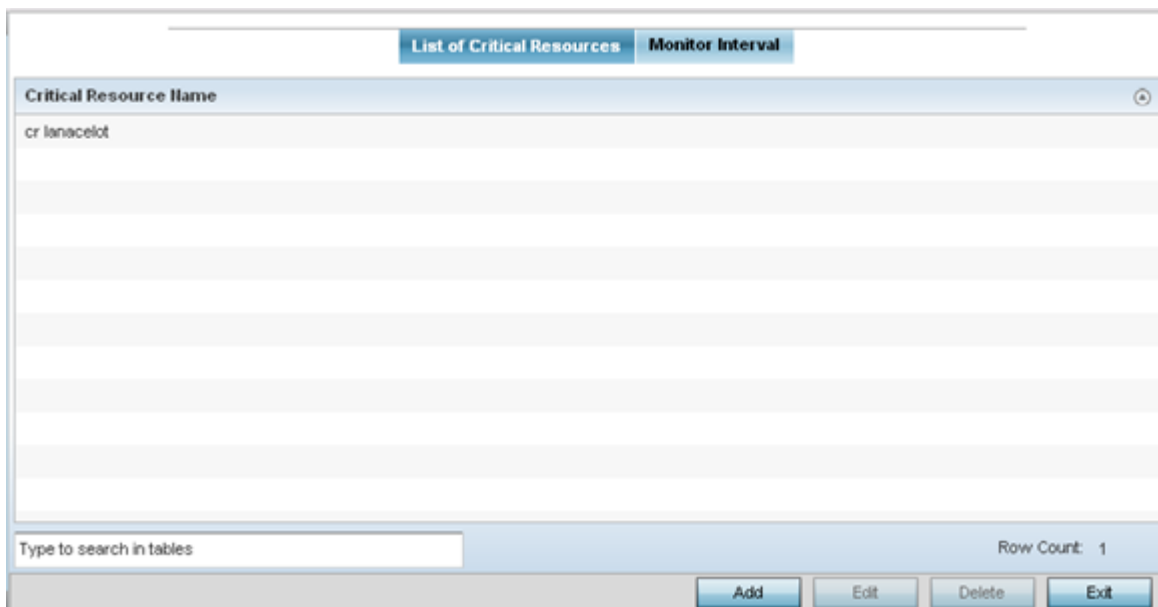
- 2 Select a target device in the lower left-hand side of the UI.

You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.

- 3 Select **Profile Overrides**.

- 4 Select **Critical Resources**.

In the List of Critical Resources tab, the **Critical Resource Name** table displays the name of the resources configured on this device.



**Figure 136: Device Overrides - 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. However, a VLAN, WWAN, or PPPoE must be monitored behind an interface.

- 5 Click **Add** to add a new critical resource and connection method.

Click **Edit** to modify or override the configuration for an existing critical resource. If you are adding a new critical resource, assign it a name up to 32 characters.

Critical Resource Monitoring

Critical Resource Name \*

Settings

Use Flows  Sync Adoptees

Offline Resource Detection Any

Monitor Criteria cluster-master

Monitor Via  IP . . .  Interface vlan 1

Resources:

IP Address	Mode	Port	VLAN	

+ Add Row

OK Reset Exit

**Figure 137: Critical Resources Screen - Adding a Critical Resource**

- 6 Select **Use Flows** so that the critical resource will monitor using firewall flows for DHCP or DNS instead of ICMP or ARP packets.

This reduces the amount of traffic on the network. This setting is disabled by default.

- 7 To sync adopted devices to state changes with a resource-state change message, select **Sync Adoptees**.

This setting is 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 you select **Any**, an event is generated when the state of any single critical resource changes. If you select **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 you select **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, set **Monitoring Criteria** to **All** because the controller might not know the VLAN bridged locally by the devices in the RF Domain monitoring DHCP.

- 10 In the **Monitor Via** field at the top of the screen, select the **IP** option to monitor a critical resource directly (within the same subnet) using the provided IP address as a network identifier.
- 11 In the **Monitor Via** field at the top of the screen, select the **Interface** check box to monitor a critical resource using the critical resource's **VLAN**, **WWAN1**, or **PPPoE1** interface.

If you select **VLAN**, use the spinner control to define the destination VLAN ID used as the interface for the critical resource.

- 12 Click **+ 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: <ul style="list-style-type: none"> <li>• <b>arp-only</b> - Use only the Address Resolution Protocol (ARP) for pinging the critical resource. ARP is used to resolve hardware addresses when only the network layer address is known.</li> <li>• <b>arp-and-ping</b> - Use both ARP and Internet Control Message Protocol (ICMP) for pinging the critical resource and sending control messages (for example, <i>device not reachable</i> or <i>requested service not available</i>).</li> </ul>
Port	Define the interface on which to monitor critical resource. This field lists the available hardware interfaces. This option is available only when the selected mode is <b>arp-only</b> .
VLAN	Using the spinner control, define the VLAN on which the critical resource is available.

- 13 Select the **Monitor Interval** tab.

**Figure 138: Critical Resources Screen - Monitor Interval Tab**

- 14 Use **Monitor Interval** to set the duration, in seconds, between two successive pings to the critical resource.
- Select a duration between 5 and 86,400 seconds. The default setting is 30 seconds.
- 15 Use **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 ARP packets used to detect critical resources. However, some devices do not support that 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.
- 16 Use **Monitor Retry Count** to set 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.
- 17 Click **OK** to save the changes to the critical resource configuration and monitor interval.
- Click **Reset** to revert to the last saved configuration.

### *Overriding a Services Configuration*

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:

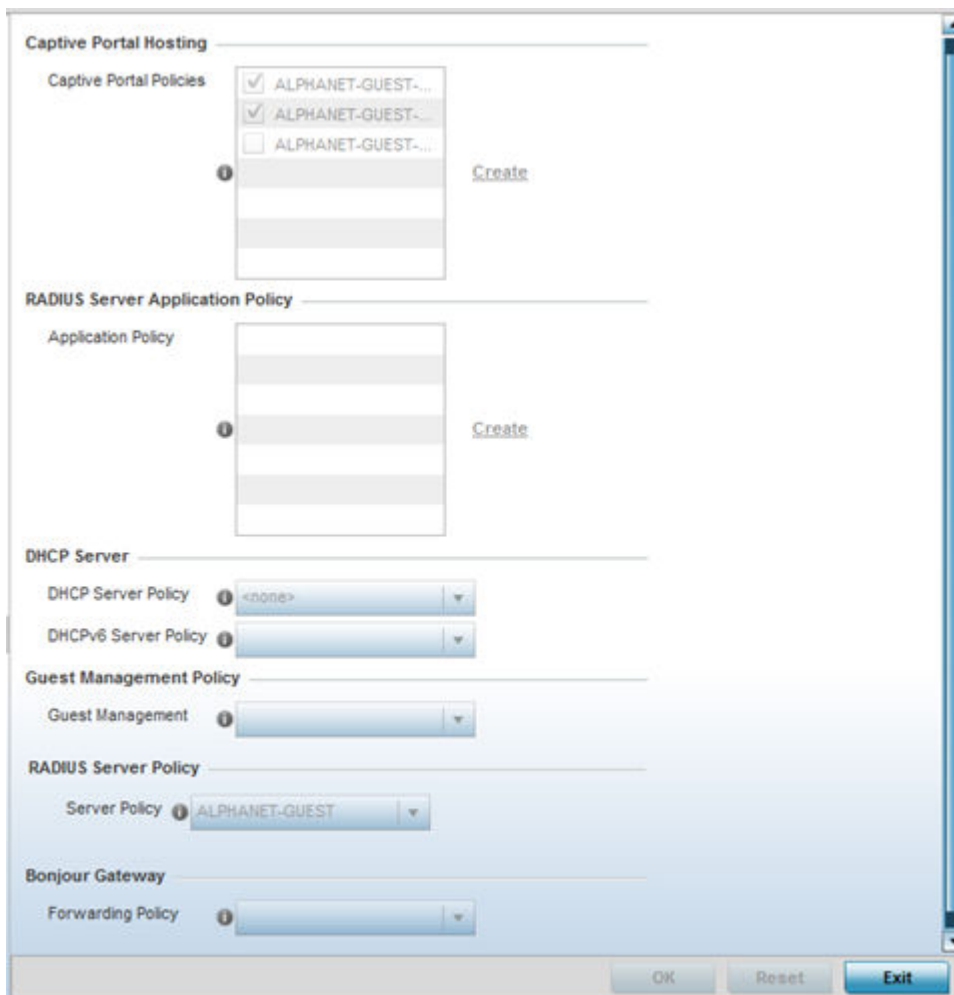
- 1 Select **Configuration > Devices** from the web UI.
- The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.

- 2 Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- 3 Select **Profile Overrides**.
- 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 **Clear Overrides**. This removes all overrides from the device.



**Figure 139: Device Overrides - Services Screen**

- 5 Refer to the **Captive Portal Hosting** field to set or override a guest access configuration (captive portal) for use with this profile.

A captive portal is guest access policy for providing temporary and restrictive access to the wireless network.

A captive portal configuration provides secure authenticated access using a standard Web browser. A captive portal provides authenticated access by capturing and re-directing a user's Web browser session to a captive portal login page where the user must enter valid credentials to access to the network. After the administrator has logged into the captive portal, additional Agreement, Welcome, and Fail pages provide the administrator with several options for the captive portal's screen flow and user appearance.

Select an existing captive portal policy, use the default captive portal policy, or click 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 777.

- 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 a 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, click 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, click the **Create** icon to create a new policy configuration that can be applied to this profile, or click 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 a predetermined interval. Before a lease expires, wireless clients (to which leases are assigned) are expected to renew them to continue to use the addresses. When 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, click the **Create** icon to create a new policy configuration that can be applied to this profile, or click 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 a Captive Portal Policy](#) on page 778.

- 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 838.

- 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.

From the **Forwarding Policy** drop-down menu, select the Bonjour Gateway forwarding policy.

- 12 Click **OK** to save the changes or overrides made to the profile's services configuration.

Click **Reset** to revert to the last saved configuration.

### *Overriding a Management Configuration*

Controllers and service platforms have mechanisms to allow or deny management access to the network for separate interfaces and protocols: HTTP, HTTPS, Telnet, SSH, and SNMP.

These management access configurations can be applied strategically to profiles as resource permissions dictate for the profile. Additionally, overrides can be applied to customize a device's management configuration, if deployment requirements change and a device's 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 cluster member, 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 **Configuration > Devices** from the web UI.  
The **Device Configuration** screen displays a list of managed devices or peer controllers, service platforms, or access points.
- 2 Select a target device in the lower left-hand side of the UI.  
You can also select a target device by double-clicking it in the list in the **Device Configuration** screen.
- 3 Select **Profile Overrides**.

4 Select **Management**.**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 **Clear Overrides**. This removes all overrides from the device.

**Management Policy**

Management Policy

**Message Logging**

Enable Message Logging

Remote Logging Host	Port	
172.168.1.200	514	
172.168.1.113	514	

Facility to Send Log Messages  local0

Syslog Logging Level  Debug

Console Logging Level  Debug

Buffered Logging Level  Debug

Time to Aggregate Repeated Messages   (0 to 60)

Forward Logs to Controller  Error

**System Event Messages**

Event System Policy  ADSP-Alarms

Enable System Events

Enable System Event Forwarding

**Events E-mail Notification**

SMTP Server

Port of SMTP  (1 to 65,535)

Sender Email Address

Recipient's Email Address

OK Reset Exit

**Figure 140: Device Overrides - Management Settings Screen**

- 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 there are no management policies that meet the data access requirements of this profile, click the **Create** icon to access screens used to define administration, access control, and SNMP configurations. Alternatively, select an existing policy and click the **Edit** icon to modify the configuration of an existing management policy. For more information, see [Viewing Management Access Policies](#) on page 855.

- 6 Refer to the **Message Logging** field to define how the profile logs system events.

It is important to log individual events to discern an overall pattern that might be negatively 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 <b>Delete</b> 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
System 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 this option to define a log level for forwarding event logs to the control. 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** field to define or override how controller or service platform system messages are logged and forwarded on behalf of the profile.
- Select an **Event System Policy** from the drop-down menu.  
If an appropriate policy does not exist, click **Create** to make a new policy.
  - Select **Enable System Events** to allow the profile to capture system events and append them to a log file.  
It is 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.
  - Select **Enable System Event Forwarding** 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** field 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 <i>from</i> address on notification email.
Recipient's E-mail Address	Specify up to 6 email addresses to be the recipients 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 an username and password before sending email through the server.
Password for SMTP Server	Specify password associated with the username of the sender on the outgoing SMTP server. Many SMTP servers require users to authenticate with an username and password before sending email through the server.

- 9 In the **Persist Configuration Across Reloads** field, use the **Configure** drop-down menu to define whether configuration overrides should persist when the device configuration is reloaded.  
Options include **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 data 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 pushing buffered packets. The default setting is 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.

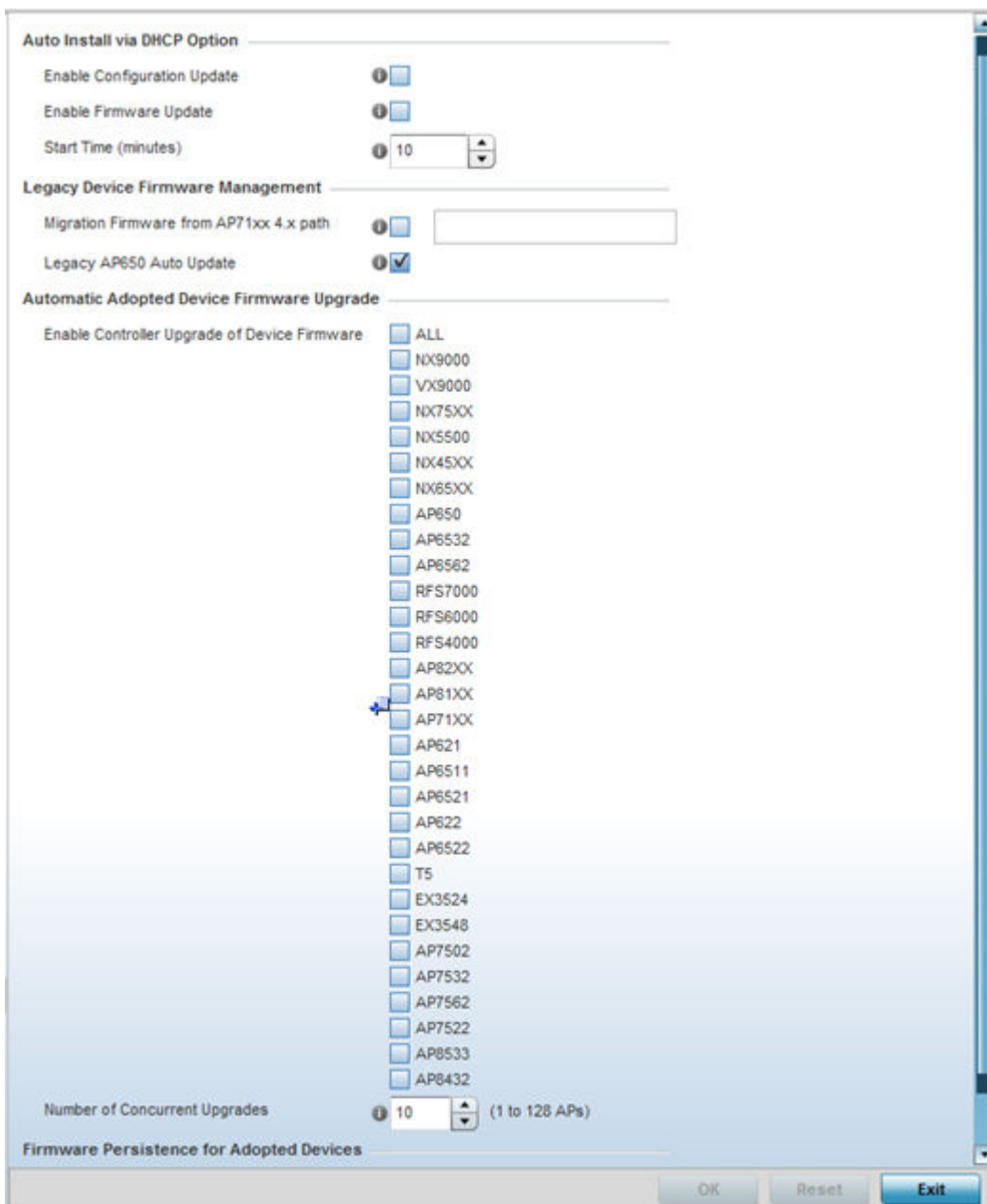


Controller	Select this option to provide service platform analytics to a local device. This setting is enabled by default.
URL	When using an external analytics engine with an NX 9000 series service platform, enter the IP address or uniform resource locator (URL) for the system providing external analytics functions.
User Name	Enter the user name needed to access the external analytics engine.
P:assword	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 is 1 minute.

12 Click **OK** to save the changes and overrides made to the profile's management settings.

Click **Reset** to revert to the last saved configuration.

13 Select the Firmware tab from the Management menu.



**Figure 141: 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 this option from within the <b>Automatic Configuration Update</b> field to enable automatic profile configuration file updates from an external location. If this option is enabled (it 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 updates for this profile from a user-defined remote location. This value is disabled by default.
Start Time (minutes)	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 in the **Legacy Device Firmware Management** to set legacy access point firmware provisions:

Migration Firmware from AP71xx 4.x path	Provide a path to a firmware image used to provision AP 7161 model access points currently using a 4.x version legacy firmware file. When a valid path is provided, the update is enabled to the version maintained locally for AP 7161 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 in the **Automatic Adopted AP Firmware Upgrade** section to define an automatic firmware upgrade from a local file.

Enable Configuration Update 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 **Persist AP Images on Controller** (in 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 stored on the RF domain manager only when there is enough space to accommodate it. The upgrade sequence is different depending on whether the designated RF domain manager is a controller/service platform or an access point.

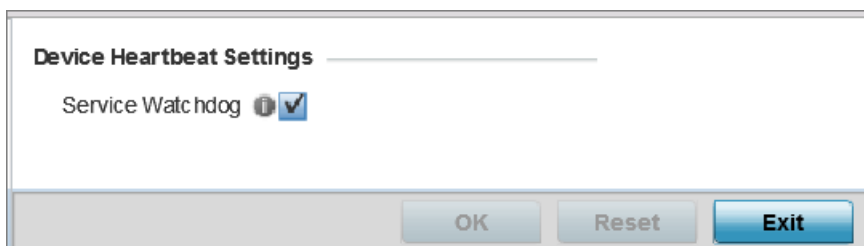
- When the RF domain manager is an access point - The NOC uploads a provisions an access point model's firmware on to the access point RF domain manager. The NOC initiates an auto-update for access points using that model's firmware. If the **Persist Image on Controller** option is selected, the RF domain 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 is expected that 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 Click **OK** to save the changes and overrides made to the profile's management firmware configuration.

Click **Reset** to revert to the last saved configuration.

- 19 Select **Heartbeat** from the Management menu.



**Figure 142: Device Overrides - Management Heartbeat Screen**

20 Select the **Service Watchdog** option to implement heartbeat messages.

This ensures that associated devices are up and running and can interoperate effectively. The Service Watchdog is enabled by default.

21 Click **OK** to save the changes and overrides made to the profile's configuration.

Click **Reset** to revert to the last saved configuration.

*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 set or override a profile's mesh point configuration:

1 Select **Configuration > Devices** from the web UI.

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

2 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 **Clear Overrides**. This removes all overrides from the device.

Mesh Connex	Is Root	Preferred Root	Root Selection Method	Preferred Neighbor	Preferred Interface	Monitor Critical Resources	Monitor Primary Port Link	Path Method
+	✗ No		None		None	✗ No	✗ No	None
+	✗ No		None		None	✓ Yes	✓ Yes	None

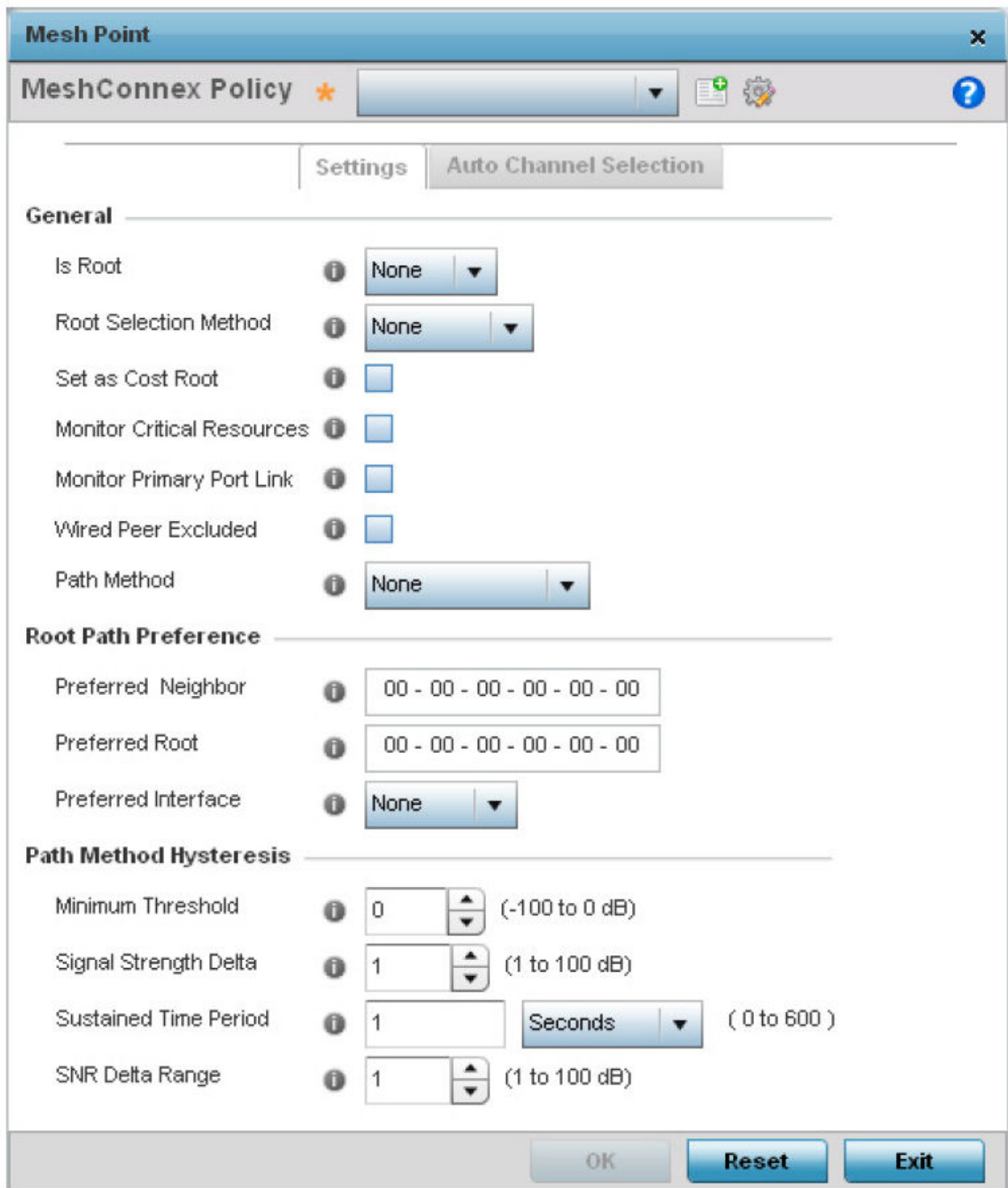
Type to search in tables Row Count: 2

**Figure 143: Device Overrides - Mesh Point Screen**

Refer to the **Mesh Point** screen to view existing Mesh Point overrides.



- 3 Click **Add** to create a new mesh point configuration, if an existing configuration does not meet your requirements.  
Click **Edit** to modify or override the attributes of a existing mesh point configuration. If necessary, existing configurations can be selected and permanently removed by clicking **Delete**.



**Figure 144: Mesh Point Settings Screen**

4 Define the following **General** mesh point settings:

MeshConnex Policy	If you are 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 access point. <b>True</b> means that this access point is a root node for this mesh network, and <b>False</b> means that it is not a root node.
Root Selection Method	Use the drop-down menu to determine whether this meshpoint is the root or non-root meshpoint. Select either <b>None</b> , <b>auto-mint</b> , or <b>auto-proximity</b> . When <b>auto-mint</b> 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 <b>auto-proximity</b> is selected, root selection is based on signal strength of candidate roots. <b>None</b> , which is the default setting, indicates no preference in root selection.
Set as Cost Root	Select this option to set the mesh point as the cost root for mesh point 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	Select the method used for path selection in a mesh network. Available options include: <ul style="list-style-type: none"> <li>• <b>None</b> - No criteria are used in root path selection.</li> <li>• <b>uniform</b> - The path selection method is uniform (two paths are considered equivalent if the average value is the same for these paths).</li> <li>• <b>mobile-snr-leaf</b> - The access point is mounted on a vehicle or a mobile platform (AP 7161 models only). The path to the route is selected based on the Signal To Noise Ratio (SNR) with the neighbor device.</li> <li>• <b>snr-leaf</b> - The path with the best signal to noise ratio is always selected.</li> <li>• <b>bound-pair</b> - Select this option to bind one mesh point connection at a time. Once established, other mesh point connection requests are denied.</li> </ul>

**Note**

An AP 7161 model access point can be deployed as a vehicular mounted modem (VMM) to provide wireless network access to a mobile vehicle such as a car or train.. 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 293.

**Note**

When using 4.9GHz, the root preferences selection for the radio's preferred interface still displays as 5GHz.

- 5 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 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. <b>None</b> defines the interface as open to any radio band.

- 6 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 <b>Minimum Threshold</b> and <b>Signal Strength Delta</b> 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.



- Click the Auto Channel Selection tab to configure the parameters for the MeshConnex Auto Channel Selection policy.

The screenshot shows the 'Mesh Point' configuration window for 'MeshConnexPolicy\_01'. The 'Auto Channel Selection' tab is active, and the 'Dynamic Root Selection' sub-tab is selected. The configuration is split into two sections: 'For 2.4 GHz' and 'For 5.0/4.9 GHz'. Each section contains the following settings:

- Channel Width:** Automatic (dropdown)
- Priority Meshpoint:**  (checkbox)
- Off-channel Duration:** 50 (spinner), (20 to 250 milliseconds)
- Off-channel Scan Frequency:** 6 (spinner), Seconds (dropdown), (1 to 60)
- Meshpoint Root:**
  - Sample Count:** 5 (spinner), (1 to 10 samples)
  - Channel Hold Time:** 30 (spinner), Minutes (dropdown), (0 to 1,440)

At the bottom of the window are 'OK', 'Reset', and 'Exit' buttons.

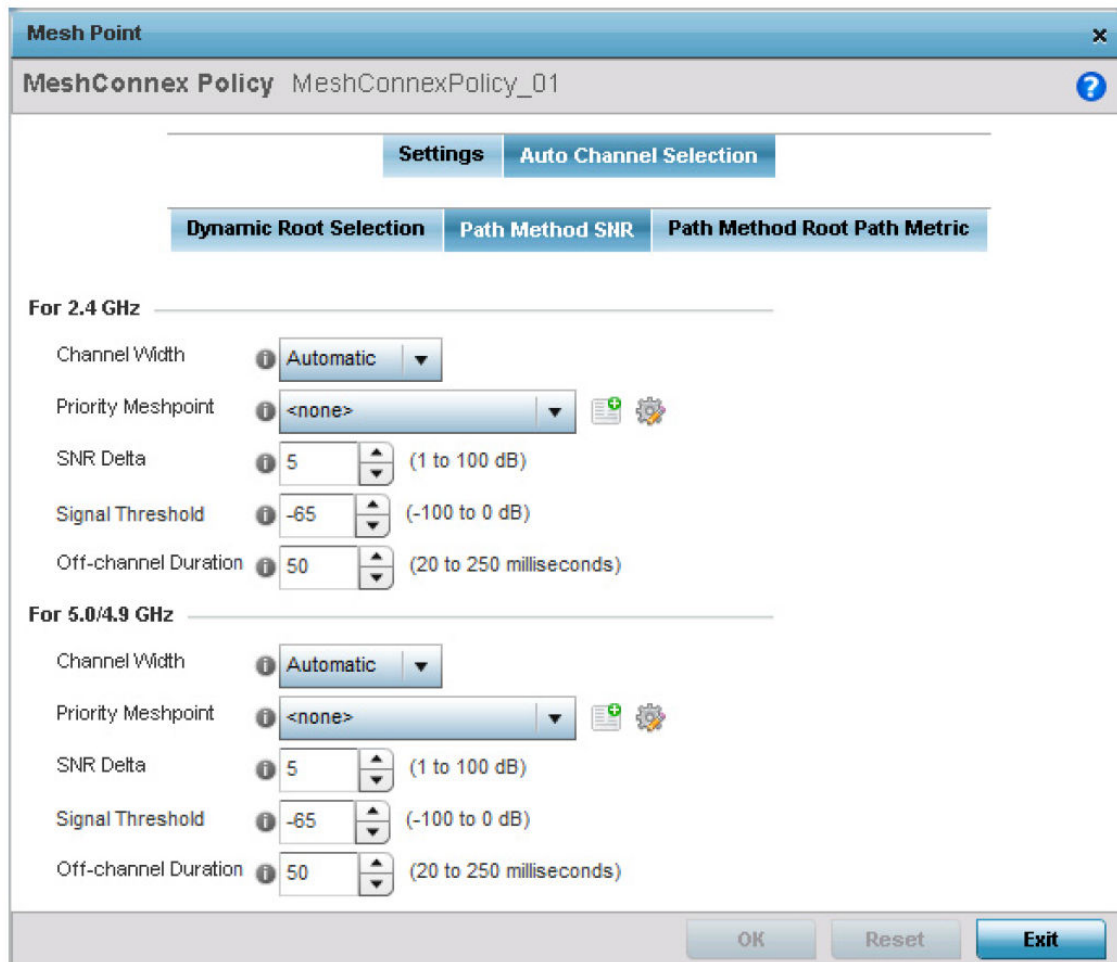
**Figure 145: Mesh Point Auto Channel Selection Screen - Dynamic Root Selection Tab**

The **Dynamic Root Selection** screen displays by default. This screen provides configuration for the 2.4 GHz and 5.0/4.9 GHz frequencies.

- 8 Refer to the following for more information on the Auto Channel Selection **Dynamic Root Selection** screen. These descriptions are common for configuring 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: <ul style="list-style-type: none"> <li>• <b>Automatic</b> - The channel width is calculated automatically. This is the default value.</li> <li>• <b>20 MHz</b> - Sets the width between adjacent channels as 20 MHz.</li> <li>• <b>40 MHz</b> - Sets the width between adjacent channels as 40 MHz.</li> <li>• <b>80 MHz</b> - Sets the width between adjacent channels as 80 MHz. (Used for 802.11ac access points in the 5 GHz frequency.)</li> </ul>
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.

- 9 Select the Path Method SNR tab to configure signal to noise (SNR) ratio values when selecting the path to the meshpoint root.



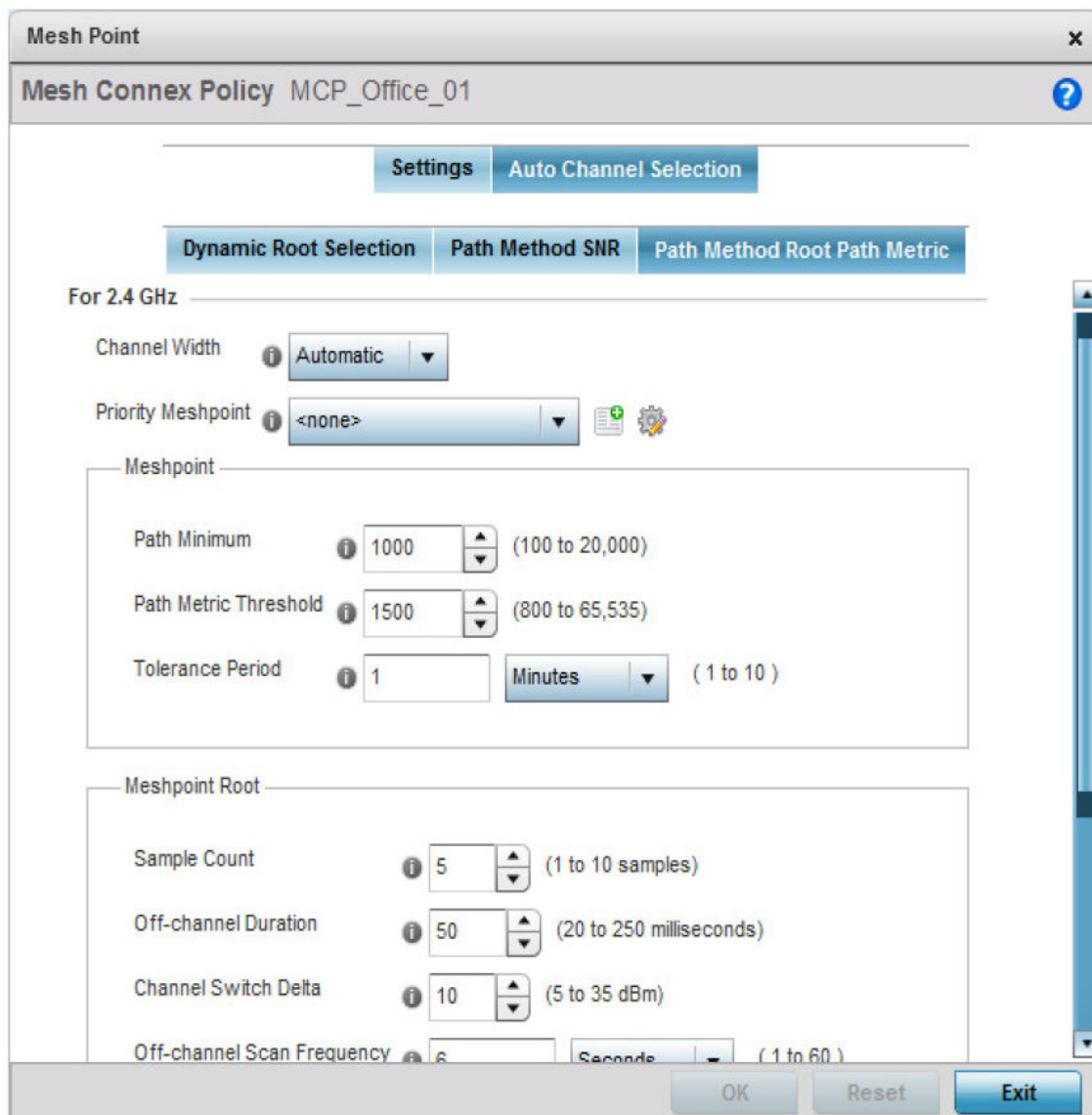
**Figure 146: Mesh Point Auto Channel Selection Screen - Path Method SNR Tab**

- 10 Set the following for 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: <ul style="list-style-type: none"> <li>• <b>Automatic</b> - The channel width is calculated automatically. This is the default value.</li> <li>• <b>20 MHz</b> - Sets the width between adjacent channels as 20 MHz.</li> <li>• <b>40 MHz</b> - Sets the width between adjacent channels as 40 MHz.</li> <li>• <b>80 MHz</b> - Sets the width between adjacent channels as 80 MHz. (Used for 802.11ac access points in the 5 GHz frequency.)</li> </ul>
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.

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	Set the duration (from 20 - 250 milliseconds) the scan dwells on each channel when performing an off channel scan. The default is 50 milliseconds.

- 11 Select the Path Method Root Path Metric tab to calculate root path metrics.



**Figure 147: Mesh Point Auto Channel Selection Screen - Path Method Root Path Metric Tab**

- 12 Set the following **Path Method Root Path Metric** values. These descriptions apply to both 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: <ul style="list-style-type: none"> <li>• <b>Automatic</b> - The channel width is calculated automatically. This is the default value.</li> <li>• <b>20 MHz</b> - Sets the width between adjacent channels as 20 MHz.</li> <li>• <b>40 MHz</b> - Sets the width between adjacent channels as 40 MHz.</li> <li>• <b>80 MHz</b> - Sets the width between adjacent channels as 80 MHz. (Used for 802.11ac access points in the 5 GHz frequency.)</li> </ul>
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.
Meshpoint: Path Minimum	Set the minimum path metric (from 100 - 20,000) for establishing mesh connections. 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 the duration to wait before triggering an automatic channel selection for the next hop. The default is 1 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 (from 20 - 250 milliseconds) that 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.

- 13 Click **OK** to save the changes made to the mesh point configuration.  
Click **Reset** to revert to the last saved configuration.

### 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.
- Set the RTS threshold value to 1 on all mesh devices. The default value is 65,536. For more information on defining radio settings, see [Access Point Radio Configuration](#) on page 555.
- Use **Opportunistic** as the rate selection settings for the AP 7161 radio. The default is **Standard**. For more information on defining this setting, see [Radio Override Configuration](#) on page 136.
- Disable Dynamic Chain Selection (radio setting). The default value is enabled. This setting is disabled from the Command Line Interface (CLI) using the `dynamic-chainselection` command, or, in the UI (refer to [Radio Override Configuration](#) on page 136).

- Disable A-MPDU Aggregation if the intended vehicular speed is greater than 30 mph. For more information, see [Radio Override Configuration](#) on page 136.
- 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)#
```

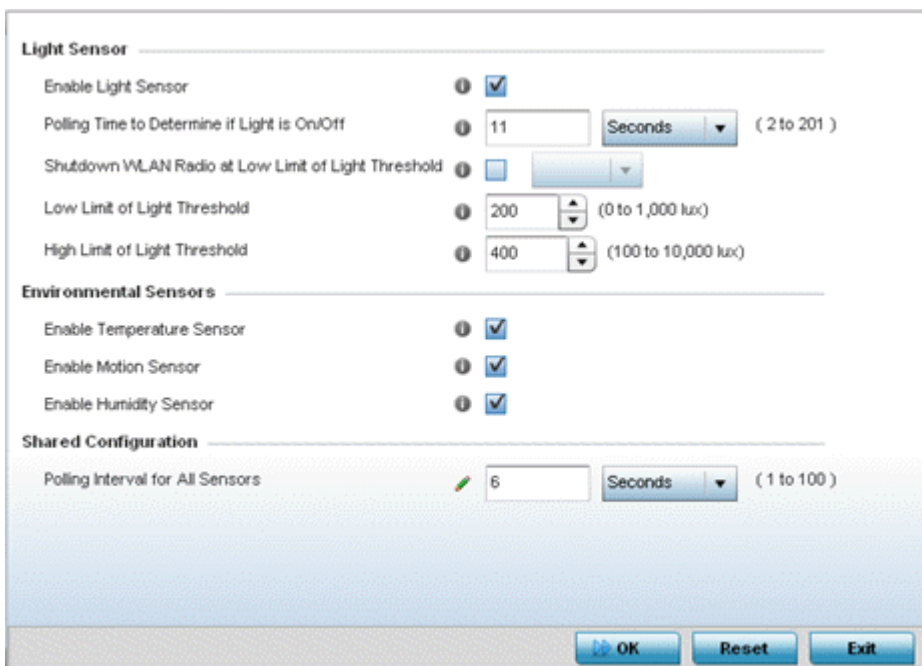
### *Overriding an Environmental Sensor Configuration (AP 8132 Only)*

A sensor module is a USB environmental sensor extension to an AP 8132 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 the **Environmental Sensor** screen.

To set or override an environmental sensor configuration for an AP 8132 model access point:

- 1 Select **Configuration > Devices > Profile Overrides** from the web UI.

2 Select **Environmental Sensor**.



**Figure 148: Profile Overrides - Environmental Sensor Screen**

3 Override or set the following **Light Sensor** settings for the AP 8132 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 access point's 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 assess light intensity in its environment 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 radios when the light intensity falls below the set threshold. Select <b>All</b> (both AP 8132 radios), <b>radio-1</b> , or <b>radio-2</b> .
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 location. In daytime, the light sensor's value is between 350-450. The default value for the low threshold is 200 - that is, the radios are turned off when the average reading value is lower than 200 lux.
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 location. The default high threshold is 400 - that is, the radios are turned on when the average value is higher than 400 lux.



- 4 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 <b>Environment</b> screens (in 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 <b>Environment</b> screens (in 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 <b>Environment</b> screens (in the Statistics node). This setting is enabled by default.

- 5 In **Shared Configuration**, set the interval in either seconds (1 - 100) or minutes (1 - 2) between environmental polling transmissions (both light and environment).

The default setting is 5 seconds.

- 6 Click **OK** to save the changes made to the **Environmental Sensor** screen.  
Click **Reset** to revert to the last saved configuration.

### *Overriding an Advanced Configuration*

Use the profile's advanced configuration screens to set client load balance calculations and ratios, a MiNT configuration, and miscellaneous settings.

- [Advanced Client Load Balance Configuration](#) on page 296
- [Advanced MiNT Protocol Configuration](#) on page 299
- [Advanced Profile Miscellaneous Configuration](#) on page 308

### **Advanced Client Load Balance Configuration**

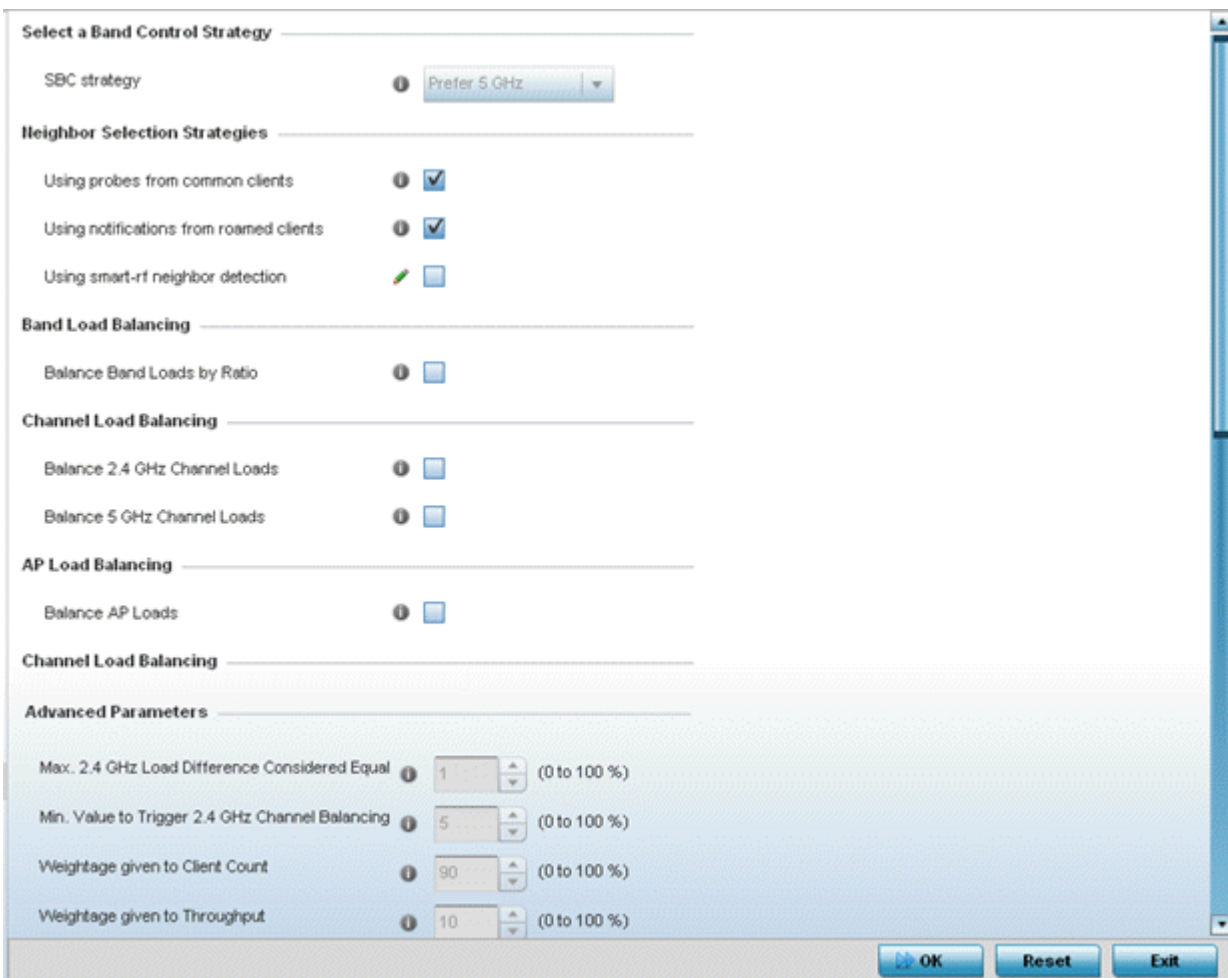
Set the ratios and calculation values used by access points to distribute client loads both among neighbor devices and the 2.4 and 5 GHz radio bands.

To define or override client load balance algorithms for access points:

- 1 Select **Configuration > Devices > Profile Overrides** from the web UI.
- 2 Select **Advanced** to expand its sub-menu items.



3 Select **Client Load Balancing**.



**Figure 149: Profile Overrides - Client Load Balancing Screen**

- 4 Use the **Group ID** field to define a group ID of up to 32 characters to differentiate this profile from others with similar configurations.
- 5 Use the **SBC strategy** 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 associates in the 5 GHz band only.

- 6 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 the Smart RF neighbor detection algorithm. This setting is enabled by default.

- 7 Enable **Balance Band Loads by Ratio** (in the **Band Load Balancing** field) to distribute an access point's client traffic load across both the 2.4 and 5 GHz radio bands.

- 8 Configure 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.

- 9 Enable **Balance AP Loads** (in the **AP Load Balancing** field) to distribute client traffic evenly among neighbor access points.
- 10 Set the following **Advanced** parameters:

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 weight 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 weight (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 weight (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 weight (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 weight (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 weight (from 1- 100%) applied to client throughput in an access point's overall load calculation. The default setting is 10%.

- 12 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%.

13 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 each other 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 among 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.

14 Click **OK** to save the changes made to the profile's advanced client load balance configuration

Click **Reset** to revert to the last saved configuration.

### Advanced MiNT Protocol 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 **Configuration > Devices > Profile Overrides** from the web UI.
- 2 Select **Advanced** to expand its sub-menu items.

3 Select **MiNT Protocol**.

The Settings tab displays by default.

The screenshot shows the 'Settings' tab of the 'Advanced Profile Overrides MiNT Screen'. The interface includes several sections with configuration options:

- Area Identifier:** Level 1 Area ID is set to 1 (ID) or \$ (Alias).
- Priority Adjustment:** Designated IS Priority Adjustment is 0 (-255 to 255); Control Priority is 1 (1 to 255).
- Shortest Path First (SPF):** Latency of Routing Recalculation is 0 (0 to 60 seconds).
- MINT Link Settings:** MLCP IP, MLCP IPv6, and MLCP VLAN are checked; Tunnel MiNT across extended VLAN is unchecked.
- Tunnel Controller Load Balancing:** Tunnel Controller Load Balancing (Level1) is unchecked.
- Inter Tunnel Bridging:** Inter Tunnel Bridging (Level2) is unchecked.
- Tunnel Controller Group:** Tunnel Controller Name is empty.

Buttons for 'OK', 'Reset', and 'Exit' are located at the bottom right.

**Figure 150: Advanced Profile Overrides MiNT Screen - Settings Tab**

- 4 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.
-----------------	--

- 5 Define or override the following **Priority Adjustments** settings in respect to devices supported by the profile:

Designated IS Priority Adjustment	Use the spinner control to set a Designated IS Priority Adjustment setting from -255 - +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.
-----------------------------------	---

- 6 Select the **Latency of Routing Recalculation** option (in the **Shortest Path First (SPF)** field) to enable the spinner control used for defining or overriding a latency period (from 0 - 60 seconds). The option is disabled by default.
- 7 Define or override the following **MiNT Link Settings** in respect to devices supported by the profile:

MLCP IP	Select this option to enable MiNT Link Creation Protocol (MLCP) by IP Address. MLCP is used to create 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 another access point with a path to the controller or service platform. This setting is enabled by default.
MLCP IPv6	Select this option to enable MLCP for automated MiNT UDP/IP link creation. This setting is enabled by default.
MLCP VLAN	Select this option to enable MiNT MLCP by VLAN. MLCP is used to create one VLAN 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.
Tunnel MiNT across extended VLAN	Select this option to tunnel MiNT protocol packets across an extended VLAN. This setting is disabled by default.

- 8 Select **Tunnel Controller Load Balancing (Level 1)** to enable load balancing through a WLAN tunnel controller. This setting is disabled by default.
- 9 Select **Inter Tunnel Bridging (Level 2)** to enable inter tunnel bridging. This setting is disabled by default.
- 10 Enter a 64-character maximum **Tunnel Controller Name** for this tunneled-WLAN-controller interface.
- 11 Enter a 64-character maximum **Preferred Tunnel Controller Name** to which this access point prefers to tunnel traffic over an extended VLAN..
- 12 Click **OK** to save the changes made to the MiNT protocol configuration. Click **Reset** to revert to the last saved configuration.

- 13 Select the IP tab to display the link IP network address information shared by the devices managed by the MiNT configuration.

	Settings	IP	VLAN	Rate Limits						
	IP	Routing Level	Listening Link	Port	Forced Link	Link Cost	Hello Packet Interval	Adjacency Hold Time	IPSec Secure	IPSec GW
+	192.168.	1	0	20	X	100	15s	46s	X	

Row Count: 1

Add Edit Delete Replace Exit

**Figure 151: Advanced Profile Overrides MiNT Screen - IP Tab**

The IP tab displays the IP address, Routing Level, Listening Link, Port, Forced Link, Link Cost, Hello Packet Interval, Adjacency Hold Time, IPSec Secure, and IPSec GW information that managed devices use to communicate securely with each other.

- 14 Click **Add** to create a new link IP configuration or **Edit** to override an existing configuration.

**Figure 152: Advanced Profile Overrides MiNT Screen - Add IP MiNT Link**

- 15 Set the following **Link IP** parameters for 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 list to select the type of IP address provided. The available choices are <b>IPv4 Address</b> and <b>IPv6 Address</b> .
Port	To specify a custom port for MiNT links, select this option and use the spinner control to define or override the port number from 1 - 65,535.
Routing Level	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 does not 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	Select this option to specify the MiNT link as a forced link.
Link Cost	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	Select this option to use a secure link for IPSec traffic. This setting 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.

- 16 Click **OK** to save the changes made to the MiNT protocol network address configuration.  
Click **Reset** to revert to the last saved configuration.
- 17 Select the VLAN tab to display the link IP VLAN information shared by the access points managed by the MiNT configuration.

Settings IP VLAN Rate Limits					
VLAN	Routing Level	Link Cost	Hello Packet Interval	Adjacency Hold Time	
+	1	1	10	4s	13s
+	103	1	10	10s	10s

Type to search in tables Row Count: 2

**Figure 153: Advanced Profile Overrides MiNT Screen - VLAN Tab**

The VLAN tab displays the VLAN, Routing Level, Link Cost, Hello Packet Interval, and Adjacency Hold Time managed devices use to communicate securely with each another.



- 18 Click **Add** to create a new VLAN link configuration or **Edit** to override an existing configuration.

**Figure 154: Advanced Profile Overrides MiNT Screen - Add/Edit VLAN**

- 19 Set the following **VLAN** parameters for the MiNT configuration:

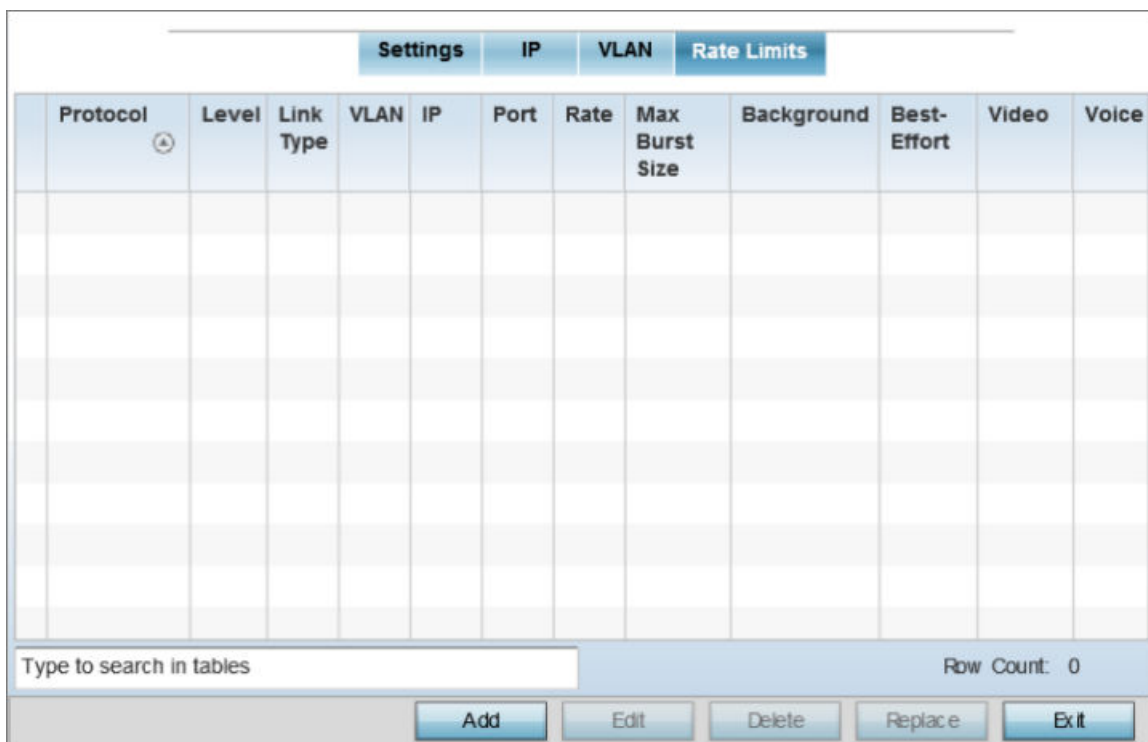
VLAN	Define a VLAN ID from 1 - 4094 used by peer controllers for interoperation when supporting the MiNT protocol
Routing Level	Define or override a routing level of either 1 or 2.
Link Cost	Use the spinner control to define or override a link cost from 1 - 10,000. The default value is 100.
Hello Packet 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 Click **OK** to save the changes made to the MiNT protocol configuration.  
Click **Reset** to revert to the last saved configuration.

21 Select the Rate Limits tab.

The Rate Limits tab displays 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 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). Existing rate limit configurations display along with their virtual connection protocols and data traffic QoS customizations.



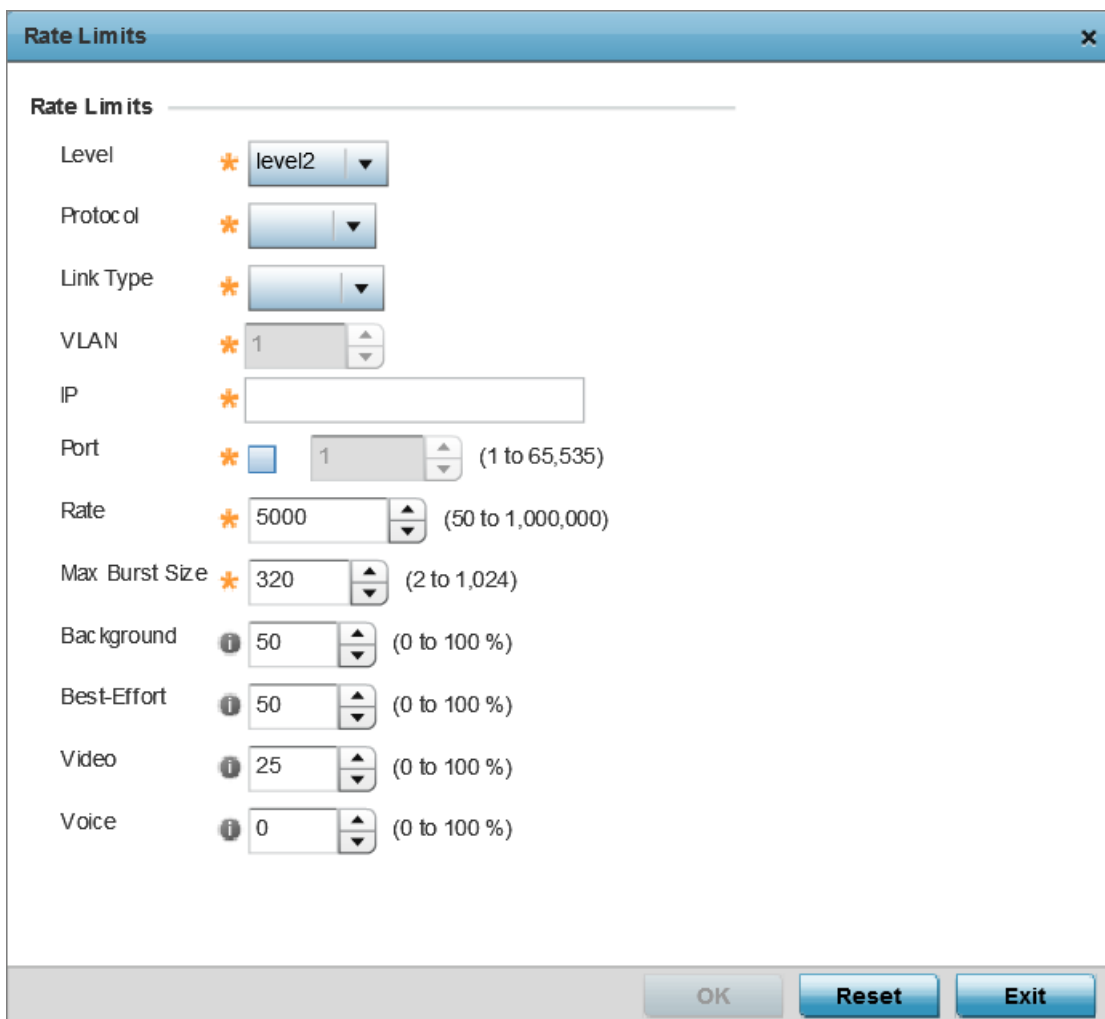
Protocol	Level	Link Type	VLAN	IP	Port	Rate	Max Burst Size	Background	Best-Effort	Video	Voice

Type to search in tables Row Count: 0

Add Edit Delete Replace Exit

**Figure 155: Advanced Profile Overrides MINT Screen - Rate Limits Tab**

22 Click **Add** to create a new MiNT rate limiting configuration or **Edit** to override an existing configuration.



**Figure 156: Advanced Profile Overrides MiNT Screen - Add/Edit Rate Limit**

23 Set the following **Rate Limits** to complete the MiNT configuration:

Level	Select <b>level2</b> to apply rate limiting for all links on level 2.
Protocol	Select either <b>mlcp</b> or <b>link</b> 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 <b>link</b> to rate limit using statically configured MiNT links.
Link Type	Select either <b>VLAN</b> , to configure a rate limit configuration on a specific virtual LAN, or <b>IP</b> to set rate limits on a static IP address/port configuration.
VLAN	When <b>Protocol</b> is set to <b>link</b> and <b>Link Type</b> is set to <b>VLAN</b> , select a virtual LAN from 1 - 4094 to refine the rate limiting configuration to a specific VLAN.
IP	When <b>Protocol</b> is set to <b>link</b> and <b>Link Type</b> is set to <b>VLAN</b> , enter the IP address as the network target for rate limiting.



Port	When <b>Protocol</b> is set to <b>link</b> and <b>Link Type</b> is set to <b>VLAN</b> , 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	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	Configure 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	Configure 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	Configure 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	Configure 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 Click **OK** to save the changes made to the MiNT protocol rate limit configuration.

Click **Reset** to revert to the last saved configuration.

### Advanced Profile Miscellaneous 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 an access point, controller, or service platform 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 the **Miscellaneous** screen.

To define or override a profile's miscellaneous configuration attributes:

- 1 Select **Configuration** > **Devices** > **Profile Overrides** from the web UI.
- 2 Select **Advanced** to expand its sub-menu items.
- 3 Select **Miscellaneous**.

The Settings tab displays by default.

**Device RADIUS Authentication Parameters**

NAS-Identifier Attribute

NAS-Port-Id Attribute

**LEDs (Light Emitting Diodes)**

Turn on LEDs  Off (0)  On (1)  Flash Pattern (2)

**MeshConnex Parameters**

Root Path Monitor Interval  Seconds (1 to 65,535)

**RADIUS Dynamic Authorization**

Additional Port  (1 to 65,535) (Cisco ISE:1700)

OK Reset

**Figure 157: Advanced Profile Overrides - Miscellaneous Screen**

- 4 Set a **NAS-Identifier Attribute** up to 253 characters in length.  
This is the RADIUS NAS-Identifier attribute that typically identifies where a RADIUS message originates.
- 5 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.
- 6 Select **Turn on LEDs**, in the **LEDs (Light Emitting Diodes)** section, to enable the LEDs on an access point.  
This parameter is not available for controllers or service platforms.
- 7 Select **Flash Pattern(2)**, in the **LEDs (Light Emitting Diodes)** section, to flash an access point's LEDs in a distinct manner (different from its operational LED behavior).  
With this option enabled, an administrator can verify that an access point has received its configuration from its managing controller or service platform (perhaps remotely at the site of deployment) without having to log into the managing controller or service platform. This feature is disabled by default.
- 8 Select **Capable**, in 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.

- 9 Select **Priority**, in 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 you select, the higher the priority in the RF Domain manager election process.
- 10 Configure a **Root Path Monitor Interval** (from 1 - 65,535 seconds) to specify how often to check if the mesh point is up or down.
- 11 Set the **Additional Port** value, in the **RADIUS Dynamic Authorization** section, to enable a Cisco Identity Services Engine (ISE) Authentication, Authorization and Accounting (AAA) server to dynamically authenticate a client.  
The allowed port range is 1 to 65,535.

When a client device requests access to the network, the Cisco ISE RADIUS 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). The check verifies, for example, that the device's anti-virus or anti-spyware software is valid. If the device complies, it is allowed access to the network.

- 12 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.

- 13 Click **OK** to save the changes made to the profile's advanced miscellaneous configuration.  
Click **Reset** to revert to the last saved configuration.

## Auto-Provisioning Policies

Wireless devices can adopt and manage other wireless devices. For example, a wireless controller can adopt any number of access points. When a device is adopted, the device configuration is provisioned by the adopting device. Since multiple configuration policies are supported, an adopting device needs to define which configuration policies are used for a given adoptee. **Auto-Provisioning Policies** determine which configuration policies are applied to an adoptee based 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:

## Configuring an Auto-Provisioning Policy

Auto-Provisioning Policies can be created or modified as unique deployment requirements dictate changes in the number of access point radios within a specific radio coverage area.

### Rules

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.

The screenshot shows the 'Auto-Provisioning Policy' configuration page for a policy named 'mypolicy'. The 'Rules' tab is active, displaying a table with 12 rows of rule configurations. Each row includes a 'Rule Precedence' value, an 'Operation' (all are 'allow'), a 'Device Type', a 'Match Type', two 'Argument' fields (MAC addresses), an 'RF Domain Name', and a 'Profile Name'. The 'Row Count' is 20. At the bottom, there are buttons for 'Add', 'Edit', 'Delete', and 'Exit'.

Rule Precedence	Operation	Device Type	Match Type	Argument 1	Argument 2	RF Domain Name	Profile Name
1	allow	ap71xx	MAC Address	00-23-68-0F-40-6	00-23-68-0F-40-68	rf 2	RF2 Profile
3	allow	ap6511	Any			rf 3	default-ap6511
4	allow	ap6532	MAC Address	00-23-68-31-18-E	00-23-68-31-18-E0	rf 2	default-ap6532
5	allow	ap6532	MAC Address	5C-0E-8B-34-50-3	5C-0E-8B-34-50-3C	rf 1	default-ap6532
6	allow	ap6521	MAC Address	5C-0E-8B-08-73-A	5C-0E-8B-08-73-A	rf 4US	default-ap6521
7	allow	ap71xx	MAC Address	00-23-68-8F-C3-9	00-23-68-8F-C3-94	rf US	default-ap71xx
8	allow	ap71xx	MAC Address	5C-0E-8B-0E-3C-4	5C-0E-8B-0E-3C-4	rf 2	RF2 Profile
9	allow	ap6532	MAC Address	5C-0E-8B-34-78-5	5C-0E-8B-34-78-54	mesh domain	meshpoint-profile
10	allow	ap6532	MAC Address	5C-0E-8B-34-71-1	5C-0E-8B-34-71-1E	mesh domain	meshpoint-profile
11	allow	ap6532	MAC Address	5C-0E-8B-33-B4-2	5C-0E-8B-33-B4-2E	mesh domain	meshpoint-profile
12	allow	ap71xx	MAC Address	00-15-70-88-93-6	00-15-70-88-93-64	rf 2	RF2 Profile

- 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:

<b>Rule Precedence</b>	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.
<b>Operation</b>	Lists the operation taken upon receiving an adoption request from an access point: The following operations are available: <i>allow</i> - Allows the normal provisioning of connected access points upon request. <i>deny</i> - Denies (prohibits) the provisioning of connected access point upon request. <i>redirect</i> - 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. <i>upgrade</i> - Conducts the provisioning of requesting access points from this controller resource.

<b>Device Type</b>	Sets the access point model for which this policy applies. Adoption rules are specific to the selected model. access point models have different radio configurations. AP 7131N models can house a maximum of three radios, all other models have two radios with the exception of AP 6511 and AP 6521 models that utilize a single radio.
<b>Match Type</b>	Lists the matching criteria used in the policy. This is like a filter and further refines the APs available for adoption. The Match Type can be one of the following: <i>MAC Address</i> – The filter type is a MAC Address of the selected access point model. <i>IP Address</i> – The filter type is the IP address of the selected access point model. <i>VLAN</i> – The filter type is a VLAN. <i>Serial Number</i> – The filter type is the serial number of the selected access point model. <i>Model Number</i> – The filter type is the access point model number. <i>DHCP Option</i> – The filter type is the DHCP option value of the selected access point model.
<b>Argument 1</b>	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.
<b>Argument 2</b>	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.
<b>RF Domain Name</b>	Sets the name of the RF Domain to which the device is adopted automatically. Select the <i>Create</i> icon to define a new RF Domain configuration or select the <i>Edit</i> icon to revise an existing configuration.
<b>Profile Name</b>	Defines the name of the profile used when the Auto-Provisioning Policy is applied to a device. Select the <i>Create</i> icon to define a new Profile configuration or the <i>Edit</i> icon to revise an existing configuration. For more information, see <a href="#">General Profile Configuration</a> .

- 4 If a rule requires addition or modification, select either **Add** or **Edit** to define the required parameters using the **Rule** screen.



- 5 Specify the following parameters in the **Rule** screen:

<b>Operation</b>	<p>Define the operation taken upon receiving an adoption request from an access point: the following operations are available:</p> <p><i>Allow</i> - Allows the normal provisioning of connected access points upon request.</p> <p><i>Deny</i> - Denies (prohibits) the provisioning of connected access point upon request.</p> <p><i>Redirect</i> - When selected, an access point seeks a steering controller (upon adoption request), will forward the network credentials of a designated controller resource that initiates the provisioning process.</p> <p><i>Upgrade</i> - Conducts the provisioning of requesting access points from this controller resource.</p>
<b>Device Type</b>	<p>Set the access point model for which this policy applies. Adoption rules are specific to the selected model.</p>
<b>Match Type</b>	<p>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:</p> <p><i>MAC Address</i> - The filter type is a MAC Address of the selected access point model.</p> <p><i>IP Address</i> - The filter type is the IP address of the selected access point model.</p> <p><i>VLAN</i> - The filter type is a VLAN.</p> <p><i>Serial Number</i> - The filter type is the serial number of the selected access point model.</p> <p><i>Model Number</i> - The filter type is the access point model number.</p> <p><i>DHCP Option</i> - The filter type is the DHCP option value of the selected access point model.</p>

<b>RF Domain Name</b>	Set the RF Domain to which the device is adopted automatically. Select the <i>Create</i> icon to define a new RF Domain configuration or select the <i>Edit</i> icon to revise an existing configuration. For more information, see <a href="#">General Profile Configuration</a> .
<b>Profile Name</b>	Define the profile used when an Auto-Provisioning Policy is applied to a device. Select the <i>Create</i> icon to define a new Profile configuration or select the <i>Edit</i> icon to revise an existing configuration. For more information, see <a href="#">General Profile Configuration</a> .
<b>Area</b>	Enter a 64 character maximum deployment area name assigned to this policy.
<b>Floor</b>	Enter a 32 character maximum deployment floor name assigned to this policy.
<b>1st Controller</b>	When redirect is selected as the operation, provide a 1st choice steering controller <i>Hostname</i> or <i>IP Address</i> and port to forward network credentials for a controller resource to initiate the provisioning process.
<b>2nd controller</b>	When redirect is selected as the operation, provide a 2nd choice steering controller <i>Hostname</i> or <i>IP Address</i> and port to forward network credentials for a controller resource to initiate the provisioning process.
<b>Routing Level</b>	When redirect is selected as the operation, specify the routing level as <i>1</i> or <i>2</i> .

### Default

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.
- 3 Select the **Default** tab to define the Auto-Provisioning Policy's rule matching adoption configuration.

The screenshot shows the 'Auto-Provisioning Policy' configuration window for a policy named 'mypolicy'. The window has a title bar with a question mark icon. Below the title bar, there are two tabs: 'Rules' and 'Default', with 'Default' being the active tab. The main content area is titled 'Auto-Provisioning Default' and contains a single configuration option: 'Adopt if No Rules Match' with an information icon and a checked checkbox. At the bottom of the window, there are three buttons: 'OK', 'Reset', and 'Exit'.

- 4 Select the **Adopt if No Rules Match** option to adopt when no matching filter rules apply. This setting is disabled by default.
- 5 Select **OK** to save the updates to the Auto-Provisioning Policy screen. Selecting **Reset** reverts the screen to the last saved configuration.

## Managing an Event Policy

**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. 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.

Existing policies can have their event notification configurations modified as device profile requirements warrant.

To define an event policy configuration:

- 1 Select **Configuration > Devices > Event Policy**.

Event Name	SNMP <input checked="" type="checkbox"/>	Syslog <input checked="" type="checkbox"/>	Forward to Controller <input type="checkbox"/>	Email Notification <input type="checkbox"/>

- 2 Ensure the **Activate Event Policy** button is selected to enable the screen for configuration. This option needs to remain selected to apply the event policy configuration to the access point profile.
- 3 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.
- 4 Review each event and select (or deselect) the *SNMP*, *Syslog*, *Forward to Switch* 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.

- 5 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration. **Delete** obsolete rows as needed.

## Managing MINT Policies

To add or modify a MINT Policy:

- 1 Select **Devices > MINT Policy** to display the MINT Policy screen.

The screenshot shows the 'Mint Policy' configuration window. It has a title bar with a question mark icon. Below the title bar is a 'Settings' section with three rows of configuration options, each with an information icon on the left and a range in parentheses on the right:

- Level 2 Area ID:** A text box containing '1' and a range of '(1 to 16,777,215)'.
- MTU:** A text box containing '1500' and a range of '(900 to 1,500)'.
- UDP/IP Encapsulation Port:** A text box containing '24576' and a range of '(2 to 65,534)'.

At the bottom of the window are three buttons: 'OK', 'Reset', and 'Exit'.

- 2 Configure the following parameters to configure the MINT policy:

<b>Level 2 Area ID</b>	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.
<b>MTU</b>	Specify a MTU value for the mint policy between 900 and 1,500. The MTU setting specifies the maximum packet size 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.
<b>UDP/IP Encapsulation Port</b>	Specify the port to use for UDP/IP encapsulation between 2 and 65,534. This value specifies an alternate UDP port used by mint packets (and must be an even number). This port is used by mint control packets, and this port's value plus 1 is 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

Wireless LAN Policies  
WLAN QoS Policies  
Radio QoS Policies  
Association ACL  
Smart RF Policies  
MeshConnex Policies  
Mesh QoS Policy  
Passpoint Policy  
Sensor Policy

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 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 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 provide 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.

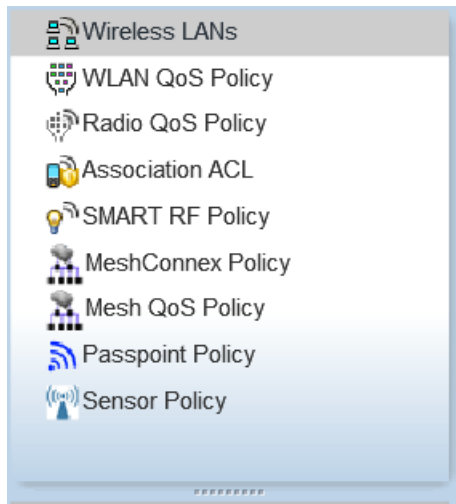
RFS 4000 model controllers support a maximum of 32 WLANs. NX 7500 model service platforms support up to 256 WLANs. An NX 9000 Series service platform (NX 9500, NX 9510, or NX 9600) supports up to 1000 WLANs. Access points can support a maximum of 16 WLANs per model.

The wireless configuration is comprised the following policies:

- [Wireless LAN Policies](#) on page 318
- [Configuring WLAN QoS Policies](#)
- [Radio QoS Policy](#)
- [Association ACL](#)

- [Smart RF Policy](#)
- [MeshConnex Policy](#)
- [Mesh QoS Policy](#)
- [Passpoint Policy](#)
- [Sensor Policy](#) on page 435

WLAN policies can be separately selected and refined in the **Configuration > Wireless** pane located on the top left-hand side of the UI.



**Figure 158: Configuration > Wireless Pane**

## Wireless LAN Policies

To review the attributes of existing WLANs (policies) and, if necessary, modify their configurations:

- 1 Select **Configuration > Wireless > Wireless LANs** to display existing WLANs.

WLAN	SSID	Description	WLAN Status	VLAN Pool	Bridging Mode	DHCP Option 82	DHCPv6 LDRA	Authentication Type	Encryption Type	QoS Policy	Association ACL
ccmp_enc	ccmp		✓ Enabled	1	Local	✗	✗	None	CCMP	default	
eapauth	eapauth		✓ Enabled	1	Local	✗	✗	EAP	CCMP	default	
open	open		✓ Enabled	1	Local	✗	✗	None	None	default	

Type to search in tables Row Count: 3

**Figure 159: Wireless LANs Screen**

2 Refer to the following (read only) information to assess the attributes of the each WLAN available:

WLAN	Displays the name of each available WLAN. Individual WLANs can be selected and their SSID and client management properties modified. RFS 4000 series wireless controllers support a maximum of 32 WLANs. The NX 7500 service platforms support up to 256 WLANs.
SSID	Displays the name of the SSID assigned to the WLAN when created or last modified. Optionally, select a WLAN and click <b>Edit</b> 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 <i>Active</i> or <i>Shutdown</i> . 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 is not available for clients to associate.
VLAN Pool	Lists each WLAN's current VLAN mapping. Mapping a WLAN to more than one VLANs is permitted. 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	Lists each WLAN's current bridging mode as either <b>Local</b> or <b>Tunnel</b> .
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.
Authentication Type	Displays the name of the user authentication scheme each listed WLAN is using to secure its client membership transmissions. <i>None</i> is listed if authentication is not used within this WLAN. Refer to the <b>Encryption type</b> 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 type each listed WLAN is using to secure its client membership transmissions. <b>None</b> is listed if encryption is not used within this WLAN. Refer to the <b>Authentication</b> column to verify that 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 connection between wireless clients and 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](#) on page 320
- [Configuring WLAN Security](#) on page 323
- [Configuring WLAN Firewall Settings](#) on page 342
- [Configuring WLAN Client Settings](#) on page 350
- [Configuring WLAN Accounting Settings](#) on page 354
- [Configuring WLAN Service Monitoring Settings](#) on page 356

- [Configuring Client Load Balancing Settings](#) on page 358
- [Configuring Advanced WLAN Settings](#) on page 360
- [Configuring Auto Shutdown Settings](#) on page 366

## Basic WLAN Configuration

When creating or modifying a WLAN, the **Basic Configuration** screen is the first screen that displays as part of the WLAN configuration screen flow. Use this screen to enable a WLAN and to and define its SSID, client behavior, and VLAN assignments.

To define a WLAN's basic configuration:

- 1 Select **Configuration > Wireless**.
- 2 Select **Wireless LAN Policy** to display a high-level display of the existing WLANs.
- 3 Select **Add** to create an additional WLAN, or select an existing WLAN then click **Edit** to modify its properties.

RFS 4000 controllers support a maximum of 32 WLANs. An NX 95XX & NX 96XX series service platform supports up to 1000 WLANs. Access points support a maximum of 16 WLANs per model.



**WLAN Configuration**

SSID: sanjose

Description: San Jose Office WLAN

WLAN Status:  Disabled  Enabled

QoS Policy: default

Bridging Mode: Local

DHCP Option 82:

DHCPv6 LDRA:

Bonjour Gateway Discovery Policy:

**Other Settings**

Broadcast SSID:

Answer Broadcast Probes:

**VLAN Assignment**

Single VLAN  VLAN Pool

VLAN:

**RADIUS VLAN Assignment**

Allow RADIUS Override:

**URL Filter**

URL Filter:

OK Reset Exit

**Figure 160: WLAN Basic Configuration Screen**

- 4 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 or characters are not permitted. The name could be a logical representation of the WLAN support function (engineering, marketing etc.). If editing an existing WLAN, the WLAN's name appears at the top of the screen and cannot be modified. A WLAN 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 <b>Enabled</b> radio button to make this WLAN active and available to clients on all radios where it has been mapped. Select the <b>Disabled</b> radio button to make this WLAN inactive, meaning even if the WLAN is mapped to radios, it is 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 <i>Create</i> icon to define a new QoS policy or select the <i>Edit</i> 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 <a href="#">WLAN QoS Policies</a> on page 367.
Bridging Mode	Use the drop-down menu to specify a bridging mode for the WLAN. Available bridging policy modes are <b>Local</b> , <b>Tunnel</b> or <b>split-tunnel</b> .
DHCP Option 82	Select this option to enable DHCP option 82. DHCP Option 82 provides additional information about the physical attachment of a client. 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.

- 5 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.

- 6 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 <b>Single VLAN</b> radio button to assign just one VLAN to this WLAN. Enter the name of the VLAN within the VLAN parameter field when the <b>Single VLAN</b> 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 <b>VLAN Pool</b> 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 <b>+ Add Row</b> button to add additional VLANs to the WLAN.

- 7 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 returns VLAN-ID is ignored and the VLAN configuration (defined earlier) is used.
- 8 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.

- 9 Select **OK** when completed to update the WLAN's basic configuration. Select **Reset** to revert the screen to the last saved configuration.

## Configuring WLAN Security

A WLAN can be assigned a security policy supporting authentication, captive portal or encryption schemes.

**Select Authentication**

EAP  EAP-PSK  EAP-MAC  MAC  PSK / None

AAA Policy

Reauthentication  (30 to 86,400)

---

**Captive Portal**

Enforcement  Captive Portal Enable Captive Portal if Primary Authentication Fails

Captive Portal Policy

---

**Passpoint Policy**

Passpoint Policy

---

**Registration**

Type of Registration

Radius Group Name

Expiry Time  (1 to 43,800 hours)

Agreement Refresh  (0 to 144,000 minutes)

---

**External Controller**

Enable  Follow AAA

Host

Send Mode

---

**Select Encryption**

OK Reset Exit

**Figure 161: WLAN Security Screen**

Authentication ensures that 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](#)
- [WLAN Security 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](#) 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](#).

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](#)

### 802.1x EAP, EAP-PSK and EAP MAC

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 an 802.1X capable RADIUS server to authenticate users and a 802.1X client installed on each device 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 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
- 3 Select **Security**.
- 4 Select **EAP, EAP-PSK or EAP-MAC** as the **Authentication Type**.

Each option enables the radio buttons for various encryption mechanisms as an additional measure of WLAN security.



**Figure 162: EAP, EAP-PSK or EAP MAC Authentication Screen**

- 5 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** option to force EAP supported clients to reauthenticate.  
Use the spinner control set the number of seconds (between 30 - 86,400) that, when exceeded, forces the EAP supported client to reauthenticate to use the WLAN.
- 7 Select **OK** when completed to update the WLAN's EAP configuration.  
Select **Reset** to revert to the last saved configuration.

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.

### *MAC Authentication*

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 access restrictions based on time and date.

MAC authentication can only validate devices, not users. MAC authentication only references a client's 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 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. For information on defining a new AAA policy that can be applied to the WLAN supporting MAC, see [AAA Policy](#).

- 2 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 to use the resources supported by the controller, service platform or Access Point WLAN.
- 3 Select **OK** when completed to update the WLAN's MAC configuration. Select **Reset** to revert the screen back to the last saved configuration.

- 1 Select **Configuration > Wireless > Wireless LAN Policy** to display available WLANs.
- 2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
- 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 163: MAC Authentication Screen**

- 5 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** option to force EAP supported clients to reauthenticate. Use the spinner control set the number of seconds (between 30 - 86,400) that, when exceeded, forces the EAP supported client to reauthenticate to use the WLAN.
- 7 Select **OK** when completed to update the WLAN's MAC configuration. Select **Reset** to revert to the last saved configuration.

*PSK / None*

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.

Such a security-free convention may be appropriate in certain guest networks wherein no proprietary information purposely exposed to requesting clients, and their access to the controller, service platform or Access Point managed network is temporary and closely administrated.



**Figure 164: PSK / None Settings Screen**

**Note**

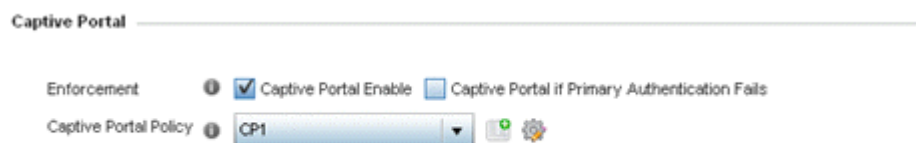
Although **None** implies no authentication, this option is also used when pre-shared keys are used for encryption (thus the PSK in the description).

*Captive Portal*

A captive portal is guest access policy for providing guests temporary and restrictive access to the 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 777.

To assign a captive portal policy to a WLAN:

- 1 Select **Configuration > Wireless > Wireless LAN Policy** to display available WLANs.
- 2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
- 3 Select **Security**.
- 4 Refer to the **Captive Portal** section in the WLAN Policy security screen.



**Figure 165: WLAN Policy Security Screen - Captive Portal Field**

- 5 Select **Captive Portal Enable** if authenticated guest access is required with the selected WLAN. This feature is disabled by default.



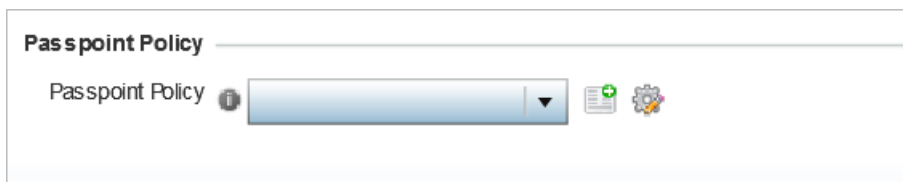
- 6 Select **Captive Portal if Primary Authentication Fails** to enable the captive portal policy if the primary authentication is unavailable.  
This option is enabled only when **Captive Portal Enable** is selected.
- 7 Select the **Captive Portal Policy** to use with the WLAN from the drop-down menu.  
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 777.
- 8 Select **OK** when completed to update the WLAN's captive portal configuration.  
Select **Reset** to revert to the last saved configuration.

### Passpoint

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.

To assign a passpoint policy to a WLAN:

- 1 Select **Configuration > Wireless > Wireless LAN Policy** to display available WLANs.
- 2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
- 3 Select **Security**.
- 4 Refer to the **Passpoint** field in the WLAN Policy security screen.



**Figure 166: 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 on Passpoint Policy, see [Passpoint Policy](#) on page 424.
- 6 Select **OK** when completed to update the WLAN's passpoint policy configuration.  
Select **Reset** to revert to the last saved configuration.

### Registration

Registration requires the validation of devices by address to continue the authentication process.

To assign Registration to a WLAN:

- 1 Select **Configuration > Wireless > Wireless LAN Policy** to display available WLANs.
- 2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
- 3 Select **Security**.

- 4 Refer to the **Registration** field in the WLAN security screen.

**Figure 167: 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.

- 6 Enter a 64 character maximum RADIUS Group Name to which the registering user associates. When left blank, devices are not associated with a RADIUS group.
- 7 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.
- 8 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.
- 9 Select **OK** when completed to update the WLAN's registration settings. Select **Reset** to revert to the last saved configuration.

### *External Controller*

To set the WLAN's external controller or service platform security configuration:

- 1 Select **Configuration > Wireless > Wireless LAN Policy** to display available WLANs.
- 2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
- 3 Select **Security**.

- 4 Refer to the **External Controller** section in the WLAN Policy security screen.

**Figure 168: WLAN Policy Security Screen - External Controller Field**

- 5 Select the **Enable** option if WLAN authentication is to be handled using an external resource. This feature is disabled by default.
- 6 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**

For EGuest deployment, the authenticating and accounting server specified in the AAA policy should point to the EGuest server host.

- 7 If using an external resource, use the drop-down menu to select either **Hostname** or **IP Address**, and enter the server information in the **Host** field. Hostnames cannot include the underscore character.
- 8 Select the Send Mode as either **UDP**, **HTTP** or **HTTPS**. The default setting is **UDP**.
- 9 Select **OK** when completed to update the WLAN's external controller configuration. Select **Reset** to revert to the last saved configuration.

### TKIP-CCMP

Wi-Fi Protected Access (WPA) is an encryption scheme specified in the IEEE Wireless Fidelity (Wi-Fi) standard 802.11i. WPA provides more sophisticated data encryption than WEP. WPA is designed for corporate networks and small-business environments where more wireless traffic allows quicker discovery of encryption keys by an unauthorized person.

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.

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.

To configure TKIP-CCMP encryption on a WLAN:

- 1 Select **Configuration > Wireless > Wireless LAN Policy** to display available WLANs.
- 2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
- 3 Select **Security**.
- 4 Select the **TKIP-CCMP** check box from within the **Select Encryption** field.

The screen populates with the parameters required to define a TKIP-CCMP configuration for the WLAN.

**Figure 169: WLAN Security - 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 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, a wireless client can use two 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 interval from 30 - 86,400 seconds. 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 and decrypting broadcast traffic is alternatively rotated based on the defined interval. Define a broadcast key transmission interval from 30 - 86,400 seconds. Key rotation enhances the broadcast traffic security on the WLAN. This feature is disabled by default.

- 7 Set the following **Advanced** settings for the TKIP-CCMP encryption scheme:

TKIP Countermeasure Hold Time	The <b>TKIP Countermeasure Hold Time</b> is the time a 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 1 second.
Exclude WPA2-TKIP	Select this option to advertise and enable support for only WPA-TKIP. This option can be used if certain older clients are not compatible with 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. We recommend that you enable 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 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 to the last saved configuration.

Before defining a WPA-TKIP supported configuration on a WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Enable TKIP for legacy device support only when WPA2-CCMP support is not available.
- Although TKIP offers better security than WEP, it can be vulnerable to certain attacks.
- When both TKIP and CCMP are enabled, a mix of clients are allowed to associate with the WLAN. Some use TKIP, others use CCMP. Because broadcast traffic needs to be understood by all clients, the broadcast encryption type in this scenario is TKIP.

### WPA2-CCMP

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 a controller, service platform or Access Point provides for its connected clients.

To configure WPA2-CCMP encryption on a WLAN:

- 1 Select **Configuration > Wireless > Wireless LAN Policy** to display available WLANs.

- 2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
- 3 Select **Security**.
- 4 Select the **WPA2-CCMP** check box from within the **Select Encryption** field.

The screen populates with the parameters required to define a WPA2-CCMP configuration for the new or existing WLAN.

**Figure 170: WLAN Security - 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, a wireless client can use two 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 interval from 30 - 86,400 seconds. 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 and decrypting broadcast traffic is alternatively rotated based on the defined interval. Define a broadcast key transmission interval from 30 - 86,400 seconds. Key rotation enhances the broadcast traffic security on the WLAN. This feature is disabled by default.

- 7 Set the following **Advanced** settings for the WPA2-CCMP encryption scheme:

TKIP Countermeasure Hold Time	The <b>TKIP Countermeasure Hold Time</b> is the time a 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 1 second.
Exclude WPA2-TKIP	Select this option to advertise and enable support for only WPA-TKIP. This option can be used if certain older clients are not compatible with 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. We recommend that you enable 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 to the last saved configuration.

Before defining a WPA2-TKIP supported configuration on a 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.

#### WEP 64

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 802.1X 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 when clients are incapable of using more robust 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 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
- 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 new or existing WLAN.

**Figure 171: WLAN Security - WEP 64 Screen**

- 5 Configure the following WEP 64 settings:

Generate Keys	Specify a 4- to 32-character pass key and click <b>Generate</b> . 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 <b>Key #1-4</b> 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 <b>Show</b> displays a key in exposed plain text.
Restore Default WEP Keys	Select this button to restore the WEP algorithm to its default settings.

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 to the last saved configuration.

Before defining a WEP 64 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 be permitted access only to resources required by legacy devices.
- If WEP support is needed for WLAN legacy device support, 802.1X EAP authentication should also be configured in order for the WLAN to provide authentication and dynamic key derivation and rotation.

### WEP 128

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 and Keyguard use 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 recommended only when 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 or Keyguard 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 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
- 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 new or existing WLAN.

The screenshot shows the 'WLAN Security - WEP 128' configuration interface. At the top, under 'Select Encryption', the 'WEP 128' checkbox is checked, while others like 'WPA/WPA2-TKIP', 'WPA2-CCMP', 'WEP 64', and 'KeyGuard' are unchecked. Below this is a 'Generate Keys' section with a text input field and a 'Generate' button. The 'Key 1-4' section contains four rows, each with a text input field, a 'HEX' dropdown menu, and a 'Show' checkbox. To the right of these is a 'Transmit Key' radio button. At the bottom left is a 'Restore Default WEP Keys' button, and at the bottom right are 'OK', 'Reset', and 'Exit' buttons.

**Figure 172: WLAN Security - WEP 128 Screen**

- 5 Configure the following WEP 128 settings:

Generate Keys	Specify a 4- to 32-character pass key and click <b>Generate</b> . 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 <b>Key #1-4</b> fields 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 <b>Show</b> displays a key in exposed plain text.
Restore Default WEP Keys	Select this button to restore the WEP algorithm to its default settings.

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 to the last saved configuration.

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 be permitted access only to resources required by legacy devices.
- If WEP support is needed for WLAN legacy device support, 802.1X EAP authentication should also be configured in order for the WLAN to provide authentication and dynamic key derivation and rotation.

### Keyguard

Keyguard (a form of WEP) 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 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
- 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 new or existing WLAN.

The screenshot shows the 'Select Encryption' configuration window. At the top, there are checkboxes for 'WPA/WPA2-TKIP', 'WPA2-CCMP', 'WEP 128', 'KeyGuard' (checked), 'WEP 64', and 'Open'. Below this is a 'Generate Keys' section with a text input field and a 'Generate' button, with the instruction 'Enter 4 to 32 Characters'. Underneath is a section for four keys, each with a text input field, a dropdown menu set to 'HEX', a 'Show' checkbox, and a radio button for 'Transmit Key'. A 'Restore Default WEP Keys' button is located at the bottom left. At the bottom right are 'OK', 'Reset', and 'Exit' buttons.

**Figure 173: WLAN Security - Keyguard Screen**

## 5 Configure the following keyguard settings:

Generate Keys	Specify a 4- to 32-character pass key and click <b>Generate</b> . 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 keys manually configured as hexadecimal numbers.
Keys 1-4	Use the <b>Key #1-4</b> fields 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 <b>Show</b> displays a key in exposed plain text.
Restore Default WEP Keys	Select this button to restore the keyguard algorithm to its default settings. This might be necessary, for example, 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 to the last saved configuration.

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 largely limit its use of keyguard to those legacy devices only.

### *T5 Controller 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 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its security properties.
- 3 Select **Security**.

- 4 Refer to the **T5 PowerBroadband Security** field at the bottom of the screen.

**Figure 174: WLAN Security - 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 <b>Security Type and WEP Encryptions Type</b> 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 <b>static-wep</b> (default), <b>wpa-enterprise</b> , and <b>wpapersonal</b> .
WEP Encryption Type	If <b>static-wep</b> is selected as the <b>Encryption Type</b> , use this setting to apply either a WEP 64 or WEP 128 encryption algorithm to the T5 support WLAN configuration.
Encryption Type	If <b>wpa-enterprise</b> or <b>wpa-personal</b> is selected as the <b>Encryption Type</b> , use this setting to apply either a CCMP, TKIP or TKIP-CCMP encryption algorithm to the T5 controller WLAN security configuration.
HEX	If you are using <b>static-wep</b> , provide the 10-26 character Hex password used to derive the security key.
Passphrase	If you are using <b>static-wep</b> , 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.
Verison	If <b>wpa-enterprise</b> or <b>wpa-personal</b> is selected as the <b>Encryption Type</b> , 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 to the last saved configuration.

## Configuring WLAN Firewall Settings

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 *allowing* and *denying* data traffic in respect to administrator defined rules. For an overview of Firewalls, see [Wireless Firewall](#) on page 714.

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.

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 WLAN packet traffic.

Keep in mind that 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 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify the properties of an existing WLAN.

- 3 Select **Firewall** from the Wireless LAN Policy options..

The screenshot displays the 'WLAN Policy Firewall Screen' with the following sections and options:

- IP Firewall Rules**
  - Inbound IP Firewall Rules: <none>
  - Outbound IP Firewall Rules: <none>
  - Inbound IPv6 Firewall Rules: <none>
  - Outbound IPv6 Firewall Rules: <none>
- MAC Firewall Rules**
  - Inbound MAC Firewall Rules: <none>
  - Outbound MAC Firewall Rules: <none>
- Association ACL**
  - Association ACL: <none>
- Application Policy**
  - Application Policy: <none>
  - Enable Voice/Video Metadata:
  - Enable HTTP Metadata:
  - Enable SSL Metadata:
  - Enable TCP RTT:
- Trust Parameters**
  - ARP Trust:
  - Validate ARP Header Mismatch:
  - DHCP Trust:
- IPv6 Settings**
  - ND Trust:
  - Validate ND Header Mismatch:
  - DHCPv6 Trust:

**Figure 175: WLAN Policy Firewall Screen**

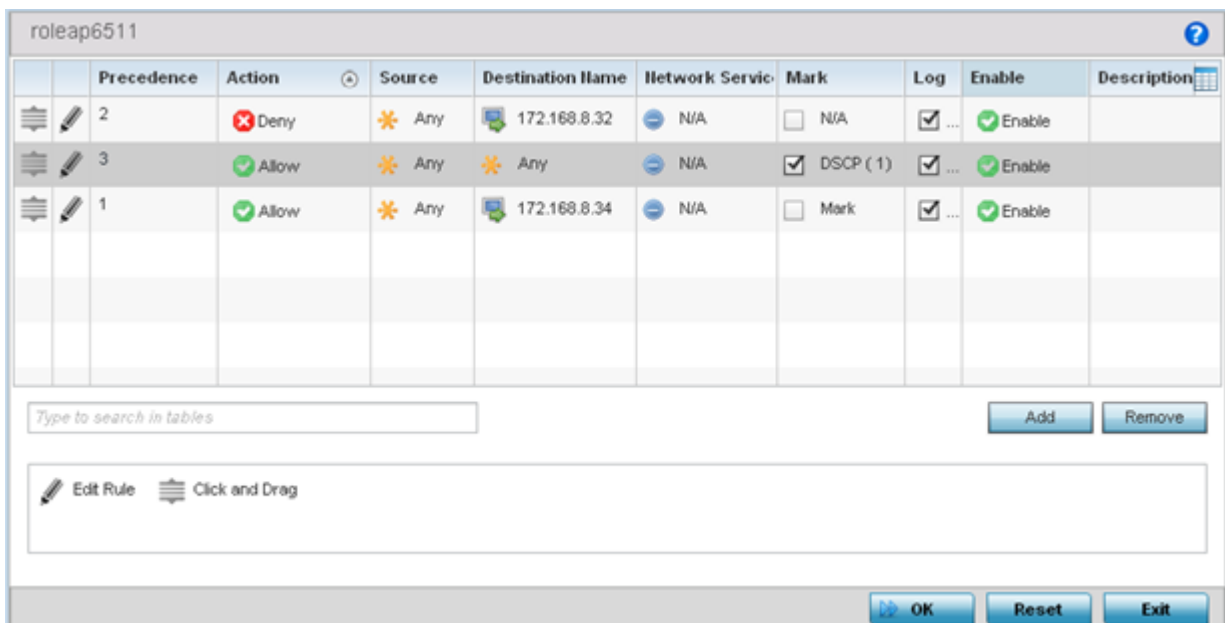
The screen displays editable fields for IP Firewall Rules, MAC Firewall Rules, Trust Parameters, and Client Deny Limits.

- 4 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.

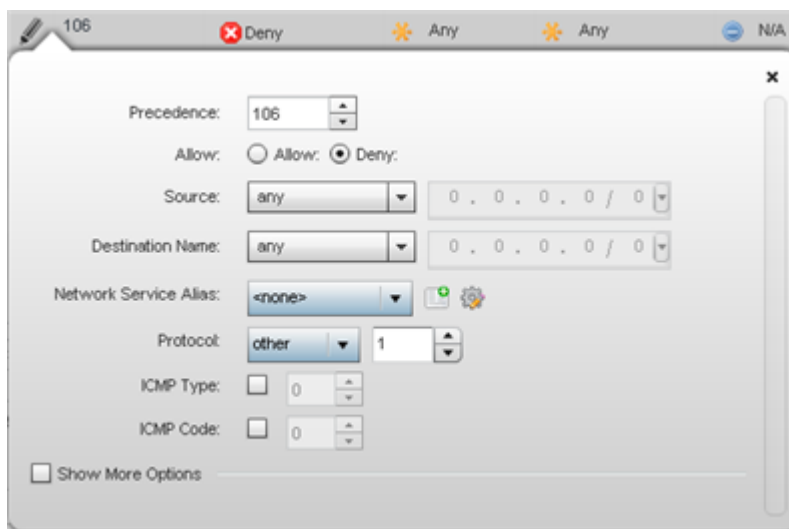
If you are creating a new IP firewall rule, provide a name up to 32 characters.

- 5 Click **Add**.



**Figure 176: IP Firewall Rules Screen**

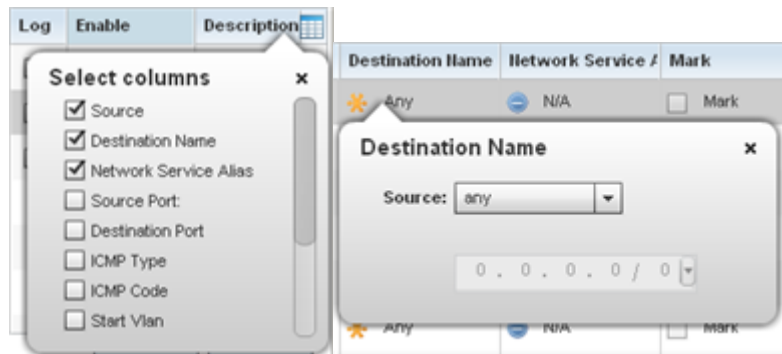
- 6 IP firewall rule configurations can either be modified as a collective group of variables or selected and updated individually as their filtering attributes require a more refined update.
- Select the **Edit Rule** icon to the left of a particular IP firewall rule configuration to update its parameters collectively.



**Figure 177: IP Firewall Rules Add Criteria Screen**



- b Click the icon in 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 178: 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:

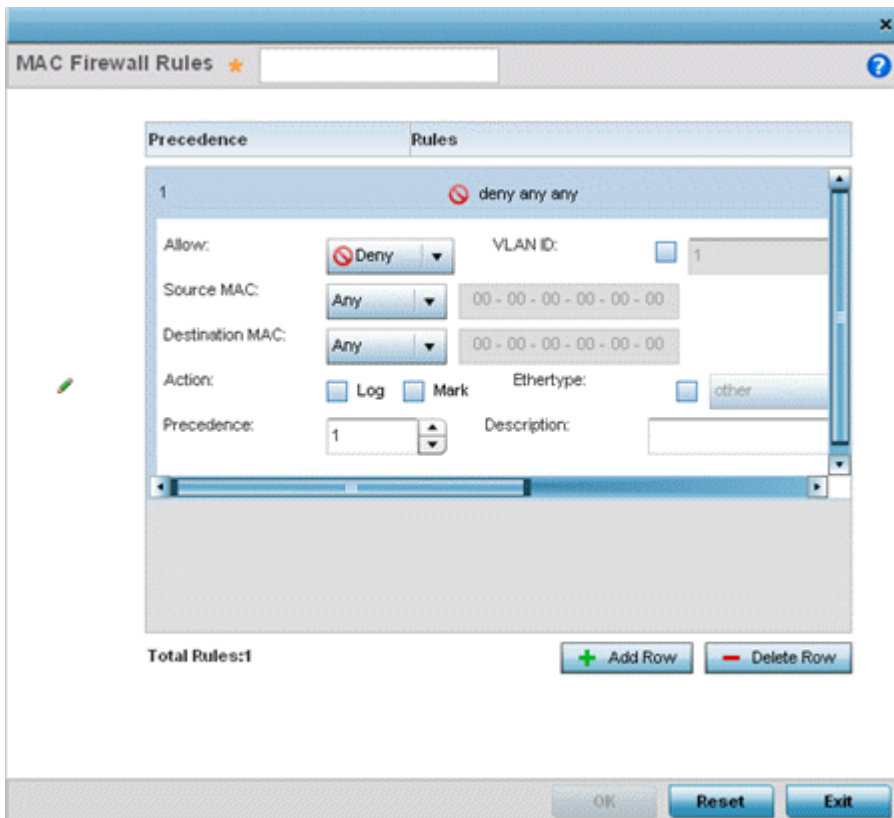
Precedence	Specify or modify a precedence for this IP policy between 1 and 5000. Rules with lower precedence are always applied to packets first. If you modify a precedence to apply a higher integer, it will move down the table to reflect its lower priority.
Action	Every IP Firewall rule is made up of matching criteria rules. The action defines what to do with the packet if it matches the specified criteria. The following actions are supported:  <b>Deny</b> Instructs the Firewall to prohibit a packet from proceeding to its destination  <b>Permit</b> 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 <b>DNS Match Type</b> 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 ( <b>any</b> ), are designated as a set of configurations consisting of protocol and port mappings (an <b>alias</b> ), set as a numeric IP address ( <b>host</b> ) or defined as <b>network IP and mask</b> . Selecting <b>alias</b> requires that 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 <b>tcp</b> or <b>udp</b> displays an additional set of specific TCP/UDP source and destination port options.
Source Port	If you are using either <b>tcp</b> or <b>udp</b> as the protocol, define whether the source port for incoming IP ACL rule application is <b>any</b> , <b>equals</b> , or an administrator defined range. If you are not using <b>tcp</b> or <b>udp</b> , this setting displays as N/A. This is the data local origination port designated by the administrator. Selecting <b>equals</b> invokes a spinner control for setting a single numeric port. Selecting <b>equals</b> invokes a spinner control for setting a single numeric port. Selecting <b>range</b> displays spinner controls for low and high numeric range settings. A source port cannot be a destination port.
Destination Port	If you are using either <b>tcp</b> or <b>udp</b> as the protocol, define whether the destination port for outgoing IP ACL rule application is <b>any</b> , <b>equals</b> , or an administrator defined range. If you are not using <b>tcp</b> or <b>udp</b> , this setting displays as N/A. This is the data destination virtual port designated by the administrator. Selecting <b>equals</b> invokes a spinner control for setting a single numeric port. Selecting <b>range</b> displays spinner controls for low and high numeric range settings. A source port cannot be a destination port.
ICMP Type	Selecting <b>ICMP</b> 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 <b>ICMP</b> 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, for example <i>0 - Net Unreachable</i> , <i>1 - Host Unreachable</i> , and <i>2 - Protocol Unreachable</i> .
Start VLAN	Select a <b>Start VLAN</b> 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 <b>End VLAN</b> 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 <b>Mark</b> 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 <b>Log</b> checkbox to enable or disable event logging for this rule's usage.
Enable	Select an IP Firewall rule's <b>Enable</b> or <b>Disable</b> 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 <b>Select Columns</b> 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 179: 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	<p>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:</p> <p><b>Deny</b> Instructs the Firewall to prohibit a packet from proceeding to its destination</p> <p><b>Permit</b> Instructs the Firewall to allow a packet to proceed to its destination</p>
VLAN ID	<p>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.</p>
Match 802.1P	<p>Configures IP DSCP to 802.1p priority mapping for untagged frames. Use the spinner control to define a setting between 0-7.</p>
Source and Destination MAC	<p>Enter both <b>Source</b> and <b>Destination</b> 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.</p>

Action	The following actions are supported:  <b>Log</b> Creates a log entry that a Firewall rule has allowed a packet to either be denied or permitted.  <b>Mark</b> Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit.  <b>Mark, Log</b> 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 <b>ipv6</b> , <b>arp</b> , <b>wisp</b> or <b>monitor 8021q</b> . 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 it from others with similar configurations.

12 If you are 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 <a href="#">Application</a> .
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 be determined only from calls that are established as 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 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 that 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 you are 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 <b>None</b> applies no consequence to an exceeded threshold.
Blacklist Duration	Select the check box and define a setting between 0 - 86,400 seconds. After 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 Click **OK** when completed to update this WLAN's Firewall settings.

Click **Reset** to revert the screen to its last saved configuration.

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.

## Configuring WLAN Client Settings

Each WLAN can maintain its own client setting configuration. These settings include wireless client inactivity timeouts and broadcast configurations.

To define a WLAN's unique client support configuration:

- 1 Select **Configuration > Wireless > Wireless LAN Policy** to display available WLANs.
- 2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its properties.
- 3 Select the Client Settings tab.

**Client Settings**

Enable Client-to-Client Communication	<input checked="" type="checkbox"/>
Wireless Client Power	20 (0 to 20 dBm)
Wireless Client Idle Time	30 Minutes (1 to 1,440)
Max Firewall Sessions per Client	10 (10 to 10,000)
Max Clients Allowed Per Radio	256 (0 to 256)
Radio Resource Measurement	<input type="checkbox"/>
Radio Resource Measurement Channel Report	<input checked="" type="checkbox"/>
Enforce Client Load Balancing	<input type="checkbox"/>
Enforce DHCP Client Only	<input type="checkbox"/>
Proxy ARP Mode	Dynamic
Proxy ND Mode	Dynamic
Enforce DHCP-Offer Validation	<input type="checkbox"/>

**WLAN Client Extensions**

Move Operations	<input type="checkbox"/>
Smart Scan	<input type="checkbox"/>
Symbol Information Element	<input checked="" type="checkbox"/>
WMM Load Information Element	<input type="checkbox"/>
Scan Assist	<input type="checkbox"/>
FT Aggregate	<input type="checkbox"/>
Channel Info Interval	8

**Figure 180: 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 (0 - 24), or Days (0 - 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 for 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 allows packets from clients only 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 <b>Strict</b> or <b>Dynamic</b> . Proxy ARP is the technique used by the access point 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** for the WLAN:

Move Operations	Select the check box to enable the use of Hyper-Fast Secure Roaming (HFSR) for clients on this WLAN. This feature applies only to certain client devices and is disabled by default.
Smart Scan	Enable a smart scan to refine a clients channel scans to just 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 (0-1), Hours (0-24), Minutes (1-1440), or Seconds (60-86,4000). The default setting is 1 hour.
VLAN Cache Timeout	Set a timeout period for the VLAN cache in Days (0-1), Hours (0-24), Minutes (1-1440), or Seconds (60-86,4000). The default setting is 1 hour.

- 9 Select **Controller Assisted Mobility** 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**, in 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 Click **OK** when completed to update the WLAN's client settings. Click **Reset** to revert the screen to the last saved configuration.

### *WLAN Client Setting Deployment Considerations*

Before defining client support settings for a controller, service platform, or access point managed WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- Clients on the same WLAN associated to an AP 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.
- Access points can support up to 256 clients per access point or radio.

## 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 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 > Wireless LAN Policy** to display available WLANs.
- 2 Click **Add** to create an additional WLAN, or select an existing WLAN and click **Edit** to modify its properties.
- 3 Select **Accounting**.

**Syslog Accounting**

Enable Syslog Accounting

Syslog Host  Hostname

Syslog Port 514

Proxy Mode None

Format Dash Delimiter (aa-bb-cc-dd-ee-ff)

Case Uppercase

**RADIUS Accounting**

Enable RADIUS Accounting

OK Reset Exit

**Figure 181: WLAN Accounting Screen**

- 4 Set the following **Syslog 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 <b>Through RF Domain Manager</b> or <b>Through Wireless Controller</b> . If no proxy is needed, select <b>None</b> .
Format	Specify the delimiter format for the MAC address to be packed in the syslog request. Available formats are <b>No Delimiter</b> (aabbccddeeff), <b>Colon Delimiter</b> (aa:bb:cc:dd:ee:ff), <b>Dash Delimiter</b> (aa-bb-cc-dd-ee-ff), <b>Dot Delimiter</b> (aabb.ccdd.eeff) and <b>Middle Dash Delimiter</b> (aabbcc-ddeeff).
Case	Specify to send the MAC addresses in either <b>Uppercase</b> or <b>Lowercase</b> 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, an **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 Click **OK** when completed to update the WLAN's accounting settings. Click **Reset** to revert the screen to the last saved configuration.

### *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 exist, 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.

## Configuring WLAN Service Monitoring Settings

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 becomes unavailable.

To configure Service Monitoring settings:

- 1 Select **Configuration > Wireless LANs > Wireless LAN Policy** to display a high-level display of the existing WLANs.
- 2 Click **Add** to create an additional WLAN, or click **Edit** to modify the properties of an existing WLAN.

- 3 Click **Service Monitoring**.

The screenshot shows the 'WLAN Policy Service Monitoring' configuration screen. It is organized into four main sections, each with a title and a horizontal line separator:

- AAA Server Monitoring:** Includes an 'Enable' checkbox (disabled) and an information icon.
- Adoption Monitoring:** Includes an 'Enable' checkbox (disabled), a 'VLAN' dropdown menu (set to 1, range 1 to 4,094), and an information icon.
- DHCP Server Monitoring:** Includes an 'Enable' checkbox (disabled), a 'VLAN' dropdown menu (set to 1, range 1 to 4,094), and a 'CRM Name' text input field.
- DNS Server Monitoring:** Includes an 'Enable' checkbox (disabled), a 'VLAN' dropdown menu (set to 1, range 1 to 4,094), and a 'CRM Name' text input field.

At the bottom of the screen, there are three buttons: 'OK', 'Reset', and 'Exit'.

**Figure 182: WLAN Policy Service Monitoring Screen**

- 4 Select **AAA Server monitoring** to monitor a dedicated external RADIUS server and ensure its adoption resource availability.  
This setting is disabled by default.
- 5 Select **Captive Portal External Server monitoring** to monitor externally hosted captive portal activity, and to set 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	Select this option to verify access points' adoption status to their controllers or service platform. When the connection is lost, captive portal users are automatically migrated to the VLAN defined in the <b>VLAN</b> field. This option is disabled by default.
VLAN	Select the VLAN to which users are migrated when an access point's connection to its adopting controller or service platform is lost. The available range is from 1 to 4,094.

- 7 Refer to the **DHCP Server Monitoring** field to set the WLAN's adoption service monitoring configuration.

Enable	Select to enable monitoring of the configured DHCP server. When the connection to the monitored DHCP server is lost, all captive portal data users are automatically migrated to the VLAN defined in the <b>VLAN</b> field.
VLAN	Select the VLAN to which users are migrated when the configured DHCP server becomes available. The available range is from 1 to 4,094.
CRM Name	Enter the name of the DHCP server to monitor for availability. When this DHCP server resource becomes unavailable, the device falls back to the 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 adoption service monitoring configuration.

Enable	Select to enable monitoring of the configured DNS server. When the connection to the monitored DNS server is lost, all captive portal data users are automatically migrated to the VLAN defined in the <b>VLAN</b> field. This option is disabled by default.
VLAN	Select the VLAN to which users are migrated when the configured DNS server becomes available. The available range is from 1 to 4,094.
CRM Name	Enter the name of the DNS server to monitor for availability. When this DNS server resource becomes unavailable, the device falls back to the defined VLAN. This VLAN has a DNS server configured that provides DNS address resolution until the primary DNS server becomes available.

- 9 Click **OK** when completed to update this WLAN's service monitor settings.  
Click **Reset** to revert the screen to its last saved configuration.

## Configuring Client Load Balancing Settings

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 Click **Add** to create an additional WLAN, or click **Edit** to modify the properties of an existing WLAN.

3 Select **Client Load Balancing**.**Figure 183: WLAN Policy Client Load Balancing Screen**

**Load Balancing Settings**

Enforce Client Load Balancing

Band Discovery Interval  Seconds ( 0 to 10,000 )

Capability Ageout Time  Hours ( 0 to 3 )

**Load Balancing Settings (2.4GHz)**

Single Band Clients

Max Probe Requests  ( 0 to 10,000 )

Probe Request Interval  Seconds ( 0 to 10,000 )

**Load Balancing Settings (5GHz)**

Single Band Clients

Max Probe Requests  ( 0 to 10,000 )

Probe Request Interval  Seconds ( 0 to 10,000 )

OK Reset Exit

- 4 Refer to the **Load Balancing Settings** section to configure load balancing for the WLAN. These settings are generic to both the 2.4 GHz and 5.0 GHz bands.

Enforce Client Load Balancing	Select this option to enforce a client load balance distribution on this WLAN's Access Point radios. The following models can support 256 clients per access point: AP 6522, AP 6532, AP 6562, AP 7161, AP 7602, AP 7622, AP 81XX. The following models can support 512 clients per access point: AP 7612, AP 7632, AP 7662. 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 enabled 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)** field to configure load balancing for the 2.4 GHz WLAN.

Single Band Clients	Select this option to enable association for single 2.4GHz clients, 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 from 0 - 10,000 to set an interval for client probe requests, beyond which association is allowed for clients on the 2.4 GHz frequency. The default is 10 seconds.

- 6 Refer to the **Load Balancing Settings (5GHz)** field to configure load balancing for the 5GHz WLAN.

Single Band Clients	Select this option to enable the association of single 5GHz clients, 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 client associations on the 5.0 GHz frequency. 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 in 5GHz. The default is 10 seconds.

- 7 Click **OK** when completed to update this WLAN's client load balance settings.  
Click **Reset** to revert the screen to its last saved configuration.

## Configuring Advanced WLAN Settings

- 1 Select **Configuration > Wireless LANs > Wireless LAN Policy** to display a high-level display of the existing WLANs.
- 2 Click **Add** to create an additional WLAN, or click **Edit** to modify the properties of an existing WLAN.
- 3 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 <b>Disabled</b> , <b>Optional</b> or <b>Mandatory</b> ). <b>Disabled</b> is the default setting.
SA Query Attempts	Use the spinner control to set the number of security association query attempts, between 1 and 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.



4. Click **Advanced**.

**Advanced RADIUS Configuration**

NAS Identifier

NAS Port

RADIUS Dynamic Authorization

**Radio Rates**

Rates for 2.4 GHz WLAN

Rates for 5 GHz WLAN

**Transition**

Fast BSS Transition

Fast BSS Transition Over DS

**HTTP Analysis**

Enable

**Filter**

Filter Out Images

Filter Post

Strip Query String

**Forward To Syslog Server**

Enable

Host

Port

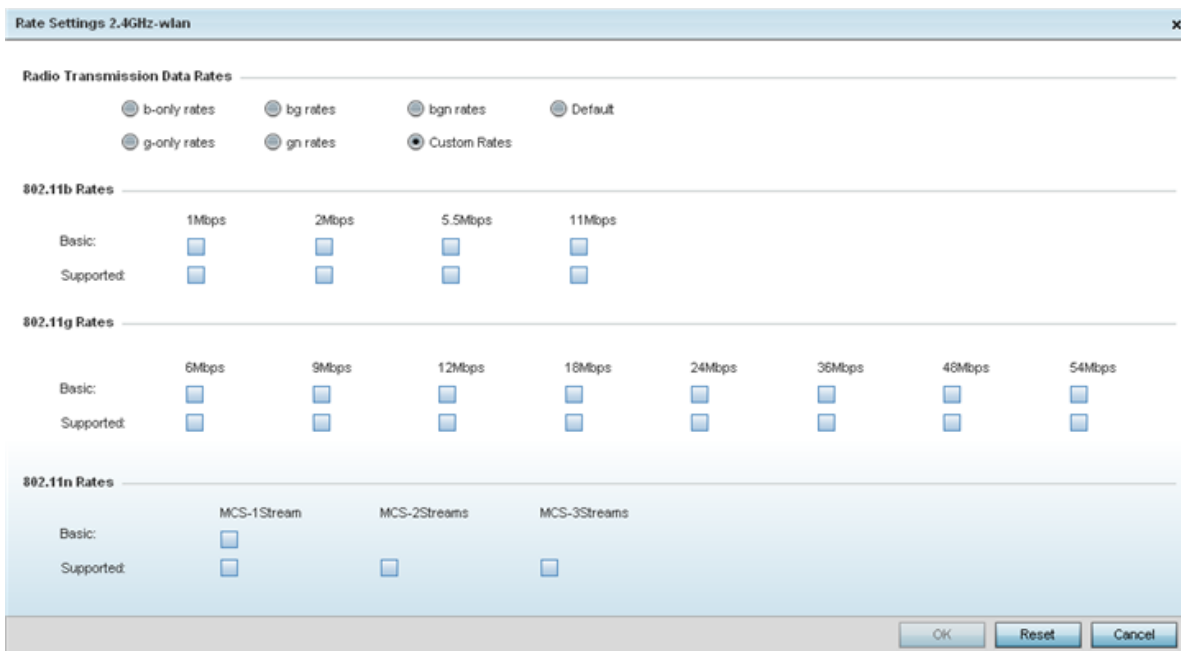
Proxy Mode

**Figure 184: WLAN - Advanced Configuration Screen**

- 5 Refer to the **Advanced RADIUS Configuration** field to set the WLAN's NAS configuration and RADIUS Dynamic Authorization.

NAS Identifier	Specify what is included in the <b>RADIUS NAS-Identifier</b> field for authentication and accounting packets. This is an optional setting, and defaults are used if no values are provided.
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 user name representing a physical port. When the access point authorizes users, it queries the user profile database using a user name representative of the physical NAS port making the connection. Set the numeric port value between 0 and 4,294,967,295.
RADIUS Dynamic Authorization	Select this check box to enable 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 cause a session to terminate immediately. This option is disabled by default.

- 6 Refer to the **Radio Rates** field to define selected data rates for both the 2.4 GHz and 5.0 GHz bands.



**Figure 185: Advanced WLAN Rate Settings 2.4 GHz Screen**

**Figure 186: 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 9: MCS-1 Stream**

MCS Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz 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 10: MCS-2 Stream**

MCS-2Stream Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz With SGI
0	2	13	14.4	27	30
1	2	26	28.9	54	60
2	2	39	43.4	81	90

**Table 10: MCS-2  
Stream (continued)**

MCS-2Stream Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz With SGI
3	2	52	57.8	108	120
4	2	78	86.7	162	180
5	2	104	115.6	216	240
6	2	117	130	243	270
7	2	130	144.4	270	300

**Table 11: MCS-3  
Stream**

MCS-3Stream Index	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz 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 12:  
MCS-802.11ac  
(Theoretical  
Throughput for  
Single Spatial  
Streams)**

MCS Index	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz With SGI	80 MHz No SGI	80 MHz 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

**Table 12:**  
**MCS-802.11ac**  
**(Theoretical**  
**Throughput for**  
**Single Spatial**  
**Streams) (continued)**

MCS Index	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz With SGI	80 MHz No SGI	80 MHz With SGI
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 <b>Fast BSS Transition</b> 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 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 <b>Fast BSS Transition Over DS</b> 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 **Filter** settings for HTTP analysis on this 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 <b>Hostname</b> or <b>IP Address</b> 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 <b>Through RF Domain Manager</b> or <b>Through Wireless Controller</b> . If no proxy is needed, select <b>None</b> .

- 11 Click **OK** when completed to update this WLAN's advanced settings.

Click **Reset** to revert the screen to its last saved configuration.

## Configuring Auto Shutdown Settings

The Auto Shutdown feature causes the WLAN to shut down 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 auto shutdown for a WLAN:

- 1 Select **Configuration > Wireless LANs > Wireless LAN Policy** to display a high-level display of the existing WLANs.
- 2 Click **Add** to create an additional WLAN, or click **Edit** to modify the properties of an existing WLAN.
- 3 Select **Auto Shutdown**.

**Figure 187: WLAN - Auto Shutdown Screen**

- 4 Refer to the **Auto Shutdown** field to set the WLAN's shutdown criteria.

Shutdown on Mesh Point Loss	Select this option to automatically disable the WLAN when its associated mesh point (mesh dedicated access 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 accesspoints are unadopted. This setting is disabled by default.

- 5 Refer to the **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	Select this option to automatically disable the WLAN 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 keep the selected WLAN online.

- 6 To configure **Time Based Access** for this WLAN, click **+ Add Row** and configure each of the following options:

Days	Select a day of the week to apply this access policy. Selecting <b>All</b> will apply the policy every day. Selecting <b>weekends</b> will apply the policy on Saturdays and Sundays only. Selecting <b>weekdays</b> 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(s).
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 <b>AM</b> or <b>PM</b> .
End Time	This value sets the ending time of day(s) the WLAN is disabled. Use the spinner controls to select the hour and minute, in a 12h time format. Then use the radio button to choose <b>AM</b> or <b>PM</b> .

- 7 Click **OK** when completed to update this WLAN's auto shutdown settings. Click **Reset** to revert the screen to its last saved configuration.

## WLAN QoS Policies

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.

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, for example **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 existing QoS policies supports an ideal QoS configuration for the intended data traffic of this WLAN, click **Add** to create new policy. Select the radio button of an existing WLAN and click **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 radios 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.

WLAN Quality of Service (QoS) <span style="float: right;">?</span>					
WLAN QoS Policy <span style="font-size: small;">⊖</span>	Wireless Client Classification	SVP Prioritization	WMM Power Save	Multicast Mask Primary	Multicast Mask Secondary
default	WMM	✗	✓	00-00-00-00-00-00-FF-FF-F	00-00-00-00-00-00-FF-FF-FF-
WMMQOS	WMM	✗	✓	00-00-00-00-00-00-FF-FF-F	00-00-00-00-00-00-FF-FF-FF-

Type to search in tables Row Count: 2

Add Edit Delete Copy Rename

**Figure 188: WLAN QoS Screen**

- 2 Refer to the following read-only information on each listed QoS policy to determine whether a new policy needs to be created, an existing policy can be edited, or an existing policy can be used as is:

WLAN QoS Policy	The name assigned to this WLAN QoS policy. The assigned policy name cannot be modified.
Wireless Client Classification	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: <ul style="list-style-type: none"> <li>• <b>WMM</b> - 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.</li> <li>• <b>Voice</b> - Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio.</li> <li>• <b>Video</b> - Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio.</li> <li>• <b>Normal</b> - Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio.</li> <li>• <b>Low</b> - Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.</li> <li>• <b>Non-Unicast</b> - Optimized for non-Unicast traffic. Implies all traffic on this WLAN is designed for broadcast or multicast.</li> </ul>



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	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	The secondary multicast mask defined for each listed QoS policy.

- 3 Click **Add** to define a new WLAN QoS policy, or select an existing WLAN QoS policy and click **Edit** to modify its configuration. Existing QoS policies can be selected and deleted 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](#)
- [Configuring Multimedia Optimizations](#)

## Configuring a WLAN's QoS WMM Settings

Using Wi-Fi Multimedia (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 a controller, service platform or access point managed WLAN. Access categories were designed to correspond to 802.1d priorities to facilitate interoperability with QoS policy management mechanisms. WMM enabled controllers, service platforms and access points can 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 available to WLANs.
- 2 Click **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.

WLAN QoS Policy WMMQOS ?

**WMM** Rate Limit Multimedia Optimizations

---

**Settings**

Wireless Client Classification i WMM ▼

Non-Unicast Classification i Default ▼

Enable Voice Prioritization i

Enable SVP Prioritization i

Enable WMM Power Save i

Enable QBSS Load IE i

Configure Non WMM Client Traffic i Normal ▼

---

**Voice Access**

Transmit Ops i 47 (0 to 65,535)

AIFSN i 2 (2 to 15)

ECW Min i 2 (0 to 15)

ECW Max i 3 (0 to 15)

---

**Normal (Best Effort) Access**

Transmit Ops i 0 (0 to 65,535)

AIFSN i 3 (2 to 15)

ECW Min i 4 (0 to 15)

ECW Max i 10 (0 to 15)

---

**Video Access**

Transmit Ops i 94 (0 to 65,535)

AIFSN i 2 (2 to 15)

ECW Min i 3 (0 to 15)

ECW Max i 4 (0 to 15)

---

**Low (Background) Access**

Transmit Ops i 0 (0 to 65,535)

AIFSN i 7 (2 to 15)

ECW Min i 4 (0 to 15)

ECW Max i 10 (0 to 15)

---

**Other Settings**

Trust IP DSCP i

Trust 802.11 WMM QoS i

OK Reset **Exit**

**Figure 189: WLAN QoS Policy Screen - WMM Tab**

- 3 Configure the following settings in respect to the WLAN's intended WMM radio traffic and user requirements:

Wireless Client Classification	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>WMM</b> - 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. <b>WMM</b> is the default setting.</li> <li>• <b>Voice</b>- Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio.</li> <li>• <b>Video</b> - Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio.</li> <li>• <b>Normal</b> - Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio.</li> <li>• <b>Low</b> - Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.</li> </ul>
Non-Unicast Classification	<p>Use the drop-down menu to select the Non-Unicast Classification for this WLAN's intended traffic. Non-unicast classification types include:</p> <ul style="list-style-type: none"> <li>• <b>Voice</b>- Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio.</li> <li>• <b>Video</b> - Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio.</li> <li>• <b>Normal</b> - Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio.</li> <li>• <b>Low</b> - Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.</li> </ul> <p><i>Voice</i> - Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio.</p>
Enable Voice Prioritization	<p>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.</p>
Enable SVP Prioritization	<p>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.</p>
Enable WMM Power Save	<p>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. This feature is enabled by default.</p>

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 point radios. This feature is enabled by default.
Configure Non WMM Client Traffic	Use the drop-down menu to select the Non-WMM client traffic Classification. brNon-WMM classification types include: <ul style="list-style-type: none"> <li>• <b>Voice</b>– Optimized for voice traffic. Implies all traffic on this WLAN is prioritized as voice traffic on the radio.</li> <li>• <b>Video</b> – Optimized for video traffic. Implies all traffic on this WLAN is prioritized as video traffic on the radio.</li> <li>• <b>Normal</b> – Optimized for best effort traffic. Implies all traffic on this WLAN is prioritized as best effort traffic on the radio.</li> <li>• <b>Low</b> – Optimized for background traffic. Implies all traffic on this WLAN is low priority on the radio.</li> </ul>

- 4 Set the following **Voice 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 47.
AIFSN	Set the current Arbitrary Inter-frame Space Number (AIFSN) between 2 and 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 <b>ECW Min</b> is combined with the <b>ECW Max</b> 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 <b>ECW Max</b> is combined with the <b>ECW Min</b> 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 **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 and 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 <b>ECW Min</b> is combined with the <b>ECW Max</b> 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 <b>ECW Max</b> is combined with the <b>ECW Min</b> 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.

- 6 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 Arbitrary Inter-frame Space Number (AIFSN) between 2 and 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 <b>ECW Min</b> is combined with the <b>ECW Max</b> 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 <b>ECW Max</b> is combined with the <b>ECW Min</b> 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.

- 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. The default value is 0.
AIFSN	Set the current Arbitrary Inter-frame Space Number (AIFSN) between 2 and 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 <b>ECW Min</b> is combined with the <b>ECW Max</b> 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 <b>ECW Max</b> is combined with the <b>ECW Min</b> 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.

- 8 Set the following **Other Settings** for the WLAN's QoS policy:

Trust IP DSCP	Select this option to trust (utilize) IP DSCP values for WLANs. The default value is enabled.
Trust 802.11 WMM QoS	Select this option to trust (utilize) 802.11 WMM QoS values for WLANs. The default value enabled.

- 9 Click **OK** when completed to update this WLAN's QoS settings. Click **Reset** to revert the screen to its last saved configuration.

## Configuring a WLAN's QoS 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 at the branch. Rate limiting limits the maximum rate sent to 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. An administrator can set separate QoS rate limit configurations for data transmitted

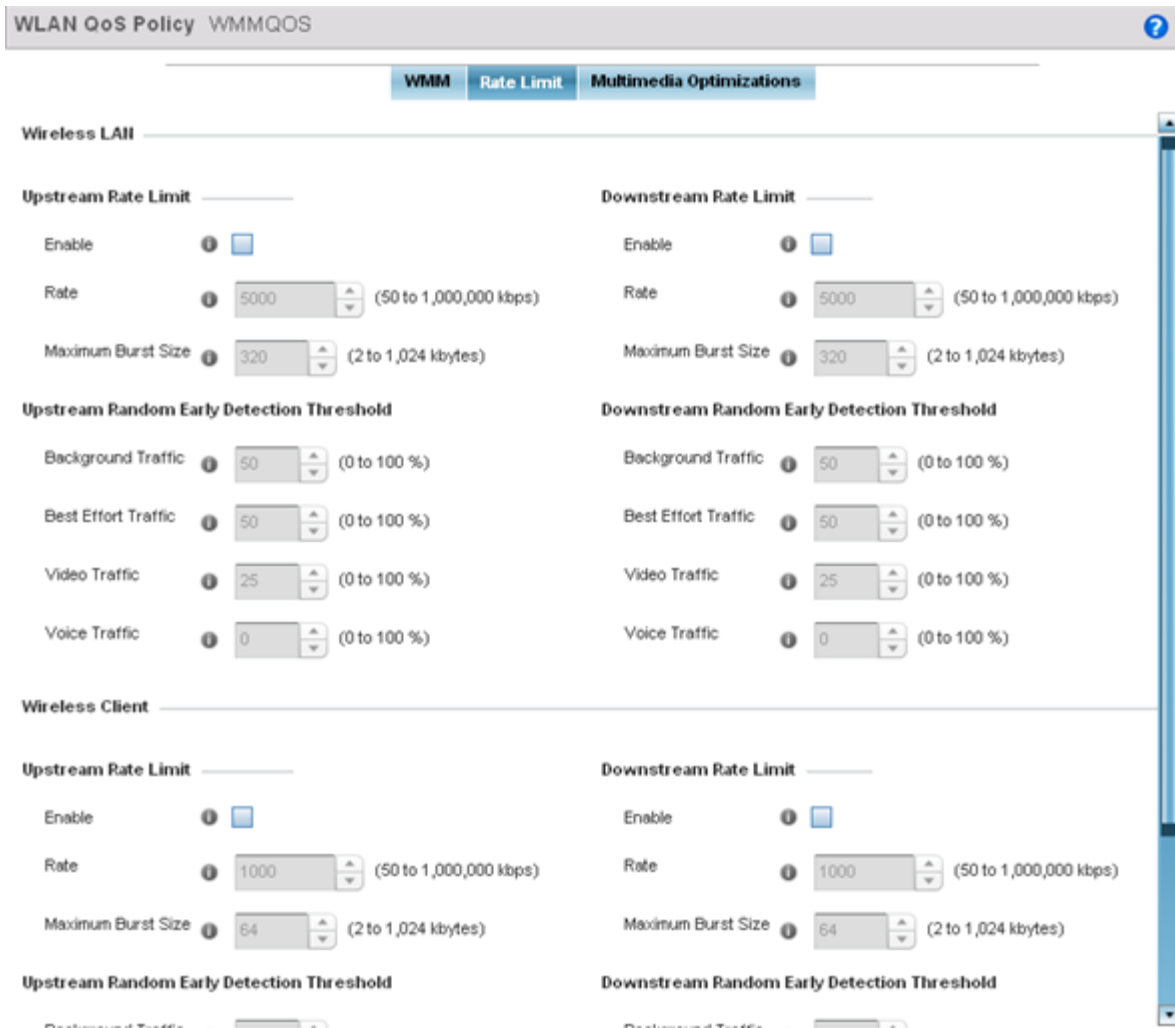
from the access point (upstream) and data transmitted from a WLAN's wireless clients back to their associated access point radios (downstream).

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 Click **Add** button to create a new QoS policy or **Edit** to modify the properties of an existing WLAN QoS policy.
- 3 Select the Rate Limit tab.



**Figure 190: WLAN QoS Policy Screen - Rate Limit Tab**

- Configure the following parameters to define the **WLAN Upstream Rate Limit**. These values apply to traffic from the controller to associated access point radios and connected wireless clients.

Enable	Select this option to enable rate limiting for data transmitted from the controller 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 an upstream packet transmission will result in congestion for the WLAN's client traffic. 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 for the intended **WLAN Downstream Rate Limit**.

These values apply to traffic from wireless clients to associated access point radios and the controller or service platform.

Enable	Select this option 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 om drops will occur.

- 8 Configure the following parameters for the intended **Upstream Rate Limit** for wireless client traffic:

Enable	Select this option 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 **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 value 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 will occur.

- 10 Configure the following parameters for the **Downstream Rate Limit**.

These values apply to traffic from a controller or service platform to associated access point radios and the wireless client.

Enable	Select this option to enable rate limiting for data transmitted from 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 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 **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 will occur.

- 12 Click **OK** when completed to update this WLAN's QoS rate limit settings. Click **Reset** to revert the screen to its last saved configuration.

## Configuring Multimedia Optimizations

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 a QoS rate limit configuration 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 Click **Add** button to create a new QoS policy or **Edit** to modify the properties of an existing WLAN QoS policy.
- 3 Select the Multimedia Optimizations tab.

**WLAN QoS Policy** WMMQOS

WMM Rate Limit **Multimedia Optimizations**

**Multicast Mask**

Multicast Mask Primary 00 - 00 - 00 - 00 - 00 - 00 / FF - FF - FF - FF - FF - FF

Multicast Mask Secondary 00 - 00 - 00 - 00 - 00 - 00 / FF - FF - FF - FF - FF - FF

**Accelerated Multicast**

Disable Accelerated Multicast

Automatically Detect Multicast Streams

Forwarding QoS Classification Trust QoS Values

Manually Configure Multicast Addresses

Multicast IP Address	Classification
* . . .	Video

+ Add Row

OK Reset Exit

**Figure 191: WLAN QoS Policy Screen - Multimedia Optimizations Tab**

- 4 Configure the following parameters for to the **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 accelerated 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, a number of classification mechanisms can be applied to the stream, and the administrator can select the desired classification type.
Manually Configure Multicast Addresses	Select this option and specify a list of multicast addresses and classifications. Packets are accelerated when the destination addresses matches.

- 6 Click **OK** when completed to update this WLAN's multimedia optimization settings. Click **Reset** to revert the screen to its last saved configuration.

## WLAN QoS Deployment Considerations

Before defining a QoS configuration on a controller, service platform or access point managed WLAN, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- WLAN QoS configurations differ significantly from QoS policies configured for associated 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 radios support.
- Enabling WMM support on a WLAN only advertises WMM capability to wireless clients. The wireless clients must also support WMM and use the parameters correctly while accessing the wireless network to truly benefit.
- Rate limiting is disabled by default on 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 because the bandwidth requirements are consistent and can be realistically trended over time. Applications such as web, database, and email are harder to estimate because bandwidth usage varies depending on how the applications are used.

## Radio QoS Policies

Without a dedicated QoS policy, any wireless network operates on a best-effort delivery basis, meaning all traffic has equal priority and 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.

WiNG managed controllers and their associated access point radios and wireless clients support several Quality of Service (QoS) techniques enabling real-time applications (such as voice and video) to coexist

with lower priority background applications (such as web, email, 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.

In a wireless network, 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 than 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 the controller or service platform, their associated access points and 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 apply to both connected access point radios and their wireless clients. Parameters that affect 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 managed controllers, service platforms and access points include Session Initiation Protocol (SIP), Skinny Call Control Protocol (SCCP), and Application Layer Gateways (ALGs) that enable devices to identify voice streams and dynamically set voice call bandwidth. Controllers use the data to provide prioritization and admission control to these devices without requiring TSPEC or WMM client support.

WiNG managed controllers, service platforms, and access points 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 prioritizes traffic to the client, but does not prioritize traffic 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.

## Configuring a Radio QoS Policy

To configure an access point radio's QoS policy:

- 1 Select **Configuration > Wireless > Radio QoS Policy** to display existing radio QoS policies.

**Figure 192: Radio QoS Policy Screen**

Radio QoS Policy	Firewall detection traffic Enable (e.g., SIP)	Implicit TSPEC	Voice	Best Effort	Video	Background
default	✓	✓	✗	✗	✗	✗

Type to search in tables

Row Count: 1

Add Edit Delete Copy Rename

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 TPSEC frames only.
Implicit TPSEC	A green check mark defines the policy as requiring wireless clients to send their traffic specifications 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 TPSEC frames only.
Voice	A green check mark indicates that Voice prioritization QoS is enabled on the radio. A red X indicates that <b>Voice</b> 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 that <b>Best Effort</b> 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 that <b>Video</b> 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 that <b>Background</b> prioritization QoS is disabled on the radio.



- Click **Add** to create a new radio QoS policy, or select an existing policy and click **Edit** to modify its configuration.

Optionally, **Copy** or **Rename** QoS policies as needed.

**Figure 193: 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 radio QoS policy.

- 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 realtime session), receives priority, maintaining a high level of voice quality. For higher-priority traffic categories (like voice), the <b>Transmit Ops</b> 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 AIFSN values 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 <b>ECW Min</b> is combined with the <b>ECW Max</b> 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 <b>ECW Max</b> is combined with the <b>ECW Min</b> 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 between 1-15. Higher priority traffic voice categories should have lower AIFSN values than lower priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 3.
ECW Min	The <b>ECW Min</b> is combined with the <b>ECW Max</b> 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 4.
ECW Max	The <b>ECW Max</b> is combined with the <b>ECW Min</b> 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 6.

- 6 Set the following **Video Access** settings for the radio QoS policy:

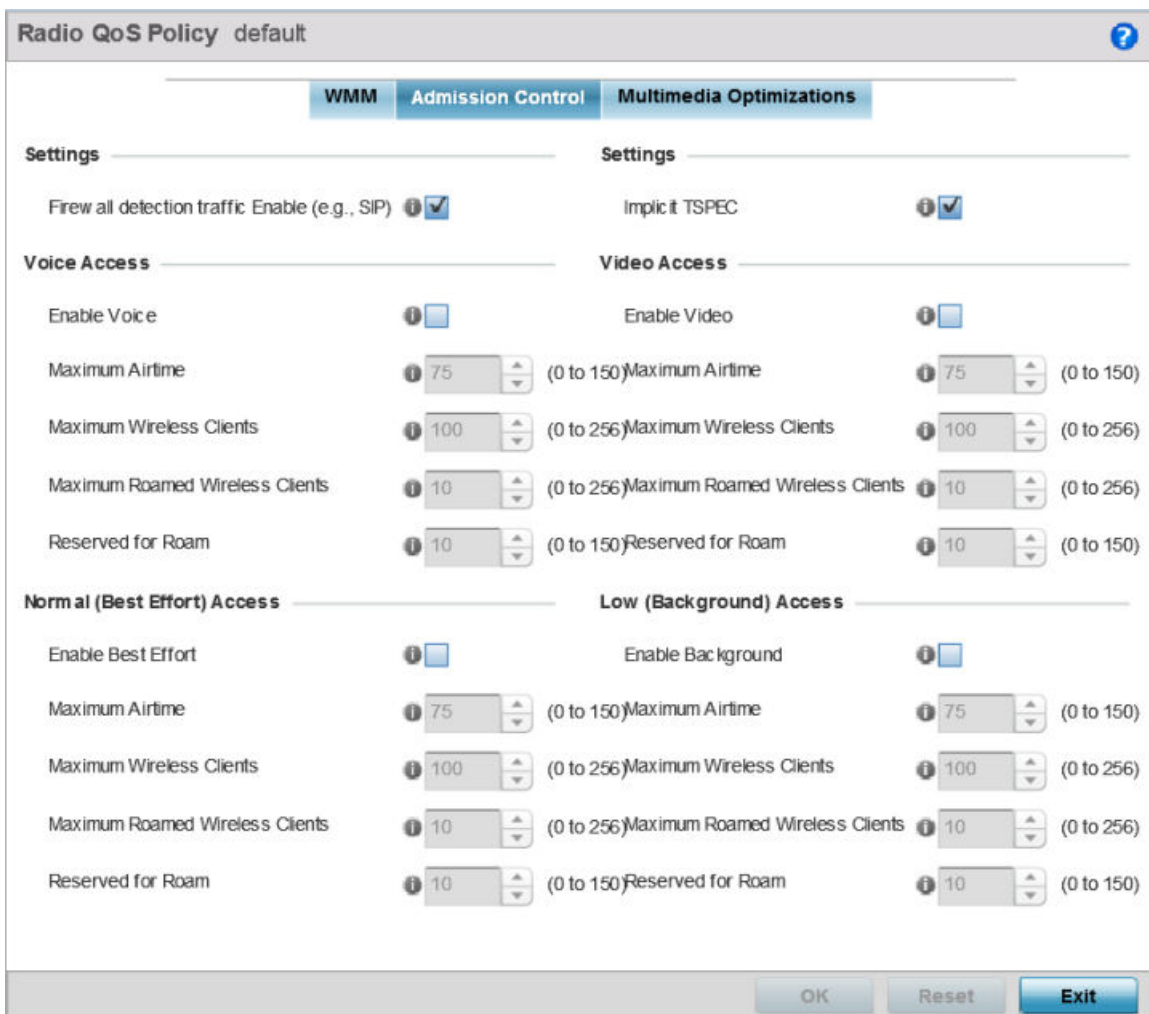
Transmit Ops	Use the slider to set the maximum duration a device can transmit after obtaining a transmit opportunity. For higher-priority traffic categories, this value should be set to a low number. The default value is 94.
AIFSN	Set the current AIFSN between 1-15. Higher priority traffic voice categories should have lower AIFSN values 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 <b>ECW Min</b> is combined with the <b>ECW Max</b> 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.
ECW Max	The <b>ECW Max</b> is combined with the <b>ECW Min</b> 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 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. Higher priority traffic voice categories should have lower AIFSN values than lower priority traffic categories. This will cause lower-priority traffic to wait longer before attempting access. The default value is 7.

ECW Min	The <b>ECW Min</b> is combined with the <b>ECW Max</b> 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 4.
ECW Max	The <b>ECW Max</b> is combined with the <b>ECW Min</b> 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 10.

- Click **OK** when completed to update the radio QoS settings for this policy.  
Click **Reset** to revert the WMM screen to its last saved configuration.
- Select the Admission Control tab to configure an admission control configuration for the 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.



**Figure 194: Radio QoS Policy Admission Control Screen**

The name of the radio QoS policy for which the admission control settings apply displays in the banner of the **QoS Policy** 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 the QoS policy for this radio only. 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 normal traffic. Only normal 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 normal best effort 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 best effort data support. The default value is 75%.
Maximum Wireless Clients	Set the number of wireless clients supporting best effort 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 normal 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 best effort 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 video 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% available to account 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 background traffic. Only low background 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 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). 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 low and background 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.

**Radio QoS Policy default**

WMM Admission Control **Multimedia Optimizations**

**Accelerated Multicast**

Maximum multicast streams allowed: 25 (0 to 256)

When wireless client count exceeds the above limit: Reject

Maximum multicast streams per client: 2 (1 to 4)

Packets per second for multicast flow for it to be accelerated: 25 (1 to 500)

Timeout for wireless clients: 60 (5 to 6,000)

**Smart Aggregation**

Smart Aggregation:

Max Delay for Best Effort: 150 (0 to 1,000)

Max Delay for Background: 250 (0 to 1,000)

Max Delay for Streaming Video: 150 (0 to 1,000)

Max Delay for Video Conferencing: 40 (0 to 1,000)

Max Delay for Voice: 0 (0 to 1,000)

Minimum Frames per Aggregate limit: 8 (0 to 64)

Max Mesh Links: 3 (1 to 10)

OK Reset Exit

**Figure 195: 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 <b>Reject</b> new wireless clients or <b>Revert</b> 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 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:

- A preconfigured number of aggregated frames is reached
- An administrator defined interval has elapsed since the first frame (of a set of frames to be aggregated) was received
- 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.

19 Click **OK** when completed to update the radio QoS settings for this policy.

Click **Reset** to revert to the last saved configuration.

## Radio QoS Configuration and Deployment Considerations

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 coexist with non-WMM clients on the same WLAN. Non-WMM clients are always assigned a best effort access category.
- Use default WMM values for all deployments. Changing these values can lead to unexpected traffic blockages, and these 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 of its users.
- TSPEC admission control is available only with newer voice over WLAN phones. Many legacy voice devices do not support TPSEC or even support WMM traffic prioritization.

## Association ACL

---

An association ACL is a policy-based ACL that either allows or denies clients from connecting to a controller, service platform or access point managed WLAN. An association ACL affords a system administrator the ability to restrict access by specifying a client MAC address or range of addresses to either include or exclude from WLAN connectivity.

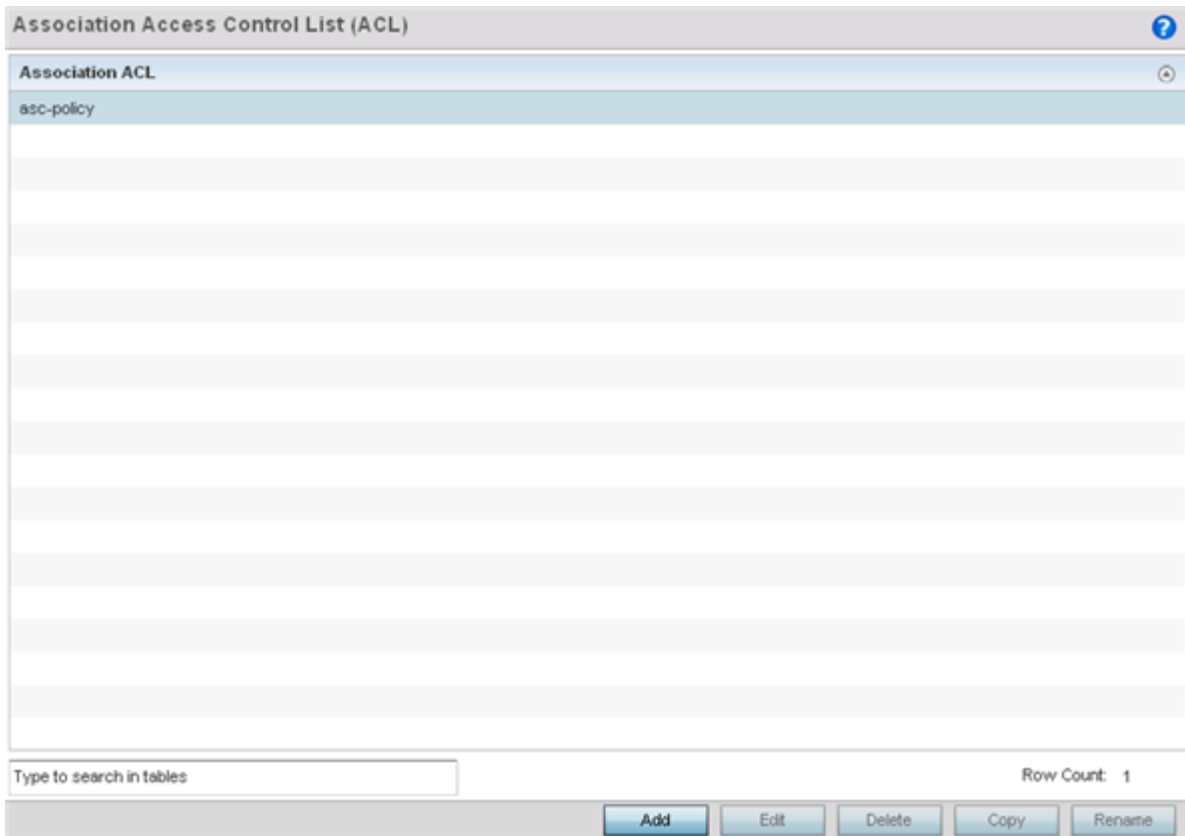
Association ACLs are applied to WLANs as an additional access control mechanism. They can be applied to WLANs from within a WLAN Policy's **Advanced Configuration** screen. For more information on applying an existing association ACL to a WLAN, see [Configuring Advanced WLAN Settings](#) on page 360.

To define an association ACL deployable with a WLAN:

- 1 Select **Configuration > Wireless > Association ACL** to display existing association ACLs.

Any of the policies listed in the **Association Access Control List (ACL)** screen can be selected and applied.

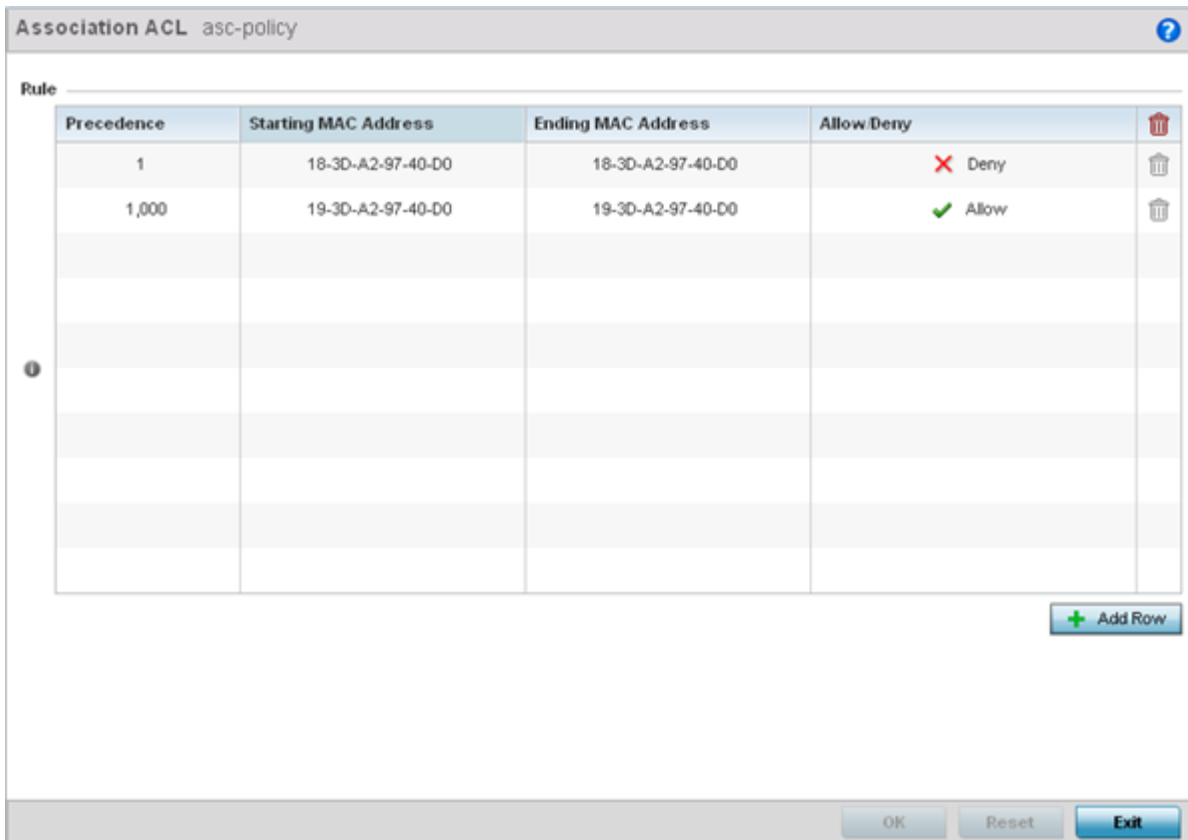




**Figure 196: Association Access Control List (ACL) Screen**

- 2 Select **Add** to define a new ACL configuration, **Edit** to modify an existing ACL configuration, or **Delete** to remove one. Select **Copy** to make a copy of an existing ACL for further modifications. Select **Rename** to rename an existing ACL.

An **Association ACL** screen displays for defining a new ACL or modifying a selected ACL.



**Figure 197: Association ACL Screen**

- 3 Select the **+ Add Row** button to add an association ACL template.
- 4 Set the following parameters to create or modify the association ACL:

Association ACL	If you are creating a new Association ACL, provide a name specific to its function. Avoid naming it after the WLAN it supports. The name cannot exceed 32 characters.
Precedence	The rules within a WLAN's ACL are applied to packets based on precedence. Every rule has a unique sequential precedence value you define. You cannot add two rules 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 address for clients requesting association.
Ending MAC Address	Provide an ending MAC address for clients requesting association.
Allow/Deny	Use the drop-down menu to <b>Allow</b> or <b>Deny</b> access if a MAC address matches this rule.

- 5 Select the **+ Add Row** button to add MAC address ranges and allow/deny designations.
- 6 Click **OK** to update the association ACL settings. Click **Reset** to revert to the last saved configuration.

### Association ACL Deployment Considerations

Before defining an association ACL configuration and applying it to a controller, service platform or access point managed 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 to which they apply. Be careful, however, not to name ACLs after specific WLANs, because 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.

## Smart RF Policies

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 radio performance improvements.

A Smart RF policy can reduce deployment costs by scanning the RF environment to determine the best channel and transmit power for each radio. Smart RF policies can be added to specific RF Domains to apply site specific deployment configurations and self-healing values to device groups.

Smart RF centralizes the decision process and makes intelligent RF configuration decisions using data obtained from the RF environment. Smart RF helps reduce ongoing management and maintenance costs by constantly monitoring the network for external WiFi interference, neighbor WiFi 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, an individual controller, service platform or access point manages the calibration and monitoring phases. In clustered environments, a single device 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 channel 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.

## Configuring Smart RF Basic Settings

To define a Smart RF policy:

- 1 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.

- 2 Click **Add** to create a new Smart RF policy, select an existing policy and click **Edit** to modify its configuration, or select an existing policy and click **Delete** to remove an obsolete policy. Optionally, **Copy** or **Rename** Smart RF policies as needed.

The **Basic Configuration** screen displays by default for new or modified Smart RF policies.

**Figure 198: SMART RF - Basic Configuration Screen**

- 3 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 <b>Low</b> , <b>Medium</b> , <b>High</b> , and <b>Custom</b> . <b>Medium</b> is the default setting. The <b>Custom</b> option allows an administrator to adjust the parameters and thresholds for <b>Interference Recovery</b> , <b>Coverage Hole Recovery</b> , and <b>Neighbor Recovery</b> . Using the <b>Low</b> , <b>Medium</b> (recommended), and <b>High</b> settings still allows these features to be utilized.
Smart RF Policy Enable	Select this option to enable Smart RF for immediate inclusion within an RF Domain. Smart RF is enabled by default.
Interference Recovery	Select this option 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 this option to enable coverage compensation from neighboring radios when a radio coverage hole is detected within the Smart RF supported radio coverage area. When a 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 this option 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 <b>Medium</b> .

- 4 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.
- 5 Click **OK** to update the Smart RF basic settings for this policy.  
Click **Reset** to revert to the last saved configuration.

## Configuring Smart RF Channel & Power Settings

To configure Smart RF Channel and Power settings:

1 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.



**Note**

The **Power Settings** and **Channel Settings** parameters are enabled only when **Custom** or **Medium** is selected as the **Sensitivity** setting from the **Basic Configuration** screen.

**Power Settings**

5 GHz Minimum Power  (1 to 20 dBm)

5 GHz Maximum Power  (1 to 20 dBm)

2.4 GHz Minimum Power  (1 to 20 dBm)

2.4 GHz Maximum Power  (1 to 20 dBm)

**Channel Settings**

5 GHz Channels

5 GHz Channel Width  20MHz  40MHz  80MHz  Automatic

2.4 GHz Channels

2.4 GHz Channel Width  20MHz  40MHz  Automatic

**Area Based Channel Settings**

Area	Band	Channel List	<input type="button" value="X"/>

**Figure 199: SMART RF - Channel and Power Screen**

- 2 Refer to the **Power Settings** field to define Smart RF recovery settings for 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 5.0 GHz band. The default setting is 4 dBm.
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 5.0 GHz band. The default setting is 17 dBm.
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. The default setting is 4 dBm.
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. The default setting is 17 dBm.

- 3 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 <b>Automatic</b> 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 you are 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 <b>Automatic</b> 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.

- 4 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	Select the radio band, either 2.4 GHz or 5 GHz, for the Smart RF policy assigned to the specified area.
Channel List	Select the channels associated with the Smart RF policy for the specified area and band.

- 5 Click **OK** to update the Smart RF and Power settings for this policy.  
Click **Reset** to revert to the last saved configuration.



## Configuring Smart RF Scanning Configuration

To configure the Smart RF scanning configuration:

- 1 Select **Scanning Configuration**.

**Figure 200: SMART RF - Scanning Configuration Screen**



### Note

The monitoring and scanning parameters in the **Scanning Configuration** screen are enabled only when **Custom** is selected as the **Sensitivity** setting from the **Basic Configuration** screen.

- 2 Enable or disable **Smart Monitoring Enable**.  
The feature is enabled by default. When it is enabled, detector radios monitor their coverage areas for potential failed peers or coverage area holes requiring transmission adjustments for coverage compensation.
- 3 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 <b>All</b> will apply the policy every day. Selecting <b>weekends</b> will apply the policy on Saturdays and Sundays only. Selecting <b>weekdays</b> 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 days.
Start Time	Set the starting time of day when 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 <b>AM</b> or <b>PM</b> .
End Time	Set the ending time of day when 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 <b>AM</b> or <b>PM</b> .

- 4 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) that 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 an RF Domain. The default setting is 50 milliseconds for both 2.4 GHz and 5.0 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 on which 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 a radio gathers before it sends 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 (1 - 255) during off channel scans for either the 2.4 or 5.0 GHz radio.
Power Save Aware Scanning	Select either the <b>Dynamic</b> , <b>Strict</b> , or <b>Disable</b> radio button to define how power save scanning is set for Smart RF. <b>Strict</b> disables smart monitoring as long as a power save capable client is associated to a radio. <b>Dynamic</b> disables smart monitoring as long as there is data buffered for a power save client at the radio. The default setting is <b>Dynamic</b> for both the 5 and 2.4 GHz bands.
Voice Aware Scanning	Select either the <b>Dynamic</b> , <b>Strict</b> , or <b>Disable</b> radio button to define how voice aware recognition is set for Smart RF. <b>Strict</b> disables smart monitoring as long as a power save capable client is associated to a radio. <b>Dynamic</b> disables smart monitoring as long as there is data buffered for a voice client at the radio. The default setting is <b>Dynamic</b> 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.

- 5 Click **OK** to update the Smart RF Scanning Configuration settings for this policy.  
Click **Reset** to revert to the last saved configuration.

## Configuring Smart RF Neighbor Recovery Settings

To configure Smart RF recovery settings:

- 1 Select **Recovery**.



#### Note

The recovery parameters within the Neighbor Recovery, Interference, and Coverage Hole Recovery tabs are enabled only 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 that affects the Smart RF supported network, and detected coverage holes that require intervention by neighbor radios.

- 2 Use the **Power Hold Time** field to define 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.

The screenshot displays the 'Neighbor Recovery' configuration screen. It features three tabs: 'Neighbor Recovery', 'Interference Recovery', and 'Coverage Hole Recovery'. The 'Neighbor Recovery' tab is active. The 'Hold Time' section includes a 'Power Hold Time' field set to 0, with a unit dropdown set to 'Seconds' and a range of '( 0 to 3,600 )'. The 'Neighbor Recovery' section contains two power threshold fields: '5 GHz Neighbor Power Threshold' and '2.4 GHz Neighbor Power Threshold', both set to -70 dBm with a range of '(-85 to -55 dBm)'. The 'Dynamic Sample Recovery' section has a 'Dynamic Sample Enabled' checkbox checked, 'Dynamic Sample Retries' set to 3 (range 1 to 10), and 'Dynamic Sample Threshold' set to 5 (range 1 to 30). A warning note at the bottom explains that some parameters are disabled based on the sensitivity setting and that the 'Custom' option is required to enable them. At the bottom right, there are 'OK', 'Reset', and 'Exit' buttons.

**Figure 201: SMART RF - Advanced Configuration Screen - Neighbor Recovery Tab**

- 3 Set the following **Neighbor Recovery** parameters:



**Note**

The recovery parameters within the Neighbor Recovery, Interference and Coverage Hole Recovery tabs are enabled only when **Custom** is selected as the **Sensitivity** setting from the **Smart RF Basic Configuration** screen.

5 GHz Neighbor Power Threshold	Set the maximum power increase threshold (from -85 to -55 dBm) the 5.0 GHz radio uses if it 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	Set the maximum power increase threshold (from -85 to -55 dBm) the 2.4 GHz radio uses if it 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.

- 4 Set the following **Dynamic Sample Recovery** parameters:

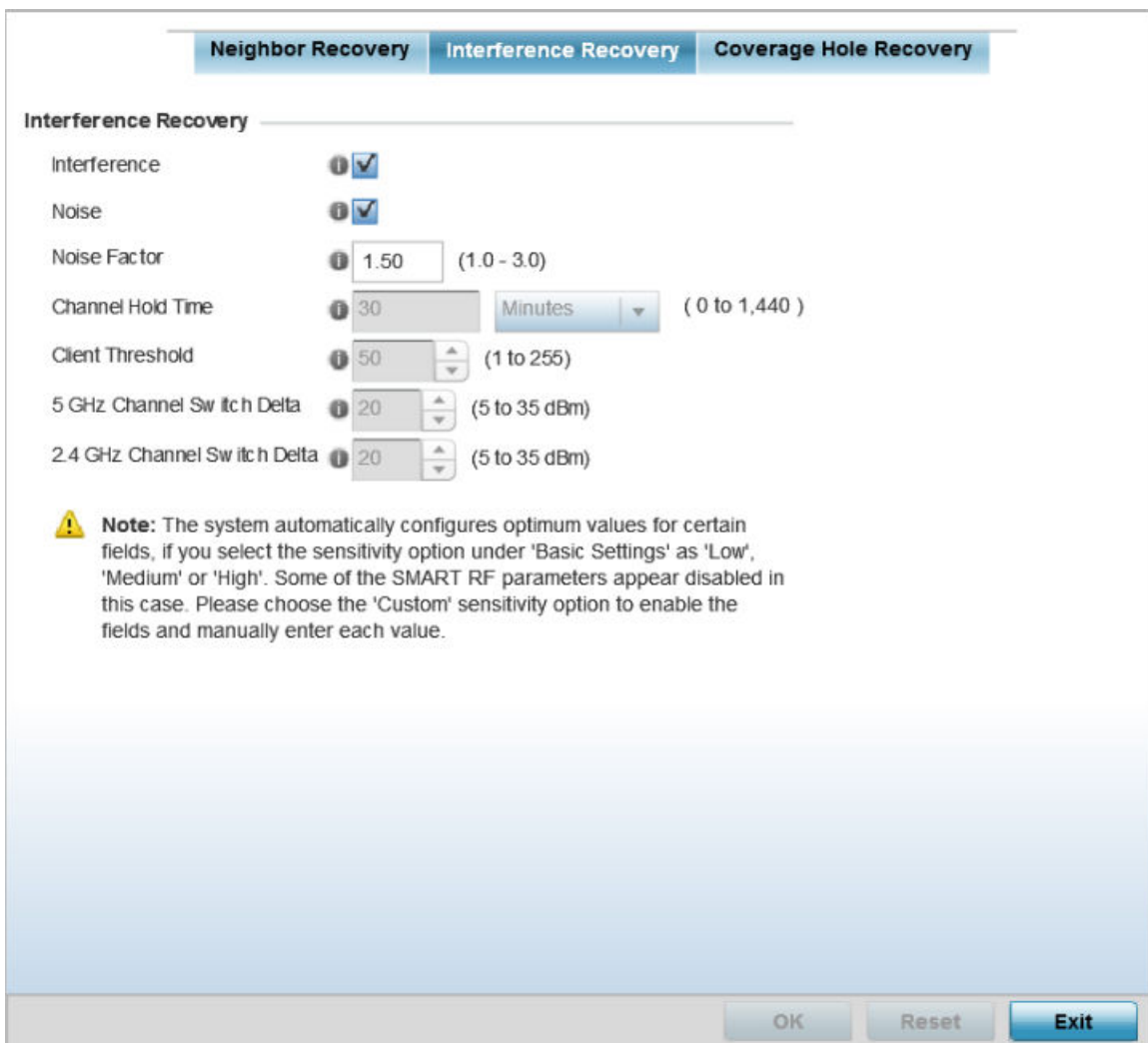
Dynamic Sample Enabled	Select this option to enable dynamic sampling. Dynamic sampling enables an administrator to define how Smart RF adjustments are triggered by locking retry and threshold values. This option is disabled by default.
Dynamic Sample Retries	Set the number of retries (from 1 - 10) attempted 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) used before a Smart RF power compensation requires dynamic sampling. The default setting is 5.

- 5 Click **OK** to update the Smart RF Neighbor Recovery settings for this policy.  
Click **Reset** to revert to the last saved configuration.

### *Configuring Smart RF Interference Recovery Settings*

To configure Smart RF Interference Recovery Settings:

- 1 Select **Interference Recovery**.



**Figure 202: SMART RF - Advanced Configuration Screen - Interference Recovery Tab**

- 2 Set the following **Interference Recovery** parameters:

Interference	Select this option 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 this option 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	Set the noise factor (level of network interference detected) taken into consideration by Smart RF during interference recovery calculations. The default setting is 1.50.
Channel Hold Time	Define the minimum time between channel changes during neighbor recovery. Set the time in either seconds (0 - 86,400), minutes (0 - 1,440), hours (0 - 24), or days (0 - 1). The default setting is 30 minutes.



Client Threshold	Set a client threshold for the Smart RF policy between 1 - 255. If the set threshold number of clients are connected to a radio, the radio does not change its channel, even though required, based on the interference recovery determination made by the smart master. The default setting is 50.
5 GHz Channel Switch Delta	Set a channel switch delta (interference delta), from 5 - 35 dBm, for the 5.0 GHz radio. This parameter is the difference between noise 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	Set a channel switch delta (interference delta), from 5 - 35 dBm, for the 2.4 GHz radio. This parameter is the difference between noise 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.

- 3 Click **OK** to update the Smart RF Interference Recovery settings for this policy.  
Click **Reset** to revert to the last saved configuration.

### *Configuring Smart RF Coverage Hole Recovery Settings*

1 Select **Coverage Hole Recovery**.

**Neighbor Recovery   Interference Recovery   Coverage Hole Recovery**

**Coverage Hole Recovery for 5.0 GHz**

Client Threshold  (1 to 255)

SNR Threshold  (1 to 75 dB)

Coverage Interval  Seconds (1 to 120)

Interval  Seconds (1 to 120)

**Coverage Hole Recovery for 2.4 GHz**

Client Threshold  (1 to 255)

SNR Threshold  (1 to 75 dB)

Coverage Interval  Seconds (1 to 120)

Interval  Seconds (1 to 120)

**Note:** The system automatically configures optimum values for certain fields, if you select the sensitivity option under 'Basic Settings' as 'Low', 'Medium' or 'High'. Some of the SMART RF parameters appear disabled in this case. Please choose the 'Custom' sensitivity option to enable the fields and manually enter each value.

OK   Reset   **Exit**

**Figure 203: SMART RF - Advanced Configuration Screen - Coverage Hold Recovery Tab**

2 Set the following **Coverage Hole Recovery for 2.4 GHz and 5.0 GHz** parameters:

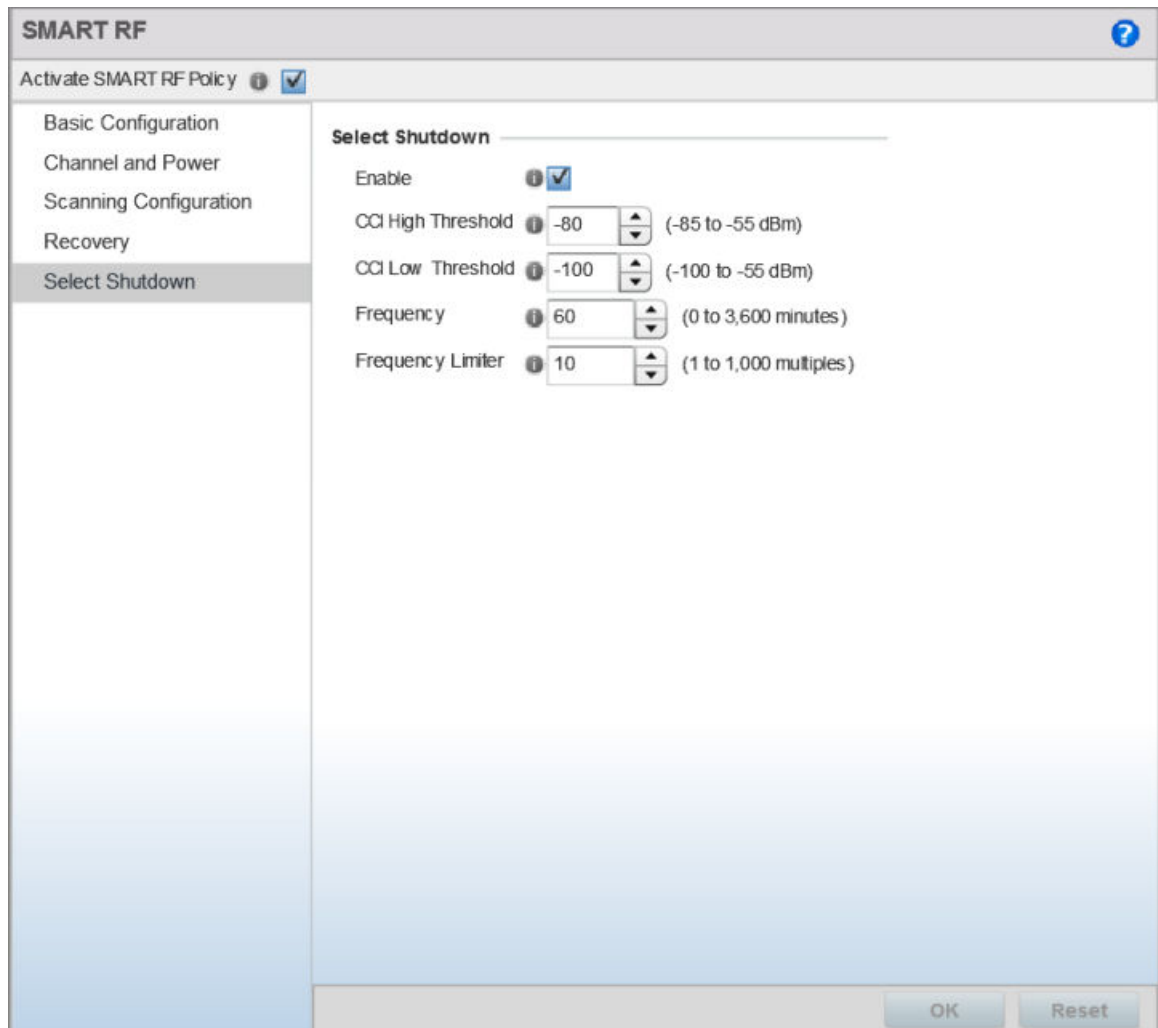
Client Threshold	Use the spinner to set a client threshold for the Smart RF policy between 1 - 255. This is the minimum number of clients a radio should have associated in order for coverage hole recovery to trigger. The default setting is 1.
SNR Threshold	Set a signal-to-noise (SNR) threshold , between 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 length of time after which coverage hole recovery should be initiated when a coverage hole is detected. The default is 10 seconds for both the 2.4 and 5.0 GHz radios.
Interval	Define the length of time 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.

- 3 Click **OK** to update the Smart RF Coverage Hole Recovery settings for this policy.  
Click **Reset** to revert to the last saved configuration.

## Configuring Smart RF Select Shutdown Settings

To enable Smart RF select and shutdown 2.4 GHz APs causing interference:

- 1 Select **Select Shutdown**, to configure parameters that will maintain CCI (co-channel interference) levels within specified limits.



The screenshot shows the SMART RF configuration window. At the top, there is a header "SMART RF" with a help icon. Below the header, there is a section "Activate SMART RF Policy" with a checked checkbox. A sidebar on the left lists configuration categories: Basic Configuration, Channel and Power, Scanning Configuration, Recovery, and Select Shutdown (which is highlighted). The main area is titled "Select Shutdown" and contains the following settings:

- Enable:
- CCI High Threshold:  (-85 to -55 dBm)
- CCI Low Threshold:  (-100 to -55 dBm)
- Frequency:  (0 to 3,600 minutes)
- Frequency Limiter:  (1 to 1,000 multiples)

At the bottom right, there are "OK" and "Reset" buttons.

**Figure 204: Smart RF Configuration - Select Shutdown screen**



Enable	<p>Select to enable auto-shutdown of radios causing interference within the Smart RF monitored network.</p> <p>Auto-shutdown of select 2.4 GHz radios, in dual-band networks, maintains CCI levels within specified limits. When enabled, Smart-RF monitors CCI levels to ensure that the deployment average CCI remains within specified minimum and maximum limits. If the deployment average CCI is found to exceed the maximum threshold, 2.4 GHz radios, causing neighbor interference, are shut down one-by-one until the deployment average CCI falls below the specified maximum threshold. The reverse process occurs when the deployment average CCI falls below the minimum threshold. In this scenario, previously disabled radios are enabled until the deployment average CCI reaches acceptable levels.</p> <p><b>Note:</b> This feature is enabled by default.</p>
CCI High Threshold	<p>Specify the maximum CCI threshold from -85 to -55 dBm. The default value is -80 dBm.</p> <p><b>Note:</b> If not specified, the system uses the default value as the upper limit for the deployment average CCI range.</p>
CCI Low Threshold	<p>Specify the minimum CCI threshold from -85 to -55 dBm. The default value is -100 dBm.</p> <p><b>Note:</b> If not specified, the system uses the default value as the lower limit for the deployment average CCI range.</p>
Frequency	<p>Configure the interval, in minutes, at which 2.4 GHz radios are selected for shut down. when the deployment average CCI exceeds the specified maximum threshold, Smart RF shuts down 2.4 GHz radios until the CCI reaches acceptable levels. Use this option, to configure the interval between successive radio shut down.</p> <p>Specify the frequency from 0 - 3600 minutes. The default is 60 minutes.</p>
Frequency Limiter	<p>Configure the minimum multiple of Interference Recovery frequency that the select-shutdown frequency can be set to.</p> <p>Specify a value from 1 - 1000. The default value is 15.</p>

- Click **OK** to update the Smart RF Select Shutdown settings for this policy.  
Click **Reset** to revert to the last saved configuration.

## Smart RF Configuration and Deployment Considerations

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.

Keep in mind, 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 channel 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 point 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.

## MeshConnex Policies

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.

## Configuring a MeshConnex Policy

To define a MeshConnex policy:

- 1 Select **Configuration > Wireless > MeshConnex Policy** to display existing MeshConnex policies.

Mesh Point	Mesh Id	Mesh Point Status	Descriptions	Control VLAN	Allowed VLANs	Security Mode	Mesh QoS Policy
policy1	101	✓ Enabled		1	2	None	default

Type to search in tables Row Count: 1

**Figure 205: MeshConnex Policy Screen**

- 2 Refer to the following configuration data for existing MeshConnex policies:

Mesh Point Name	The administrator assigned name of each listed mesh point.
Mesh ID	The IDs (mesh identifiers) assigned to mesh points.
Mesh Point Status	The status of each configured mesh point, either <b>Enabled</b> or <b>Disabled</b> .
Description	Descriptive text provided by the administrator for each configured mesh point.
Control VLAN	The VLAN (virtual interface ID) for the control VLAN on each of the configured mesh points.
Allowed VLANs	The list of VLANs allowed on each configured mesh point.
Security Mode	The security assigned to each configured mesh point – either <b>None</b> for no security or <b>PSK</b> for pre-shared key authentication.
Mesh QoS Policy	The mesh Quality of Service (QoS) policy associated with each configured mesh point.

- 3 Click **Add** to create a new MeshConnex policy, select an existing policy and click **Edit** to modify its configuration, or select an existing policy and click **Delete** to remove an obsolete policy. Optionally, **Copy** or **Rename** MeshConnex policies as needed.

The **Configuration** screen displays by default for new or modified MeshConnex policies.

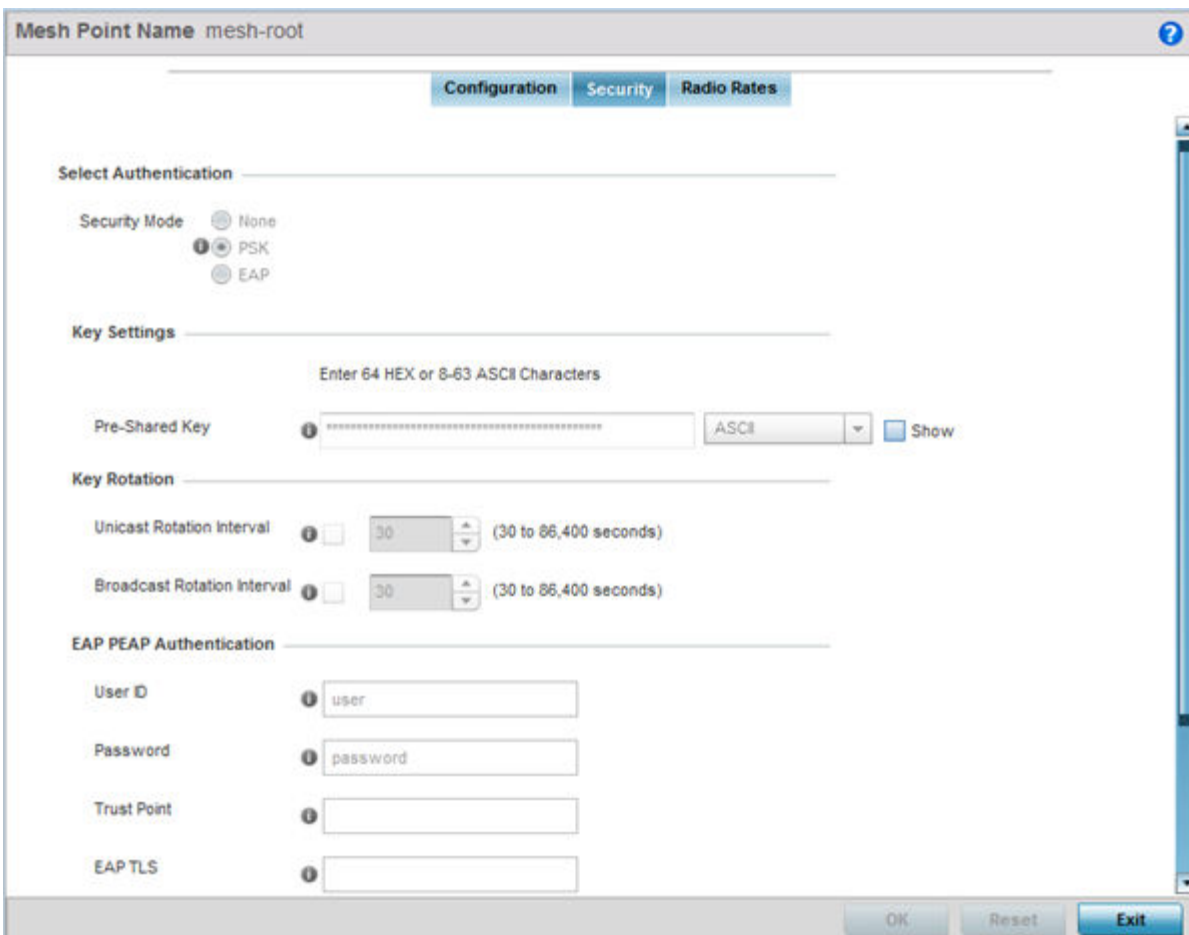
**Figure 206: MeshConnex Configuration Screen**

- 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 <b>Enabled</b> . To disable the mesh point, click <b>Disabled</b> . The default value is <b>Enabled</b> .
Mesh QoS Policy	Specify the mesh Quality of Service (QoS) policy to use on this mesh point. This value is mandatory. If no suitable mesh QoS policies exist, click the <b>Create</b> icon to create a new mesh QoS policy.
Beacon Format	Specify the format in which beacons from the mesh point are sent. To use access point style beacons, select <b>access-point</b> from the drop-down menu. To use mesh point style beacons, select <b>mesh point</b> . The default value is <b>mesh point</b> .
Is Root	Select this option to define the mesh point as a root in the mesh topology.
Control VLAN	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 that are allowed to pass traffic on the mesh point. Separate VLANs with commas. To specify a range of allowed VLANs, separate the starting VLAN and the ending VLAN with a hyphen.

Neighbor Inactivity Timeout	Specify the amount of time allowed between frames received from a neighbor before their client privileges are revoked. Specify the timeout value in seconds, minutes, hours or days, up to a maximum of 1 day. The default value is 2 minutes.
Description	Enter a 64-character maximum description for the mesh point configuration.

- Click **OK** to update the MeshConnex configuration settings for this policy.  
Click **Reset** to revert to the last saved configuration.
- Select **Security**.



**Figure 207: MeshConnex Security Screen**

- Refer to the **Select Authentication** field to define an authentication method for the mesh policy.

Security Mode	Select a security authentication point mode for the mesh point. Select <b>None</b> to have no authentication for the mesh point. Select <b>EAP</b> to use a secured credential exchange, dynamic keying and strong encryption. If selecting <b>EAP</b> , refer to the <b>EAP PEAP Authentication</b> field at the bottom of the screen and define the credentials of an EAP user and trustpoint. Select <b>PSK</b> to set a pre-shared key as the authentication for the mesh-point. If <b>PSK</b> is selected, enter a pre-shared key in the <b>Key Settings</b> field.
---------------	--

- Set the following **Key Settings** for the mesh point.

Pre-Shared Key	When the security mode is set as <b>PSK</b> , 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** settings for the mesh point.

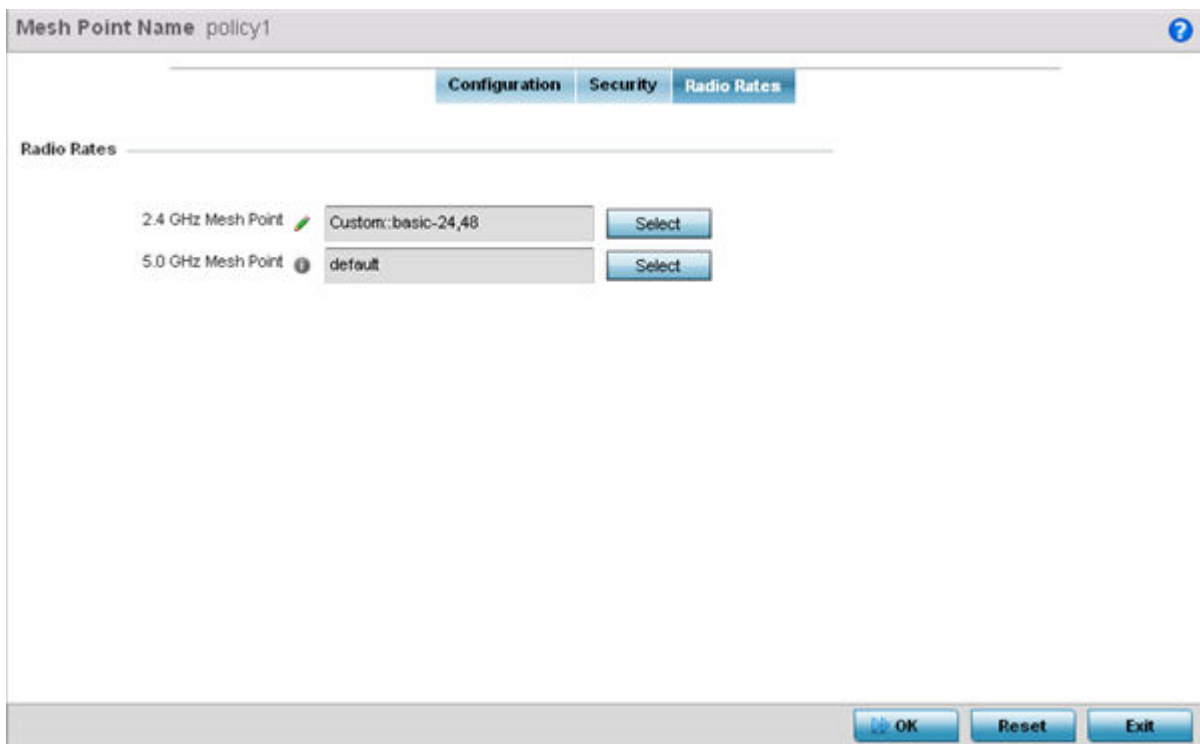
Unicast Rotation Interval	Define an interval for unicast key transmission (30 -86,400 seconds).
Broadcast Rotation Interval	When enabled, the key indices used for encrypting/decrypting broadcast traffic is alternatively rotated based on the defined interval. Define an interval for broadcast key transmission in seconds (30- 86,400). Key rotation enhances the broadcast traffic security on the WLAN.

- 10 If you are using EAP to secure the mesh point, set the following **EAP PEAP Authentication** settings.

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 user ID.
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	Configure the EAP authentication method used by the supplicant. The default EAP type is <b>PEAP-MS-CHAPv2</b> .
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 Click **OK** to save the changes made to the configuration.

Click **Reset** to revert to the last saved configuration.

12 Select **Radio Rates**.**Figure 208: Radio Rate Settings**13 Set the following **Radio Rates** for both the 2.4 and 5 GHz radio bands:

2.4 GHz Mesh Point	<p>Click <b>Select</b> to configure radio rates for the 2.4 GHz band. Define both minimum <b>Basic</b> and optimal <b>Supported</b> 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.</p> <p>If you are supporting 802.11n, select a Supported MCS index. Set an MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of eight 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).</p> <p>The selected rates apply to associated client traffic within this mesh point only.</p>
5.0 GHz Mesh Point	<p>Click <b>Select</b> to configure radio rates for the 5.0 GHz band. Define both minimum <b>Basic</b> and optimal <b>Supported</b> rates as required for the 802.11b rates, 802.11g rates 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.</p> <p>If you are supporting 802.11n, select a Supported MCS index. Set an MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of eight 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).</p> <p>The selected rates apply to associated client traffic within this mesh point only.</p>

**Rate Settings 2.4GHz-MeshPoint**

Radio Transmission Data Rates

b-only rates   
 bg rates   
 bgn rates   
 Default  
 g-only rates   
 gn rates   
 Custom Rates

**802.11b Rates**

	1Mbps	2Mbps	5.5Mbps	11Mbps
Basic:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Supported:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**802.11g Rates**

	6Mbps	9Mbps	12Mbps	18Mbps	24Mbps	36Mbps	48Mbps	54Mbps
Basic:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Supported:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**802.11n Rates**

	MCS-1Stream	MCS-2Streams
Basic:	<input type="checkbox"/>	<input type="checkbox"/>
Supported:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

OK    Reset    Cancel

**Figure 209: Advanced Rate Settings 2.4 GHz Screen**

**Rate Settings 5GHz-MeshPoint**

Radio Transmission Data Rates

a-only rates   
 Default  
 an rates   
 Custom Rates

**802.11a Rates**

	6Mbps	9Mbps	12Mbps	18Mbps	24Mbps	36Mbps	48Mbps	54Mbps
Basic:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Supported:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**802.11n Rates**

	MCS-1Stream	MCS-2Streams
Basic:	<input type="checkbox"/>	<input type="checkbox"/>
Supported:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

OK    Reset    Cancel

**Figure 210: Advanced Rate Settings 5.0 GHz Screen**

- 14 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 you are supporting 802.11n, select a Supported MCS index. Set an MCS (modulation and coding scheme) in respect to the radio's channel width and guard interval. An MCS defines (based on RF channel conditions) an optimal combination of eight 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).



- 15 Click **OK** to save the changes made to the configuration.  
Click **Reset** to revert to the last saved configuration.

## 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 ensures that each mesh point on the mesh network receives a fair share of the overall bandwidth, either equally or per the proportion configured. Packets directed to clients are classified into data types (video, voice, data, and so forth). Packets within each category are processed based on the weight (prioritization) set 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 existing Mesh QoS policies supports an ideal QoS configuration for the intended data traffic of this mesh point, click **Add** to create a new policy. Select an existing mesh QoS policy and select **Edit** to change the properties of the mesh QoS policy.

### Configuring a Mesh QoS Policy

To define a mesh QoS policy:

- 1 Select **Configuration > Wireless > Mesh QoS Policy** to display existing mesh QoS policies.

Mesh Quality of Service (QoS) <span style="float: right;">?</span>					
Mesh QoS Policy	Mesh Tx Rate Limit	Mesh Rx Rate Limit	Neighbor Rx Rate Limit	Neighbor Tx Rate Limit	Classification
policy1	✓ Enabled	✓ Enabled	✓ Enabled	✓ Enabled	Trust
Type to search in tables					Row Count: 1
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Copy"/> <input type="button" value="Rename"/> <input type="button" value="Replace"/>					

**Figure 211: Mesh QoS Policy Screen**

2 Refer to the following configuration data for existing mesh QoS policies:

Mesh QoS Policy	The administrator assigned name of each mesh QoS policy.
Mesh Tx Rate Limit	Whether a <b>Mesh Tx Rate Limit</b> is enabled for each mesh QoS policy. A green check mark means the rate limit is enabled. A red X means the rate limit is disabled.
Mesh Rx Rate Limit	Whether a <b>Mesh Rx Rate Limit</b> is enabled for each mesh QoS policy. A green check mark means the rate limit is enabled. A red X means the rate limit is disabled.
Neighbor Rx Rate Limit	Whether a <b>Neighbor Rx Rate Limit</b> is enabled for each mesh QoS policy. A green check mark means the rate limit is enabled. A red X means the rate limit is disabled.
Neighbor Tx Rate Limit	Whether a <b>Neighbor Tx Rate Limit</b> is enabled for each mesh QoS policy. A green check mark means the rate limit is enabled. A red X means the rate limit is disabled.
Classification	The forwarding QoS classification for each Mesh QoS policy. Classification types are <b>Trust, Voice, Video, Best Effort</b> , and <b>Background</b> .

- 3 Click **Add** to define a new mesh QoS policy, select an existing policy and click **Edit** to modify its configuration, or select an existing policy and click **Delete** to remove an obsolete policy. Optionally, **Copy** or **Rename** mesh QoS policies as needed.

The **Rate Limit** screen displays by default for new or modified mesh QoS policies.

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 like 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 you define 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 enduser 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.

The screenshot displays the configuration for a Mesh QoS Policy named 'policy1'. The interface is split into two main sections: Mesh Point Settings and Neighbor Settings. Each section contains two columns of settings: Rate Limit and Random Early Detection Threshold.

**Mesh Point Settings**

- From Air Upstream Rate Limit:** Mesh Tx Rate Limit (checked), Rate: 5000 kbps, Maximum Burst Size: 320 kbytes.
- To Air Downstream Rate Limit:** Mesh Rx Rate Limit (checked), Rate: 5000 kbps, Maximum Burst Size: 320 kbytes.
- From Air Upstream Random Early Detection Threshold:** Background Traffic: 50%, Best Effort Traffic: 50%, Video Traffic: 25%, Voice Traffic: 0%.
- To Air Downstream Random Early Detection Threshold:** Background Traffic: 50%, Best Effort Traffic: 50%, Video Traffic: 25%, Voice Traffic: 0%.

**Neighbor Settings**

- From Air Upstream Rate Limit:** Neighbor Rx Rate Limit (checked), Rate: 1000 kbps, Maximum Burst Size: 64 kbytes.
- To Air Downstream Rate Limit:** Neighbor Tx Rate Limit (checked), Rate: 1000 kbps, Maximum Burst Size: 64 kbytes.
- From Air Upstream Random Early Detection Threshold:** Background Traffic: 50%, Best Effort Traffic: 50%, Video Traffic: 25%, Voice Traffic: 0%.
- To Air Downstream Random Early Detection Threshold:** Background Traffic: 50%, Best Effort Traffic: 50%, Video Traffic: 25%, Voice Traffic: 0%.

- 4 Configure the following parameters for the **From Air Upstream Rate Limit**, or traffic from the controller to associated access point radios and their associated neighbor:

Mesh Tx Rate Limit	Select this option to enable rate limiting for all data received from any mesh point in the mesh. This feature is disabled by default.
Rate	Define a receive rate limit between 50 and 1,000,000 kbps. This limit constitutes a threshold for the maximum 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 5,000 kbps.
Maximum Burst Size	Set a maximum burst size between 2 and 1024K bytes. 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 320K bytes.

- 5 Set the following **From Air Upstream Random Early Detection Threshold** settings, for each access category.

An early random drop occurs 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 for the **To Air Upstream Rate Limit**, or traffic from neighbors to associated access point radios and the controller or service platform:

Mesh Rx Rate Limit	Select this option 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 a transmit rate limit between 50 and 1,000,000 kbps. This limit constitutes a threshold for the maximum 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 5,000 kbps.
Maximum Burst Size	Set a maximum burst size between 2 and 1024K bytes. The smaller the burst, the less likely the transmit packet transmission will result in congestion for the mesh point's 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 10% margin (minimally) to allow for traffic bursts at the site. The default burst size is 320K bytes.

- 7 Set the following **To Air Upstream Random Early Detection Threshold** settings, for each access category.

An early random drop occurs when the number 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 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 receive 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 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 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 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 upstream rate is known by the network administrator (using a time trend analysis). The default threshold is 0%.

- 8 Configure the following settings for **From Air Upstream Rate Limit** in the **Neighbor Settings** field:

Neighbor Rx Rate Limit	Select this option 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 a transmit rate limit between 50 and 1,000,000 kbps. This limit constitutes a threshold for the maximum 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 5,000 kbps.
Maximum Burst Size	Set a maximum burst size between 2 and 1024K bytes. The smaller the burst, the less likely the transmit packet transmission will result in congestion for the wireless client. The default burst size is 320K bytes.

- 9 Configure the following settings for **From Air Upstream Random Early Detection Threshold** in the **Neighbor Settings** field:

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. 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. 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. 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. The default threshold is 0%, which implies that no early random drops will occur.

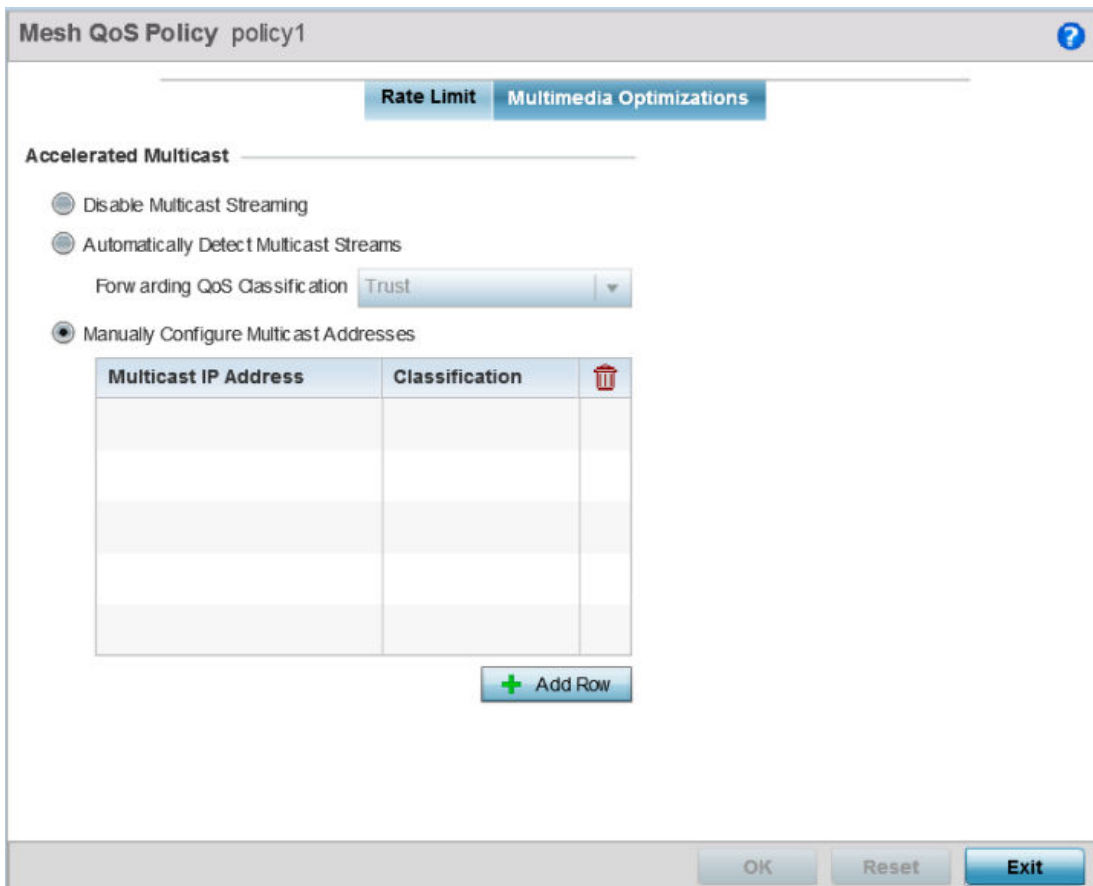
- 10 Configure the following settings for **To Air Upstream Rate Limit**, or traffic from a controller or service platform to associated access point radios and the wireless client:

Neighbor Tx Rate Limit	Select this option 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 transmit rate limit between 50 and 1,000,000 kbps. This limit constitutes a threshold for the maximum 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 setting is 1,000 kbps.
Maximum Burst Size	Set a maximum burst size between 2 and 1024K bytes. The smaller the burst, the less likely the receive packet transmission will result in congestion for the wireless client. The default burst size is 320K bytes.

- Set the following **To Air Upstream Random Early Detection Threshold** 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 and a log message is generated. 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 priority traffic. Best effort traffic exceeding the defined threshold is dropped and a log message is generated. 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. 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. The default threshold is 0%, which implies that no early random drops will occur.

- Click **OK** to update this mesh QoS rate limit settings.  
Click **Reset** to revert to the last saved configuration.
- Select **Multimedia Optimizations**.



**Figure 213: 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 have bridged 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 to be converted to unicast. When the stream is converted and being queued up for transmission, a number of classification mechanisms can be applied to the stream. The administrator can choose from the following classification types: <b>Trust</b> , <b>Voice</b> , <b>Video</b> , <b>Best Effort</b> , and <b>Background</b> .
Manually Configure Multicast Addresses	Select <b>+ Add Row</b> and specify a list of multicast addresses and classifications. Packets are accelerated when the destination addresses matches.

15 Click **OK** to update the Mesh Multimedia Optimizations settings.

Click **Reset** to revert to the last saved configuration.

## 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 policies for network hotspots. Each passpoint policy can be selected to edit its properties. If no existing passpoint policies supports the required deployment, select Add to create a new policy.

To administrate and manage existing passpoint policies:

- 1 Select **Configuration**.
- 2 Select the **Wireless** item under Configuration.
- 3 Select **Passpoint Policy** from the Wireless node on the left-hand of the screen.





- 1 Select **Configuration > Wireless > Passpoint Policy** to display existing passpoint policies.

Name	Access Network Type	Operator Name	Venue Name
policy1	private-guest	lancelot	percival

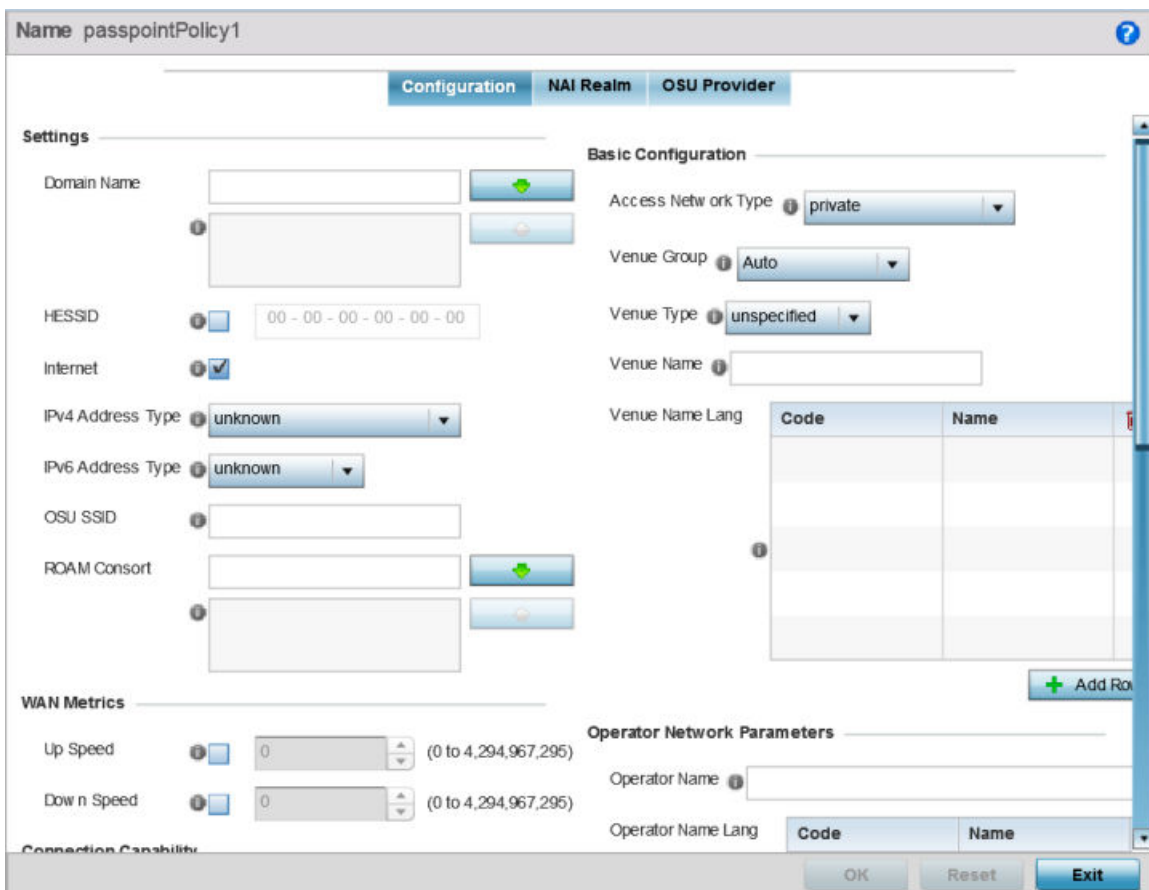
Type to search in tables Row Count: 1

**Figure 214: Passpoint Policy Screen**

- 2 Refer to the following configuration data for existing passpoint policies:

Name	The administrator assigned name of each passpoint policy.
Access Network Type	The network access permissions the administrator has set for the passpoint policy.
Operator Name	The unique name assigned to the administrator or operator responsible for the configuration and operation of the access point managed hotspot.
Venue Name	The administrator assigned name of the venue (or physical location) of the deployed access point hotspot.

- Click **Add** to define a new passpoint policy, select an existing policy and click **Edit** to modify its configuration, or select an existing policy and click **Delete** to remove an obsolete policy.  
Optionally, **Copy** or **Rename** passpoint policies as needed.



**Figure 215: Passpoint Policy - Configuration Screen**

- Configure 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	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 <b>not available</b> , <b>public</b> , <b>port-restricted</b> , <b>port-restricted-double-nat</b> , <b>single-nat</b> , <b>double-nat</b> , <b>port-restricted-single-nat</b> , and <b>unknown</b> .

IPv6 Address Type	Select the IPv6 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 <b>available</b> , <b>unavailable</b> , and <b>unknown</b> .
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 the passpoint policy's FTP, HTTP, ICMP, IPSec VPN, PPTP VPN, SIP, SSH, and TLS VPN interfaces:

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.

- 7 Select **+ Add Row** to set a **Connection Capability Variable** to make specific virtual ports **open** or **closed** for Wi-Fi connection attempts and to set rules for how the user can connect with routing preference using this passpoint policy.
- 8 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.
- 9 Refer to the **Basic Configuration** field to set the following:

Access Network Type	Select the network access method for this passpoint policy. Access network types include:  <table border="0"> <tr> <td><b>private</b></td> <td>General access to a private network hotspot (default setting)</td> </tr> <tr> <td><b>private-guest</b></td> <td>Access to a private network hotspot with guest services</td> </tr> <tr> <td><b>chargeable-public</b></td> <td>Access to a public hotspot with billable services</td> </tr> <tr> <td><b>personal-device</b></td> <td>Access to a hotspot for personal devices such as wireless routers</td> </tr> <tr> <td><b>emergency services</b></td> <td>Dedicated network hotspot access for emergency services only</td> </tr> </table>	<b>private</b>	General access to a private network hotspot (default setting)	<b>private-guest</b>	Access to a private network hotspot with guest services	<b>chargeable-public</b>	Access to a public hotspot with billable services	<b>personal-device</b>	Access to a hotspot for personal devices such as wireless routers	<b>emergency services</b>	Dedicated network hotspot access for emergency services only
<b>private</b>	General access to a private network hotspot (default setting)										
<b>private-guest</b>	Access to a private network hotspot with guest services										
<b>chargeable-public</b>	Access to a public hotspot with billable services										
<b>personal-device</b>	Access to a hotspot for personal devices such as wireless routers										
<b>emergency services</b>	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 Long	Hotspot operators can list venue names in multiple languages. Select the <b>+ Add Row</b> button to add venue name languages. Enter the two- or three-character ISO-14962-1997 encoded string that defines the language used in the <b>Code</b> field. Enter the name of the venue in the <b>Name</b> field. The name cannot exceed 252 characters.

10 Refer to the **Operator Network Parameters** field to define the following:

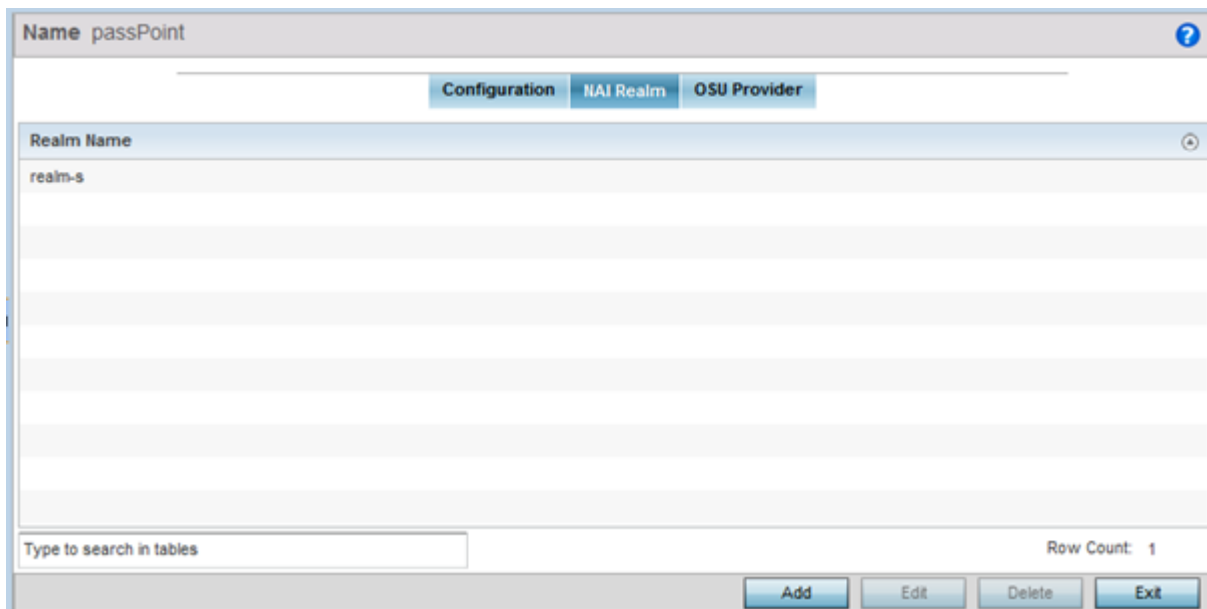
Operator Name	Provide the unique name (in English) of the administrator or operator responsible for the configuration and management of the hotspot. The name cannot exceed 64 characters.
Operator Name Long	Operator names can be listed in multiple languages. Select the <b>+ Add Row</b> button to add operator name languages. Enter the two- or three-character ISO-14962-1997 encoded string that defines the language used in the <b>Code</b> field. Enter the name of the operator in the <b>Name</b> 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 <b>+ Add Row</b> 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.

11 Click **OK** to update the passpoint policy settings.  
Click **Reset** to revert to the last saved configuration.

12 Select **NAI Realm**.

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 216: Passpoint Policy - NAI Realm Screen**

- 13 Click **Add** to create a new NAI realm configuration for passpoint hotspot utilization, **Edit** to modify the attributes of an existing configuration, or **Delete** to remove a selected configuration from those available.

Provide a realm name or names (32 characters maximum), delimited by semicolons. Click **+ Add Row** to create an EAP Method configuration for the NAI realm.

**Figure 217: Passpoint Policy - NAI Realm EAP Method 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. NAs are often user identifiers in the EAP authentication protocol.
Method	Set an EAP method for the NAI realm. Options include <b>identity</b> , <b>otp</b> , <b>gtc</b> , <b>rsa-public-key</b> , <b>tls</b> , <b>sim</b> , <b>ttls</b> , <b>peap</b> , <b>ms-auth</b> , <b>ms-authv2</b> , <b>fast</b> , <b>psk</b> , and <b>ikev2</b> .
Authentication Type	Specify the EAP method authentication type. Options include <b>expanded-eap</b> , <b>non-eap-inner</b> , <b>inner-eap</b> , <b>expanded-inner-eap</b> , <b>credential</b> , <b>tunn-eap-credential</b> , and <b>vendor</b> .
Authentication Value	If you are setting the authentication type to either <b>non-eap-inner</b> , <b>inner-eap</b> , <b>credential</b> , or <b>tunnel-eap-credential</b> , 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 <b>expanded-eap</b> or <b>expanded-inner-eap</b> , set a six-character authentication vendor ID. This ID must match the ID 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 in an <b>a- FA -F0-9</b> format.
Authentication Vendor Type	Set an eight-character authentication vendor type used exclusively for the <b>expanded-eap</b> or <b>expanded-inner-eap</b> authentication types.

- 15 Click **OK** to save the updates to the NAI realm.  
Click **Reset** to revert to the last saved configuration.



16 Select **OSU Provider**.

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 the following 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.

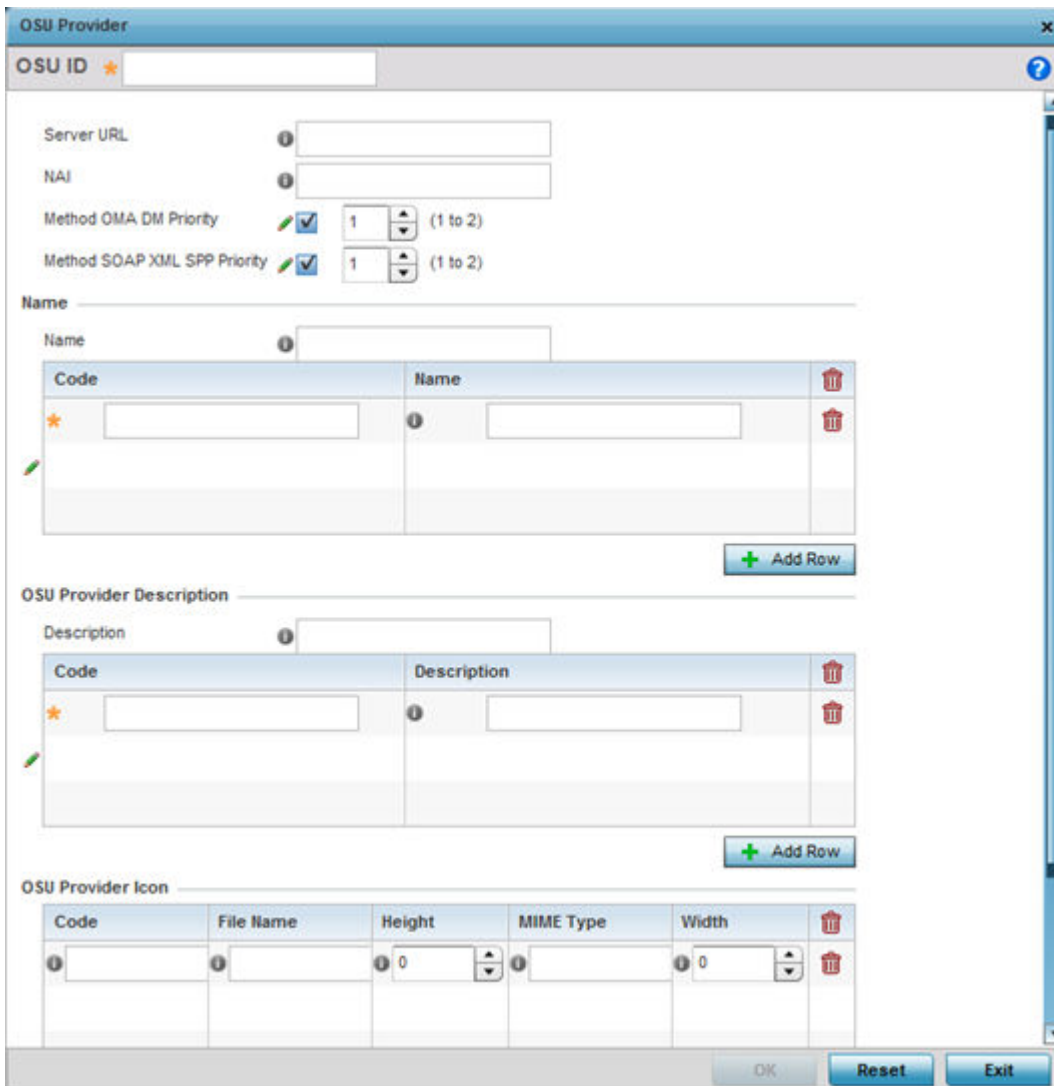
The **OSU Provider** screen displays those provider configurations created thus far for use with a passpoint policy.

OSU ID	Name	Description	Server URL	IAI
osu	sssis	sadfsadf	https://123.org.in/	ssss

Type to search in tables Row Count: 1

**Figure 218: Passpoint Policy - OSU Provider Screen**

- Click **Add** to create a new OSU provider configuration for passpoint hotspot utilization, **Edit** to modify the attributes of an existing configuration, or **Delete** to remove a selected configuration from those available.



**Figure 219: Passpoint Policy - OSU Provider - Add/Edit Screen**

- If you are creating a new OSU provider configuration, provide it a 32-character maximum OSU ID that will serve as an online sign up identifier.
- Set the following attributes to secure the Network Access Identifier (NAI) submitted by the hotspot during OSU authentication:

Server URL	Provide a 255 character maximum sign up server URL for the OSU provider.
NAI	Enter a 255 character maximum 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. 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.

- 20 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 than 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.

- 21 Refer to the **OSU Provider Description** field to set an online sign up description in a language other than English.

Select **+ Add Row** and provide a 3-character maximum ISO-639 language code to apply the sign up name in a language other than 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.

- 22 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 for the icon file.
Height	Provide the icon's height in pixels from 0 - 65,535. The default setting is 0.
MIME Type	Set the icon's 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's width in pixels from 0 - 65,535. The default setting is 0.

- 23 Click **OK** to save the updates to the OSU Provider configuration.

Click **Reset** to revert to the last saved configuration.

## Sensor Policy

In addition to WIPS support, sensor functionality has now been added for Extreme Networks' locationing system (ExtremeLocation). The ExtremeLocation system for Wi-Fi locationing includes WiNG controllers and access points functioning as sensors. Within the ExtremeLocation architecture, sensors scan for RSSI data on an administrator defined interval and send to a dedicated ExtremeLocation server resource, as opposed to an ADSP server. The ExtremeLocation server collects the RSSI data from WiNG sensor devices, and calculates the location of Wi-Fi devices.

### Configuring a Sensor Policy

To administer and manage existing sensor policies:

- 1 Select **Configuration > Wireless > Sensor Policy** to display existing sensor policies.

The screenshot shows the 'Sensor Policy' configuration window. At the top, there is a search bar with the text 'Type to search in tables' and a 'Row Count: 2' indicator. Below the search bar is a table with the following content:

Name
99
policy1

At the bottom of the window, there are five buttons: 'Add', 'Edit', 'Delete', 'Copy', and 'Rename'.

**Figure 220: Sensor Policy Screen**

- 2 Click **Add** to define a new sensor policy, select an existing policy and click **Edit** to modify its configuration, or select an existing policy and click **Delete** to remove an obsolete policy. Optionally, **Copy** or **Rename** sensor policies 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, not the WiNG interface, to configure the sensor.

The screenshot shows the 'Add New Sensor Policy' configuration window for 'policy1'. It includes the following settings:

- RSSI Scan Interval:** 1 Seconds (range: 1 to 60)
- Channel Settings:**
  - Scan Mode:**  Default-Scan,  Custom-Scan,  Channel-Lock
- Channel List Table:**

Channel	Channel Width	Scan Weight
Ch 1(2.412) GHz	40MHz-Upper	1000
Ch 6(2.437) GHz	40MHz-Lower	1000
Ch 11(2.462) GHz	40MHz-Lower	1000
Ch 36(5.18) GHz	80MHz	1000
Ch 40(5.2) GHz	80MHz	1000
Ch 44(5.22) GHz	80MHz	1000
Ch 48(5.24) GHz	80MHz	1000

At the bottom of the window, there are three buttons: 'OK', 'Reset', and 'Exit'.

**Figure 221: Wireless - Sensor Policy - Add New Sensor Policy Screen**

- 3 Provide a name for this sensor policy in the **Name** field.

Sensor policy name cannot exceed 32 characters and cannot contain spaces. Define a name unique to the policy's channel and scan mode configuration to help differentiate it from other policies.

- 4 Select **Continue** to create the sensor policy.

The **Sensor Policy Addition** screen displays with the **Scan Mode** set to **Default-Scan**. The user configurable parameters on this screen differ, depending on which **Scan Mode** is selected.

- 5 Use the **RSSI Scan Interval** drop-down menu to set a scan interval from 1 - 60 seconds.

This is the scan period used by dedicated sensors (access point radios) for RSSI (signal strength) assessments. Once the sensor obtains the RSSI data, the sensor sends the data to a specified ExtremeLocation server resource (not an ADSP server) for calculating Wi-Fi device locations. The default is 1 second.

- 6 Set the following **Scan Mode** values.

The values you can select depend on whether you have selected **Default-Scan**, **Custom-Scan**, or **Channel-Lock** as the mode for scan operation.

Channel	<p>With <b>Default-Scan</b> selected: The list of available scan channels is fixed and defaulted in a spread pattern of 1, 6, 11, 36, 40, 44 and 48. You cannot change this channel pattern.</p> <p>With <b>Custom-Scan</b> selected: 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.</p> <p>With <b>Channel-Lock</b> selected: The <b>Channel</b>, <b>Channel Width</b>, and <b>Scan Weight</b> fields are replaced by a <b>Lock Frequency</b> drop-down menu. Use this menu to lock the RSSI scan to one specific channel.</p>
Channel Width	<p>With <b>Default-Scan</b> selected: 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).</p> <p>With <b>Custom-Scan</b> selected: You can define the width for each selected channel. Note that many channels have their width fixed at 20MHz. 802.11a radios support 20 and 40 MHz channel widths.</p> <p>With <b>Channel-Lock</b> selected: You cannot adjust the width between adjacent channels, because only one channel is locked.</p>
Scan Weight	<p>With <b>Default-Scan</b> selected: 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.</p> <p>With <b>Custom-Scan</b> selected: 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.</p> <p>With <b>Channel-Lock</b> selected: With one channel locked for an RSSI scan, you cannot adjust scan weights for other, unlocked channels.</p>

- 7 Click **OK** to save the updates to the sensor policy configuration.

Click **Reset** to revert to the last saved configuration.

# 7 Network Configuration

Policy Based Routing (PBR)  
L2TP V3 Configuration  
Crypto CMP Policy  
AAA Policy  
AAA TACACS Policy  
IPv6 Router Advertisement Policy  
Border Gateway Protocol (BGP)  
Alias  
Application Policy  
Application  
Application Group  
Schedule Policy  
URL Filtering  
Web Filtering  
Configuring EX3500 QoS Class  
Configuring EX3500 QoS Policy Map  
Network Deployment Considerations

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 \(PBR\)](#) on page 439
- [L2TP V3 Configuration](#) on page 444
- [Crypto CMP Policy](#) on page 447
- [AAA Policy](#) on page 451
- [AAA TACACS Policy](#) on page 462
- [IPv6 Router Advertisement Policy](#) on page 469
- [Border Gateway Protocol \(BGP\)](#) on page 472
- [Alias](#) on page 486
- [Application Policy](#) on page 491
- [Application](#) on page 495
- [Application Group](#) on page 497
- [Schedule Policy](#) on page 500
- [URL Filtering](#) on page 501
- [Web Filtering](#) on page 505
- [Configuring EX3500 QoS Class](#) on page 506

- [Configuring EX3500 QoS Policy Map](#) on page 510
- [Network Deployment Considerations](#) on page 515

## Policy Based Routing (PBR)

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. Routemaps 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:
  - If a defined next hop is reachable, it's used. If fallback is configured refer to (b).
  - Do normal destination based route lookup. If a next hop is found its used, if not refer to (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.



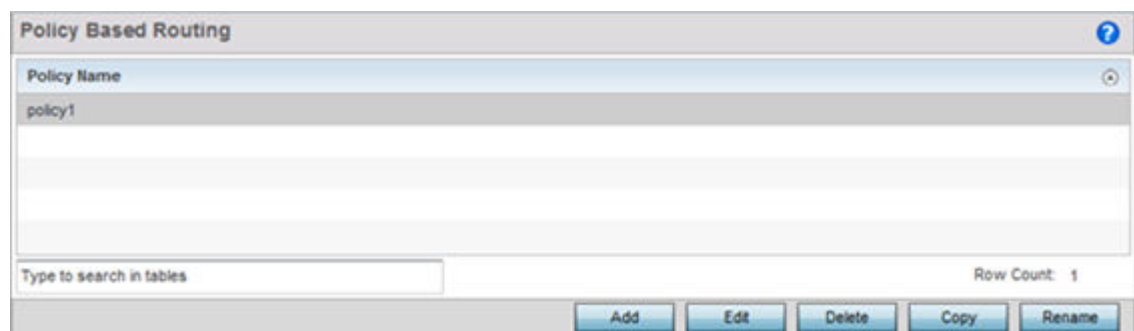
#### Note

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 **Configuration > Network > Policy Based Routing** .

The **Policy Based Routing** screen displays.



- 2 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. Select **Copy** to copy the selected PBR configuration or **Rename** to rename the PBR configuration.



- 3 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.

Precedence	DSCP	Role Policy	User Role	Access Control List	WLAN	Incoming Interface
3	0	STORES	Role3	from_ipad_to_windo	RF1WLAN	vlan2

Type to search in tables Row Count: 1

Add Edit Delete Exit

- 4 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.

- 5 Select **Add** or **Edit** to create or modify a route-map configuration. Configurations can optionally be removed by selecting **Delete**.

The screenshot shows the 'Route Map' configuration window for 'Precedence 3'. The 'Match Clauses' section includes:
 

- DSCP:  [0] (0 to 63)
- Role Policy: STORES
- User Role: Role3
- Access Control List: from\_ipad\_to\_windows
- WLAN: RF1WLAN
- Incoming Interface:  [ ] or  VLAN ID [2]

 The 'Action Clauses' section includes:
 

- Next Hop(Primary):  IP [157, 235, 121, 212] Interface: vlan [1]
- Next Hop(Secondary):  IP [157, 235, 121, 213] Interface: vlan [1]
- Default Next Hop:  IP [157, 235, 121, 214] Interface: vlan [1]
- Use Destination Routing:
- Mark:  [ ] (0 to 63)

 Buttons for OK, Reset, and Exit are at the bottom right.

- 6 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).
- 7 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.

- 8 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.

- 9 Select **OK** to save the updates to the route-map configuration. Select **Reset** to revert to the last saved configuration.

---

## 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 supported controllers 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 managed devices and other vendor devices supporting the L2TP V3 protocol.

Multiple pseudowires can be created within an L2TP V3 tunnel. WiNG managed 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 pseudowire 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 > L2TP V3**.

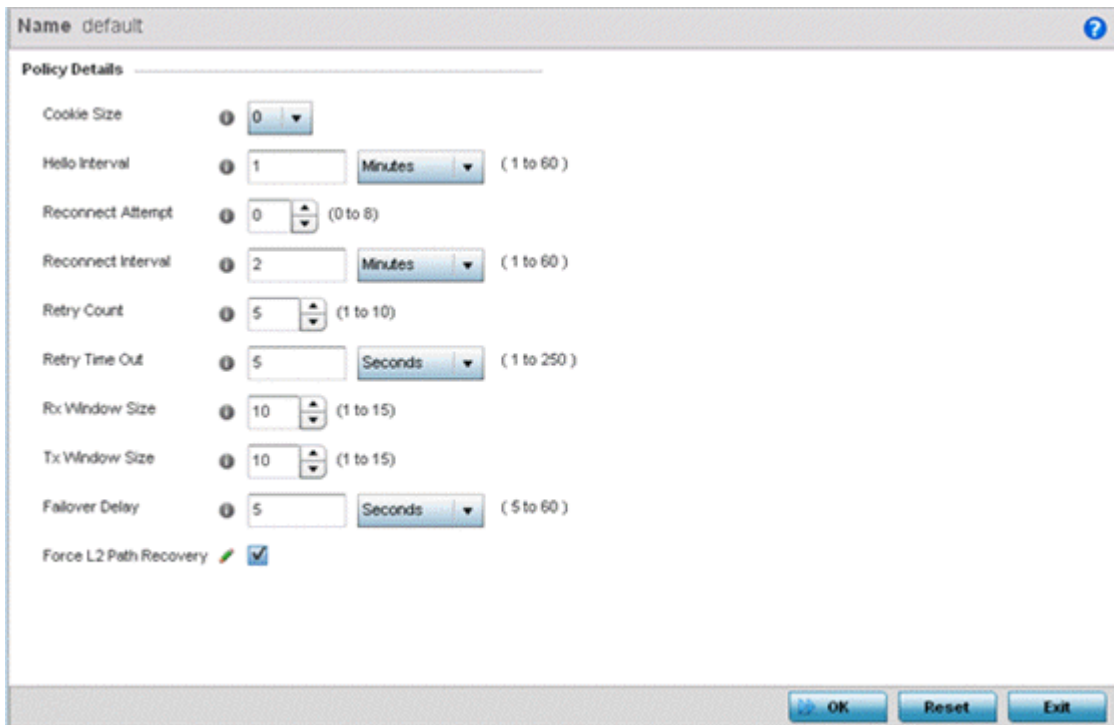
The **L2TP V3** screen opens and lists the policy configurations defined thus far.

Name	Cookie Size	Hello Interval	Reconnect Attempt	Reconnect Interval	Retry Count	Retry Time Out	Rx Window Size	Tx Window Size	Failover Delay	Force L2 Path Recovery
default	0	1m 0s	0	2m 0s	5	5s	10	10	5s	X

- 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 upon creation.
Cookie size	Displays the size of each policy's cookie field 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, the cookie size can't be configured per session, and are the same size for all sessions with in a tunnel.
Hello Interval	Displays each policy's interval between L2TP V3 hello keep alive messages exchanged within the L2TP V3 connection.
Reconnect Attempts	Lists each policy's maximum number of re-connection attempts to reestablish a tunnel between peers.
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. Select **Copy** to copy the selected L2TPv3 policy or **Rename** to rename the L2TPv3 policy.



- 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 with in a tunnel.
Hello Interval	Define an interval in <i>Seconds</i> (1 - 3,600), <i>Minutes</i> (1 -60) or <i>Hours</i> (1) between L2TP V3 hello keep alive messages exchanged within the L2TP V3 control connection. The default setting is 1 minute.
Reconnect Attempts	Use the spinner control to set a value (from 0 - 250) representing the maximum number of reconnection attempts to reestablish the tunnel. The default interval is 0.
Reconnect Interval	Define an interval in either <i>Seconds</i> (1 - 3,600), <i>Minutes</i> (1 -60) or <i>Hours</i> (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 set the interval (in seconds) before initiating the retransmission of a L2TP V3 signaling message. The range is from 1 - 250, with a default of 5.
Rx Window Size	Specify the number of packets received without sending an acknowledgment. The range is from 1 - 15, with a default of 10.



Tx Window Size	Specify the number of packets transmitted without receiving an acknowledgment. The range is from 1 - 15, with a default of 10.
Failover Delay	Set the time in <i>Seconds</i> (5 - 60) or <i>Minutes</i> (1) for establishing a tunnel after a failover (VRRP/RF Domain/Cluster). The default is 5 seconds
Force L2 Path Recovery	Determine whether force L2 path recovery is <i>enabled</i> or <i>disabled</i> . 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.

## 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.

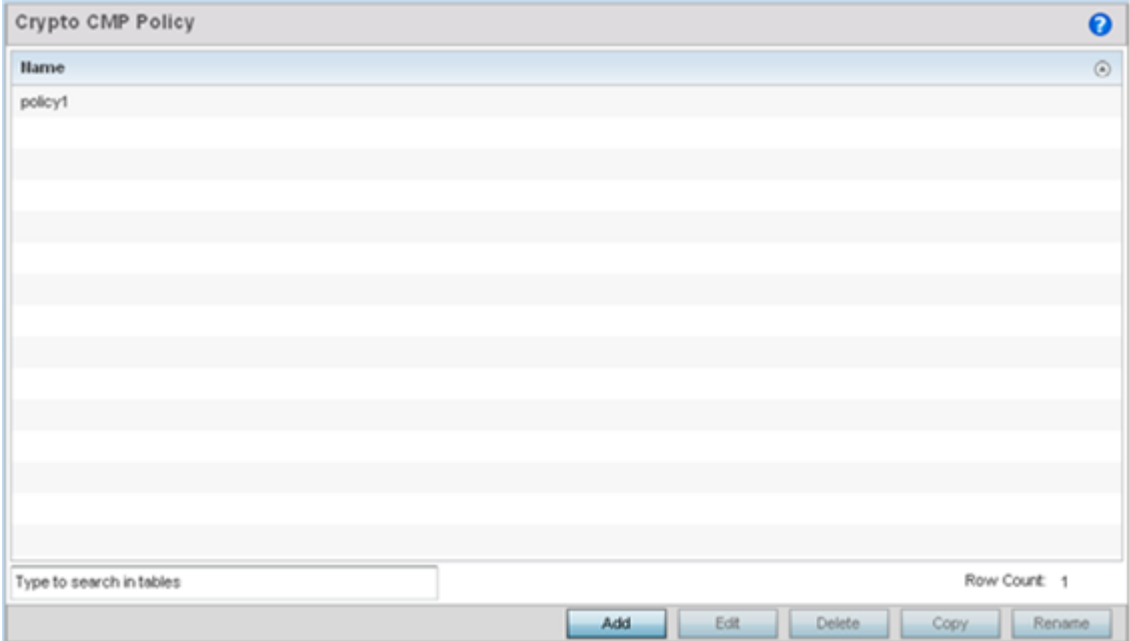
Using CMP, a device can communicate to a CMP supported CA server, initiate a certificate request and download the required certificates from the CA server. CMP supports multiple request options through for device communicating to a CMP supported CA server. The device can initiate a request for getting 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 **ConfigurationNetworkCrypto CMP Policy**.

The **Crypto CMP Policy** screen lists the policy configuration 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.

**Name** \*

**Crypto CMP Policy Details**

Certificate Renewal Timeout: 14 (1 to 60 days)

Certificate Update:

Certificate Validate:

Auto-gen Unique ID:

Certificate Key Size: 2048 (bits)

Hash Algorithm: sha1

**CMS Server Configuration**

Enable	IP	Path	Port	

+ Add Row

**Trust Points**

Name	Subject Name	Reference ID	Secret	Sender Name	Recipient Name	

+ Add Row

**Subject Alt Name**

SAN Type: \*

SAN Value: \*

OK Reset Exit

**Figure 222: 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 automatically validate the cross certificate with the factory certificate.
- 7 Select **Auto-gen Unique ID** to prepend the device's auto-generated unique ID in the subject and sender fields
- 8 Set the **Certificate Key Size** value. Set a value in the range 2,048 - 4,096 bits. The default value is 2048 bits. The larger the key size, the more secure the certificate.

- 9 Use the **Hash Algorithm** drop-down menu, to set the hashing algorithm as **sha1**, **sha256**, **sha384** or **sha512**. Hashing algorithms are mathematical functions that convert a string of characters (of indefinite length) to a fixed numerical value, much smaller than the original string. Hashing algorithms are used to sign digital certificates. The hash-algorithm type configured here is sent, in the request for certification (new or renewal), to the CA server. The CA uses the hash algorithm specified here to sign the digital certificate. The default setting is sha1.

The sha256, sha384 and sha512 hash functions belong to the SHA-2 family of algorithms.

- 10 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.

- 11 Set the following **Trust Points** settings. Use the **+ Add Row** button to add a row to this table. 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.

- 12 Set the following **Subject Alt Name** settings:

SAN Type	Use the drop-down menu to set the Subject Alt Name type as either IP Address, Distinguished Name, Email, String, or FQDN. This field is mandatory.
SAN Value	Provide a Subject Alt Name value of up to 128 characters for the certificate template example. The value provided depends on the Subject Alt Name type selected. This field is mandatory.

- 13 Select **OK** to save the updates to the Crypto CMP policy, **Reset** to revert to the last saved configuration, or **Exit** to close the screen.

## AAA Policy

---

*Authentication, Authorization, and Accounting (AAA)* provides the mechanism network administrators define access control within the network.

A controller, service platform or Access Point can interoperate with external RADIUS and LDAP Servers (AAA Servers) to provide an additional user database and authentication resource. 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 controller, service platform or Access Point WLAN AAA configurations:

1 Select **Configuration > Network > AAA Policy**.

The **Authentication, Authorization, and Accounting (AAA)** screen lists those AAA policies created thus far. Any of these policies can be selected and applied.

Authentication, Authorization, and Accounting (AAA) <span style="float: right;">?</span>				
AAA Policy	Accounting Packet Type	Request Interval	NAC Policy	Server Pooling Mode
AAAPolicy1	Start/Stop	30m 0s		Failover
AAAPolicy2	Start/Stop	30m 0s		Failover
AAAPolicy3	Start/Interim/Stop	1m 0s		Failover
EXTERNAL-AAA-SERVERS	Start/Stop	30m 0s		Failover
INTERNAL-AAA-SERVER	Start/Stop	30m 0s		Failover
Type to search in tables <span style="float: right;">Row Count: 5</span>				
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Copy"/> <input type="button" value="Rename"/>				

2 Refer to the following information listed for each existing AAA policy:

AAA Policy	Displays the name assigned to the AAA 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: <ul style="list-style-type: none"> <li><i>Start Only</i> - Sends a start accounting notice to initiate user accounting.</li> <li><i>Start/Stop</i> - 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.</li> </ul>
Request Interval	Lists each AAA policy's interval used to send a RADIUS accounting request to the RADIUS server.
NAC Policy	Lists the name <i>Network Access Control</i> (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 <i>Failover</i> results in working down the list of servers if a server is unresponsive and unavailable. The <i>Load Balanced</i> option uses all available servers transmitting requests in round robin.

- 3 To configure a new AAA policy, click **Add**. To modify an existing AAA configuration, select it from amongst those available and click **Edit**. Existing policies can be copied or renamed as needed.

AAA Policy EXTERNAL-AAA-SERVERS

RADIUS Authentication RADIUS Accounting Settings

Server Id	Server Type	Host	Port	Request Proxy Mode	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable
1	Host	172.168.1.104	1,812	Through Wirele	3	3s	0	✗	✗
2	onboard-contr		1,812	None	3	3s	0	✗	✗

Type to search in tables

Row Count: 2

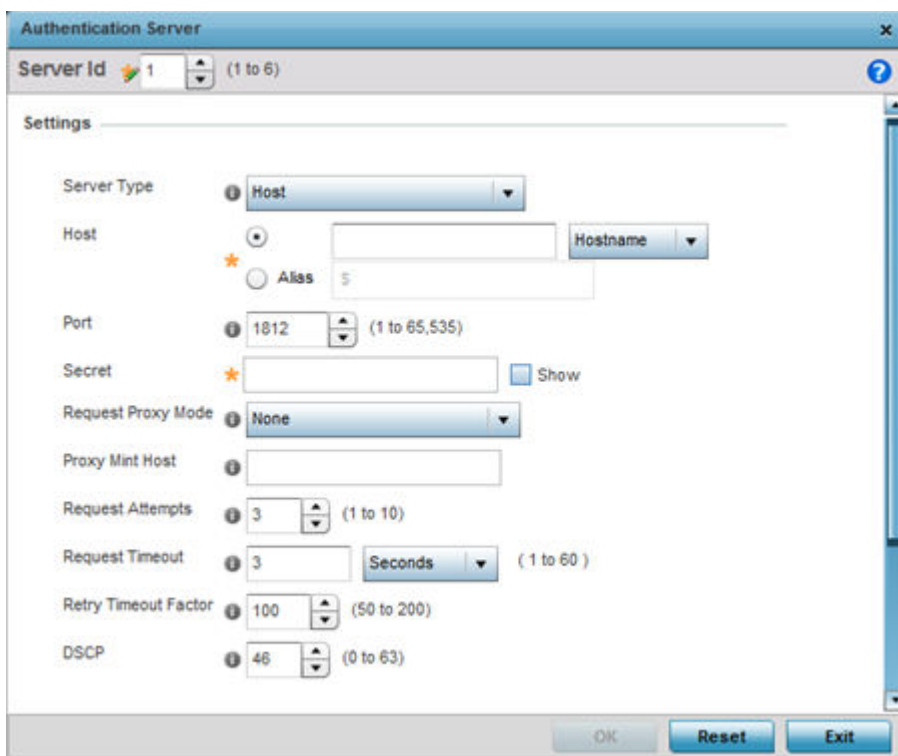
Add Edit Delete Exit

- 4 Refer to the following **RADIUS Authentication** details:

Server Id	Displays the numerical server index (1-6) for the accounting server when added to the list available to the access point.
Server Type	Displays the type of AAA server in use as 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 access point managed network. The port range is 1 - 65,535. The default port is 1812.
Request Proxy Mode	Displays whether a request is transmitted directly through the server or proxied through the Virtual Controller AP 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 from 1 - 10. The default is 3.
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.

<p>NAI Routing Enable</p>	<p>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.</p>
<p>NAC Enable</p>	<p>A green check defines NAC as enabled, while a Red X defines NAC disabled with this AAA policy.</p>

- 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.



- 6 Define the following settings to add or modify AAA RADIUS authentication server configuration:

<p>Server Id</p>	<p>Define the numerical server index (1-6) for the authentication server to differentiate it from others available to the access point's AAA policy.</p>
<p>Server Type</p>	<p>Select the type of AAA server as either Host, onboard-self or onboardcontroller.</p>

Host	Specify the IP address or hostname of the RADIUS authentication 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 server listens to traffic within then access point managed 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.
Proxy 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 from 1 - 10. The default is 3.
Request Timeout	Specify the time from 1 - 60 seconds for the access point's re-transmission of request packets. If this time is exceeded, the authentication session is terminated. The default is 5 seconds.
Request Timeout Factor	Specify the time from 50 - 200 seconds between retry timeouts for the access points's 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	Select this check box 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. 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. Each user still needs a unique security association, but these associations can be stored on a AAA server. The original purpose of 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 user credential.
Realm	Enter the realm name in the field. The name cannot exceed 64 characters. When the access point RADIUS server receives a request for a user name the server references a table of user names. If the user name is known, the server proxies the request to the RADIUS server.
Realm Type	Specify the type of realm that is being used, either Prefix or Suffix.
Strip Realm	Select this option to remove information from the packet when NAI routing is enabled.

- 8 Select **Ok** to save the changes made to this window. Click **Exit** to close this window.
- 9 Select the **RADIUS Accounting** tab.

The screenshot displays the configuration window for AAA Policy, titled 'EXTERNAL-AAA-SERVERS'. It features three tabs: 'RADIUS Authentication', 'RADIUS Accounting', and 'Settings'. The 'RADIUS Accounting' tab is selected. Below the tabs is a table with the following columns: Server Id, Host, Port, Server Type, Request Timeout, Request Attempts, DSCP, Request Proxy Mode, and NAI Routing Enable. The table contains one data row with the following values: Server Id 1, Host lancelet, Port 1,813, Server Type Host, Request Timeout 5s, Request Attempts 3, DSCP 34, Request Proxy Mode None, and NAI Routing Enable marked with a red X. At the bottom of the window, there is a search field labeled 'Type to search in tables' and a 'Row Count: 1' indicator. Navigation buttons for 'Add', 'Edit', 'Delete', and 'Exit' are located at the bottom right.





- 10 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 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 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.
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.

- 11 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.

The screenshot shows the 'Accounting Server' configuration window for 'Server Id 1'. The 'Settings' section is expanded, showing various configuration options:

- Server Type:** Host
- Host:** radius.wavespot.net (Hostname selected)
- Port:** 1813 (range: 1 to 65,535)
- Secret:** masked with asterisks (Show option available)
- Request Proxy Mode:** None
- Request Attempts:** 3 (range: 1 to 10)
- Request Timeout:** 5 (Seconds, range: 1 to 60)
- Retry Timeout Factor:** 100 (range: 50 to 200)
- DSCP:** 34 (range: 0 to 63)

The 'Network Access Identifier Routing' section is also visible:

- NAI Routing Enable:** unchecked
- Realm:** empty text field
- Realm Type:** Prefix (selected), Suffix (unselected)
- Strip Realm:** unchecked

Buttons for 'OK', 'Reset', and 'Exit' are located at the bottom right of the window.

- 12 Define the following settings to add or modify AAA RADIUS accounting server configuration:

Server Id	Displays the numerical server index (1-6) for the accounting server when added to the list available to the access point.
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.
Server Type	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. Select the Show option to display the entered secret.
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 or Through RF Domain Manager.

Proxy Mint Host	Specify a 64 character maximum hostname or the Mint ID of the Mint device used for proxying requests.
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 for the access point's 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 interval, in seconds, between two successive re-transmission attempts of request packets. Specify a value from 50 - 200 seconds. The default is 100 seconds.
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 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. The name cannot exceed 64 characters. When the access point's RADIUS server receives a request for a user name, the server references a table of user names. 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 **Ok** to save the changes made to this window. Click **Exit** to close this window.

15 Select the **Settings** tab.

The screenshot shows the 'AAA Policy WaveSpot' configuration window with the 'Settings' tab selected. The 'RADIUS Accounting' section is active, displaying the following settings:

- Protocol for MAC, Captive-Portal Authentication:** PAP (selected), CHAP, MS-CHAP, MS-CHAPV2, Cisco VSA Audit Session Id.
- Accounting Packet Type:** Start/Stop.
- Request Interval:** 30 Minutes (1 to 60).
- Accounting Server Preference:** Prefer Same Authentication Server Host.
- Access Request Attributes:** Accounting Delay Time, Accounting Multi Session Id, Chargeable User Id, Add Framed IP Address, Framed MTU (1400, 100 to 1,500), RFC5550 Location Information (None), RFC5550 Operator Name, Service-Type (framed), NAS IPv6 Address, Proxy NAS Identifier (originator), Proxy NAS IPv4/IPv6 Address (proxy).
- RADIUS Address Format:** Format (Dash Delimiter (aa-bb-cc-dd-ee-ff)), Case (Uppercase), Attributes (Username / Password).
- Server Pooling:** Server Pooling Mode (Failover selected, Load Balanced).
- EAP Wireless Client Settings:** Client Attempts (3, 1 to 10), Request Timeout (3, 1 to 60 seconds).

16 Set the following RADIUS server configuration parameters:

Protocol for MAC, Captive-Portal Authentication	Set the authentication protocol when the server is used for any non-EAP authentication. Options include Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), MSPAP and MSCHAPV2. The default setting is PAP.
Accounting Packet Type	Set the type of RADIUS Accounting Request packets generated. Options include Stop Only, Start/Stop and Start/Interim/Stop. The default setting is Start/Stop.
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: <ul style="list-style-type: none"> <li>Prefer Same Authentication Server Host - Uses the authentication server host name as the host used for RADIUS accounting. This is the default setting.</li> <li>Prefer Same Authentication Server Index - Uses the same index as the authentication server for RADIUS accounting.</li> <li>Select Accounting Server Independently - Allows users to specify a RADIUS accounting server separate from the RADIUS authentication server.</li> </ul>
Format	Select the format of the MAC address used in the RADIUS accounting packets.
Case	Lists whether the MAC address is sent using uppercase or lowercase letters. The default setting is uppercase.

Attributes	Lists whether the format specified applies only to the user name/password in mac-auth or for all attributes that include a MAC address, such as callingstation- id or called-station-id.
Server Pooling Mode	Controls how requests are transmitted across RADIUS servers. Failover implies traversing the list of servers if any server is unresponsive. Load Balanced uses all servers in a round-robin fashion. The default setting is Failover.
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.
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
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/IPv4 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).

- 17 Select **OK** to save the updates to the AAA configuration. Select **Reset** to revert to the last saved configuration.

## 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

To define a unique AAA TACACS configuration:

- 1 Select **Configuration > Network > AAA TACACS Policy**.

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.

Authentication, Authorization, and Accounting (AAA) TACACS			
AAA TACACS Policy	Accounting Access Method	Authentication Access Method	Authorization Access Method
new	All	All	Telnet

Type to search in tables Row Count: 1

- 2 Refer to the following information for each existing AAA TACACS policy:

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.

- 3 Select **Add** to configure a new AAA TACACS policy. Select an existing policy and use the **Edit** button to edit the policy or use the **Delete** button to delete it.
- 4 Provide a name for the AAA TACACS policy in the AAA TACACS Policy field. The name can be up to 32 characters long. Click **Continue**. Click **OK** to proceed.

The Server Info tab displays by default.

AAA TACACS Policy new

Server Info Settings

Authentication

Server Id	Host	Port	Secret	Request Timeout	Request Attempts	Retry Timeout Factor	
1	1.1.1.1	49	newqwer	3	3	100	

+ Add Row

Authorization

Server Preference authenticated-server-host

Authorization Server Details

Server Id	Host	Port	Secret	Request Timeout	Request Attempts	Retry Timeout Factor	

Accounting

Server Preference authenticated-server-host

Accounting Server Details

Server Id	Host	Port	Secret	Request Timeout	Request Attempts	Retry Timeout Factor	

OK Reset Exit

- 5 Under the **Authentication** table, select **+ Add Row**.

- 6 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.
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 asterisks. To see the secret being entered, select the Show option.
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.

- 7 Select **OK** to save the changes or **Exit** to close the screen.
- 8 Set the **Server Preference**, within the **Authorization** field, to specify which server, in the pool of servers, is selected to receive authorization requests. Options include None, authenticated-server-host, and authenticatedserver- number. If selecting None or authenticated-server-number select **+ Add Row** and set the server's ID, host, port, password and connection attempt parameters.
- 9 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 see the secret being entered, select the Show option.
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.

- 10 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

- 11 Set the **Server Preference**, within the **Accounting** field, to select the accounting server, from the pool of servers, to receive accounting requests. Options include 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.
- 12 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
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
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
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

- 13 Select **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

14 Select the **Settings** tab.

The screenshot shows the 'AAA TACACS Policy new' configuration window with the 'Settings' tab selected. The configuration is as follows:

- Authentication:**
  - Authentication Access Method:  All,  Console,  Telnet,  SSH,  Web
  - Directed Request:
- Authorization:**
  - Authorization Access Method:  All,  Console,  Telnet,  SSH
  - Allow Privileged Commands:
- Accounting:**
  - Accounting Access Method:  All,  Console,  Telnet,  SSH
  - Authentication Failure:
  - CLI Commands:
  - Session:
- Service Protocol Settings:**

Service Name	Service Protocol

15 Set the following AAA TACACS **Authentication** server configuration parameters:

Authentication Access Method	<p>Specify the connection method(s) for authentication requests.</p> <ul style="list-style-type: none"> <li>All – Authentication is performed for all types of access without prioritization.</li> <li>Console – Authentication is performed only for console access.</li> <li>Telnet – Authentication is performed only for access through Telnet.</li> <li>SSH – Authentication is performed only for access through SSH.</li> <li>Web – Authentication is performed only for access through the Web interface.</li> </ul>
Directed Request	<p>Select to enable the AAA TACACS authentication server to be used with the '@&lt;server name&gt;' nomenclature. The specified server must be present in the list of defined Authentication servers.</p>

16 Set the following AAA TACACS **Authorization** server configuration parameters:

Authorization Access Method	Specify the connection method(s) for authorization requests. <ul style="list-style-type: none"> <li>All – Authorization is performed for all types of access without prioritization.</li> <li>Console – Authorization is performed only for console access.</li> <li>Telnet – Authorization is performed only for access through Telnet.</li> <li>SSH – Authorization is performed only for access through SSH.</li> </ul>
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.

17 Set the following AAA TACACS **Accounting** server configuration parameters:

Accounting Access Method	Specify the connection method(s) for accounting requests. <ul style="list-style-type: none"> <li>All – Accounting is performed for all types of access without prioritization.</li> <li>Console – Accounting is performed only for console access.</li> <li>Telnet – Accounting is performed only for access through Telnet.</li> <li>SSH – Accounting is performed only for access through SSH.</li> </ul>
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.

18 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 of 5 entries can be made in the **Service Protocol Settings** table.

19 Select **OK** to save the updates to the AAA TACACS policy. Select **Reset** to revert to the last saved configuration.

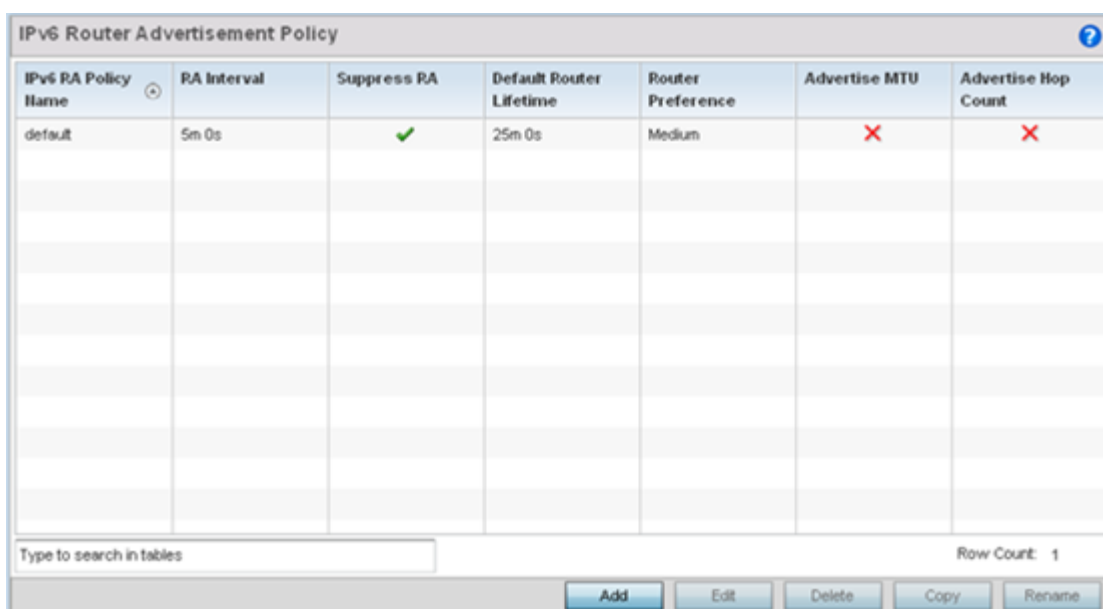
## IPv6 Router Advertisement Policy

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**.



The screenshot shows a web-based configuration interface for IPv6 Router Advertisement Policy. It features a table with the following columns: IPv6 RA Policy Name, RA Interval, Suppress RA, Default Router Lifetime, Router Preference, Advertise MTU, and Advertise Hop Count. The 'default' policy is listed with an RA Interval of 5m 0s, Suppress RA checked (green checkmark), Default Router Lifetime of 25m 0s, Router Preference of Medium, Advertise MTU disabled (red X), and Advertise Hop Count disabled (red X). Below the table is a search bar and a row count of 1. At the bottom are buttons for Add, Edit, Delete, Copy, and Rename.

IPv6 RA Policy Name	RA Interval	Suppress RA	Default Router Lifetime	Router Preference	Advertise MTU	Advertise Hop Count
default	5m 0s	✓	25m 0s	Medium	✗	✗

- 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.

- 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
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
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.
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 disable the transmission of a router advertisement within the IPv6 packet. This setting is enabled by default.
Unicast the 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.

## Border Gateway Protocol (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).

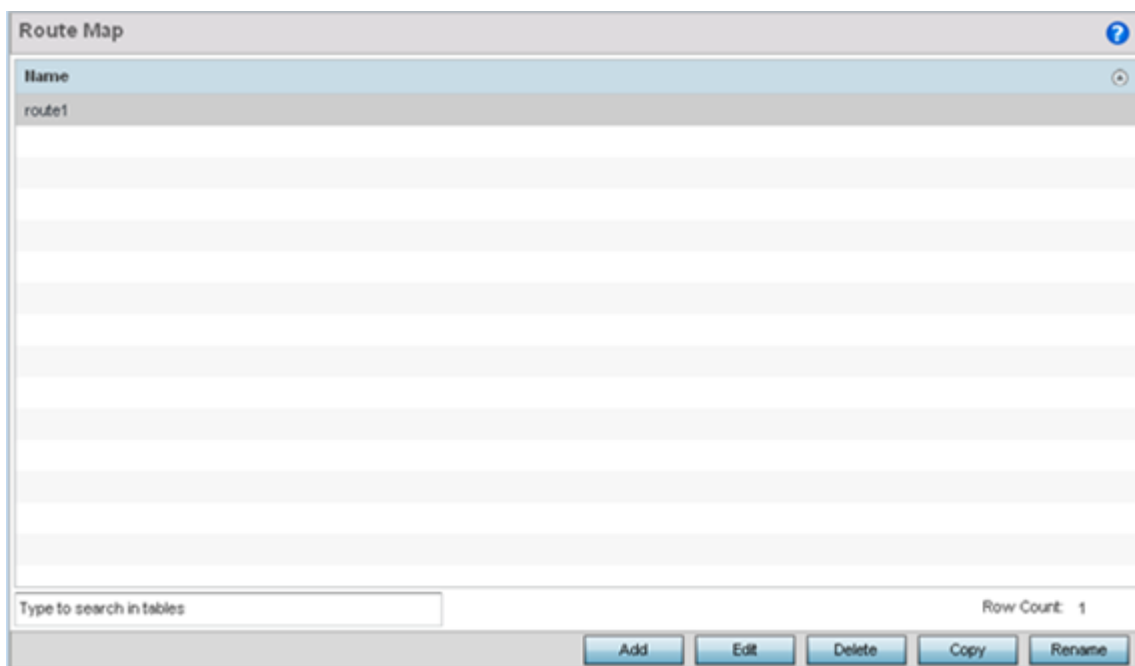
Refer to the following to configure access lists, path lists, IP prefix lists, community lists and external community lists for BGP:

- [IP Access List](#) on page 478
- [AS Path List](#) on page 480
- [IP Prefix List](#) on page 481
- [Community List](#) on page 483
- [External Community List](#) on page 485

To review existing BGP configurations or potentially create new ones:

- 1 Select the **Configuration > Network > BGP > 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.



- 2 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.

The screenshot shows a window titled "Route Map" with a close button (x) in the top right corner. Below the title bar, it says "Sequence 1" with a help icon (?) on the right. There are three tabs: "General" (selected), "Match Rule", and "Set Rule". Under the "General" tab, there are two fields: "Description" with a text input containing "route map 2" and "Access" with a dropdown menu set to "Deny". At the bottom of the window, there are three buttons: "OK", "Reset", and "Exit".

- 3 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.

- 4 Select the **Match Rule** tab.

The screenshot shows the 'Route Map' configuration window for 'Sequence 1'. The 'Match Rule' tab is active. The configuration includes:

- AS-Path:** A dropdown menu with a 'Create' icon and an 'Edit' icon.
- Metric:** A checked checkbox, a text input field containing '1', and a range '(1 to 4,294,967,295)'.
- Origin:** A dropdown menu.
- Community:** A dropdown menu with a 'Create' icon and an 'Edit' icon.
- Exact Match:** An unchecked checkbox.
- Tag:** An unchecked checkbox, a text input field containing '1', and a range '(1 to 65,535)'.
- IP Route Source:** A dropdown menu with a 'Create' icon and an 'Edit' icon.
- IP Route Source Prefix List:** A dropdown menu with a 'Create' icon and an 'Edit' icon.
- IP next Hop Prefix List:** A dropdown menu with a 'Create' icon and an 'Edit' icon.
- IP Next Hop:** A dropdown menu with a 'Create' icon and an 'Edit' icon.
- IP Address:** A dropdown menu with a 'Create' icon and an 'Edit' icon.
- IP Address Prefix List:** A dropdown menu with a 'Create' icon and an 'Edit' icon.

At the bottom right, there are buttons for 'OK', 'Reset', and 'Exit'.

- 5 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: <ul style="list-style-type: none"> <li>• <b>egp</b> - 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.</li> <li>• <b>igp</b> - 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.</li> <li>• <b>incomplete</b> - Matches if the origin of the route is not identifiable.</li> </ul>

Community	<p>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:</p> <ul style="list-style-type: none"> <li>• internet - Advertises this route to the Internet. This is a global community.</li> <li>• local-AS - Prevents the transmit of packets outside the local AS.</li> <li>• no-advertise - Do not advertise this route to any peer, either internal or external.</li> <li>• no-export - Do not advertise to BGP peers, keeping this route within an AS.</li> <li>• aa:nn - The first part (aa) represents the AS number. The second part (nn) represents a 2-byte number.</li> </ul>
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.

- 6 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.
- 7 Select the **Set Rule** tab.

The screenshot shows the 'Route Map' configuration window for 'Sequence 1'. The 'Set Rule' tab is active. The configuration fields are as follows:

- Aggregator AS ASN:** A dropdown menu with the value '1' selected. A range '(1 to 4,294,967,295)' is shown to the right.
- Aggregator IP:** A text input field with three dots '...' indicating a required IP address.
- Exclude AS path:** A text input field with a green plus icon button to its right.
- Path prepend:** A text input field with a green plus icon button to its right.
- Atomic aggregate:** A checkbox that is currently unchecked.
- Community List:** A dropdown menu with a green plus icon and a gear icon to its right.
- Community:** A text input field.
- IP Address:** A text input field with three dots '...' indicating a required IP address.

At the bottom of the window, there are three buttons: 'OK', 'Reset', and 'Exit'.

- 8 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. <ul style="list-style-type: none"> <li>• egp - Sets the origin of the route to eBGP.</li> <li>• igp - Sets the origin of the route to iBGP.</li> <li>• incomplete - Sets the origin of the route as not identifiable. Set this if the route is from a source other than eBGP or iBGP.</li> </ul>
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.

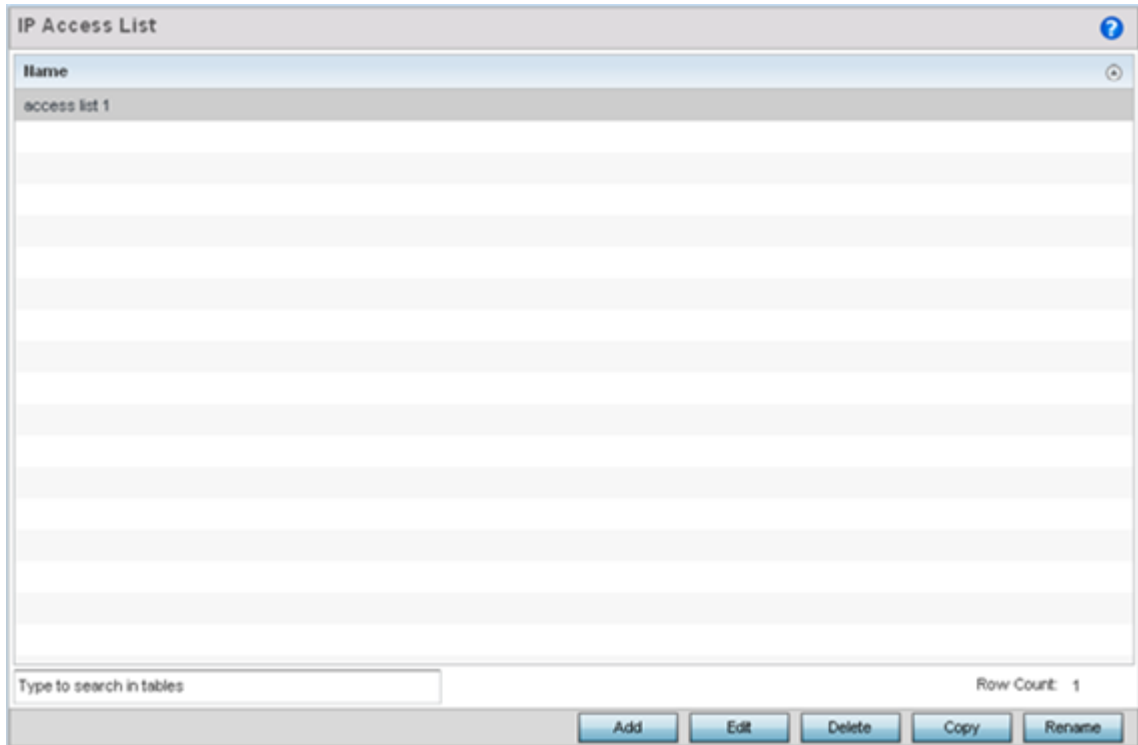
- 9 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

## IP Access List

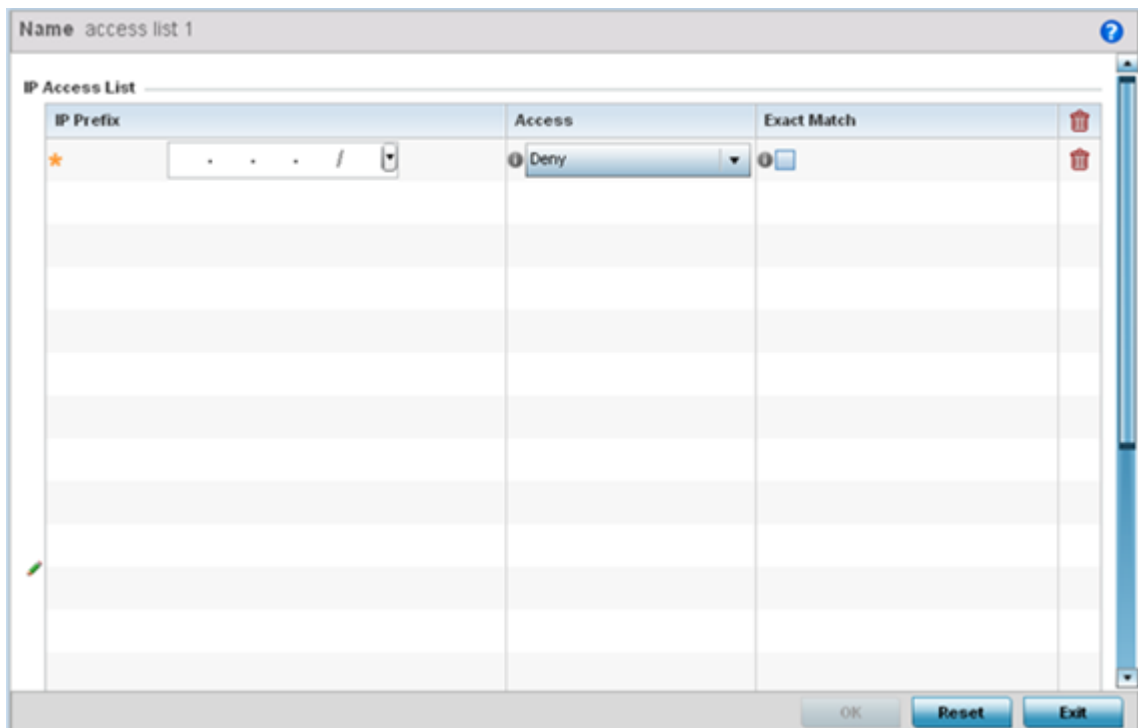
BGP peers and route maps can reference a single IP based access list. Apply IP access lists to both inbound and outbound route updates. Every route update is passed through the access list. BGP applies each rule in the access list in the order it appears in the list. When a route matches a rule, the 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 > IP Access List**.



- 2 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.



- 3 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.

- 4 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

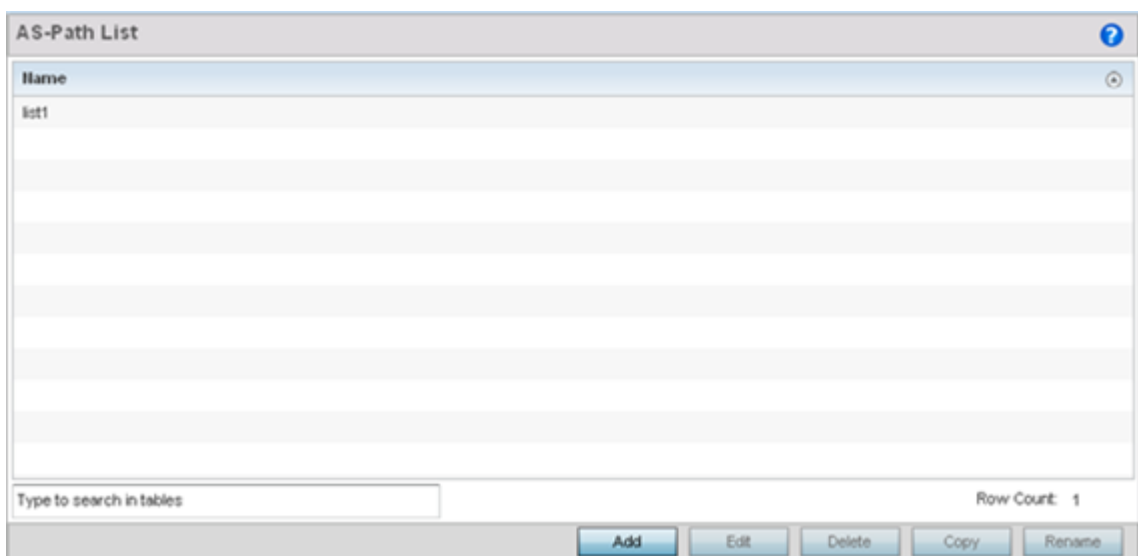
## AS Path List

BGP uses a routing algorithm to exchange network reachability information with other BGP supported devices. Network availability and 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 > AS Path List**.





- 2 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.

- 3 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.

- 4 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

## 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 **Configuration > Network > BGP > IP Prefix List**.

- 2 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.

Sequence	IP Prefix	Greater Than	Less Than	Allow
2	157.235.32.33/2	3	9	Permit

- 3 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 a 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.

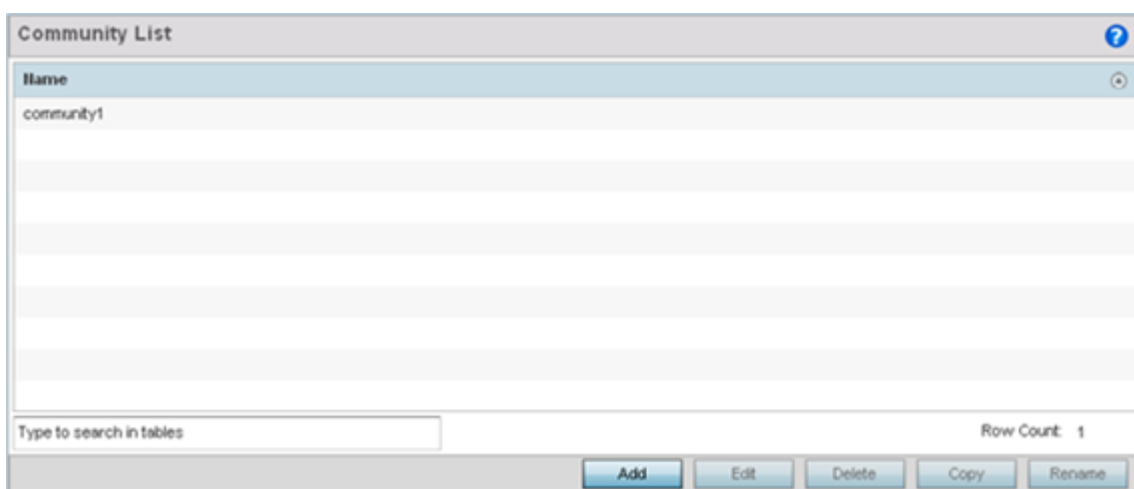
- 4 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

## 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 **Configuration > Network > BGP > Community List**.



- 2 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.

- 3 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.

- 4 Set the following **Community List** settings:

Community Id	Provide a community ID unique to this particular rule. The following are available: <ul style="list-style-type: none"> <li>internet - Advertises this route to the Internet. This is a global community.</li> <li>local-AS - Prevents the transmit of packets outside the local AS.</li> <li>no-advertise - Do not advertise this route to any peer, either internal or external.</li> <li>no-export - Do not advertise to BGP peers (keeping) this route within an AS.</li> <li>aa:nn - The first part (aa) represents the AS number. The second part (nn) represents a 2-byte number.</li> </ul>
Allow	Use the drop-down menu to Permit or Deny requests for the community ID. 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.

## 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 **Configuration > Network > BGP > External Community List**

Name
external1

Type to search in tables Row Count: 1

- 2 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.

Name

Select Option

Standard  Expanded

Standard

Community Id	Allow
local-AS	Deny

- 3 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.

- 4 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.

- 5 Click **OK** to save the changes, **Reset** to revert to the last saved configuration or **Exit** to close the screen.

## 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 a 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 Configuration](#)
- [Network Group Alias Configuration](#)
- [Network Service Alias Configuration](#)

## Network Basic 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** > **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.

Basic Alias   Network Group Alias   Network Service Alias

**i** Delete button is enabled only for entries created in this context.

**Vlan Alias**

Name	Vlan	
* \$lanelot	2	

**Host Alias**

Name	Host	
* \$mudskipper	157. 235. 35 . 255	

**Address Range Alias**

Name	Start IP	End IP	
* \$renegade	157. 235. 212	157. 235. 242	

**Network Alias**

Name	Network	
* \$percival	157. 235. 242. 42 / 42	

OK   Reset   Exit

- 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 ID 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.



<b>Name</b>	If adding a new <i>Address Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Start IP</b>	Set a starting IP address used with a range of addresses utilized with the address range alias.
<b>End IP</b>	Set an ending IP address used with a range of addresses utilized with the address range alias.

- 5 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.

<b>Name</b>	If adding a new <i>Host Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Host</b>	Set the numeric IP address set for the host.

- 6 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.

<b>Name</b>	If adding a new <i>Network Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Network</b>	Provide a network address in the form of host/mask.

- 7 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.

<b>Name</b>	If adding a new String Alias, provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Value</b>	Provide a string value to use in the alias.

- 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.

## Network Group Alias Configuration

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** > **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.

Basic Alias <b>Network Group Alias</b> Network Service Alias		
Name	Host	Network
✚ Solias2	157.235.123.131	157.235.123.123/15

Type to search in tables Row Count: 1

Add   Edit   Delete   Exit

The screen displays the attributes of existing network group alias configurations.

<b>Name</b>	Displays the administrator assigned name for the network group alias.
<b>Host</b>	Displays all the host aliases configured in the listed network group alias. Displays a blank column if no host alias is defined.
<b>Network</b>	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.

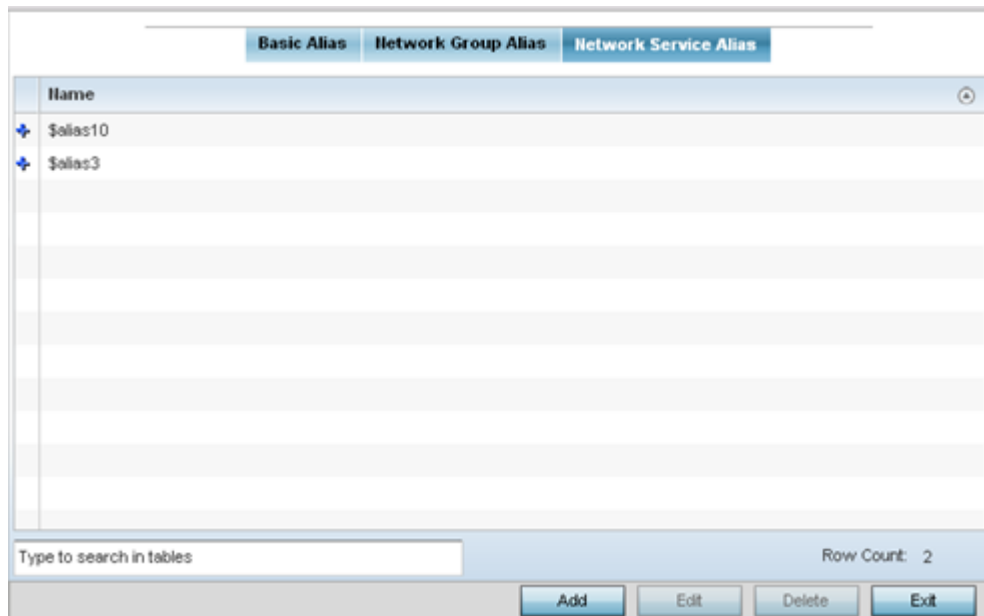
## Network Service Alias Configuration

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.



- 4 Select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies.

## 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, socialnetworking). 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. Ratelimits 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**.

The screen lists the application policy configurations defined thus far.

Name	Description
policy2	Weekends

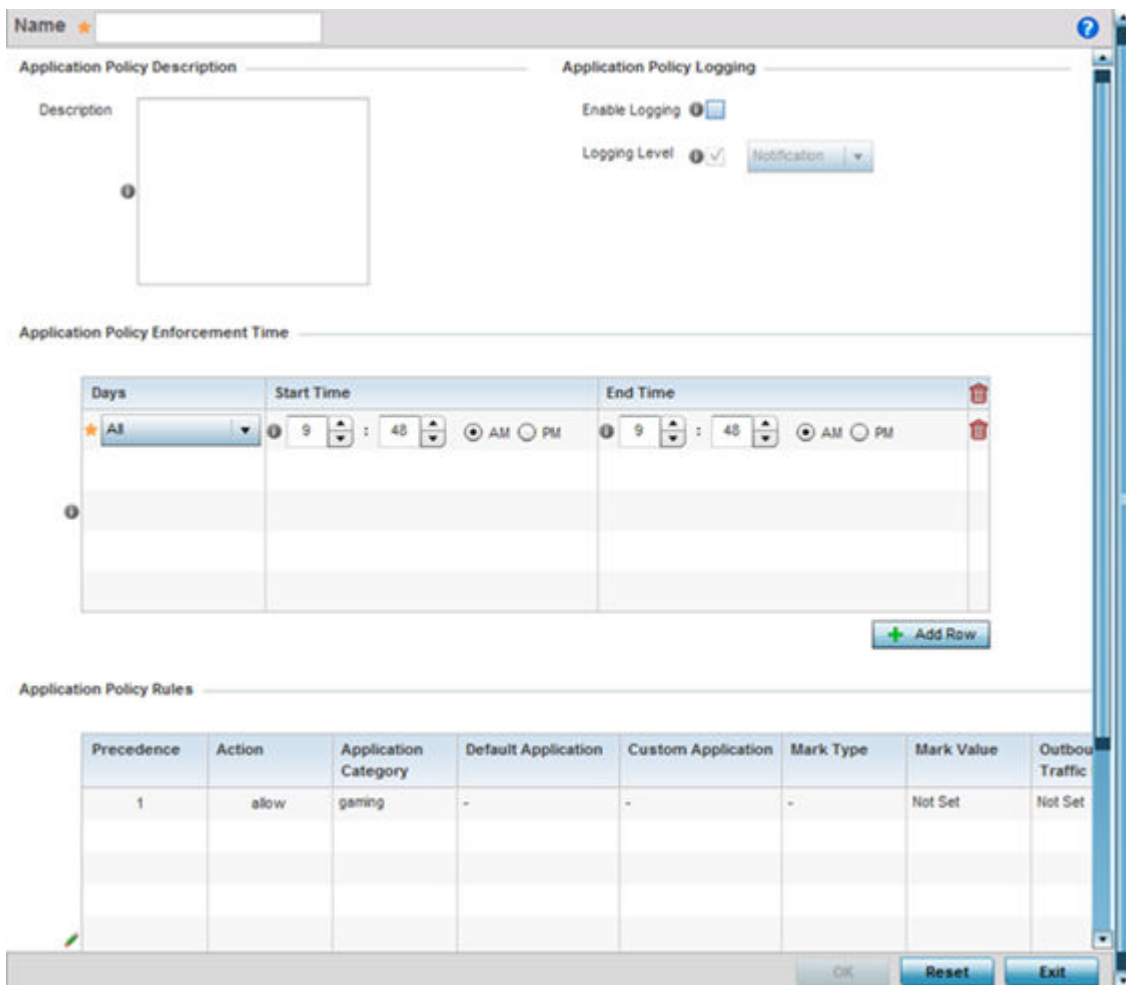
Type to search in tables Row Count: 1

Add Edit Delete Copy Rename

- 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.



- 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** to launch a screen to create a new policy rule.

**Add Row** [X]

Precedence ★ 1 (1 to 256)

Action ⓘ allow

Application ⬇ Select a Category to filter Applications or [Create Application](#)

**App-Category**

- all
- antivirus update
- audio
- business
- conference
- custom
- database
- filetransfer
- oaming
- oeneric
- im
- mail
- mobile
- network management
- other

**Application**

- All
- 1-clickshare-com
- 1-upload-com
- 1-upload-to
- 10upload-com
- 123upload-pl
- 139pan-com
- 163pan-com
- 1clickshare-net
- 1fichier-com
- 1kxun
- 2shared-com
- 360mobile
- 4fastfile-com
- 4share-ws

Schedule Policy 🍏 Monday ⚙️

[OK] [Exit]

- 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 500
- 12 Select **OK** to save the updates to the application policy. Select **Reset** to revert to the last saved configuration.

## Application

Use the **Application** screen to create custom application configurations.

To create a user-defined application:

- 1 Select **Configuration > Network > Application**.

The screen lists the application configurations defined thus far.

Name	Category	Application Description
mudkipper	audio	Custom Audio Skipper

Type to search in tables Row Count: 1

Add Edit Delete

- 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.

The screenshot shows a configuration window with the following elements:

- Name:** A text input field with a star icon and a help icon.
- Basic Configuration:**
  - Category:** A dropdown menu with a star icon.
  - Application Description:** A large text area with an information icon.
- Application Definition:**
  - Network Service:** A dropdown menu currently set to "<none>".
  - URL List:** A button.
  - HTTPS:** A button.
  - Buttons:** A gear icon, a green plus icon, and a blue minus icon.
- Footer:** Buttons for "OK", "Reset", and "Exit".

- 4 If creating a new user-defined application type, assign it a **Name** up to 32 characters. Ensure you do not create confusion by naming a user-defined application with the same name as an existing application appearing the Application Policy screen.
- 5 Use the **Category** list to classify the application. Select the appropriate pre-defined category or select custom to create a custom classification for the application.
- 6 Provide an 80 character maximum **Application Description** to each new user-defined application to further differentiate it from existing applications.



- 7 Refer to the **Application Definition** field to assign either a network service alias, predefined 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 userdefined application. If there are no existing network service alias suited to this new user-defined application, select the <b>Create</b> 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 (4) service aliases can be supported.
URL List	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 no URL list suits this new user-defined application, select the <b>Create</b> icon to define a new list or the <b>Edit</b> icon to modify an existing URL list.
HTTPS	Select the <b>+ Add Row</b> 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.

- 8 Select **OK** to save the updates to the user-defined application configuration. Select **Reset** to revert to the last saved configuration.

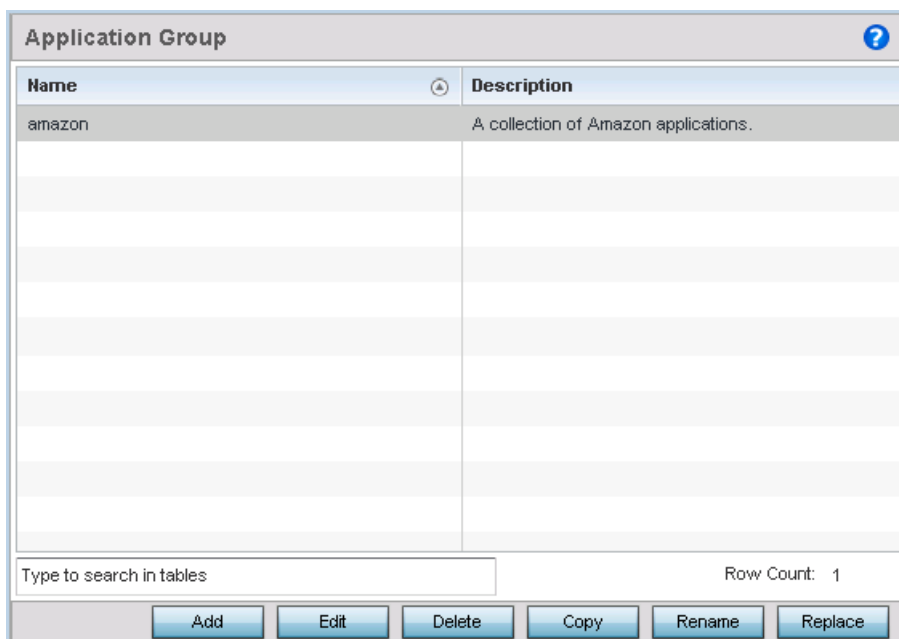
## Application Group

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**.

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.

The screenshot shows a configuration window for an application group named "amazon". At the top, the name "amazon" is displayed. Below it, there is a "Description" field containing the text "A collection of Amazon applications." with a small edit icon (pencil) to its left. Underneath the description is a search input field containing "amaz" and a placeholder text "\*Enter Application name to search".

The main area is divided into two columns: "All Applications" and "Selected Applications".

**All Applications:** A list of applications with checkboxes. The "amazon cloud web" application is selected (checked). Other applications include amazon-prime-video (stream and video), amazon cloud (amazon-cloud, apache, audio, encrypted, file-transfer, google, video), amazon shop (apache, audio, encrypted, google), and angry-birds (amazon-cloud).

**Selected Applications:** A list of applications that have been moved to this group. It includes amazon-prime-music, amazon-prime-video, and amazon cloud. There are also two arrow buttons (right and left) between the two lists to facilitate moving items.

- 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.

## 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**.

Name	Description	Time Rule
Policy1	Limited Access	Weekends(06:00-17:00)

Type to search in tables Row Count: 1

- 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.

Name Policy1

Description Limited Access

Time Rule

Days	Start Time	End Time
weekends	06:00 am	5:00 pm
<input checked="" type="radio"/> All	<input type="text" value="0"/> : <input type="text" value="0"/> <input checked="" type="radio"/> AM	<input type="text" value="0"/> : <input type="text" value="0"/> <input checked="" type="radio"/> AM

- 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.

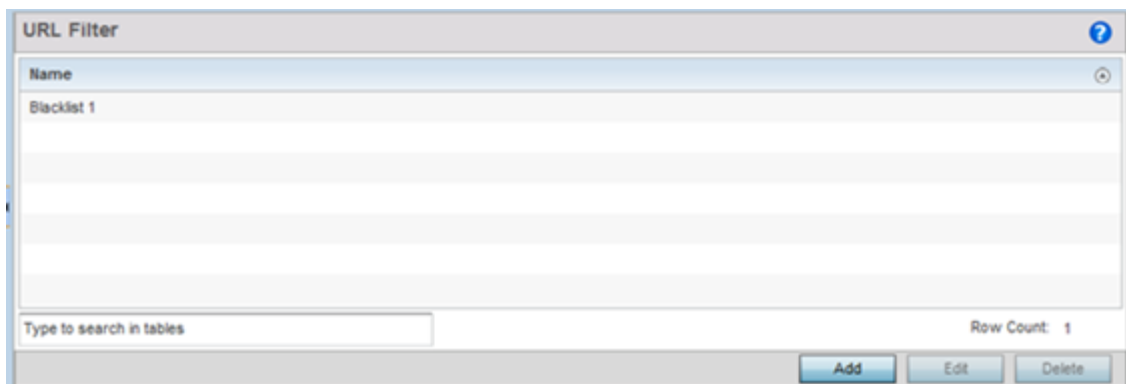
- 6 Select **OK** to save the updates to the schedule policy time rule configuration. Select **Reset** to revert to the last saved configuration.

## 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:

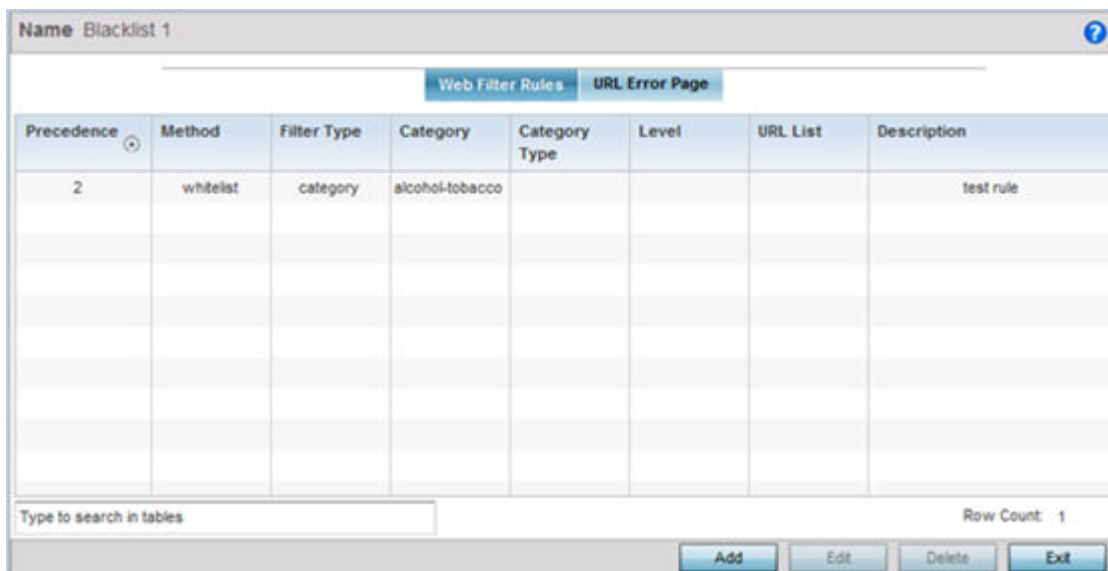
- 1 Select **Configuration > Network > URL Filter**.



- 2 Select **Add** to create a new URL Filter, **Edit** to modify the attributes of a selected URL Filter or **Delete** to remove obsolete filters from the list of those available.

- If creating a new URL Filter, assign it a Name up to 32 characters to distinguish this URL Filter from others with similar attributes. Select **Continue** to proceed to the URL Filter screen where Web filter rules and URL error page messages can be added, modified or removed. Select **Exit** to exit without creating a new URL Filter.

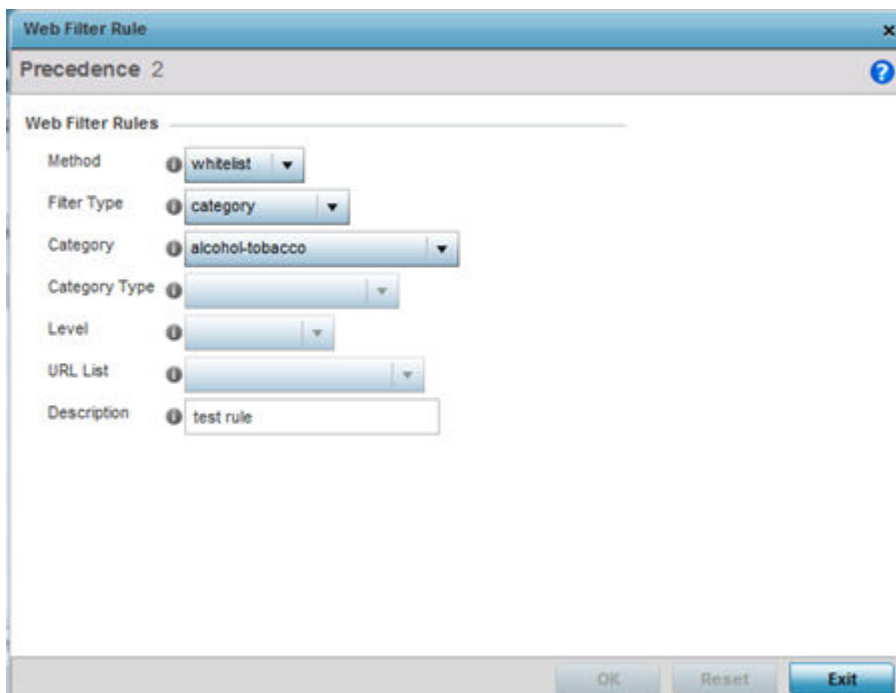
The URL Filter screen displays, with the **Web Filter Rules** tab selected by default.



The screenshot shows a configuration window titled "Name Blacklist 1". It has two tabs: "Web Filter Rules" (selected) and "URL Error Page". Below the tabs is a table with the following columns: Precedence, Method, Filter Type, Category, Category Type, Level, URL List, and Description. The table contains one row with the following values: Precedence: 2, Method: whitelist, Filter Type: category, Category: alcohol-tobacco, Category Type: (empty), Level: (empty), URL List: (empty), and Description: test rule. At the bottom of the table, there is a search box labeled "Type to search in tables" and a "Row Count: 1" indicator. Below the table are four buttons: "Add", "Edit", "Delete", and "Exit".

Precedence	Method	Filter Type	Category	Category Type	Level	URL List	Description
2	whitelist	category	alcohol-tobacco				test rule

- Select **Add** to create a new Web filter rule configuration, or select an existing configuration then Edit to modify the attributes of an existing Web filter rule.



The screenshot shows a dialog box titled "Web Filter Rule" with a close button (X) in the top right corner. Below the title bar, it says "Precedence 2" and has a help icon (question mark). The main area is labeled "Web Filter Rules" and contains several fields with dropdown menus and a text input field:

- Method: whitelist
- Filter Type: category
- Category: alcohol-tobacco
- Category Type: (empty)
- Level: (empty)
- URL List: (empty)
- Description: test rule

At the bottom of the dialog box are three buttons: "OK", "Reset", and "Exit".

## 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 their expected Web 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.

## Web Filtering

A Web filter policy is a means of managing the number of records and time cached URLs are retained. When configured and applied, the policy also determines whether to filter access to a cached URL when a categorization server is unreachable or is 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 Filtering**.

Name	Maximum Cached Records	Time Validity for Cached URL	Access To Unreachable Server	Access To Uncategorized URL
Large Cache	100,001 records	60 secs	pass	pass

Type to search in tables Row Count: 1

- 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.

- 3 If creating a new Web Filtering Policy, assign it a **Name** up to 32 characters to distinguish this policy from others with similar attributes. Modify the new Web Filtering Policy parameters and click **OK** to save the policy, **Reset** to revert back to default settings or **Exit** to exit without creating a new Web Filtering Policy.

- 4 Set 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.

## Configuring 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**.

- 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.

- 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.

The screenshot shows a dialog box titled "Add Row" with a close button (X) in the top right corner. Below the title bar, the text "Standard Rule" is followed by a horizontal line. There are three configuration fields, each with a small icon to its left:

- Source IP Address:** A dropdown menu with a blue arrow icon on the left and the text "Any" inside.
- Allow:** A dropdown menu with a blue star icon on the left and the text "Permit" inside.
- Time Range:** A dropdown menu with a blue information icon (i) on the left and an empty field inside.

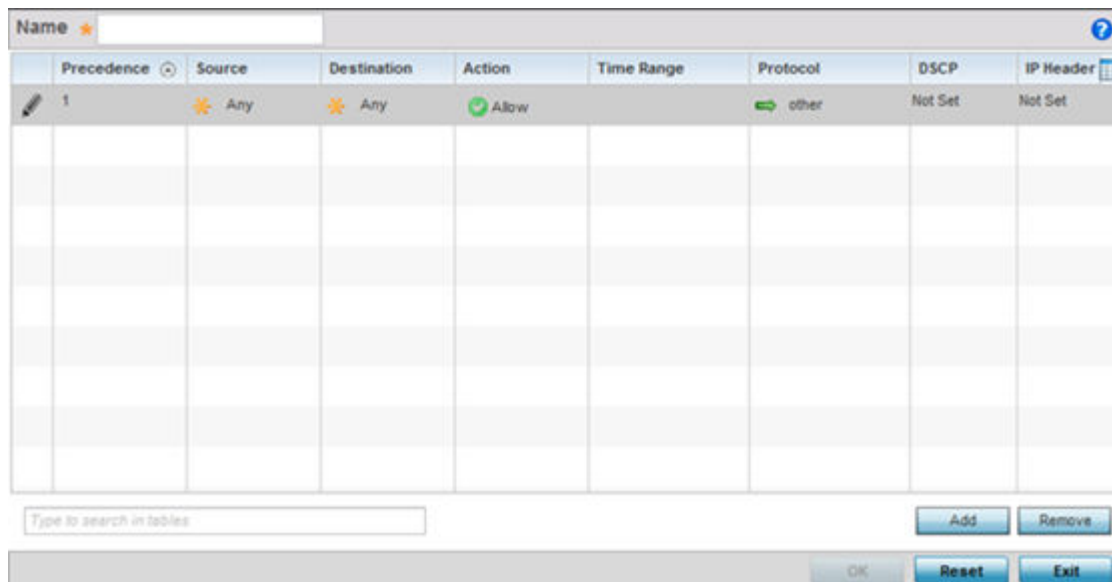
At the bottom right of the dialog, there are two buttons: "OK" and "Exit".

- 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.



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: <ul style="list-style-type: none"> <li>Deny - Instructs the ACL to restrict a packet from proceeding to its destination when filter conditions are matched.</li> <li>Allow - Instructs the ACL to allow a packet to proceed to its destination when filter conditions are matched.</li> </ul>

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.

## Configuring 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**.

Name	Description
default	
map2	QoS Voice Map

Type to search in tables Row Count: 2

- 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.

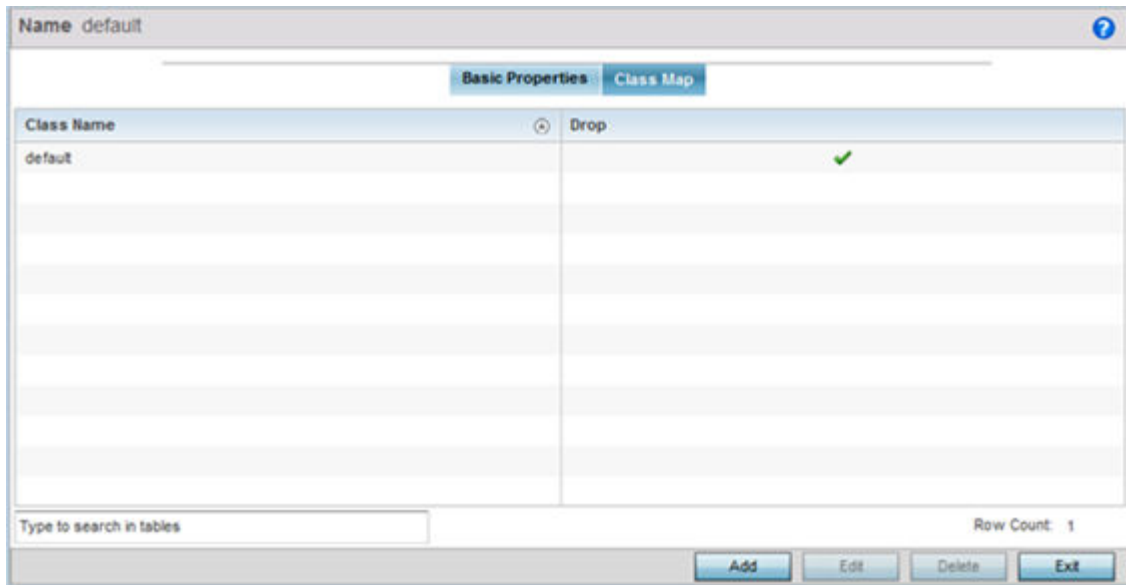
Name map2

Description:

- 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.

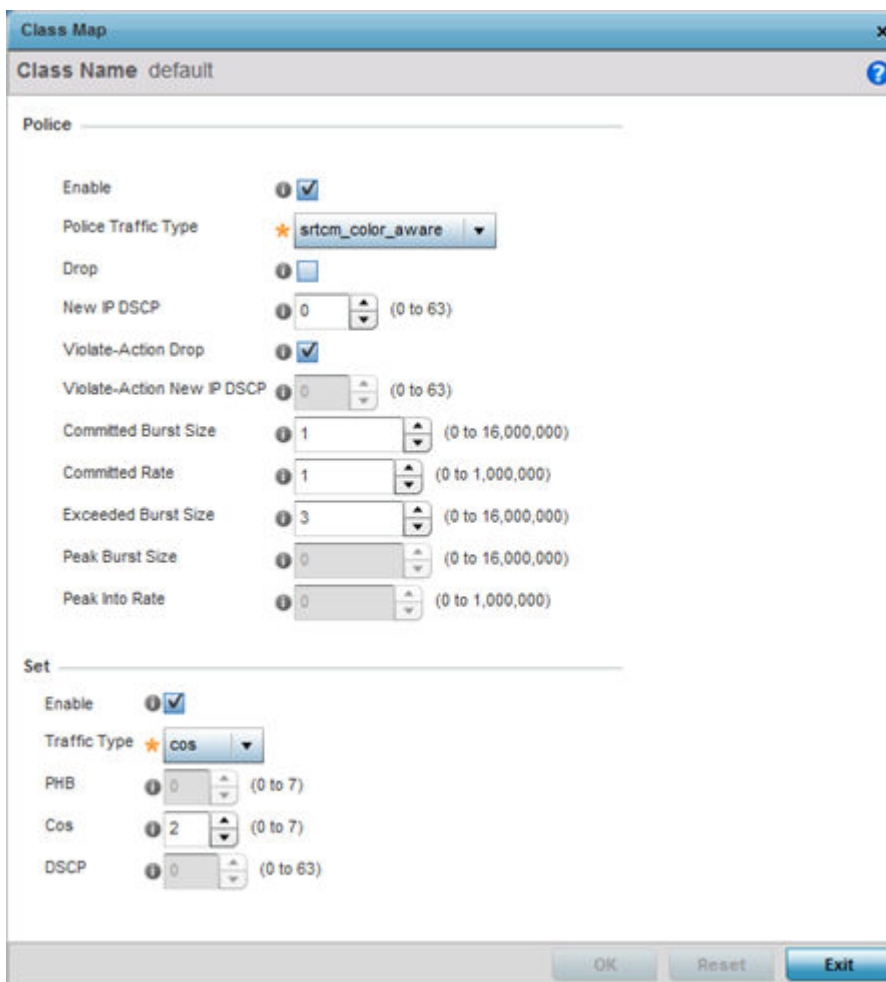
6 Select the **Class Map** tab.

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.





- 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.



- 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 <code>srtcm_color_aware</code> or <code>srtcm_color_blind</code> are selected as the Police Traffic Type, set an excess burst size (from 0 - 16,000,000 bytes). The excess burst size allows for periods of bursting traffic exceeding both the committed information rate (CIR) and committed burst size.
Peak Burst Size	When <code>trtcm_color_aware</code> or <code>trtcm_color_blind</code> 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 Info Rate	When <code>trtcm_color_aware</code> or <code>trtcm_color_blind</code> 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.

## 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 Manage Profiles

**General Profile Configuration**  
**Profile Cluster Configuration (Controllers Only)**  
**Profile Adoption Configuration (Access Points Only)**  
**Profile Adoption Configuration (Controllers Only)**  
**Access Point Radio Power Overrides (AP 7161 Only)**  
**Profile 802.1x Configuration**  
**Profile Interface Configuration**  
**Profile Network Configuration**  
**Profile Security Configuration**  
**VRRP Configuration**  
**Critical Resources Configuration**  
**Profile Services Configuration**  
**Profile Management Configuration**  
**Profile Mesh Point Configuration**  
**Environmental Sensor Configuration (AP 8132 Only)**  
**Advanced Profile Configuration**

Profiles enable administrators to assign a common set of configuration parameters and policies to RFS controllers, NX series service platforms and access points. Profiles can be used to assign common or *unique* network, wireless and security parameters to controllers, service platforms 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, 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 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 a 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 device is automatically assigned a default profile unless an AP Auto-Provisioning policy is defined that specifically assigns an 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 provisioned. Default profiles can also be manually added prior to discovery when needed. Default profiles are ideal for single site deployments where controllers, service platforms and access points share a common configuration.

Device Model	Default Profile
AP621	default-ap621
AP650	default-ap650
AP 6511	default-ap6511
AP 6521	default-ap6521
AP 6522	default-ap6522
AP 6532	default-ap6532
AP 6562	default-ap6562
AP71XX	default-ap71xx
AP 81XX	default-ap81xx
AP 82XX	default-ap82xx
NX 4500, NX 4524	default-nx45xx
NX 6500, NX 6524	default-nx65xx
NX 75XX	default-nx75xx
NX 9000, NX 9500, NX 9510	default-nx9000
RFS 4000	default-rfs4000
RFS 6000	default-rfs6000
RFS 7000	default-rfs7000

User defined profiles are manually created for each supported device 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 should be utilized in larger deployments 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.

Profile	Type	Auto-Provisioning Policy	Firewall Policy	Wireless Client Role Policy	Advanced WIPS Policy	DHCP Server Policy	Management Policy	RADIUS Server Policy
1-new	AP6532		default				default	
2-new	AP6532		default				default	
AP650-profile	AP650		default				default	
AP6532OUS-profile	AP6532		default				default	
default-ap621	AP621		default				default	
default-ap622	AP622		default				default	
default-ap650	AP650		default				default	
default-ap6511	AP6511		default				default	
default-ap6521	AP6521		default				default	
default-ap6532	AP6532		default	STORES			default	
default-ap71xx	AP71XX		default				default	
default-nx9000	NX9000	mypolicy	default			addresspool	default	policy1
meshpoint-profile	AP6532		default				default	
RF2 Profile	AP71XX		default				default	

Type to search in tables Row Count: 14

Add Edit Delete

4 Review the following information on existing profiles:

<b>Profile</b>	Lists the user-assigned name defined for each profile when created. Profile names cannot be edited with a profiles configuration.
<b>Type</b>	Displays the device type (and subsequent device specific configuration) supported by each listed profile. Available device types include: <Supported_AP_Table> <Supported_Controller_Table> <Supported_NX_Table>
<b>Auto-Provisioning Policy</b>	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 or access point 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.
<b>Firewall Policy</b>	Displays an existing firewall policy, if any, assigned to each listed profile. Firewall policies can be assigned when creating or editing a profile.
<b>Wireless Client Role Policy</b>	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. This policy can be applied to controllers, service platforms or access points.
<b>Advanced WIPS Policy</b>	Lists the name of the Advanced WIPS Policy used with each listed profile to (among other things) block up to 100 client MAC address from connectivity.
<b>DHCP Server Policy</b>	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.

<b>Management Policy</b>	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 ( <i>HTTP, HTTPS, Telnet, SSH or SNMP</i> ). Management access can be enabled/disabled as required for each policy.
<b>RADIUS Server Policy</b>	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.

The following tasks comprise required profile configuration activities:

- [General Profile Configuration](#)
- [Profile Cluster Configuration \(Controllers Only\)](#)
- [Profile Adoption Configuration \(APs Only\)](#)
- [Profile Interface Configuration](#)
- [Profile Network Configuration](#)
- [Profile Security Configuration](#)
- [Profile Services Configuration](#)
- [Profile Management Configuration](#)
- [Advanced Profile Configuration](#)

## 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 (Controller APs of the same model, service platforms or controllers) 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 RFS 4000 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.

**Location**

Area

Floor

Floor Number  (1 to 4,094)

**Statistics**

NoC Update Interval  (0,5-3600 seconds)

**Network Time Protocol (NTP)**

Server IP	Key Number	Key	Preferred	Autokey	Version	

**RAID Alarm**

RAID Alarm Enable

OK Reset Exit

- 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. Controllers, service platforms and access points can only utilize profile resources with other device's of the same model type.
- 7 Refer to the **Location** field to define the device's deployment location area.

<b>Area</b>	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.
<b>Floor</b>	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.
<b>Floor Number</b>	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.

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 the used to obtain system time. 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 used by this NTP server resource. The default setting is 0.

- 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 NX 95XX series service platform.

RAID controller drive arrays are available within NX 95XX series service platforms (NX 9500, NX 9510) only. However, they can be administrated on behalf of a NX 95XX profile by a different model service platform or controller.

NX9000 series 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. With the WING 5.5 release, 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.

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

## General Profile Configuration and Deployment Considerations

Before defining a general profile configuration for a RFS controller, NX series service platform or access point, 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 access points discovered and provisioned by controllers and service platforms.
- Each user administrator configured profile requires a unique name.
- User defined profiles can be automatically assigned to access points using AP adoption policies.
- Controllers, service platforms and access points are automatically assigned a default profile based on the hardware type selected when the profile is initially created.

## Profile Cluster Configuration (Controllers Only)

Configuration and network monitoring are two tasks a network administrator faces as a network grows in terms of the number of managed nodes (controllers, service platforms, wireless devices etc.). Such scalability requirements lead network administrators to look for managing and monitoring each node from a single centralized management entity. A RFS controller or NX service platform not only provides a centralized management solution, it provides a centralized management profile that can be shared by any single controller or service platform cluster member. This eliminates dedicating a management entity to manage all cluster members and eliminates a single point of failure.

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

A cluster's load balance is typically distributed evenly amongst its members. An administrator needs to define how often the profile is load balanced for radio distribution, as radios can come and go and members 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 be set.

- 5 Define the following **Cluster Settings** parameters to set this profile's cluster mode and deployment settings:

<b>Cluster Mode</b>	A member can be in either an Active or <i>Standby</i> 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.
<b>Cluster Name</b>	Define a name for the cluster name unique to its configuration or profile support requirements. The name cannot exceed 64 characters.
<b>Master Priority</b>	Set a priority value from 1 - 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.

<b>Handle STP Convergence</b>	Select the check box to enable <i>Spanning Tree Protocol (STP)</i> 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 cluster members. 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.
<b>Force Configured State</b>	Select the check box to enable this cluster member to take over for an active member if it were to fail. A standby controller or service platform takes over APs adopted by the failed member. If the failed cluster member were to come available again, 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.
<b>Force Configured State Delay</b>	Specify a delay interval in either <i>Seconds</i> (1 - 1,800) or <i>Minutes</i> (1 - 30). This is the interval a standby cluster member waits before releasing adopted APs and goes back to a monitoring mode when a controller becomes active again after a failure. The default interval is 5 seconds.

- 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 in the range of 1 - 4094.

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

- 7 Select **OK** to save the changes made to the profile's cluster configuration. Select **Reset** to revert to the last saved configuration.

## Controller Cluster Profile Configuration and Deployment Considerations

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 and license provisions allow. 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 amongst one of the cluster members, 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 deprecated.

## Profile Adoption Configuration (Access Points 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:

- 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 **Adoption**.

- 5 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.
- 6 Select the check box to define a **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.

- 7 Set the following **Controller Hello Interval** parameters:

<b>Hello Interval</b>	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.
<b>Adjacency Hold Time</b>	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 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.

<b>Host</b>	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.
<b>Pool</b>	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.
<b>Routing Level</b>	Define a routing level (either 1 or 2) for the link between adopting devices. The default setting is 1.
<b>IPSec Secure</b>	Enable this option to provide IPSec secure peer authentication on the connection (link) between the adopting devices. This option is disabled by default.
<b>IPSec GW</b>	Select the numerical IP address or administrator defined hostname of the adopting controller resource.
<b>Force</b>	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.
<b>Remote VPN Client</b>	Displays whether a secure controller link has been established using a remote VPN client.

- 9 Select **OK** to save the changes to the access point profile adoption configuration. Select **Reset** to revert to the last saved configuration.

## Profile Adoption Configuration (Controllers Only)

Adoption is the process a controller or service platform uses to discover available access points and/or peer controllers/service platforms, establish an association and provision the requesting device. Adoption settings are configurable and supported within a 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:

- 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 **Adoption**.

- 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 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 <i>Create</i> icon or modify an existing one by selecting the <i>Edit</i> 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.

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

<b>Allow Adoption of Devices</b>	Select either <i>access points</i> or <i>Controllers</i> (or both) to refine whether this controller or service platform can adopt just networked access points or peer controller devices as well.
<b>Allow Adoption of this Controller</b>	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.

<b>Preferred Group</b>	If <i>Allow Adoption of this Controller</i> 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.
<b>Hello Interval</b>	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.
<b>Adjacency Hold Time</b>	Select this option to set a hold time interval (from 2 - 600 seconds) for the transmission of hello packets.

- 8 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.
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 Refer to the **AP300 Adoption** settings:

<b>Adopt List</b>	Select this option to enable the controller or service platform adoption of an AP300 before it has been provisioned with its configuration. This setting is enabled by default.
<b>Adopted List</b>	If the Adopt List setting is disabled, add AP300 MAC addresses that the controller or service platform will optimally adopt.
<b>Deny List</b>	If the Adopt List setting is enabled, add AP300 MAC addresses that the controller or service platform will deny from adoption and configuration provisioning.

- 10 Select **OK** to save the changes to the controller or service platform profile adoption configuration. Select **Reset** to revert to the last saved configuration.

## Access Point Radio Power Overrides (AP 7161 Only)

This option is only available for AP 7161 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 radio 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 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:

- 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**.
- 5 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.

- 6 Set or override the Access Point radio's 802.3af Power Mode and the radio's 802.3at Power Mode.
- 7 Use the drop-down menu 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 and overrides made to the Access Point power configuration. Select **Reset** to revert to the last saved configuration.

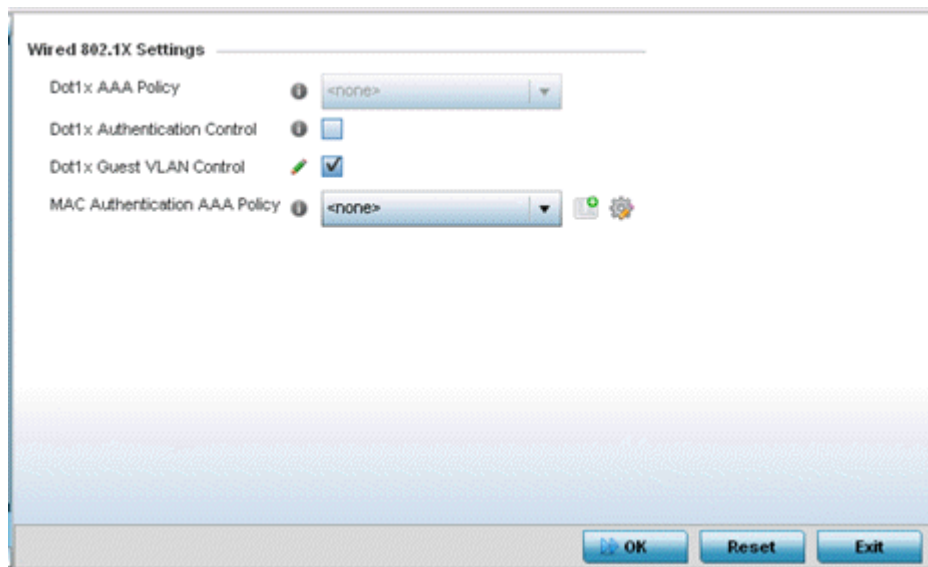


## Profile 802.1x Configuration

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**.



- 5 Set the following **Wired 802.1x Settings**:

<b>Dot1x Authentication Control</b>	Select this option to globally enable 802.1x authentication for the selected device. This setting is disabled by default.
<b>Dot1x AAA Policy</b>	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 <i>Create</i> icon to create a new policy or the <i>Edit</i> icon to modify an existing policy.
<b>Dot1x Guest VLAN Control</b>	Select this option to globally enable 802.1x guest VLANs for the selected device. This setting is disabled by default.
<b>MAC Authentication Control</b>	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 <i>Create</i> icon to create a new policy or the <i>Edit</i> 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.

## Profile Interface Configuration

A profile's device interface configuration can be refined to support separate physical Ethernet configurations both unique and specific to RFS 4000, RFS 6000, RFS 7000 model controllers and NX

4500, NX 4524, NX 6500, NX 6524 and NX 9000 series service platforms. Ports vary depending on platform, but controller or service platform models do have some of the same physical interfaces

Controllers, service platforms and access points require their 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 device is connected to.

If the profile is configured to support an access point radio, additional options are available unique to the radio's capabilities.

A profile's interface configuration process consists of the following:

- [Ethernet Port Configuration](#)
- [Virtual Interface Configuration](#)
- [Port Channel Configuration](#)
- [Access Point Radio Configuration](#)
- [WAN Backhaul Configuration](#)
- [PPPoE Configuration](#)

For interface deployment considerations, see [Profile Interface Deployment Considerations](#).

## Ethernet Port Configuration

Port placement and quantity varies depending on controller, service platform or access point model.

The following ports are available on RFS controllers:

- *RFS 4000*- ge1, ge2, ge3, ge4, ge5, up1

The following ports are available on NX series service platforms:

- NX 4500 - up1, up2
- NX 4524 - ge1-ge24, up1, up2
- NX 6500 - up1, up2
- NX 6524 - ge1-ge24, up1, up2
- NX 9000 series - ge1, ge2 (10GigE ports (xge1-xge4) are available on NX9610 models)

*UP* ports are available on RFS 4000 wireless controllers. A UP port connects the to the backbone network. A UP port supports either RJ-45 or fiber. A UP port is the preferred means to connect to the backbone, as it has a non-blocking 1gbps connection unlike GE ports.

The following ports are available on access points:

- AP 6511 - fe1, fe2, fe3, fe4, up1
- AP 6521 - GE1/POE (LAN)
- AP 6522 - GE1/POE (LAN)
- AP 6532- GE1/POE
- AP 6562 - GE1/POE
- AP 7131 - GE1/POE (LAN), GE2 (WAN)
- AP 7131N - GE1/POE (LAN), GE2 (WAN)
- AP 7161N - GE1/POE (LAN), GE2 (WAN)

- AP 7181 - GE1/POE (LAN), GE2 (WAN)
- AP 8132 - GE1/POE (LAN), GE2 (WAN)

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.

Name	Type	Description	Admin Status	Mode	Native VLAN	Tag Native VLAN	Allowed VLANs
ge1	Ethernet		✓ Enabled	Access	1	✗	
ge2	Ethernet		✓ Enabled	Access	1	✗	
ge3	Ethernet		✓ Enabled	Access	1	✗	
ge4	Ethernet		✓ Enabled	Access	1	✗	
me1	Ethernet		✓ Enabled	Access	1	✗	

Type to search in tables Row Count: 5

[Edit](#) [Exit](#)

- 4 Refer to the following to assess port status and performance:

<b>Name</b>	Displays the physical port name reporting runtime data and statistics. Supported ports vary depending on controller, service platform or access point model.
<b>Type</b>	Displays the physical port type. Cooper is used on RJ45 Ethernet ports and Optical materials are used on fiber optic gigabit Ethernet ports.
<b>Description</b>	Displays an administrator defined description for each listed device port.
<b>Admin Status</b>	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.
<b>Mode</b>	Displays the profile's switching mode as currently either <i>Access</i> or <i>Trunk</i> (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.
<b>Native VLAN</b>	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.

<b>Tag Native VLAN</b>	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.
<b>Allowed VLANs</b>	Displays those VLANs allowed to send packets over the listed port. Allowed VLANs are only listed when the mode has been set to Trunk.

- To edit the configuration of an existing port, select it from amongst those displayed and select the **Edit** button.

### *Editing Ethernet Port Configurations*

Port placement and quantity varies depending on controller, service platform or access point model.

The following ports are available on RFS controllers:

- RFS 4000- ge1, ge2, ge3, ge4, ge5, up1

The following ports are available on NX series service platforms:

- NX 9000 series - ge1, ge2 (10GigE ports (xge1-xge4) are available on NX9610 models)

UP ports are available on RFS 4000 model wireless controller. A UP port connects the to the backbone network. A UP port supports either RJ-45 or fiber. A UP port is the preferred means to connect to the backbone, as it has a non-blocking 1gbps connection unlike GE ports.

The following ports are available on access points:

- AP 6522 - GE1/POE (LAN)
- AP 6562 - GE1/POE
- AP 7161N - GE1/POE (LAN), GE2 (WAN)

For more information, see:

- [Basic Ethernet Port Configuration](#)
- [Ethernet Port Security](#)
- [Ethernet Port Spanning Tree](#)

### **Basic Ethernet Port Configuration**

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**.
- 4 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.

5 Set the following Ethernet port **Properties**:

<b>Description</b>	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.
<b>Admin Status</b>	Select the <i>Enabled</i> radio button to define this port as active to the controller profile it supports. Select the <i>Disabled</i> radio button to disable this physical port in the profile. It can be activated at any future time when needed.
<b>Speed</b>	Select the speed at which the port can receive and transmit the data. Select either <i>10 Mbps</i> , <i>100 Mbps</i> or <i>1000 Mbps</i> . 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 <i>Automatic</i> 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.
<b>Duplex</b>	Select either <i>half</i> , <i>full</i> or <i>automatic</i> as the duplex option. Select <i>Half</i> 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 <i>Full</i> duplex to transmit data to and from the device port at the same time. Using Full duplex, the port can send data while receiving data as well. Select <i>Automatic</i> to dynamically duplex as port performance needs dictate. Automatic is the default setting.

- 6 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:

<b>Cisco Discovery Protocol Receive</b>	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.
<b>Cisco Discovery Protocol Transmit</b>	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.
<b>Link Layer Discovery Protocol Receive</b>	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.
<b>Link Layer Discovery Protocol Transmit</b>	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.

- 7 Set the following **Power Over Ethernet (PoE)** parameters for this profile's Ethernet port configuration:

<b>Enable POE</b>	Select the check box to configure the selected port to use Power over Ethernet. To disable PoE on a port, uncheck this option. Power over Ethernet is supported on RFS 4000 model controllers only. When enabled, the controller 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.
<b>Power Limit</b>	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.
<b>Power Priority</b>	Set the power priority for the listed port to either to either <i>Low</i> , <i>Medium</i> or <i>High</i> . This is the priority assigned to this port versus the power requirements of the other ports on the controller.

- 8 Define the following **Switching Mode** parameters to apply to the Ethernet port configuration:

<b>Mode</b>	Select either the <i>Access</i> or <i>Trunk</i> radio button to set the VLAN switching mode over the port. If <i>Access</i> is selected, the port accepts packets only from 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 <i>Trunk</i> , the port allows packets from a list of VLANs you add to the trunk. A port configured as <i>Trunk</i> supports multiple 802.1Q tagged VLANs and one <i>Native VLAN</i> which can be tagged or untagged. <i>Access</i> is the default mode.
<b>Native VLAN</b>	Use the spinner control to define a numerical <i>Native VLAN ID</i> 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.

<b>Tag Native VLAN</b>	Select the check box to tag the native VLAN. WiNG managed 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 to. 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.
<b>Allowed VLANs</b>	Selecting Trunk switching mode enables the <i>Allowed VLANs</i> parameter to add VLANs that exclusively send packets over the listed port.

- 9 In the **Dynamic Link Aggregation (LACP)** area, set the following parameters to enable link aggregation on the selected GE port:

<b>Port Channel</b>	Select to configure the selected port as a member of a link aggregation group (LAG). Link aggregation is supported only on the following platforms: AP 7562, AP 7602, AP 7612, AP 8432, AP 8533, NX 5500, NX 75XX, NX 95XX, NX 9600, and VX 9000. 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. It also 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. <b>Note:</b> if enabling LACP, 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.
<b>Port Mode</b>	Set the port mode as <b>Active</b> or <b>Passive</b> . If setting the port as a LAG member, specify whether the port is an active or passive member within the group. An active member initiates and participates in LACP negotiations. It is the active port that always transmits LACPDU irrespective of the remote device's port mode. The passive port only responds to LACPDU received from its corresponding active port. At least one port within a LAG, on either of the two negotiating peers, should be in the active mode. LACP negotiations are not initiated if all LAG member ports are passive. Further, the peer-to-peer LACP negotiations are always initiated by the peer with the lower system-priority value.
<b>Port Priority</b>	Select the Port Priority check box and set the selected Ethernet Port's priority value, within the LAG, from 1-65535. The selected port's actual priority within the LAG is determined by the port-priority value specified here along with the port's number. Higher the value, lower is the priority. Use this option to manipulate a port's priority. For example, in a LAG having five physical ports, four active and one standby, manually increasing the standby port's priority ensures that if one of the active port fails, the standby port is included in the LAG during re-negotiation.

- 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 Click **+ Add Row** and set or override the **Fabric Attach** parameters. This option enables WiNG devices (access points and controllers) as FA (Fabric Attach) Clients.



#### Note

To enable FA Client feature, the Ethernet port's switching mode should be set to trunk.

VLAN	Set the VLAN from 1 - 4094.
ISID	<p>User the spinner control to specify the ISID from 1 - 16777214. This is the ISID (Individual Service Identifier) associated with the VLAN interface specified above. Configuring a VLAN to ISID assignment, enables FA client operation on the selected Ethernet port.</p> <p>The FA Client requests acceptance of the VLAN to ISID mapping from the FAS within the FC (Fabric Connect) network. Once acceptance is achieved, the FC edge switch applies the ISID to the VLAN traffic from the device (AP or controller), and uses this ISID inside the Fabric.</p> <p><b>Note:</b> A maximum of 94 pairs of I-SID to VLAN mappings can be configured per Ethernet port.</p>

FA-enabled switches, in the FC network, send out LLDP messages with TLV extensions of Organization-specific TLV with OUI, to discover FA clients and advertise capabilities.

The FA-enabled client associates with the FAS (FA Server), and obtains provisioning information (management VLAN interface details, and whether the interface is tagged or not) that allows the client to be configured with parameters that allow traffic to flow through the Fabric to the WLAN controller. Use this option to configure the ISID to VLAN mapping that the FA Client uses to negotiate with the FAS.

You can configure FA Client capability on a device's profile as well as device contexts.

- 12 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.
- 13 Select **OK** to save the changes made to the Ethernet Port Basic Configuration. Select **Reset** to revert to the last saved configuration.

## Ethernet Port Security

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**.



- 4 To edit the configuration of an existing port, select it from amongst those displayed and select the **Edit** button.
- 5 Select the **Security** tab.
- 6 Refer to the **Access Control** field. As part of the port's security configuration, Inbound IP and MAC address firewall rules are required.

Use the **Inbound IP Firewall Rules** and **MAC Inbound Firewall Rules** pull-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.

- 7 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. For more information, see [Wireless Firewall](#) on page 714.
- 8 Refer to the **Trust** field to define the following:

<b>Trust ARP Responses</b>	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.
<b>Trust DHCP Responses</b>	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.
<b>ARP header Mismatch Validation</b>	Select this option to enable a mismatch check for the source MAC in both the ARP and Ethernet header. The default value is disabled.
<b>Trust 802.1p COS values</b>	Select the check box to enable 802.1p COS values on this port. The default value is enabled.
<b>Trust IP DSCP</b>	Select the check box to enable IP DSCP values on this port. The default value is enabled.
<b>Note:</b> 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.	

- 9 Set the following **802.1X Settings**:

<b>Host Mode</b>	Use the drop-down menu to select the host mode configuration to apply to this port. Options include <i>single-host</i> or <i>multi-host</i> . The default setting is single-host.
<b>Guest VLAN</b>	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.
<b>Port Control</b>	Use the drop-down menu to set the port control state to apply to this port. Options include <i>force-authorized</i> , <i>force-unauthorized</i> and <i>automatic</i> . The default setting is force-authorized.
<b>Re Authenticate</b>	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.
<b>Max Reauthenticate Count</b>	Set the maximum reauthentication attempts (1 - 10) before this port is moved to unauthorized. The default setting is 2.
<b>Maximum Request</b>	Set the maximum number of authentication requests (1 - 10) before returning a failed message to the requesting client. The default setting is 2.

<b>Quiet Period</b>	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.
<b>Reauthenticate Period</b>	Use the spinner control to set the reauthentication period for this port from 1 - 65,535 seconds. The default setting is 60 seconds.
<b>Port MAC Authentication</b>	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 RFS 4000, RFS 6000 model controllers and NX 4500, NX 6500 and NX 9000 series service platforms. Port MAC authentication may be enabled on ports in conjunction with Wired 802.1x settings for a MAC Authentication AAA policy.

- 10 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.
- 11 Select **OK** to save the changes made to the Ethernet port's security configuration. Select **Reset** to revert to the last saved configuration.

## Spanning Tree

To define an Ethernet port's spanning tree configuration:

- 1 Select **Configuration > Profiles > Interface**.
- 2 Expand the Interface menu to display its submenu options.
- 3 Select **Ethernet Ports**.
- 4 To edit the configuration of an existing port, select it from amongst those displayed and select the **Edit** button.
- 5 Select the **Spanning Tree** tab.

**Ethernet Ports** x

Name **ge2** ?

**Basic Configuration** | **Security** | **Spanning Tree**

**PortFast**

Enable PortFast

Enable PortFast BPDU Filter

Enable PortFast BPDU Guard

**MSTP Configuration**

Enable as Edge Port

Link Type  Point-to-Point  Shared

Cisco MSTP Interoperability  Enable  Disable

Force Protocol Version  STP (0)  Not Supported (1)  RSTP (2)  MSTP (3)

Guard  None  Root

**Spanning Tree Port Cost**

Instance Index	Cost
0	1
1	1

**+ Add Row**

**Spanning Tree Port Priority**

Instance Index	Priority
0	128

**+ Add Row**

**OK** **Reset** **Exit**

- 6 Define the following **PortFast** parameters for the port's MSTP configuration:

<b>Enable PortFast</b>	Select the check box to enable pull-down menus for both the Enable Portfast BPDU Filter and Enable Portfast BPDU guard options for the port.
<b>PortFast BPDU Filter</b>	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.
<b>PortFast BPDU Guard</b>	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.

- 7 Set the following **MSTP Configuration** parameters:

<b>Enable as Edge Port</b>	Select the check box to define this port as an edge port. Using an edge (private) port, isolate devices to prevent connectivity over this port.
<b>Link Type</b>	Select either the <i>Point-to-Point</i> or <i>Shared</i> 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 is a point-to-point link.
<b>Cisco MSTP Interoperability</b>	Select either the <i>Enable</i> or <i>Disable</i> radio buttons. This enables interoperability with Cisco's version of MSTP over the port, which is incompatible with standard MSTP.
<b>Force Protocol Version</b>	Sets the protocol version to either <i>STP(0)</i> , <i>Not Supported(1)</i> , <i>RSTP(2)</i> or <i>MSTP(3)</i> . MSTP is the default setting.
<b>Guard</b>	Determines whether the port enforces root bridge placement. Setting the guard to <i>Root</i> 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.

- 8 Refer to the **Spanning Tree Port Cost** table.
- 9 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

- 10 Select **+ AddRow** as needed to include additional indexes.
- 11 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 value impacts the port's likelihood of becoming a designated port.

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

- 12 Select **OK** to save the changes made to the Ethernet Port's spanning tree configuration. Select **Reset** to revert to the last saved configuration.

## Virtual 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.

- 1 To review existing Virtual Interface configurations and either create a new Virtual Interface configuration, modify an existing configuration or delete an existing configuration:
- 2 Select **Configuration > Profiles > Interface**.
- 3 Expand the Interface menu to display its submenu options.
- 4 Select **Virtual Interfaces**.

Name	Type	Description	Admin Status	VLAN	IP Address
vlan1	VLAN		❌ Disabled	1	
vlan4	VLAN		✅ Enabled	4	
vlan5	VLAN		✅ Enabled	5	dhcp

Type to search in tables Row Count: 3

- 5 Review the following parameters unique to each virtual interface configuration:

<b>Name</b>	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.
<b>Type</b>	Displays the type of Virtual Interface for each listed interface.
<b>Description</b>	Displays the description defined for the Virtual Interface when it was either initially created or edited.
<b>Admin Status</b>	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.

<b>VLAN</b>	Displays the numerical VLAN ID associated with each listed interface.
<b>IP Address</b>	Defines whether DHCP was used to obtain the primary IP address used by the Virtual Interface configuration.

- 6 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.

### *Adding and Editing Virtual Interface configurations*

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.

For more information, see:

- [Virtual Interface Basic Configuration](#)
- [Virtual Interface Security](#)

### **Virtual Interfaces Basic Configuration**

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**.
- 4 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.

The **Basic Configuration** screen displays by default, regardless of whether a new Virtual Interface is created or an existing one is being modified.

- 5 If creating a new Virtual Interface, use the **VLAN ID** spinner control to define a numeric ID from 1 - 4094.
- 6 Define the following parameters from within the **Properties** field:

<b>Description</b>	Provide or edit a description (up to 64 characters) for the Virtual Interface that helps differentiate it from others with similar configurations.
<b>Admin Status</b>	Either select either the <i>Disabled</i> or <i>Enabled</i> radio button to define this interface's current status. When set to Enabled, the Virtual Interface is operational and available. The default value is disabled.

- 7 Set the following network information from within the **IP Addresses** field:

<b>Enable Zero Configuration</b>	Define the IP address for the VLAN associated Virtual Interface. Zero Configuration can be a means of providing 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.
<b>Primary IP Address</b>	Define the IP address for the VLAN associated Virtual Interface.
<b>Use DHCP to Obtain IP</b>	Select this option to allow DHCP to provide the IP address for the Virtual Interface. Selecting this option disables the Primary IP address field.
<b>Use DHCP to obtain Gateway/DNS Servers</b>	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.
<b>Secondary Addresses</b>	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.

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

<b>Respond to DHCP Relay Packets</b>	Select the Respond to DHCP Relay Packets option to allow the onboard DHCP server to respond to relayed DHCP packets on this interface.
<b>DHCP Relay IP Address</b>	Provide IP addresses for DHCP server relay resources. The interface VLAN and gateway should have their IP addresses set. The interface VLAN and gateway interface should not have DHCP client or DHCP Server enabled. DHCP packets cannot be relayed to an onboard DHCP Server. The interface VLAN and gateway interface cannot be the same. 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.

- 9 Define the **Network Address Translation (NAT)** direction. Select either **Inside**, **Outside** or **None**.
  - *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 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.



#### Note

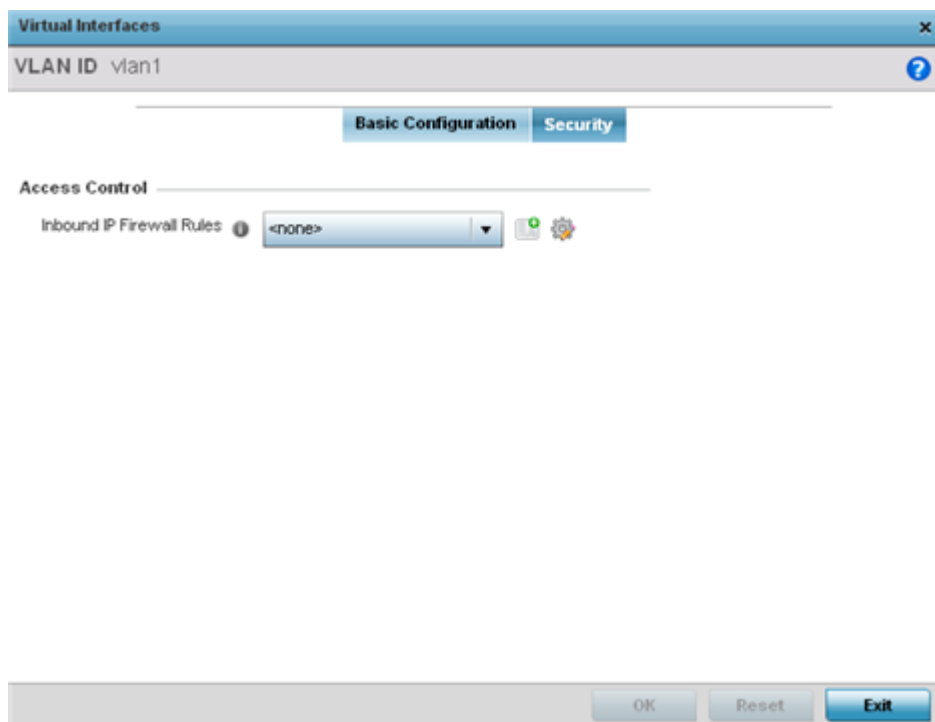
Refer to [Setting the Profile's NAT Configuration](#) for instructions on creating a profile's NAT configuration.

- 10 Select **OK** to save the changes to the basic configuration screen. Select **Reset** to revert to the last saved configuration.

## Virtual Interface Security

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**.
- 4 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.
- 5 Select the **Security** tab.



- 6 Use the **Inbound IP Firewall Rules** platform menu to select the firewall rule configuration to apply to this Virtual Interface.

The firewall inspects and packet traffic to and from connected clients.

If a firewall rule does not exist suiting the data protection needs of this Virtual Interface, select the **Create** icon to define a new firewall rule configuration or the **Edit** icon to modify an existing configuration. For more information, see [Wireless Firewall](#) on page 714.

- Use the **VPN Crypto Map** platform menu to select the Crypto Map configuration to apply 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 suit 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 [Setting the Profile's VPN Configuration](#).

- Select the **OK** button located at the bottom right of the screen to save the changes to the Security screen. Select **Reset** to revert to the last saved configuration.

## Port Channel Configuration

Controller, service platform and access point profiles can be applied customized port channel settings as part of their interface configuration.

To define a port channel configuration for a device profile:

- Select **Configuration > Profiles > Interface**.
- Expand the Interface menu to display its submenu options.
- Select **Port Channels**.

The Port Channels screen displays.

Name	Type	Description	Admin Status
port-channel1	Port Channel		✓ Enabled
port-channel2	Port Channel	lancelot	✗ Disabled

Type to search in tables Row Count: 2

- Refer to the following to review existing port channel configurations and their current status:

<b>Name</b>	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.
<b>Type</b>	Displays whether the type is port channel.



<b>Description</b>	Lists a a short description (64 characters maximum) describing the port channel or differentiating it from others with similar configurations.
<b>Admin Status</b>	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 create a new manual session, **Edit** to modify an existing configuration or **Delete** to remove a selected port channel configuration.

### Adding and Editing a Port Channel Configuration

Profiles can be applied customized port channel configurations as part of their Interface configuration.

For more information, refer to the following:

- [Port Channel Basic Configuration](#) on page 545
- [Port Channel Security](#) on page 547
- [Port Channel Spanning Tree](#) on page 548

### Port Channel Basic Configuration

To define a port channel configuration for a device profile:

- 1 Select **Configuration > Profiles > Interface**.
- 2 Expand the Interface menu to display its submenu options.
- 3 Select **Port Channels**.
- 4 To edit the configuration of an existing port channel, select it from amongst those displayed and select the **Edit** button. To add a new port channel configuration select the **Add** button.

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

**Port Channels** [x]

port-channel1 [?]

**Basic Configuration** | Security | Spanning Tree

**Properties**

Description [?]

Admin Status [?]  Disabled  Enabled

Speed [?] Automatic ▾

Duplex [?] Automatic ▾

**Switching Mode**

Mode [?]  Access  Trunk

Native VLAN [?] 1 (1 - 4094)

Tag Native VLAN [?]

Allowed VLANs [?] (\$2a xz,4,7-12,...)

**Client Load Balancing**

Port Channel Load Balance [?] Source/Destination IP ▾

OK Reset Exit

- 5 Set the following port channel **Properties**:

<b>Description</b>	Enter a brief description for the port channel (64 characters maximum). The description should reflect the port channel's intended function.
<b>Admin Status</b>	Select the <i>Enabled</i> radio button to define this port channel as active to the profile it supports. Select the <i>Disabled</i> 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.
<b>Speed</b>	Select the speed at which the port channel can receive and transmit the data. Select either <i>10 Mbps</i> , <i>100 Mbps</i> , <i>1000 Mbps</i> . 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 <i>Automatic</i> 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.
<b>Duplex</b>	Select either <i>Half</i> , <i>Full</i> or <i>Automatic</i> 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.

- 6 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.
- 7 Define the following **Switching Mode** parameters to apply to the port channel configuration:

<b>Mode</b>	Select either the <i>Accessor Trunk</i> 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 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.
<b>Native VLAN</b>	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.

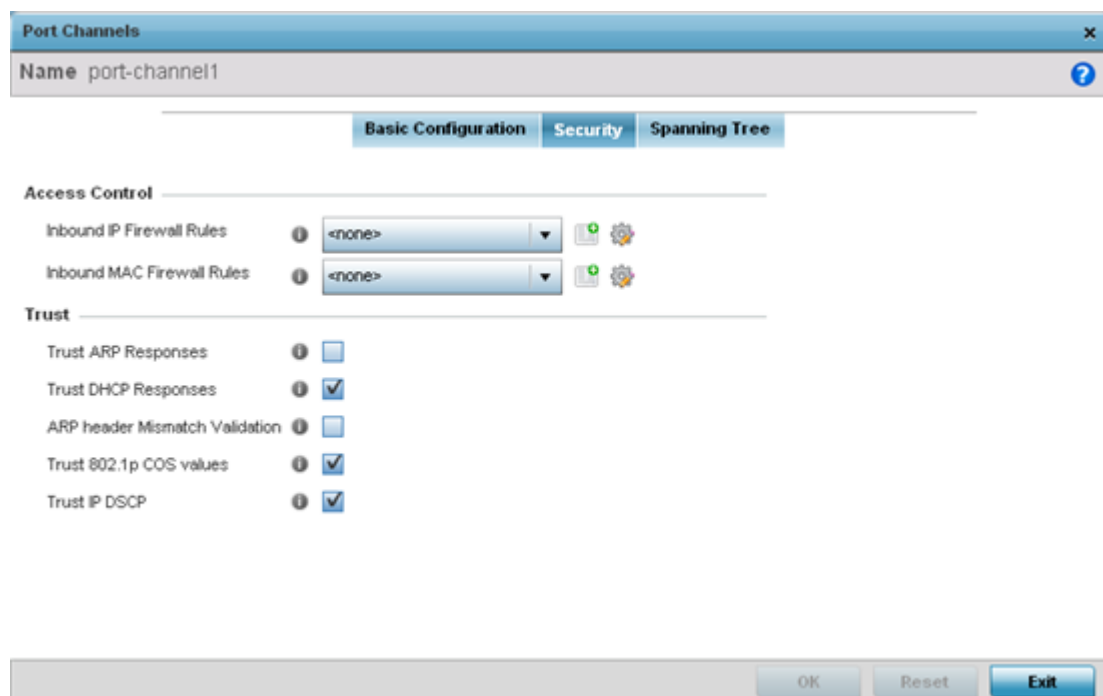
<b>Tag the Native VLAN</b>	Select the checkbox to tag the native VLAN. WiNG managed devices support the IEEE 802.1Q specification for tagging frames and coordinating VLANs between devices. IEEE 802.1Q adds four bytes to each frame identifying the VLAN ID for upstream devices that the frame belongs. If 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.
<b>Allowed VLANs</b>	Selecting <i>Trunk</i> as the mode enables the Allowed VLANs parameter. Add VLANs that exclusively send packets over the port channel.

- 8 Select **OK** to save the changes made to the port channel Basic Configuration. Select **Reset** to revert to the last saved configuration.

### Port Channel Security

To define a port channel configuration for a device profile:

- 1 Select **Configuration > Profiles > Interface**.
- 2 Expand the Interface menu to display its submenu options.
- 3 Select **Port Channels**.
- 4 To edit the configuration of an existing port channel, select it from amongst those displayed and select the **Edit** button. To add a new port channel configuration select the **Add** button.
- 5 Select the **Security** tab.



- 6 Refer to the **Access Control** section. As part of the port channel's security configuration, Inbound IP and MAC address firewall rules are required.

Use the **Inbound IP Firewall Rules** and **MAC Inbound Firewall Rules** drop-down menus to select firewall rules to apply to this profile's port channel configuration.

The firewall inspects IP and MAC traffic flows and detects attacks typically not visible to traditional wired firewall appliances.

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. For more information, see [Wireless Firewall](#) on page 714.

- 7 Refer to the **Trust** field to define the following:

<b>Trust ARP Responses</b>	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.
<b>Trust DHCP Responses</b>	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.
<b>ARP header Mismatch Validation</b>	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.
<b>Trust 802.1p COS values</b>	Select the check box to enable 802.1p COS values on this port channel. The default value is enabled.
<b>Trust IP DSCP</b>	Select the check box to enable IP DSCP values on this port channel. The default value is enabled.

- 8 Select **OK** to save the changes to the security configuration. Select **Reset** to revert to the last saved configuration.

### Port Channel Spanning Tree

To define a port channel configuration for a device profile:

- 1 Select **Configuration > Profiles > Interface**.
- 2 Expand the Interface menu to display its submenu options.
- 3 Select **Port Channels**.
- 4 To edit the configuration of an existing port channel, select it from amongst those displayed and select the **Edit** button. To add a new port channel configuration select the **Add** button.
- 5 Select the **Spanning Tree** tab.

- 6 Define the following **PortFast** parameters for the port channel's MSTP configuration:

<b>Enable PortFast</b>	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.
<b>PortFast BPDU Filter</b>	Select <i>Enable</i> 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.
<b>PortFast BPDU Guard</b>	Select <i>Enable</i> 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.

- 7 Set the following **MSTP Configuration** parameters for the port channel:

<b>Enable as Edge Port</b>	Select the check box 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.
<b>Link Type</b>	Select either the <i>Point-to-Point</i> or <i>Shared</i> 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 the wireless device is a point-to-point link. Point-to-Point is the default setting.
<b>Cisco MSTP Interoperability</b>	Select either the <i>Enable</i> or <i>Disable</i> radio buttons. This enables interoperability with Cisco's version of MSTP, which is incompatible with standard MSTP. This setting is disabled by default.

<b>Force Protocol Version</b>	Sets the protocol version to either <i>STP(0)</i> , <i>Not Supported(1)</i> , <i>RSTP(2)</i> or <i>MSTP(3)</i> . MSTP is the default setting.
<b>Guard</b>	Determines whether the port channel enforces root bridge placement. Setting the guard to <i>Root</i> 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 <i>bridge receives superior</i> (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.

- 8 Refer to the **Spanning Tree Port Cost** table.
- 9 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

- 10 Select **+ AddRow** as needed to include additional indexes.
- 11 Refer to the **Spanning Tree Port Priority** table.
- 12 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.
- 13 Select **+ Add Row** needed to include additional indexes.
- 14 Select **OK** to save the changes made to the Ethernet Port Spanning Tree configuration. Select **Reset** to revert to the last saved configuration.

## VM 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 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**.

Name	Type	Description	Admin Status	Mode	Native VLAN	Tag Native VLAN	Allowed VLANs
vmif1	VM Interface		✓ Enabled	Access	1	✗	
vmif2	VM Interface		✓ Enabled	Access	1	✗	
vmif3	VM Interface		✓ Enabled	Access	1	✗	
vmif4	VM Interface		✓ Enabled	Access	1	✗	
vmif5	VM Interface		✓ Enabled	Access	1	✗	
vmif6	VM Interface		✓ Enabled	Access	1	✗	
vmif7	VM Interface		✓ Enabled	Access	1	✗	
vmif8	VM Interface		✓ Enabled	Access	1	✗	

Type to search in tables Row Count: 8

- 4 Refer to the following to review VM interface configurations and status:

<b>Name</b>	Displays the VM interface numerical identifier assigned when it was created. The numerical name cannot be modified as part of the edit process.
<b>Type</b>	Displays whether the type is VM interface.
<b>Description</b>	Lists a short description (64 characters maximum) describing the VM interface or differentiating it from others with similar configurations.
<b>Admin Status</b>	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.
<b>Mode</b>	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.

<b>Native VLAN</b>	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.
<b>Tag Native VLAN</b>	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.
<b>Allowed VLANs</b>	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.

- To edit the configuration of an existing VM interface, select it from amongst those displayed and select the **Edit** button.

### VM Basic Configuration

To set a VM interface basic configuration for a profile:

- Select **Configuration > Profiles > Interface**.
- Expand the **Interface** menu to display its submenu options.
- Select **VM**.
- Select an existing VM interface configuration and select the **Edit** button. The **Basic Configuration** tab displays by default.

- Set the following VM interface **Properties**:



<b>Description</b>	Enter a brief description for the controller or service platform VM interface (64 characters maximum).
<b>Admin Status</b>	Select the <i>Enabled</i> radio button to define this VM interface as active to the profile it supports. Select the <i>Disabled</i> 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.

- 6 Define the following **Switching Mode** parameters to apply to the VM Interface configuration:

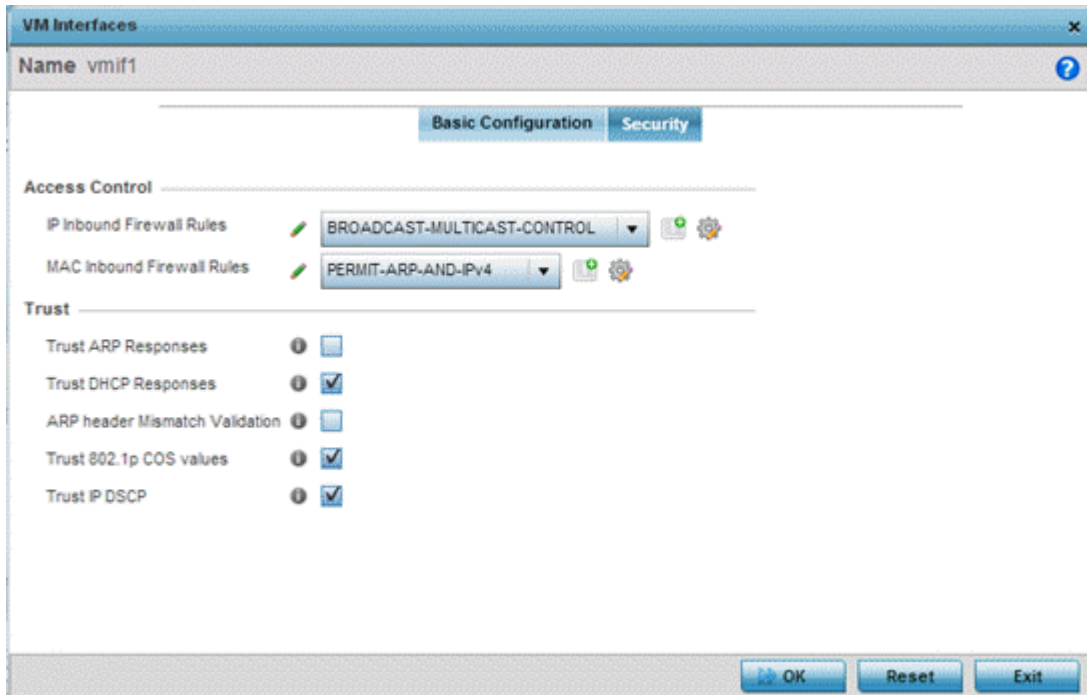
<b>Mode</b>	Select either the <i>Access</i> or <i>Trunk</i> radio button to set the VLAN switching mode over the VM interface. If <i>Access</i> is selected, the VM interface accepts packets only from the native VLAN. Frames are forwarded untagged with no 802.1Q header. All frames received on the VM port are expected as untagged and are mapped to the native VLAN. If the mode is set to <i>Trunk</i> , the VM interface allows packets from a list of VLANs you add to the trunk. A VM interface configured as <i>Trunk</i> supports multiple 802.1Q tagged VLANs and one Native VLAN which can be tagged or untagged. <i>Access</i> is the default setting.
<b>Native VLAN</b>	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.
<b>Tag the Native VLAN</b>	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.
<b>Allowed VLANs</b>	Selecting <i>Trunk</i> as the mode enables the <i>Allowed VLANs</i> 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.

- 7 Select **OK** to save the changes to the VM interface basic configuration. Select **Reset** to revert to the last saved configuration.

### VM Security Settings

To set VM interface security settings for a NX service platform profile:

- 1 Select **Configuration > Profiles > Interface**.
- 2 Expand the **Interface** menu to display its submenu options.
- 3 Select **VM**.
- 4 Select an existing VM interface configuration and select the **Edit** button.
- 5 Select the **Security** tab.



- 6 Refer to the **Access Control** field. IP Inbound and MAC Inbound address firewall rules are required.

Use the **IP Inbound Firewall Rules** and **MAC Inbound Firewall Rules** 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.

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.

- 7 Refer to the **Trust** field to define the following:

<b>Trust ARP Responses</b>	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.
<b>Trust DHCP Responses</b>	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.
<b>ARP header Mismatch Validation</b>	Select this option to enable a source MAC mismatch check in both the ARP and Ethernet header. The default value is enabled.
<b>Trust 802.1p COS values</b>	Select this option to enable 802.1p COS values on this VM interface. The default value is enabled.
<b>Trust IP DSCP</b>	Select this option to enable IP DSCP values on this VM interface. The default value is enabled.

- 8 Select **OK** to save the changes to the VM interface security configuration. Select **Reset** to revert to the last saved configuration.

## Spanning Tree Configuration

To define a network spanning tree configuration for a profile:

- 1 Select **Configuration > Profiles > Network**.
- 2 Expand the Network menu to display its submenu options.
- 3

## Access Point Radio Configuration

access points can have their radio configurations modified by their management controller, service platform or peer access point. 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 from its managing device.

To define an access point radio configuration from an associated peer access point model Controller AP, controller or NX service platform:

- 1 Select **Configuration > Profiles > Interface**.
- 2 Expand the Interface menu to display its submenu options.
- 3 Select **Radios**.

Name	Type	Description	Shutdown	RF Mode	Channel	Transmit Power
radio1	Radio	radio1	✓ Enabled	2.4 GHz WLAN	smart	smart
radio2	Radio	radio2	✓ Enabled	5 GHz WLAN	smart	smart
radio3	Radio	radio3	✓ Enabled	Sensor	smart	smart
Type to search in tables			Row Count: 3			
<input type="button" value="Edit"/> <input type="button" value="Exit"/>						

- 4 Review the following to determine whether a radio configuration requires modification to better support the managed network:

<b>Name</b>	Displays whether the reporting radio is the access point's radio1, radio2 or radio3. AP 6511 and AP 6521 models have one radio. AP 6522, AP 6532, AP 6562, AP71XX and AP 8132 models have two radios. Certain AP 7131N model SKUs have three radios.
<b>Type</b>	Displays the type of radio housed by each listed access point.

<b>Description</b>	Displays a brief description of the radio provided by the administrator when the radio's configuration was added or modified.
<b>Admin Status</b>	A green checkmark defines the listed radio as active and enabled with its supported profile. A red "X" defines the radio as currently disabled.
<b>RF Mode</b>	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.
<b>Channel</b>	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.
<b>Transmit Power</b>	Lists the transmit power for each radio displayed as a value in milliwatts.

- 5 If required, select a radio configuration and select the **Edit** button to modify its configuration.

### *Editing Radio Configurations*

The configuration screen supporting an access point's radio configuration is partitioned into 4 tabs, each supporting a unique configuration attribute of the radio.

For more information, see:

- [Radio Settings](#)
- [WLAN Mapping and Mesh Mapping](#)
- [Legacy Mesh](#)
- [Advanced Settings](#)

### **Radio Settings**

Use the **Radio Settings** screen to apply QoS, ACL, operational mode, WLAN attributes and sensor configuration settings to the radio.

To define an access point's radio settings:

- 1 Select **Configuration > Profiles > Interface**.
- 2 Expand the Interface menu to display its submenu options.
- 3 Select **Radios**.
- 4 If required, select a radio configuration and select the **Edit** button to modify its configuration.

The **Radio Settings** tab displays by default.

- 5 Define the following radio configuration parameters from within the **Properties** field:

<b>Description</b>	Provide or edit a description (1 - 64 characters in length) for the radio that helps differentiate it from others with similar configurations.
<b>Admin Status</b>	Select the <i>Enabled</i> radio button to define this radio as active to the profile it supports. Select the <i>Disabled</i> 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.
<b>Radio QoS Policy</b>	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 <i>Create</i> icon to define a new QoS policy that can be applied to this profile.
<b>Association ACL</b>	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 <i>Create</i> icon to define a new Association ACL that can be applied to this profile.

- 6 Set the following profile **Radio Settings** for the selected access point radio:

<b>RF Mode</b>	Set the mode to either <i>2.4 GHz WLAN</i> or <i>5 GHz WLAN</i> depending on the radio's intended client support requirement. Set the mode to <i>Sensor</i> if using the radio for rogue device detection. To a radio as a detector, disable <i>Sensor</i> support on the other access point radio. Set the mode to <i>scan-ahead</i> 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.
<b>Lock RF Mode</b>	Select the check box to lock Smart RF for this radio. The default setting is disabled.
<b>DFS Revert Home</b>	Select this option to revert to the home channel after a DFS evacuation period.
<b>Channel</b>	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 <i>Smart</i> 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 <i>Smart</i> . 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, and are unique to the 80 MHz band.
<b>Transmit Power</b>	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.
<b>Antenna Gain</b>	Set the antenna between 0.00 - 15.00 dBm. The access point's <i>Power Management Antenna Configuration File (PMACF)</i> 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.
<b>Antenna Mode</b>	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. 3x3x3 is used for transmissions and receipts over three antennas models. The default setting is dynamic based on the access point model deployed and its transmit power settings.
<b>Enable Antenna Diversity</b>	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.
<b>Wireless Client Power</b>	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.
<b>Dynamic Chain Selection</b>	Select this option for the radio to dynamically change the number of transmit chains. This option is enabled by default.

<b>Data Rates</b>	<p>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).</p> <p>If dedicating the radio to either 2.4 or 5 GHz support, a Custom Rates option is available to set a <i>modulation and coding scheme</i> (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 AP 8132 model access points and its ability to provide 3x3x3 MIMO support.</p> <p>Refer to the bottom of this page for 802.11an and 802.11ac MCS data rates in detail, both with and without <i>short guard intervals</i> (SGI).</p>
<b>Radio Placement</b>	Use the drop-down menu to specify whether the radio is located <i>Indoors</i> or <i>Outdoors</i> . The placement should depend on the country of operation and its regulatory domain requirements for radio emissions. The default setting is <i>Indoors</i> .
<b>Max Clients</b>	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. AP 6511 and AP 6521 model access points can only support 128 clients.
<b>Rate Selection Method</b>	Specify a radio selection method for the radio. The selection methods are: <i>Standard</i> : standard monotonic radio selection method will be used. <i>Opportunistic</i> : sets opportunistic radio link adaptation as the radio selection method. This mode uses opportunistic data rate selection to provide the best throughput.

- 7 Set the following profile **WLAN Properties** for the selected access point radio.

<b>Beacon Interval</b>	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.
<b>DTIM Interval BSSID</b>	Set a DTIM Interval to specify a period for <i>Delivery Traffic Indication Messages</i> (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 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.

<b>RTS Threshold</b>	<p>Specify a <i>Request To Send</i> (RTS) threshold (between 1 - 2,347 bytes) for use by the WLAN's adopted access point radios. RTS is a transmitting station's signal that requests a <i>Clear To Send</i> (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.</p> <p>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.</p> <p>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.</p>
<b>Short Preamble</b>	<p>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.</p>
<b>Guard Interval</b>	<p>Use the drop-down menu to specify a <i>Long</i> or <i>Any</i> guard interval. The guard interval is the space between the packets being transmitted. The guard interval is there to eliminate <i>inter-symbol interference</i> (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.</p>
<b>Probe Response Rate</b>	<p>Use the drop-down menu to specify the data transmission rate used for the transmission of probe responses. Options include, <i>highest-basic</i>, <i>lowest-basic</i> and <i>follow-probe-request</i> (default setting).</p>
<b>Probe Response Retry</b>	<p>Select the check box to retry probe responses if they are not acknowledged by the target wireless client. The default value is enabled.</p>

- 8 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.

#### SUPPORTED DATA RATES

802.11n MCS rates are defined as follows for MCS 1-3 streams, both with and without *short guard intervals* (SGI):

<i>MCS-1Stream Index</i>	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz With SGI
0	1	6.5	7.2	13.5	15
1	1	13	14.4	27	30



<i>MCS-1Stream Index</i>	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz With SGI
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

<i>MCS-2Stream Index</i>	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz 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
6	2	117	130	243	270
7	2	130	144.4	270	300

<i>MCS-3Stream Index</i>	Number of Streams	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz 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 (theoretical throughput for single spatial streams) are defined as follows, both with and without *short guard intervals* (SGI):

<i>MCS Index</i>	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz With SGI	80 MHz No SGI	80 MHz 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

<i>MCS Index</i>	20 MHz No SGI	20 MHz With SGI	40 MHz No SGI	40 MHz With SGI	80 MHz No SGI	80 MHz With SGI
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

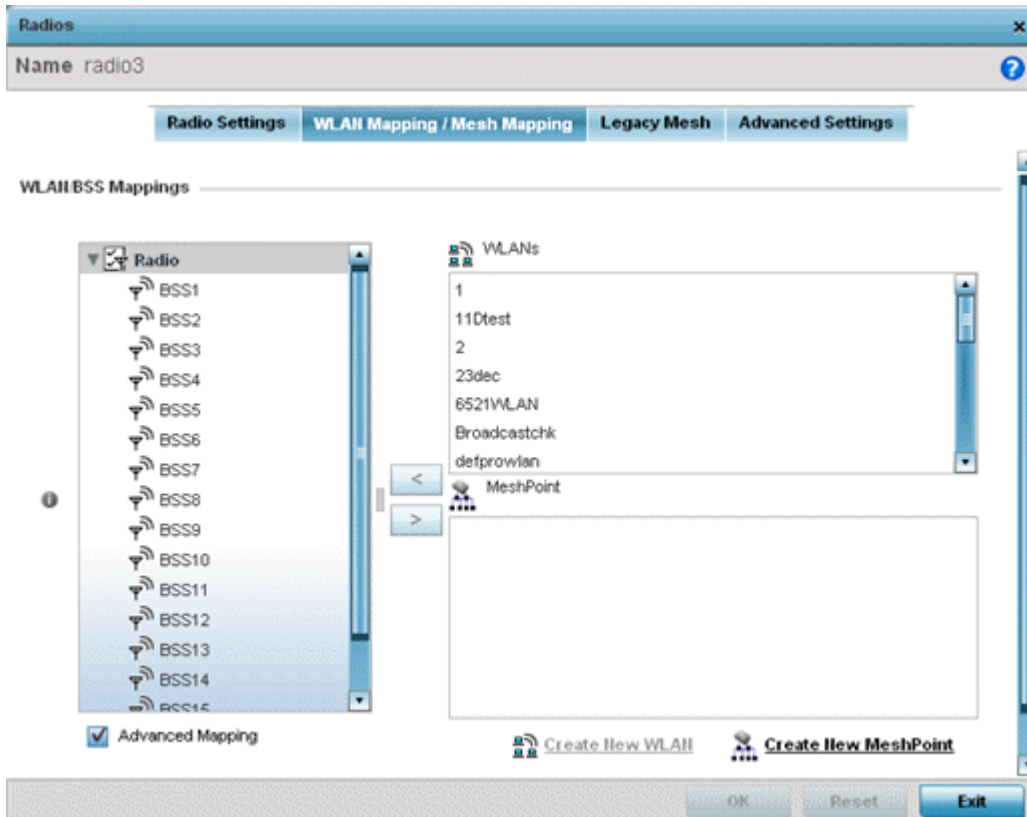
- 9 Select **OK** to save the changes made within the screen. Select **Reset** to revert to the last saved configuration.

### WLAN Mapping / Mesh Mapping

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.

To set a radio's WLAN mapping configuration:

- 1 Select **Configuration > Profiles > Interface**.
- 2 Expand the Interface menu to display its submenu options.
- 3 Select **Radios**.
- 4 If required, select a radio configuration and select the **Edit** button to modify its configuration.
- 5 Select the **WLAN Mapping** tab.



- 6 Refer to the **WLAN/BSS Mappings** field to set WLAN BSSID assignments for an existing access point deployment.
- 7 Select **Advanced Mapping** to enable WLAN mapping to a specific BSS ID.
- 8 Select **OK** to save the changes to the WLAN Mapping. Select **Reset** to revert to the last saved configuration.

### Mesh Legacy

Each radio profile can have a unique mesh mode and link configuration. This provides a customizable set of connections to other mesh supported radios within the same radio coverage area.

To set a radio's legacy mesh configuration:

- 1 Select **Configuration > Profiles > Interface**.
- 2 Expand the Interface menu to display its submenu options.
- 3 Select **Radios**.
- 4 If required, select a radio configuration and select the **Edit** button to modify its configuration.
- 5 Select the **Legacy Mesh** tab.

The screenshot shows the 'Radios' configuration window for 'radio2'. The 'Advanced Settings' tab is selected. Under 'Settings', 'Mesh' is set to 'Disabled', 'Mesh Links' is set to 6, and 'Mesh PSK' is set to ASCII. The 'Preferred Peer Devices' table contains one entry with MAC address '00-00-00-00-00-00' and Priority '1'. The window includes 'OK', 'Reset', and 'Exit' buttons at the bottom.

- 6 Refer to the **Advanced Settings** field to define basic mesh settings for the access point radio.

<b>Mesh</b>	Use the drop-down menu to set the mesh mode for this radio. Available options are <i>Disabled</i> , <i>Portal</i> or <i>Client</i> . Setting the mesh mode to <i>Disabled</i> deactivates all mesh activity on this radio. Setting the mesh mode to <i>Portal</i> 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 <i>client</i> enables the radio to operate as a mesh client and scan and connect to mesh portals or nodes connected to portals.
<b>Mesh Links</b>	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 <i>Portal</i> or <i>Client</i> .
<b>Mesh PSK</b>	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 <i>Show</i> to expose the characters used in the PSK.
<b>Note:</b> Only single hop mesh links are supported at this time.	
<b>Note:</b> The mesh encryption key is configurable from the <i>Command Line Interface</i> (CLI) using the command ' <b>mesh psk</b> '. Administrators must ensure 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.	

- 7 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.

- 8 Select the **+ Add Row** button to add preferred peer devices for the radio to connect to in mesh mode.
- 9 Select **OK** to save the changes. Select **Reset** to revert to the last saved configuration.

### Advanced Settings

A radio's profile configuration is customizable to define how transmit and receive data frames are processed. A radio's sniffer redirect settings can be refined to adjust how captured packets are directed. Additionally, channel scanning settings can be refined in respect to channel scanning requirements on either the 2.4 or 5 GHz radio bands.

To a radio's advanced settings:

- 1 Select **Configuration > Profiles > Interface**.
- 2 Expand the Interface menu to display its submenu options.
- 3 Select **Radios**.
- 4 If required, select a radio configuration and select the **Edit** button to modify its configuration.
- 5 Select the **Advanced Settings** tab.

- 6 Refer to the **Aggregate MAC Protocol Data Unit (A-MPDU)** field to define how MAC service frames are aggregated by the access point radio.

<b>A-MPDU Modes</b>	Use the drop-down menu to define the A-MPDU mode supported. Options include <i>Transmit Only</i> , <i>Receive Only</i> , <i>Transmit and Receive</i> and <i>None</i> . 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).
<b>Minimum Gap Between Frames</b>	Use the drop-down menu to define the minimum gap between A-MPDU frames (in microseconds). The default value is 4 microseconds.
<b>Received Frame Size Limit</b>	If a support mode is enabled allowing A-MPDU frames, define an advertised maximum limit for received A-MPDU aggregated frames. Options include <i>8191</i> , <i>16383</i> , <i>32767</i> or <i>65535</i> bytes. The default value is 65535 bytes.
<b>Transmit Frame Size Limit</b>	Use the spinner control to set limit on transmitted A-MPDU aggregated frames. The available range is between 0 - 65,535 bytes). The default value is 65535 bytes.

- 7 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.

- 8 Set the following **Aeroscout Properties**:

<b>Forward</b>	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.
<b>MAC to be Forwarded</b>	Specify the MAC address to be forwarded.

- 9 Set the following **Ekahau Properties**:

<b>Forward Host</b>	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.
<b>Forwarding Host</b>	Use the spinner control to set the Ekahau TZSP port used for processing information from locationing tags.
<b>MAC to be Forwarded</b>	Specify the MAC address to be forwarded.

- 10 Set the following **Non-Unicast Traffic** values for the profile's supported access point radio and its connected wireless clients:

<b>Broadcast/Multicast Transmit Rate</b>	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.
<b>Broadcast/Multicast Forwarding</b>	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.

- 11 Refer to the **Sniffer Redirect (Packet Capture)** field to define the radio's captured packet configuration.

<b>Host for Redirected Packets</b>	If packets are re-directed from a connected access point radio, define an IP address resource (additional host system) to capture the re-directed packets. This address is the numerical (non DNS) address of the host used to capture re-directed packets.
<b>Channel to Capture Packets</b>	Use the drop-down menu to specify the specific channel used to capture re-directed packets. The default value is channel 1.

- 12 Refer to the **Channel Scanning** field to define the radio's captured packet configuration.

<b>Enable Off Channel Scan</b>	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.
<b>Off Channel Scan list for 5GHz</b>	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.
<b>Off Channel Scan list for 2.4GHz</b>	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.
<b>Max Multicast</b>	Set the maximum number (from 0 - 100) of multicast/broadcast messages used to perform off channel scanning. The default setting is four.
<b>Scan Interval</b>	Set the interval (from 2 - 100 dtims) off channel scans occur. The default setting is 20dtims.
<b>Sniffer Redirect</b>	Specify the IP address of the host to which captured off channel scan packets are redirected.

- 13 Set the following **AP7161/AP7181** settings:

<b>Enable Antenna Downtilt</b>	Enable this settings (on AP7181 models only) to allow the access point to physically transmit in a downward orientation (ADEPT mode).
<b>Extended Range</b>	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.

- 14 Select **OK** to save the changes to the advanced settings screen. Select **Reset** to revert to the last saved configuration.

## WAN Backhaul 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. AP71XX model access points, RFS 4000 and RFS 6000 controllers NX 4500, NX 6500 all utilize 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.

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**.

- 4 Refer to the **WAN (3G) Backhaul** configuration to specify WAN card settings:

<b>WAN Interface Name</b>	Displays the WAN Interface name for the WAN 3G Backhaul card.
<b>Enable WAN (3G)</b>	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.

- 5 Set the following authentication parameters from within the **Basic Settings** field:

<b>Username</b>	Provide a username for authentication support by the cellular data carrier.
<b>Password</b>	Provide a password for authentication support by the cellular data carrier.
<b>Access Point Name (APN)</b>	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, the middle east and Asia.
<b>Authentication Type</b>	Use the pull-down menu to specify authentication type used by your cellular data provider. Supported authentication types are <i>None</i> , <i>PAP</i> , <i>CHAP</i> , <i>MSCHAP</i> , and <i>MSCHAP-v2</i> .

- 6 Define the following NAT parameters from within the **Network Address Translation (NAT)** field:



<b>NAT Direction</b>	Define the Network Address Translation (NAT) direction. Options include: <i>Inside</i> - 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. <i>Outside</i> - 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. <i>None</i> - No NAT activity takes place. This is the default setting.
----------------------	---

- 7 Set the following security parameters from within the **Security Settings** field:

<b>IP Inbound Firewall Rules</b>	Use the drop-down menu to select an inbound IP ACL to associate with traffic on the WAN backhaul. If an appropriate IP ACL does not exist, select the Add button to create a new one.
<b>VPN Crypto Map</b>	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:

<b>WWAN Default Route Priority</b>	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.

## PPPoE 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 controllers, service platforms and access points to establish 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.

**Note:** PPPoE is supported on AP 6522, AP 6532, AP 6562, AP71XX, and AP 8132 models, and is not available on AP 6521 and AP 6511 model access points.

When PPPoE client operation is enabled, a requesting client discovers an available server and establishes a PPPoE link for its traffic flow. 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, client 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**.

The screenshot displays the PPPoE configuration window with the following sections and fields:

- Basic Settings:**
  - Enable PPPoE: Radio buttons for Disabled (selected) and Enabled.
  - Service: Text input field.
  - DSL Modem Network (VLAN): Spinner control set to 1, range (1 to 4,094).
  - Client IP Address: Text input field with a blue checkbox to its left.
- Authentication:**
  - Username: Text input field.
  - Password: Text input field with a Show button to its right.
  - Authentication Type: Dropdown menu set to PAP.
- Connection:**
  - Maximum Transmission Unit (MTU): Spinner control set to 1492, range (500 to 1,492).
  - Client Idle Timeout: Text input field set to 10, unit dropdown set to Minutes, range (1 to 1,093).
  - Keep Alive: Blue checkbox.
- Network Address Translation (NAT):**
  - NAT Direction: Radio buttons for Inside, Outside, and None (selected).
- Security Settings:**
  - Inbound IP Firewall Rules: Dropdown menu set to <none>, with a gear icon to its right.
- Default Route Priority:**
  - PPPoE Default Route Priority: Spinner control set to 2000, range (1 to 8,000).

Buttons at the bottom: OK, Reset, Exit.

- 4 Use the **Basic Settings** field to enable PPPoE and define a PPPoE client

<b>Enable PPPoE</b>	Select <i>Enable</i> to support a high speed client mode point-to-point connection using the PPPoE protocol. The default setting is disabled.
<b>Service</b>	Enter the 128 character maximum PPPoE client service name provided by the service provider.
<b>DSL Modem Network (VLAN)</b>	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
<b>Client IP Address</b>	Provide the numerical (non hostname) IP address of the PPPoE client.

- 5 Define the following **Authentication** parameters for PPPoE client interoperation:

<b>Username</b>	Provide the 64 character maximum username used for authentication support by the PPPoE client.
<b>Password</b>	Provide the 64 character maximum password used for authentication by the PPPoE client.
<b>Authentication Type</b>	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 <i>None</i> , <i>PAP</i> , <i>CHAP</i> , <i>MSCHAP</i> , and <i>MSCHAP-v2</i> .

- 6 Define the following **Connection** settings for the PPPoE point-to-point connection with the PPPoE client:

<b>Maximum Transmission Unit (MTU)</b>	Set the PPPoE client <i>maximum transmission unit</i> (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.
<b>Client Idle Timeout</b>	Set a timeout in either <i>Seconds</i> (1 - 65,535), <i>Minutes</i> (1 - 1,093) or <i>Hours</i> . 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.
<b>Keep Alive</b>	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:

<b>Inbound IP Firewall Rules</b>	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 <i>Create</i> icon to define a new rule configuration or the <i>Edit</i> icon to modify an existing rule.
<b>VPN Crypto Map</b>	Use the drop-down menu to apply an existing crypt map configuration to this PPPoE interface.

- 9 Use the spinner control to set the **Default Route Priority** for the default route learnt using PPPoE.

Select a priority 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.

## Profile Interface Deployment Considerations

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 RFS 4000 and RFS 6000 model controllers and NX 4524 and NX 6524 model service platforms only. When enabled, the 802.3af PoE is supported on each ge ports.
- When changing from a default DHCP address to a fixed IP address, set a static route first. This is critical when a controller or service platform is accessed from a subnet not directly connected 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 controller or service platform 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.

## 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](#) on page 572
- [ARP](#) on page 574
- [L2TPV3 Configuration](#) on page 575
- [GRE](#) on page 179
- [IGMP Snooping](#) on page 587
- [Quality of Service \(QoS\) Configuration](#) on page 583
- [Spanning Tree Configuration](#) on page 555
- [Routing Configuration](#) on page 589
- [OSPF](#) on page 590
- [Forwarding Database](#) on page 601
- [Bridge VLAN](#) on page 602
- [Cisco Discovery Protocol Configuration](#) on page 608
- [Link Layer Discovery Protocol Configuration](#) on page 609
- [Miscellaneous Network Configuration](#) on page 610

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](#).

### Setting a Profile's DNS 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**.

- 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:

<b>Name Servers</b>	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 <i>Clear</i> link (next to each DNS server) to clear the DNS name server's IP address from the list.
---------------------	--

- 6 Select **OK** to save the changes made to the DNS configuration. Select **Reset** to revert to the last saved configuration.

## ARP

*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.

Switch VLAN Interface	IP Address	MAC Address	Device Type
1	. . .	00-00-00-00-00-00	Host

- 5 Set the following parameters to define the ARP configuration:

Switch VLAN Interface	Use the spinner control to select a virtual interface for an address requiring resolution with the controller, service platform or access point.
IP Address	Define the IP address used to fetch a MAC Address recognized on the wireless network.

MAC Address	Displays 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 settings select **+ Add Row** 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.

## L2TPV3 Configuration

L2TP V3 is an IETF standard used for transporting different types of layer 2 frames in an IP network (and 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 managed devices and 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 pseudowire 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*.

### General

To define an L2TPV3 configuration for a 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.

- 4 Set the following **General Settings** for a L2TPv3 profile configuration:

<b>Host Name</b>	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 ( <i>SCCRQ</i> , <i>SCCRP</i> and <i>SCCN</i> ) with the peer. Tunnel IDs and capabilities are exchanged during the tunnel establishment with the host.
<b>Router ID</b>	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 tunneled peer.
<b>UDP Listen Port</b>	Select this option to set the virtual port used for listening to incoming traffic. Select a port from 1,024 - 65,353.
<b>Device Type</b>	Select this option to <i>enable</i> or <i>disable</i> bridge packets between two tunnel end points. This setting is disabled by default.

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

### *L2TPv3 Tunnel*

To define an L2TPv3 configuration for a profile:

- 1 Select **Configuration > Profiles > Network**.
- 2 Expand the Network menu to display its submenu options.



- 3 Expand the **Network** menu and select **L2TPv3**.
- 4 Select the **L2TPv3 Tunnel** tab.

General <b>L2TPv3 Tunnel</b> Manual Session									
Name	Local IP Address	MTU	Use Tunnel Policy	Local HostName	Local Router ID	Establishment Criteria	Critical Resource	Peer IP Address	Hostname
tunnel1	Not Set	1,460	default		Not Set	Always		Not Set	Not Set
Type to search in tables								Row Count: 1	

- 5 Review the following L2TPv3 tunnel configuration data:

<b>Name</b>	Displays the name of each listed L2TPv3 tunnel assigned upon creation.
<b>Local IP Address</b>	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.
<b>MTU</b>	Displays the <i>maximum transmission unit</i> (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.
<b>Use Tunnel Policy</b>	Lists the L2TPv3 tunnel policy assigned to each listed tunnel.
<b>Local Hostname</b>	Lists the tunnel specific hostname used by each listed tunnel. This is the host name advertised in tunnel establishment messages.
<b>Local Router ID</b>	Specifies the router ID sent in the tunnel establishment messages.

- 6 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.

### Adding and Editing L2TPV3 Tunnels

To define an L2TPV3 configuration for a profile:

- 1 Select **Configuration > Profiles > Network**.
- 2 Expand the Network menu to display its submenu options.
- 3 Expand the **Network** menu and select **L2TPv3**.

- 4 Select the **L2TPv3 Tunnel** tab.
- 5 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.

- 6 If creating a new tunnel configuration, assign it a 31 character maximum **Name**.
- 7 Define the following **Settings** required for the L2TP tunnel configuration:

<b>Local IP Address</b>	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.
<b>MTU</b>	Set the <i>maximum transmission unit</i> (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.
<b>Use Tunnel Policy</b>	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.
<b>Local Hostname</b>	Provide the tunnel specific hostname used by this tunnel. This is the host name advertised in tunnel establishment messages.
<b>Local Router ID</b>	Specify the router ID sent in tunnel establishment messages with a potential peer device.

- 8 Refer to the **Peer** table to review the configurations of the peers available for tunnel connection.
- 9 Select **+ Add Row** to populate the table with a maximum of two peer configurations.

- 10 Define the following Peer parameters:

<b>Peer ID</b>	Define the primary peer ID used to set the <i>primary</i> and <i>secondary</i> 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.
<b>Peer IP Address</b>	Select this option to enter the numeric IP address used as the tunnel destination peer address for tunnel establishment.
<b>Host Name</b>	Assign the peer a hostname used as matching criteria in the tunnel establishment process.
<b>Router ID</b>	Specify the router ID sent in tunnel establishment messages with this specific peer.
<b>Encapsulation</b>	Select either <i>IP</i> or <i>UDP</i> as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes.
<b>UDP Port</b>	If UDP encapsulation is selected, use the spinner control to define the UDP encapsulation port.

- 11 Select **OK** to save the peer configuration.
- 12 Refer to the **Session** table to review the configurations of the peers available for tunnel connection.
- 13 Select **+ Add Row** to populate the table with configurable session parameters for this tunnel configuration.

- 14 Define the following **Session** parameters:

<b>Name</b>	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.
<b>Pseudowire ID</b>	Define a pseudowire ID for this session. A pseudowire is an emulation of a layer 2 point-to-point connection over a <i>packet-switching network</i> (PSN). A pseudowire was developed out of the necessity to encapsulate and tunnel layer 2 protocols across a layer 3 network.
<b>Traffic Source Type</b>	Lists the type of traffic tunneled in this session.
<b>Traffic Source Value</b>	Define a VLAN range to include in the tunnel session. Available VLAN ranges are from 1 - 4,094.
<b>Native VLAN</b>	Select this option to provide a VLAN ID that will not be tagged in tunnel establishment and packet transfer.

- 15 Select **OK** to save the changes within the L2TP Tunnel screen. Select **Reset** to revert the screen to its last saved configuration.

### Manual Session

To define an L2TPv3 configuration for a profile:

- 1 Select **Configuration > Profiles > Network**.
- 2 Expand the Network menu to display its submenu options.
- 3 Expand the **Network** menu and select **L2TPv3**.
- 4 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.

- 5 Refer to the following manual session configurations to determine whether one should be created or modified:

<b>IP Address</b>	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 tunnel session and responding to incoming requests.
<b>Local Session ID</b>	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.
<b>MTU</b>	Displays each sessions's <i>maximum transmission unit</i> (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.
<b>Name</b>	Lists the name assigned to each listed manual session.
<b>Remote Session ID</b>	Lists the remote session ID passed in the establishment of the tunnel session.

- 6 Select **Add** to create a new manual session, **Edit** to modify an existing session configuration or **Delete** to remove a selected manual session.

### Adding and Editing Manual Sessions

To define an L2TPV3 configuration for a profile:

- 1 Select **Configuration > Profiles > Network**.
- 2 Expand the Network menu to display its submenu options.
- 3 Expand the **Network** menu and select **L2TPv3**.
- 4 Select the **Manual Session** tab.
- 5 Select **Add** to create a new manual session, **Edit** to modify an existing session configuration or **Delete** to remove a selected manual session.

- 6 Set the following session parameters:

<b>Name</b>	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.
<b>IP Address</b>	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.
<b>IP</b>	Set the IP address of an L2TP tunnel peer. This is the peer allowed to establish the tunnel.
<b>Local Session ID</b>	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.
<b>MTU</b>	Define the session <i>maximum transmission unit</i> (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.
<b>Remote Session ID</b>	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.
<b>Encapsulation</b>	Select either <i>IP</i> or <i>UDP</i> as the peer encapsulation protocol. The default setting is IP. UDP uses a simple transmission model without implicit handshakes.
<b>UDP Port</b>	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.

<b>Source VLAN</b>	Define the VLAN range (1 - 4,094) to include in the tunnel. Tunnel session data includes VLAN tagged frames.
<b>Native VLAN</b>	Select this option to define the native VLAN that will not be tagged.

- 7 Select the **+ Add Row** button to set the following:

<b>Cookie Size</b>	Set the size of the cookie field within each L2TP data packet. Options include 0, 4 and 8. The default setting is 0.
<b>Value 1</b>	Set the cookie value's first word.
<b>Value 2</b>	Set the cookie value's second word.
<b>End Point</b>	Define whether the tunnel end point is <i>local</i> or <i>remote</i> .

- 8 Select **OK** to save the changes to the session configuration. Select **Reset** to revert to the last saved configuration.

## Quality of Service (QoS) Configuration

QoS values need administration 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 in high priority voice traffic networks.

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 mappings:

- 1 Select **Configuration > Profiles > Network**.
- 2 Expand the Network menu to display its submenu options.
- 3 Select **Quality of Service**.

Quality of Service (QoS)

DSCP Mapping

DSCP	802.1p Priority
0	0
1	0
2	0
3	0
* 4	0
5	0
6	0
7	0
8	1
9	1

OK Reset Exit

- 4 Set the following parameters for IP DSCP mappings for untagged frames:

<b>DSCP</b>	Lists the DSCP value as a 6-bit parameter in the header of every IP packet used for packet classification.
<b>802.1p Priority</b>	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 - <i>Best Effort</i> 1 - <i>Background</i> 2 - <i>Spare</i> 3 - <i>Excellent Effort</i> 4 - <i>Controlled Load</i> 5 - <i>Video</i> 6 - <i>Voice</i> 7 - <i>Network Control</i>

- 5 Use the spinner controls within the **802.1p Priority** field for each **DSCP** row to change the priority value.
- 6 Select the **OK** button located to save the changes. Select **Reset** to revert to the last saved configuration.

## GRE

GRE tunneling can be configured to bridge Ethernet packets between WLANs and a remote WLAN gateway over an IPv4 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 server using IPv4.

To review a profile's GRE settings:

- 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.

### *GRE Configuration*

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.

- 5 If creating a new GRE configuration, assign it a name to distinguish its configuration.
- 6 Define the following settings for the GRE configuration:

<b>DSCP Options</b>	Use the spinner control to set the tunnel DSCP / 802.1q priority value from encapsulated packets to the outer packet IPv4 header.
<b>Tunneled VLANs</b>	Define the VLAN connected clients use to route GRE tunneled traffic within their respective VLANs.
<b>Native VLAN</b>	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.
<b>Tag Native VLAN</b>	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.

- 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:

<b>Peer Index</b>	Assign a numeric index to each peer to help differentiate tunnel end points.
<b>Peer IP Address</b>	Define the IP address of the added GRE peer to serve as a network address identifier.

- 9 Define the following **Failover** parameters to apply to the GRE tunnel configuration:

<b>Enable Failover</b>	Select this option to periodically ping the primary gateway to assess its availability for failover support.
<b>Ping Interval</b>	Set the duration between two successive pings to the gateway. Define this value in seconds from 0 - 86,400.
<b>Number of Retries</b>	Set the number of retry ping opportunities before the session is terminated.

- 10 Select the **OK** button located to save the changes. Select **Reset** to revert to the last saved configuration.

## IGMP Snooping

The *Internet Group Management Protocol* (IGMP) is used for managing IP multicast group members. Controllers 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 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**.
- 2 Expand the Network menu to display its submenu options.
- 3 Select **IGMP Snooping**.

**General**

Enable IGMP Snooping

Forward Unknown Multicast Packets

**IGMP Querier**

Enable IGMP Querier

IGMP Version  (1 to 3)

IGMP Query Interval  Minutes (1 to 300)

IGMP Robustness Variable  (1 to 7)

Maximum Response Time  seconds (1 to 25)

Other Querier Time Expiry  Minutes (1 to 5)

OK Reset Exit

- 4 Set the following **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 unknown multicast forward feature is also disabled for individual VLANs. This setting is enabled by default.

- 5 Within the **Multicast Router** section, select those interfaces used as multicast router interfaces. Multiple interfaces can be selected and overridden. 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.
- 6 Optionally select **Snoop PIM-DVMRP Packets** to snoop packets across the selected interface(s). This option is enabled by default.
- 7 Set 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 packets 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. This parameter is used only when the querier functionality is enabled. Define an interval value in <i>Seconds</i> (1 - 18,000), <i>Minutes</i> (1 - 300) and <i>Hours</i> (1 - 5). The default setting is one minute.
IGMP Robustness Variable	Sets the IGMP robustness variable. The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. Define a robustness variable from 1 - 7. The default robustness value 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. Only multicast packets are forwarded 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 <i>Seconds</i> (60 - 300) or <i>Minutes</i> (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute.

- 8 Select the **OK** button to save the changes to the IGMP Snooping tab. Select **Reset** to revert to the last saved configuration.

## Routing Configuration

Routing is the process of selecting IP paths to strategically route and segregate 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.

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 screenshot shows a configuration window for IP Routing. It is divided into three main sections: IP Routing, Policy Based Routing, and Static Routes. The IP Routing section has a checked checkbox. The Policy Based Routing section has a dropdown menu. The Static Routes section contains a table with the following columns: Network Address, Gateway, Default Gateway, and a delete icon. The first row in the table has a red 'X' in the Default Gateway column. There are 'Add Row', 'OK', 'Reset', and 'Exit' buttons at the bottom of the window.

- 4 Select **IP Routing** to enable static routes using IP addresses. This option is enabled by default.
- 5 Use the drop-down menu to select a **Policy Based Routing** policy. If a suitable policy is not available, click the add button to create a new policy.
- 6 Select **Add Row +** as needed to include single rows with in the static IPv4 route table.
- 7 Add IP addresses and network masks in the **Network** column.
- 8 Provide the **Gateway** used to route traffic.
- 9 Refer to the **Default Route Priority** field and set the following parameters:

<b>Static Default Route Priority</b>	Use the spinner control to set the priority value (1 - 8,000) for the default static route. This is the weight (priority) assigned to this static route versus others that have been defined to avoid potential congestion. The default setting is 100.
<b>DHCP Client Default Route Priority</b>	Use the spinner control to set the priority value (1 - 8,000) for the default client route learnt from the DHCP client. The default setting is 1000.
<b>Enable Routing Failure</b>	When selected, all default gateways are monitored for activity. The system will failover to a live gateway if the current gateway is unavailable. This feature is enabled by default.

- 10 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.

## OSPF

*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 be 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.

### OSPF Settings

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**.

- 4 Enable/disable OSPF and provide the following dynamic routing settings:

<b>Enable OSPF</b>	Select this option to enable OSPF. OSPF is disabled by default.
<b>Router ID</b>	Select this option to define a router ID (numeric IP address). 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.
<b>Auto-Cost</b>	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.
<b>Passive Mode on All Interfaces</b>	When selected, all layer 3 interfaces are set as an OSPF passive interface. This setting is disabled by default.
<b>Passive Removed</b>	If <i>enabling</i> Passive Mode on All Interfaces, use the spinner control to select VLANs (by numeric ID) as OSPF <i>non</i> passive interfaces. Multiple VLANs can be added to the list.
<b>Passive Mode</b>	If <i>disabling</i> 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.
<b>VRRP State Check</b>	Select this option to use OSPF only if the VRRP interface is not in a backup state. The <i>Virtual Router Redundancy Protocol</i> (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:



<b>Number of Routes</b>	Use the spinner control to set the maximum number of OSPN routes permitted. The available range is from 1 - 4,294,967,295.
<b>Retry Count</b>	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.
<b>Retry Time Out</b>	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.
<b>Reset Time</b>	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**:

<b>Originate</b>	Select this option to make the default route a distributed route. This setting is disabled by default.
<b>Always</b>	Enabling this setting continuously maintains a default route, even when no routes appear in the routing table. This setting is disabled by default.
<b>Metric Type</b>	Select this option to define the exterior metric type (1 or 2) used with the default route.
<b>Route Metric</b>	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*.

- 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.

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.

- 10 Set an **OSPF Default Route Priority** (1 - 8,000) as the priority of the default route defined from OSPF.
- 11 Select **OK** to save the changes made within the screen. Select **Reset** to revert to the last saved configuration.

### Area Settings

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**.
- 4 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.

Area ID	Authentication Type	Type
0.0.0.0	message-digest	totally-stub
0.0.0.30	None	non-stub

Type to search in tables Row Count: 2

Add Edit Delete Exit

- 5 Review existing **Area Setting** configurations using:

<b>Area ID</b>	Displays either the <i>IP address</i> or <i>integer</i> representing the OSPF area.
<b>Authentication Type</b>	Lists the authentication (user validation) types used to validate and authenticate the credentials of the dynamic route connections.
<b>Type</b>	Lists the OSPF area type in each listed configuration.

- 6 Select **Add** to create a new OSPF configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.

### Adding and Editing Area Settings

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**.
- 4 Select the **Area Settings** tab.
- 5 Select **Add** to create a new OSPF configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.

- 6 Set the **OSPF Area** configuration.

<b>Area ID</b>	Use the drop-down menu and specify either an <i>IP address</i> or <i>Integer</i> for the OSPF area.
<b>Authentication Type</b>	Select either <i>None</i> , <i>simple-password</i> or <i>message-digest</i> as the credential validation scheme used with the OSPF dynamic route. The default setting is <i>None</i> (no data protection).
<b>Type</b>	Set the OSPF area type as either <i>stub</i> , <i>totally-stub</i> , <i>nssa</i> , <i>totally-nssa</i> or <i>non-stub</i> .
<b>Default Cost</b>	Select this option to set the default summary cost advertised if creating a stub. Set a value from 1 - 16, 777,215.
<b>Translate Type</b>	Define how messages are translated. Options include <i>translate-candidate</i> , <i>translate-always</i> and <i>translate-never</i> . The default setting is <i>translate-candidate</i> .
<b>Range</b>	Specify a range of addresses for routes matching address/mask for OSPF summarization.

- 7 Select the **OK** button to save the changes to the area configuration. Select **Reset** to revert to the last saved configuration.

### Virtual Interface Settings

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**.
- 4 Select the **Interface Settings** tab.

OSPF Settings		Area Settings		Interface Settings	
Name	Type	Description	Admin Status	VLAN	IP Address
vlan3	VLAN	lanelot	✖ Disabled	3	dhcp

Type to search in tables Row Count: 1

- 5 Review existing **Interface Settings** using the following:

<b>Name</b>	Displays the name defined for the interface configuration.
<b>Type</b>	Displays the type of interface.
<b>Description</b>	Lists each interface's 32 character maximum description.
<b>Admin Status</b>	Displays whether Admin Status privileges have been <i>enabled</i> or <i>disabled</i> for the OSPF route's virtual interface connection.
<b>VLAN</b>	Lists the VLAN IDs set for each listed OSPF route virtual interface.
<b>IP Address</b>	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 set.

- 6 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.

## Basic Configuration

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**.
- 4 Select the **Interface Settings** tab.
- 5 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. The **Basic Settings** tab displays by default.

**Virtual Interfaces** x

VLAN ID vlan3 ?

**Basic Configuration** **Security**

**Properties**

Description ⓘ lanelot

Admin Status ⓘ  Disabled  Enabled

**IP Addresses**

Enable Zero Configuration  None  Primary  Secondary

Primary IP Address ⓘ . . . /

Use DHCP to Obtain IP

Use DHCP to obtain Gateway/DNS Servers ⓘ  (Allowed on 1 virtual interface)

Secondary Addresses . . . /

**DHCP Relay**

Respond to DHCP Relay Packets ⓘ

DHCP Relays

IP Address	
0 . . . 0 . 0	Clear
0 . . . 0 . 0	Clear
0 . . . 0 . 0	Clear
0 . . . 0 . 0	Clear

**Network Address Translation (NAT)**

NAT Direction ⓘ  Inside  Outside  None

OK Reset **Exit**

- 6 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 privileges as needed. They're enabled by default.
- 7 Use the **IP Addresses** Area to set how route addresses are created for the virtual configuration.

Zero Configuration can be enabled and set as the *Primary* or *Secondary* means of providing IP addresses for the OSPF virtual route. 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.

- 8 Select **Use DHCP to Obtain IP** to use the access point's DHCP server resource as the means of providing requested IP addresses to the OSPF route's virtual interface.
- 9 Select **Use DHCP to Obtain Gateway/DNS Servers** to learn default gateway, name servers and the domain name on just this interface. Once selected, specify an IP address and mask in dot decimal format.
- 10 Refer to the **DHCP Relay** field to set or override the DHCP relay server configuration used with the virtual interface:

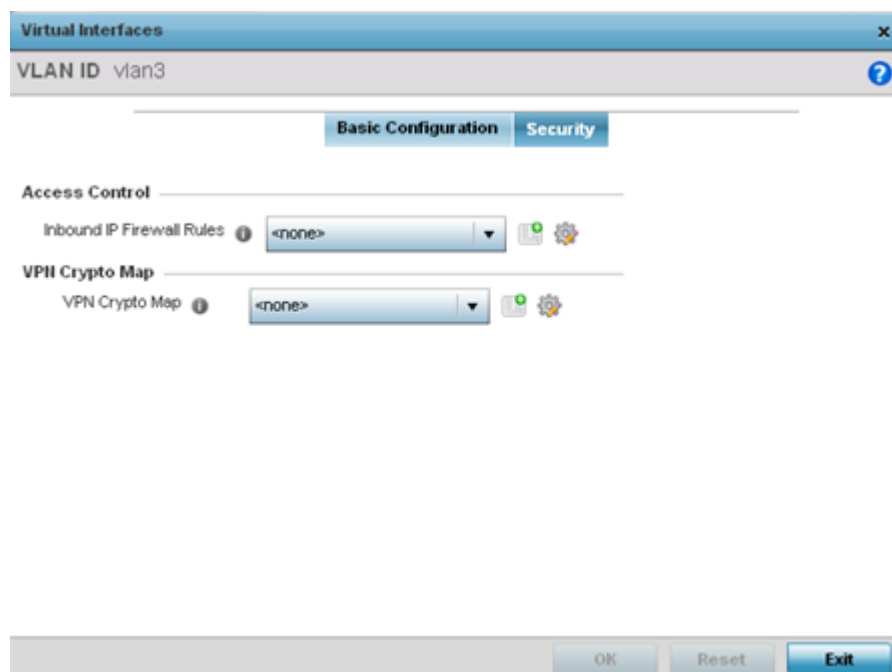
<b>Respond to DHCP Relay Packets</b>	Select the Respond to DHCP Relay Packets option to allow the onboard DHCP server to respond to relayed DHCP packets on this interface. This setting is disabled by default.
<b>DHCP Relay</b>	Provide IP addresses for DHCP server relay resources. The interface VLAN and gateway should have their IP addresses set. The interface VLAN and gateway interface should not have DHCP client or DHCP Server enabled. DHCP packets cannot be relayed to an onboard DHCP Server. The interface VLAN and gateway interface cannot be the same. 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 and the default route was set from DHCP.

- 11 Define the **NAT Direction** as either Inside, Outside or None. *Network Address Translation* (NAT), is an Internet standard that enables a (LAN) to use IP addresses for internal traffic (inside) and a second set of addresses for external (outside) traffic.
- 12 Select **OK** to save the changes to the basic configuration. Select **Reset** to revert to the last saved configuration.

## Security

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**.
- 4 Select the **Interface Settings** tab.
- 5 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.
- 6 Select the **Security** tab.



- 7 Use the **Inbound IP Firewall Rules** drop-down menu to select the IP access and deny rule set to apply to the OSPF dynamic route.

Either select an existing IP firewall policy or use the default set of IP firewall rules. The firewall inspects OSPF route traffic flows and detects potential attacks on the dynamic route not visible to traditional wired firewall appliances. Select the **Create** icon to define a new set of IP firewall rules that can be applied to the OSPF route configuration. Selecting **Edit** allows for the modification of an existing IP firewall rules configuration.

- 8 Use the **VPN Crypto Map** drop-down menu to select or override the Crypto Map configuration applied to this virtual interface.

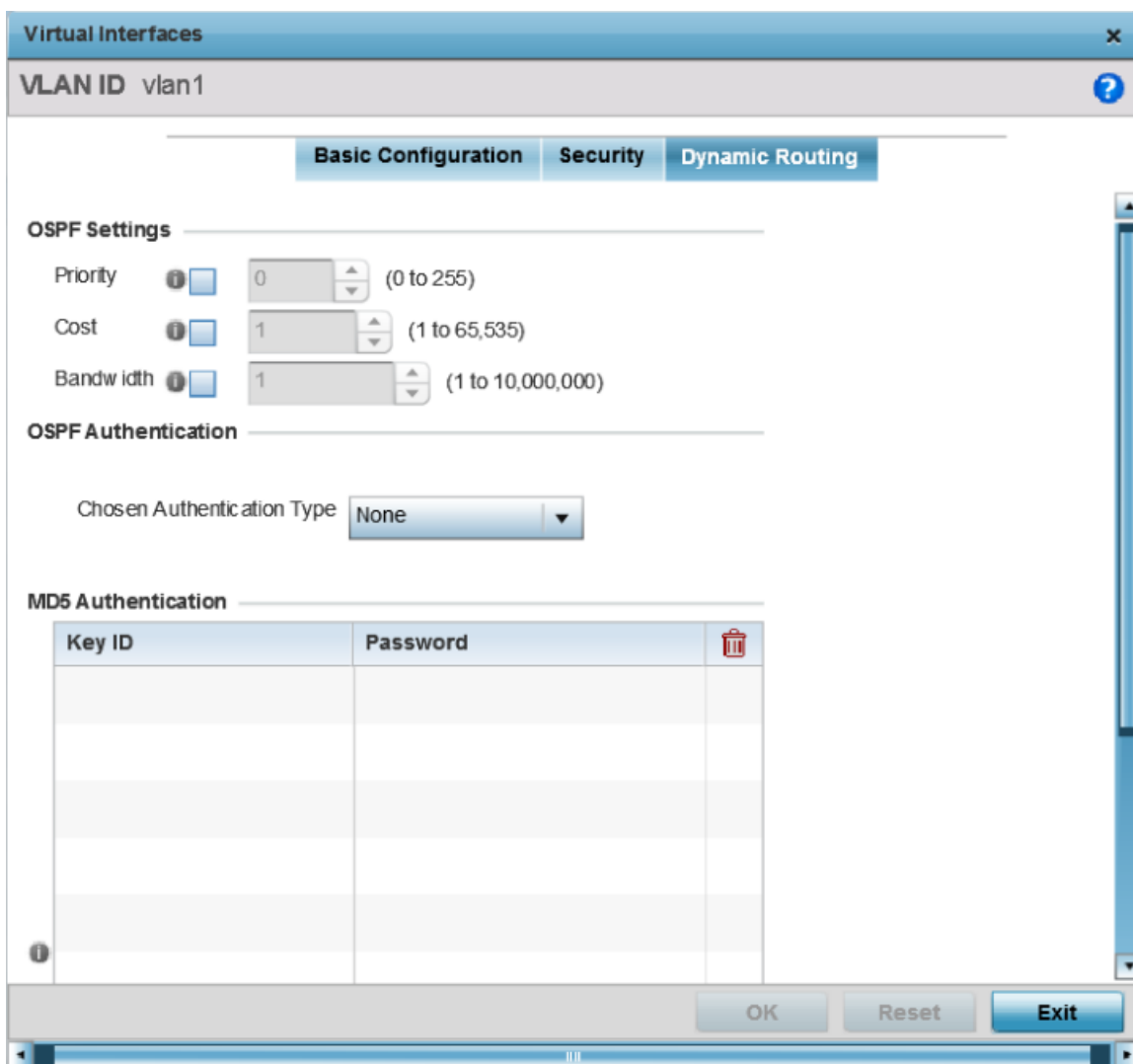
Crypto Map entries are sets of configuration parameters for encrypting packets passing through the VPN Tunnel. If a Crypto Map configuration does not exist suiting the needs of this virtual interface, select the **Create** icon to define a new Crypto Map configuration or the **Edit** icon to modify an existing configuration.

- 9 Select **OK** to save the changes to the OSPF route security configuration. Select **Reset** to revert to the last saved configuration.

### Dynamic Routing

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**.
- 4 Select the **Interface Settings** tab.
- 5 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.
- 6 Select the **Dynamic Routing** tab.



**Figure 223: Profiles OSPF Virtual Interface Dynamic Routing Screen**

- 7 Set the following OSPF Settings:

<b>Priority</b>	Select this option to set the OSPF priority used in dynamic route election. Use the spinner control to set the value from 0 - 255.
<b>Cost</b>	Select this option to set the cost of the OSPF interface. Use the spinner control to set the value from 1 - 65,353.
<b>Bandwidth</b>	Set the OSPF interface bandwidth (in Kbps) from 1 - 10,000,000.

- 8 Set the following OSPF Authentication settings for the dynamic route:

<b>Chosen Authentication Type</b>	Select the authentication type used to validate credentials within the OSPF dynamic route. Options include <i>simple-password</i> , <i>message-digest</i> , <i>null</i> and <i>None</i> .
<b>Authentication Key</b>	Enter and confirm the authentication key required by connecting nodes using the OSPF dynamic route.

- 9 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).

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

## Forwarding Database

A *Forwarding Database* is used to forward or filter packets on behalf of a controller, service platform or access point. The packet's destination MAC address is read and the controller, service platform or access point 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**.

**Aging Time**

Bridge Aging Time  (0,10-1000000 seconds)

L3e Lite Entry Aging Time  (10 to 1,000,000 seconds)

**Static Forwarding Table**

MAC Address	VLAN Id	Interface Name
00 - 00 - 00 - 00 - 00 - 00	1	

- 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.

## Bridge VLAN

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**.



The **General** tab displays by default. For more information, see:

- [General](#)
- [IGMP Snooping](#)

## General

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**.
- 4 Select **Add** to define a new Bridge VLAN configuration, **Edit** to modify an existing Bridge VLAN configuration or **Delete** to remove a VLAN configuration.

**Bridge VLAN**

**VLAN 1**

**General** | IGMP Snooping | MLD Snooping

Description

Per VLAN Firewall

**URL Filter**

URL Filter

**Application Policy**

Application Policy

**Extended VLAN Tunnel**

Bridging Mode

IP Outbound Tunnel ACL

IPv6 Outbound Tunnel ACL

MAC Outbound Tunnel ACL

Tunnel Over Level 2

**Extended VLAN Tunnel Authentication**

Mac Authentication

Captive Portal Enforcement

**VLAN Tunnel Optimizations**

Level 2 Tunnel Broadcast Optimization

Level 2 Forward Additional Packet Types

**Tunnel Rate Limit**

Mint Link Level	Rate	Max Burst Size	Background	Best-Effort	Video

OK Reset Exit

The **General** tab displays by default.

- 5 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.
- 6 Set the following **General** bridge VLAN parameters:

<b>Description</b>	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.
<b>Per VLAN Firewall</b>	Enable this setting to provide firewall allow and deny conditions over the bridge VLAN. This setting is enabled by default.

- 7 Set or override the following URL Filter parameters. Web filters are used to control the access to resources on the Internet:

<b>URL Filter</b>	Use the drop-down menu to select a URL filter to use with this Bridge VLAN.
-------------------	---

- 8 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.
- 9 Set the following **Extended VLAN Tunnel** parameters:

<b>Bridging Mode</b>	Specify one of the following bridging modes for the VLAN. <i>Automatic</i> : Select automatic to let the controller, service platform or access point determine the best bridging mode for the VLAN. <i>Local</i> : Select Local to use local bridging mode for bridging traffic on the VLAN. <i>Tunnel</i> : Select Tunnel to use a shared tunnel for bridging traffic on the VLAN. <i>isolated-tunnel</i> : Select isolated-tunnel to use a dedicated tunnel for bridging VLAN traffic.
<b>IP Outbound Tunnel ACL</b>	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 <i>Create</i> button to make a new one.
<b>MAC Outbound Tunnel ACL</b>	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 <i>Create</i> button to make a new one.
<b>Tunnel Over Level 2</b>	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.

- 10 Set the following **Extended VLAN Tunnel Authentication** settings:

<b>MAC Authentication</b>	Select to enable source MAC authentication for extended VLAN and tunneled traffic (MiNT and L2TPv3) on this bridge VLAN. When enabled, it provides fast path authentications of clients, whose captive portal session has expired. This option is disabled by default.
<b>Captive-Portal Authentication</b>	Use the drop-down menu to specify authentication mode used for extended VLAN and tunneled traffic, on this Bridge VLAN. <i>None</i> - No Authentication mode used. This is the default setting. <i>Authentication Failure</i> - Configures MAC Authentication as the primary and Captive-Portal Authentication as the fall-back authentication mode. <i>Always</i> - Configures Captive-Portal Authentication as the only mode of Authentication
<b>Edge VLAN Mode</b>	Select this option to enable edge VLAN mode. When selected, the edge controller'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.

- 11 Set the following **Layer 2 Firewall** parameters:

<b>Trust ARP Response</b>	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.
<b>Trust DHCP Responses</b>	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.
<b>Edge VLAN Mode</b>	Select this option to enable edge VLAN mode. When selected, the edge controller'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.

- 12 Select the **OK** button to save the changes to the General tab. Select **Reset** to revert to the last saved configuration.

### Bridge VLAN IGMP Snooping

The *Internet Group Management Protocol* (IGMP) is used for managing IP multicast group members. Controllers 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 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 bridge VLAN IGMP settings:

- 1 Select **Configuration > Profiles > Network**.
- 2 Expand the Network menu to display its submenu options.
- 3 Select **Bridge VLAN**.
- 4 Select **Add** to define a new bridge VLAN configuration or **Edit** to modify an existing bridge VLAN configuration.
- 5 Select the **IGMP Snooping** tab.
- 6 Define the following **General** parameters for the bridge VLAN configuration:

<b>Enable IGMP Snooping</b>	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.
<b>Forward Unknown Unicast Packets</b>	Select the check box to enable to forward multicast packets from unregistered multicast groups. If disabled (the default setting), the unknown multicast forward feature is also disabled for individual VLANs.
<b>Enable Fast Leave Processing</b>	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.
<b>Last Member Query Count</b>	Specify the number of group specific queries sent before removing an IGMP snooping entry.

- 7 Within the **Multicast Router** section, select those interfaces used as multicast router interfaces. Multiple interfaces can be selected and overridden. 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.

- 8 Set the following **IGMP Querier** parameters for the profile's bridge VLAN configuration:

<b>Enable IGMP Snooping</b>	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.
<b>Source IP Address</b>	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 <i>Seconds</i> (60 - 300) or <i>Minutes</i> (1 - 5) used as a timeout interval for other querier resources. The default setting is 1 minute.

- 9 Select the **OK** button to save the changes to the bridge VLAN IGMP Snooping tab. Select **Reset** to revert to the last saved configuration.

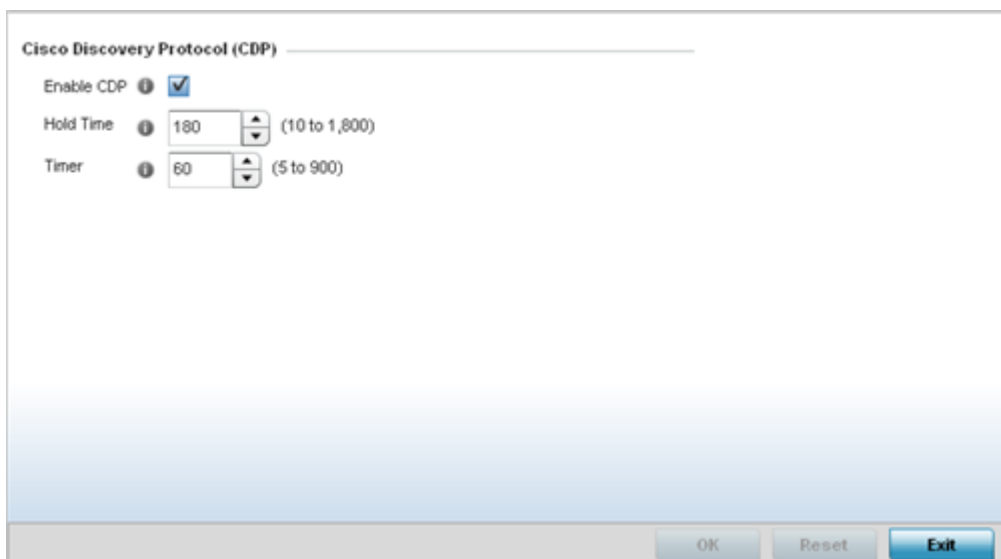
## Cisco Discovery Protocol Configuration

The *Cisco Discovery Protocol* (CDP) is a proprietary Data Link Layer network protocol implemented in Cisco networking equipment and used to share network information amongst different vendor wireless 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**.





- 4 Check the **Enable CDP** box to enable 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.

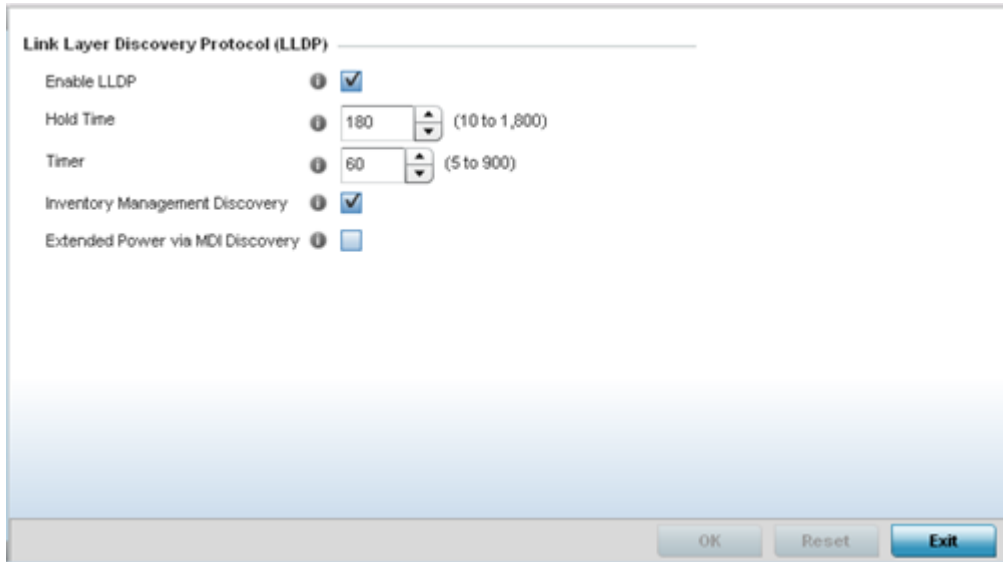
## Link Layer Discovery Protocol Configuration

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 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**.



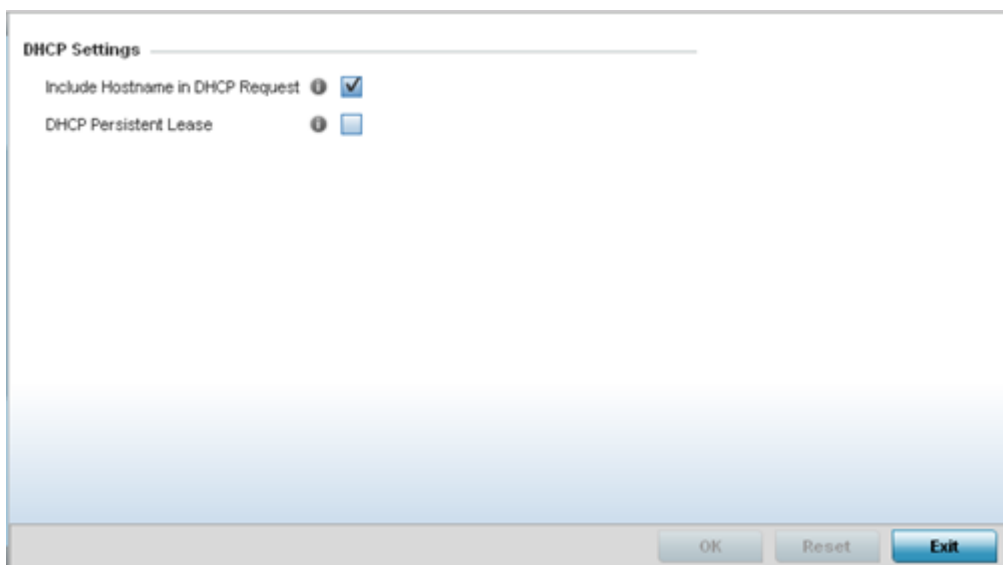
- 4 Check the **Enable LLDP** box to enable Link Layer Discovery Protocol on the device.
- 5 Refer to the **Hold Time** field and use the spinner control to define a hold time from 10 - 1800 seconds for transmitted LLDP packets. The default value is 180 seconds.
- 6 Refer to the **Timer** field and use 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 Enable **Extended Power via MDI Discovery** to provide detailed power information from end points and other connected devices.
- 9 Select the **OK** button to save the changes. Select **Reset** to revert to the last saved configuration.

## Miscellaneous Network Configuration

A profile can be configured to include a hostname within a DHCP lease for a requesting device and its profile. This helps an administrator track a profile's leased DHCP IP addresses by assigned (and recognizable) hostnames for easier administration.

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**.



- 4 Refer to the **DHCP Settings** field to configure miscellaneous DHCP Settings.

<b>Include Hostname in DHCP Request</b>	Select <i>Include Hostname in DHCP Request</i> to include a hostname in a DHCP lease for a requesting device. This feature is disabled by default.
<b>DHCP Persistent Lease</b>	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.

## Profile Alias 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 a 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 works 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:

- [Profile Basic Alias](#)
- [Profile Network Group Alias](#)
- [Profile Network Service Alias](#)

### *Profile 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 profile's network basic alias configuration:

- 1 Select **Configuration > Profiles > Network**.
- 2 Expand **Network** to display its sub menu options.
- 3 Select **Alias**.

The **Basic Alias** tab displays by default.

The screenshot shows a configuration window with four main sections, each with a table and an 'Add Row' button:

- VLAN Alias:** Table with columns 'Name' and 'VLAN'. One row is visible with Name '\$lancelot' and VLAN '1'.
- Host Alias:** Table with columns 'Name' and 'Host'. One row is visible with Name '\$mudskipper' and Host '157.235.233.232'.
- Address Range Alias:** Table with columns 'Name', 'Start IP', and 'End IP'. One row is visible with Name '\$percy', Start IP '157.235.232.3', and End IP '157.235.232.99'.
- Network Alias:** Table with columns 'Name' and 'Network'. One row is visible with Name '\$marion' and Network '157.235.232.32 / 24'.

At the bottom of the window are buttons for 'OK', 'Reset', and 'Exit'.

- 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.

<b>Name</b>	If adding a new <i>String Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Value</b>	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.

<b>Name</b>	If adding a new <i>Host Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Host</b>	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.

<b>Name</b>	If adding a new <i>Network Alias</i> , provide it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
<b>Network</b>	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.

### *Profile 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 profile's network alias configuration:

- 1 Select **Configuration** > **Profiles** > **Network**.
  - 2 Expand **Network** to display its sub menu options.
  - 3 Select **Alias**.
  - 4 Select the **Network Group Alias** tab. The screen displays the attributes of existing network group alias configurations.
- 1 Refer to the following fields for more information:

<b>Name</b>	Displays the name of the network group alias configuration.
<b>Host</b>	Displays all host aliases configured in this network group alias. Displays a blank column if no host alias is configured in this network group alias.
<b>Network</b>	Displays all network aliases configured in this network group alias. Displays a blank column if no network alias is configured in this network group alias.

- 2 Select **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available. Select **Add** to create a new network group alias.

### Adding or Editing a Profile's 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.

To add or edit a network group alias configuration:

- 1 From the **Network Group Alias** screen, select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies.
- 2 Select the added row to expand it into configurable parameters for defining the network group alias rule.

The screenshot shows the configuration window for a network group alias named 'networkalias1'. The window is divided into several sections:

- Host:** A text input field with a dropdown arrow, currently showing '192.168.0.24'. There is an information icon (i) to the left and a delete icon (trash) to the right.
- Network:** A text input field with a dropdown arrow, currently showing '255.255.255.255/24'. There is an information icon (i) to the left and a delete icon (trash) to the right.
- Range:** A table with two columns: 'Start IP' and 'End IP'. The first row contains '192, 168, 0, 25' and '192, 168, 0, 48' respectively. There are information icons (i) and delete icons (trash) for each cell. A star icon is visible in the first row. Below the table is an 'Add Row' button.

At the bottom of the window, there are three buttons: 'OK', 'Reset', and 'Exit'.

- 3 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 (\$).
- 4 Define the following network group alias parameters:

<b>Host</b>	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.
<b>Network</b>	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.

- 5 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 alias range entry to edit it.
- 6 Select **OK** when completed to update the network alias rules. Select **Reset** to revert the screen back to its last saved configuration.

### Profile 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 set a device's service alias configuration:

- 1 Select **Configuration > Profiles > Network**.
  - 2 Expand **Network** to display its sub menu options.
  - 3 Select **Alias**.
  - 4 Select the **Network Service Alias** tab. The screen displays the attributes of existing network service alias configurations.
- 1 Select **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies from the list of those available. Select **Add** to create a new **Network Service Alias**.

### Adding or Editing a Profile's 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.

To add or edit a network service alias configuration:

- 1 From the **Network Service Alias** screen, select **Add** to create a new policy, **Edit** to modify the attributes of an existing policy or **Delete** to remove obsolete policies.
- 2 Select the added row to expand it into configurable parameters for defining the network service alias rule.



- 3 If adding a new **Network Service Alias Rule**, provide it a name up to 32 characters. Ensure a \$ precedes the name.
- 4 Select **+ Add Row** and provide the following configuration parameters:

<b>Protocol</b>	Specify the protocol for which the alias has to be created. Use the drop down to select the protocol from <i>eigrp</i> , <i>gre</i> , <i>icmp</i> , <i>igmp</i> , <i>ip</i> , <i>vrrp</i> , <i>igp</i> , <i>ospf</i> , <i>tcp</i> and <i>udp</i> . Select <i>other</i> if the protocol is not listed. When a protocol is selected, its protocol number is automatically selected.
<b>Source Port (Low and High)</b>	This field is only relevant if the protocol is either <i>tcp</i> or <i>udp</i> . Specify the source ports for this protocol entry. A range of ports can be specified. Select the <i>Enter Ranges</i> button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.
<b>Destination Port (Low and High)</b>	This field is only relevant if the protocol is either <i>tcp</i> or <i>udp</i> . Specify the destination ports for this protocol entry. A range of ports can be specified. Select the <i>Enter Ranges</i> button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

- 5 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.
- 6 Select **OK** when completed to update the service alias rules. Select **Reset** to revert the screen back to its last saved configuration.

## Profile Network Configuration and Deployment Considerations

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, an administrator 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  $N \times N$  routes. Thus, for a network with nine routers, you'll need a minimum of 81 routes ( $9 \times 9 = 81$ ).

## Profile Security Configuration

A profile can have its own firewall policy, wireless client role policy, WEP shared key authentication, NAT policy and VPN policy (controller only) applied. If an existing firewall, client role or NAT policy is unavailable, an administrator can 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 controller, service platform or access point model supported by the profile.

For more information, refer to the following:

- [Defining Security Settings](#)
- [Setting the Certificate Revocation List \(CRL\) Configuration](#)
- [Setting the Profile's VPN Configuration](#)
- [Auto IPSec Tunnel](#)
- [Setting the Profile's NAT Configuration](#)
- [Bridge NAT Configuration](#)

## Defining Security Settings

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 controller, service platform or access point device model and its unique data protection requirements.

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**.

- 6 Refer to the **General** field to assign or create the following security policy's to the profile:

<b>Firewall Policy</b>	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 <i>denying</i> and <i>permitting</i> data traffic within the network. If an existing Firewall policy does not meet your requirements, select the <i>Create</i> 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 <i>Edit</i> icon.
<b>Wireless Client Role Policy</b>	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 <i>Create</i> 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 <i>Edit</i> icon.
<b>WEP Shared Key Authentication</b>	Select this option to require devices to use a WEP key to access the network using this profile. Controllers, service platforms and access points, other proprietary routers, and clients 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.
<b>Client Identity Group</b>	Client Identity is a set of unique fingerprints used to identify a class of devices. This information is then used to configure the permissions and access rules for the class of devices in the network. Client Identity Group is a collection of client identities that identifies devices and apply specific permissions and restrictions on these devices. From the drop-down select the client identity group to use with this device profile. For more information, see <a href="#">Device Fingerprinting</a> .
	<b>Note:</b> An Advanced WIPS Policy is only supported on controllers and service platforms and requires a dedicated WIPS sensor, but does not require a sensor license. Standard WIPS is available on all RF Domain managers and supports on channel, off channel and dedicated sensor scanning modes.

- 7 Select an **Advanced WIPS Policy** from the drop-down menu. Define an advanced WIPS configuration to optionally remove (terminate) unwanted device connections, and *sanction* (allow) or *unsanction* (disallow) specific events within the network.

If an existing Advanced WIPS policy does not meet the profile's data protection requirements, select the **Create** icon to create a new configuration that can be applied to the profile. An existing policy can also be selected and edited as needed using the **Edit** icon.

- 8 Select **OK** to save the changes made within the Settings screen. Select **Reset** to revert to the last saved configuration.

## Setting the Certificate Revocation List (CRL) 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**.

Trustpoint Name	URL	Hours
<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

+ Add Row

OK Reset Exit

- 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.
- 7 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.
- 8 Select **OK** to save the changes made within the Certificate Revocation screen. Select **Reset** to revert to the last saved configuration.

## Setting the Profile's VPN Configuration

IPSec VPN provides a secure tunnel between two networked peers. Administrators can define which packets are sent within the tunnel, and how they're protected. When a tunneled 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 tunneled 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.

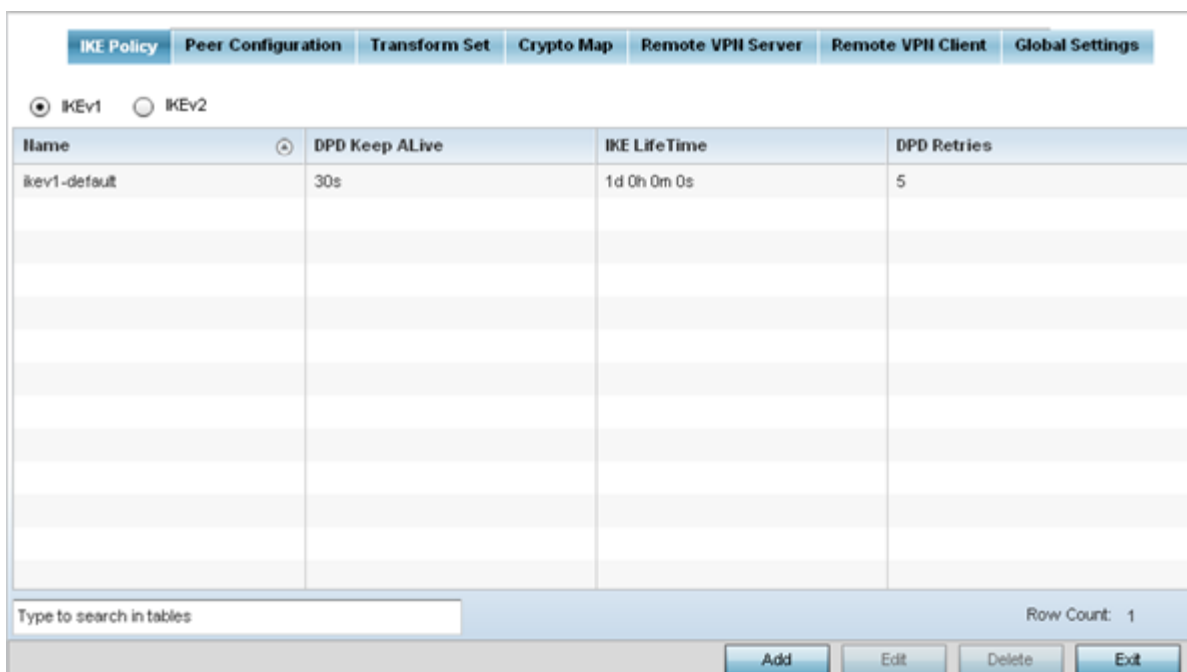
*Internet Key Exchange* (IKE) protocol is a key management protocol standard used in conjunction with IPSec. IKE enhances IPSec by providing additional features, flexibility, and configuration simplicity for the IPSec standard. IKE automatically negotiates IPSec SAs, and enables secure communications without time consuming manual pre-configuration.

### *IKE Policy*

*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 policy 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**.
- 6 The **IKE Policy** 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.



- 7 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.

- 8 Refer to the following to determine whether an IKE Policy requires creation, modification or removal:

<b>Name</b>	Displays the 32 character maximum name assigned to the IKE policy.
<b>DPD Keep Alive</b>	Lists each policy's IKE keep alive message interval defined for IKE VPN tunnel dead peer detection.
<b>IKE LifeTime</b>	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.
<b>DPD Retries</b>	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.

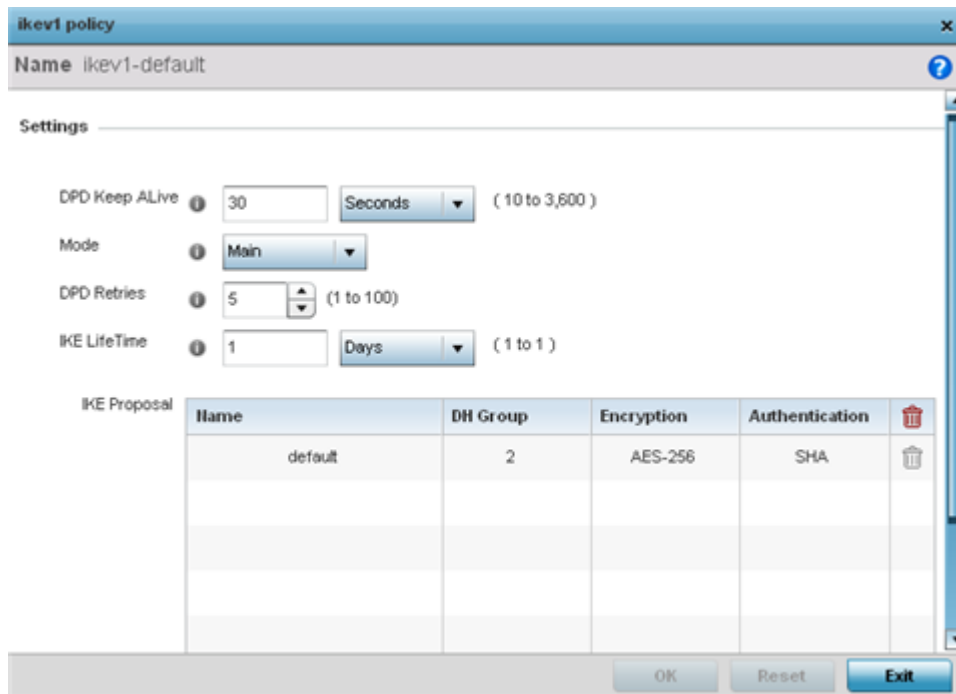
- 9 Select **Add** to define a new IKE Policy configuration, **Edit** to modify an existing configuration or **Delete** to remove an existing configuration.

### Adding and Editing an IKE V1 Policy

To add or edit 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.
- 6 Select **Add** to define a new IKE Policy configuration, **Edit** to modify an existing configuration or **Delete** to remove an existing configuration.



<b>Name</b>	If creating a new IKE policy, assign it a 32 character maximum name to help differentiate this IKE configuration from others with similar parameters.
<b>DPD Keep Alive</b>	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 <i>Seconds</i> (10 - 3,600), <i>Minutes</i> (1 - 60) or <i>Hours</i> (1). The default setting is 30 seconds. This setting is required for both IKEv1 and IKEv2.
<b>Mode</b>	If using IKEv1, use the pull-down menu to define the IKE mode as either <i>Main</i> or <i>Aggressive</i> . 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.
<b>DPD Retries</b>	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.
<b>IKE LifeTime</b>	Set the lifetime defining how long a connection (encryption/authentication keys) should last from successful key negotiation to expiration. Set this value in either <i>Seconds</i> (600 - 86,400), <i>Minutes</i> (10 - 1,440), <i>Hours</i> (1 - 24) or <i>Days</i> (1). This setting is required for both IKEv1 and IKEv2.

- 7 Select **+ Add Row** to define the network address of a target peer and its security settings.

<b>Name</b>	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.
<b>DH Group</b>	Use the drop-down menu to define a <i>Diffie-Hellman</i> (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.

<b>Encryption</b>	Select an encryption method used by the tunneled peers to securely interoperate. Options include <i>3DES</i> , <i>AES</i> , <i>AES-192</i> , <i>AES-256</i> . The default setting is AES-256.
<b>Authentication</b>	Select an authentication hash algorithm used by the peers to exchange credential information. Options include <i>SHA</i> , <i>SHA256</i> and <i>MD5</i> . The default setting is SHA.

- 8 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.

### Adding and Editing an IKE V2 Policy

To add or edit 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**.
- 6 Select **Add** to define a new IKE Policy configuration, **Edit** to modify an existing configuration or **Delete** to remove an existing configuration.

<b>Name</b>	If creating a new IKE policy, assign it a 32 character maximum name to help differentiate this IKE configuration from others with similar parameters.
<b>DPD Keep Alive</b>	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 <i>Seconds</i> (10 - 3,600), <i>Minutes</i> (1 - 60) or <i>Hours</i> (1). The default setting is 30 seconds. This setting is required for both IKEv1 and IKEv2.
<b>IKE LifeTime</b>	Set the lifetime defining how long a connection (encryption/authentication keys) should last from successful key negotiation to expiration. Set this value in either <i>Seconds</i> (600 - 86,400), <i>Minutes</i> (10 - 1,440), <i>Hours</i> (1 - 24) or <i>Days</i> (1). This setting is required for both IKEv1 and IKEv2.

- 7 Select **+ Add Row** to define the network address of a target peer and its security settings.

<b>Name</b>	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.
<b>DH Group</b>	Use the drop-down menu to define a <i>Diffie-Hellman</i> (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.
<b>Encryption</b>	Select an encryption method used by the tunneled peers to securely interoperate. Options include <i>3DES</i> , <i>AES</i> , <i>AES-192</i> and <i>AES-256</i> . The default setting is AES-256.
<b>Authentication</b>	Select an authentication hash algorithm used by the peers to exchange credential information. Options include <i>SHA</i> and <i>MD5</i> . The default setting is SHA.

- 8 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.

### Peer Configuration

To define a profile's VPN peer 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 **Security**.
- 5 Select **VPN**.
- 6 Select the **Peer Configuration** tab to assign additional network address and IKE settings to the an intended VPN tunnel peer destination.

Name	IP/Hostname	Authentication Type	LocalID	RemoteID	IKE Policy Name
peer1	lancelot	PSK	mudskipper	vfvasdvasdvascv	ikev1-default

- 7 Select either the **IKEv1** or **IKEv2** radio button to enforce VPN key exchanges using either *IKEv1* or *IKEv2*.
- 8 Refer to the following to determine whether a new VPN **Peer Configuration** requires creation, an existing configuration requires modification or a configuration requires removal.

<b>Name</b>	Lists the 32 character maximum name assigned to each listed peer configuration upon creation.
<b>IP/Hostname</b>	Displays the IP address (or host address FQDN) of the IPSec VPN peer targeted for secure tunnel connection and data transfer.
<b>Authentication Type</b>	Lists whether the peer configuration has been defined to use <i>pre-shared key</i> (PSK) or RSA. <i>Rivest, Shamir, and Adleman</i> (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 <i>local</i> and <i>remote</i> authentication, as both ends of the VPN connection require authentication.
<b>LocalID</b>	Lists the local identifier used within this peer configuration for an IKE exchange with the target VPN IPSec peer.
<b>RemoteID</b>	Displays the means the target remote peer is to be identified (string, FQDN etc.) within the VPN tunnel.
<b>IKE Policy Name</b>	Lists the IKEv1 or IKE v2 policy used with each listed peer configuration. If a policy requires creation, select the <i>Create</i> button.

- 9 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 be defined for the peer configuration vary depending on whether IKEv1 or IKEv2 was selected

## Adding and Editing a Peer IKE V1 Configuration

To add or edit a profile's VPN peer configuration 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**.
- 6 Select the **Peer Configuration** tab to assign additional network address and IKE settings to the an intended VPN tunnel peer destination.
- 7 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 be defined for the peer configuration vary depending on whether IKEv1 or IKEv2 was selected.

<b>Name</b>	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.
<b>IP Type or Select IP/ Hostname</b>	Enter either the <i>IP address</i> or FQDN <i>hostname</i> of the IPsec VPN peer used in the tunnel setup. If IKEv1 is used, this value is titled <i>IP Type</i> , if IKEv2 is used, this parameter is titled <i>Select IP/Hostname</i> .
<b>Authentication Type</b>	Select either <i>pre-shared key</i> (PSK) or RSA. <i>Rivest, Shamir, and Adleman</i> (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 <i>local</i> and <i>remote</i> 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).

<b>Authentication Value</b>	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.
<b>Local Identity</b>	Select the local identifier used with this peer configuration for an IKE exchange with the target VPN IPSec peer. Options include <i>IP Address</i> , <i>Distinguished Name</i> , <i>FQDN</i> , <i>email</i> and <i>string</i> . The default setting is <i>string</i> .
<b>Remote Identity</b>	Select the remote identifier used with this peer configuration for an IKE exchange with the target VPN IPSec peer. Options include <i>IP Address</i> , <i>Distinguished Name</i> , <i>FQDN</i> , <i>email</i> and <i>string</i> . The default setting is <i>string</i> .
<b>IKE Policy Name</b>	Select the IKEv1 or IKE v2 policy name (and settings) to apply to this peer configuration. If a policy requires creation, select the <i>Create</i> icon.

- 8 Select **OK** to save the changes made within the screen. Select **Reset** to revert to the last saved configuration.

### Adding and Editing a Peer IKE V2 Configuration

To add or edit a profile's VPN peer configuration 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**.
- 6 Select the **Peer Configuration** tab to assign additional network address and IKE settings to the an intended VPN tunnel peer destination.
- 7 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 be defined for the peer configuration vary depending on whether IKEv1 or IKEv2 was selected.

<b>Name</b>	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.
<b>IP Type or Select IP/ Hostname</b>	Enter either the <i>IP address</i> or <i>FQDN hostname</i> of the IPSec VPN peer used in the tunnel setup. If IKEv1 is used, this value is titled <i>IP Type</i> , if IKEv2 is used, this parameter is titled <i>Select IP/Hostname</i> .
<b>Local Authentication Type</b>	Select either <i>pre-shared key (PSK)</i> or <i>RSA. Rivest, Shamir, and Adleman (RSA)</i> 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 <i>local</i> and <i>remote</i> 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).
<b>Local Authentication Value</b>	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.

<b>Remote Identity</b>	Select the remote identifier used with this peer configuration for an IKE exchange with the target VPN IPSec peer. Options include <i>IP Address</i> , <i>Distinguished Name</i> , <i>FQDN</i> , <i>email</i> and <i>string</i> . The default setting is <i>string</i> .
<b>IKE Policy Name</b>	Select the IKEv1 or IKE v2 policy name (and settings) to apply to this peer configuration. If a policy requires creation, select the <i>Create</i> icon.

- 8 Select **OK** to save the changes made within the screen. Select **Reset** to revert to the last saved configuration.

### Transform Set

A *transform set* is a combination of security protocols, algorithms and other settings applied to IPSec protected traffic.

To define a profile's VPN transform set:

- 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**.
- 6 Select the **Transform Set** tab.

Create or modify *Transform Set* configurations to specify how traffic is protected for profile utilizing devices.

IKE Policy	Peer Configuration	Transform Set	Crypto Map	Remote VPN Server	Remote VPN Client	Global Settings																																																
		<table border="1"> <thead> <tr> <th>Transform Set</th> <th>Authentication Algorithm</th> <th>Encryption Algorithm</th> <th>Mode</th> </tr> </thead> <tbody> <tr> <td>default</td> <td>HMAC-SHA</td> <td>AES-256</td> <td>Tunnel</td> </tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td></tr> </tbody> </table>	Transform Set	Authentication Algorithm	Encryption Algorithm	Mode	default	HMAC-SHA	AES-256	Tunnel																																												
Transform Set	Authentication Algorithm	Encryption Algorithm	Mode																																																			
default	HMAC-SHA	AES-256	Tunnel																																																			
Type to search in tables						Row Count: 1																																																
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Exit"/>																																																						

- 7 Review the following attributes of existing **Transform Set** configurations:

<b>Name</b>	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.
<b>Authentication Algorithm</b>	Lists each transform sets's authentication scheme used to validate identity credentials. The authentication scheme options arer <i>HMAC-SHA,SHA256, AES-XCBC-MAC</i> or <i>HMAC-MD5</i> .
<b>Encryption Algorithm</b>	Displays each transform set's encryption method for protecting transmitted traffic.
<b>Mode</b>	Displays either <i>Tunnel</i> or <i>Transport</i> 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.

- 8 Select **Add** to define a new transform set configuration, **Edit** to modify an existing configuration or **Delete** to remove an existing transform set.

### Adding and Editing a Transform Set

To add or edit a profile's VPN transform set:

- 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**.
- 6 Select the **Transform Set** tab.
- 7 Select **Add** to define a new transform set configuration, **Edit** to modify an existing configuration or **Delete** to remove an existing transform set.

The screenshot shows a 'Transform Set' configuration window. The title bar says 'Transform Set' with a close button. Below the title bar, it says 'Transform Set default' with a help icon. The main area is titled 'IPSec Transform Set' and contains three configuration items, each with an information icon and a dropdown menu:

- Authentication Algorithm: HMAC-SHA
- Encryption Algorithm: AES-256
- Mode: Tunnel

At the bottom of the window, there are three buttons: 'OK', 'Reset', and 'Exit'.

- 8 Define the following settings for the new or modified transform set configuration:

<b>Name</b>	If creating a new transform set, define a 32 character maximum name to differentiate this configuration from others with similar attributes.
<b>Authentication Algorithm</b>	Set the transform sets's authentication scheme used to validate identity credentials. Use the pull-down menu to select either <i>HMAC-SHA</i> or <i>HMAC-MD5</i> . The default setting is HMAC-SHA.
<b>Encryption Algorithm</b>	Set the transform set encryption method for protecting transmitted traffic. Options include <i>DES</i> , <i>3DES</i> , <i>AES</i> , <i>AES-192</i> and <i>AES-256</i> . The default setting is AES-256.
<b>Mode</b>	Use the pull-down menu to select either <i>Tunnel</i> or <i>Transport</i> 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.

- 9 Select **OK** to save the changes made within the Transform Set screen. Select **Reset** to revert to the last saved configuration

### *Crypto Map*

Use *crypto maps* (as applied to IPSec VPN) to combine the elements used to create IPSec SAs (including transform sets).

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**.
- 6 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).

IKE Policy Peer Configuration Transform Set <b>Crypto Map</b> Remote VPN Server Remote VPN Client Global Settings				
Name	Type	IP Firewall Rules	IPsec Transform Set	
crypto1	Automatic Site-to-Site VPN	forrole	default	

Type to search in tables Row Count: 1

Add Edit Delete Exit

- 7 Review the following Crypto Map configuration parameters to assess their relevance:

<b>Name</b>	Lists the 32 character maximum name assigned for each crypto map upon creation. This name cannot be modified as part of the edit process.
<b>Type</b>	Displays the <i>site-to-site-manual</i> , <i>site-to-site-auto</i> or <i>remote VPN</i> configuration defined for each listed crypto map configuration. With site-to-site deployments, an IPSEC Tunnel is deployed between two gateways, each at the edge of two different remote networks. With remote VPN, an access point (located remotely) defines a tunnel with a security gateway. This facilitates the endpoints in the branch office to communicate with the destination endpoints (behind the security gateway) in a secure manner.
<b>IP Firewall Rules</b>	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.
<b>IPSec Transform Set</b>	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.

- 8 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.

### Adding and Editing a Crypto Map

To add or edit a profile's VPN crypto map 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**.
- 6 Select the **Crypto Map** tab.
- 7 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.
- 8 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.

Sequence	Type	IP Firewall Rules	IPsec Transform Set
2	Automatic Site-to-Site VPN	forrole	default

Type to search in tables Row Count: 1

- 9 Review the following before determining whether to add or modify a crypto map configuration

<b>Sequence</b>	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).
<b>Type</b>	Displays the <i>site-to-site-manual</i> , <i>site-to-site-auto</i> or <i>remote VPN</i> configuration defined for each listed crypto map configuration.
<b>IP Firewall Rules</b>	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.
<b>IPSec Transform Set</b>	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.

- 10 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.

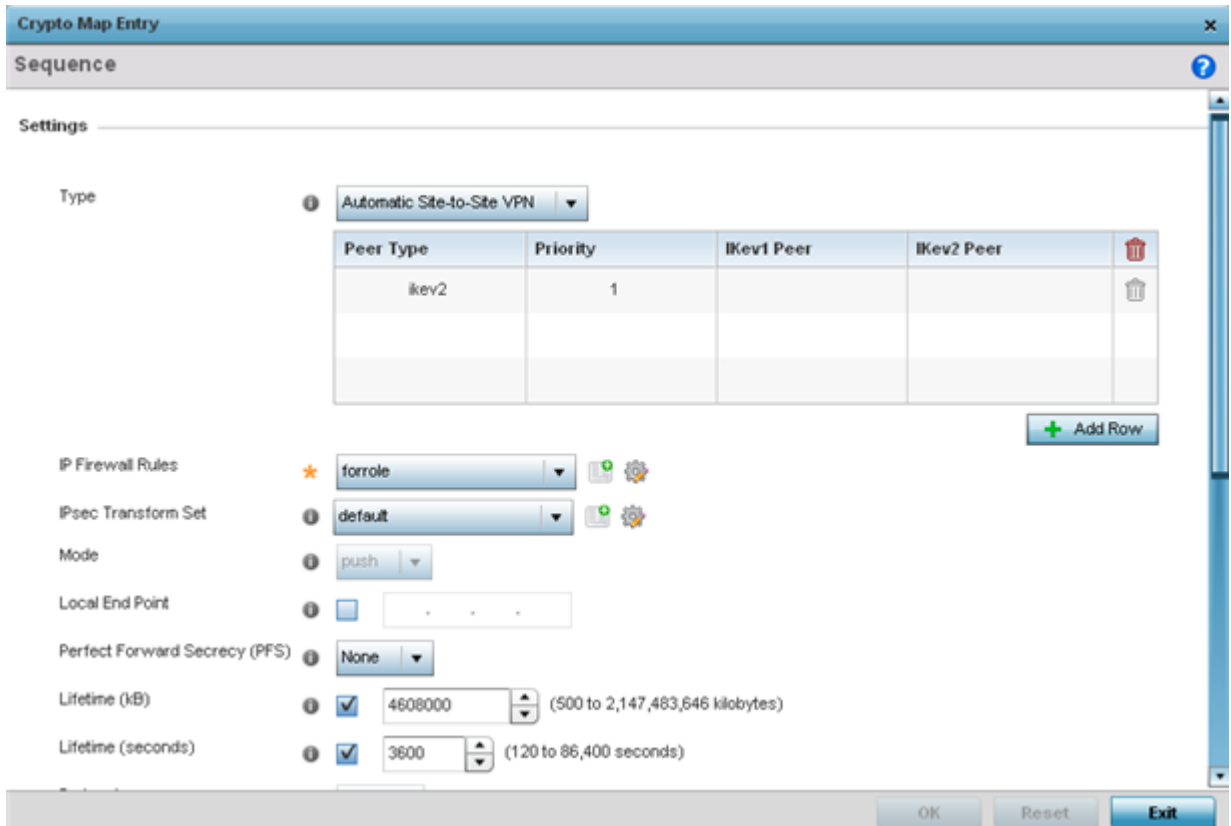
### Crypto Map Settings

To define a profile's VPN crypto map 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**.
- 6 Select the **Crypto Map** tab.
- 7 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.



- 8 If adding a new crypto map, assign it a name up to 32 characters in length as an unique identifier. Select the **Continue** button to proceed to the VPN Crypto Map screen.
- 9 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.



- 10 Define the following **Settings** to set the crypto map configuration:

<b>Sequence</b>	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).
<b>Type</b>	Define the <i>site-to-site-manual</i> , <i>site-to-site-auto</i> or <i>remote VPN</i> configuration defined for each listed crypto map configuration.
<b>IP Firewall Rules</b>	Use the pull-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 <i>Create</i> icon, or an existing set of firewall rules can be modified by selecting the <i>Edit</i> icon.
<b>IPSec Transform Set</b>	Select the transform set (encryption and hash algorithms) to apply to this crypto map configuration.
<b>Mode</b>	Use the pull-down menu to define which mode ( <i>pull</i> or <i>push</i> ) 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.
<b>Local End Point</b>	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.

<b>Perfect Forward Secrecy (PFS)</b>	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 <i>not</i> be used to derive any additional keys. Options include <i>None</i> , <i>2</i> , <i>5</i> and <i>14</i> . The default setting is <i>None</i> .
<b>Lifetime (kB)</b>	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.
<b>Lifetime (seconds)</b>	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.
<b>Protocol</b>	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 <i>ESP</i> and <i>AH</i> . The default setting is <i>ESP</i> .
<b>Remote VPN Type</b>	Define the remote VPN type as either <i>None</i> or <i>XAuth</i> . 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 <i>XAuth</i> .
<b>Manual Peer IP</b>	Select this option to define the IP address of an additional encryption/decryption peer.
<b>Time Out</b>	Set an IPSec <i>security association</i> (SA) timeout in either <i>Seconds</i> (120 - 86,400), <i>Minutes</i> (2 - 1,440), <i>Hours</i> (1 - 24) or <i>Days</i> (1). The default setting is 15 minutes.
<b>Enable NAT after IPSec</b>	Enable this setting to utilize IP/Port NAT on the VPN tunnel. This setting is disabled by default.

- 11 Select **OK** to save the updates made to the Crypto Map Entry screen. Selecting **Reset** reverts the screen to its last saved setting.

### Remote VPN Server

To define a profile's remote VPN server 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**.
- 6 Select **Remote VPN Server**.

Use this screen to define the server resources used to secure (authenticate) a remote VPN connection with a target peer.

- 7 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.

- 8 Set the following **IKEv1** or **IKe v2 Settings**:

<b>Authentication Method</b>	Use the drop-down menu to specify the authentication method used to validate the credentials of the remote VPN client. Options include <i>Local</i> (on board RADIUS resource if supported) and <i>RADIUS</i> (designated external RADIUS resource). If selecting <i>Local</i> , select the <i>+ Add Row</i> button and specify a <i>User Name</i> and <i>Password</i> for authenticating remote VPN client connections with the local RADIUS resource. The default setting is <i>Local</i> . AP 6521 and AP 6511 model access points do not have a local RADIUS resource and must use an external RADIUS server resource.
<b>AAA Policy</b>	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.

- 9 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.
- 10 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.
- 11 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.
- 12 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.
- 13 If using IKEv2, specify these additional settings (required for IKEv2 only):

<b>DHCP Server Type</b>	Specify whether the DHCP server is specified as an <i>IP address</i> , <i>Hostname (FQDN)</i> or <i>None</i> (a different classification will be defined). <i>Dynamic Host Configuration Protocol</i> (DHCP) allows hosts on an IP network to request and be assigned IP addresses and discover information about the network where they reside.
<b>DHCP Server</b>	Depending on the DHCP server type selected, enter either the numerical IP address, hostname or other (if None is selected as the server type).
<b>NetMask</b>	Specify the netmask for remote VPN clients.
<b>IP Local Pool</b>	Define an IP address and mask for a virtual IP pool used to assign IP addresses to requesting remote VPN clients.
<b>Relay Agent IP Address</b>	Select this option to define DHCP relay agent IP address.

- 14 Select **OK** to save the updates made to the Remote VPN Server screen. Selecting **Reset** reverts the screen to its last saved configuration.

### Remote VPN Client

To define a profile's remote VPN client connection 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**.
- 6 Select **Remote VPN Client**.

Use this screen to define the server resources used to secure (authenticate) a remote VPN connection with a target peer.

- 7 Set the following **Remote VPN Client Configuration** settings:

<b>Shutdown</b>	Select this option to disable the remote VPN client. The default is disabled.
<b>Transform Set</b>	Use the drop-down menu to select the transform set 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.

- 8 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.

- 9 Select **OK** to save the updates made to the Remote VPN Client screen. Selecting **Reset** reverts the screen to its last saved configuration.

### *Global Settings*

To define a profile's VPN global 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**.
- 6 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.

- 7 Define the following **IPSec Global** settings:

<b>df bit</b>	Select the DF bit handling technique used for the ESP encapsulating header. Options include <i>Clear</i> , <i>set</i> and <i>copy</i> . The default setting is <i>Copy</i> .
<b>IPsec Lifetime (kb)</b>	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.
<b>IPsec Lifetime (seconds)</b>	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 <i>Seconds</i> (120 - 86,400), <i>Minutes</i> (2 - 1,440), <i>Hours</i> (1 - 24) or <i>Days</i> (1). The default setting is 3,600 seconds.
<b>Plain Text Deny</b>	Select <i>global</i> or <i>interface</i> to set the scope of the ACL. The default setting is <i>global</i> , expanding the rules of the ACL beyond just the interface.
<b>Enable IKE Uniquelds</b>	Select this option to initiate a unique ID check. This setting is disabled by default.

- 8 Define the following **IKEV1 Settings**:

<b>DPD Keep Alive</b>	Define the interval (or frequency) for IKE keep alive messages for dead peer detection. Options include <i>Seconds</i> (10 - 3,600), <i>Minutes</i> (1 - 60) and <i>Hours</i> (1). The default setting is 30 seconds.
<b>DPD Retries</b>	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.
<b>NAT Keep Alive</b>	Define the interval (or frequency) for NAT keep alive messages for dead peer detection. Options include <i>Seconds</i> (10 - 3,600), <i>Minutes</i> (1 - 60) and <i>Hours</i> (1). The default setting is 20 seconds.

- 9 Define the following **IKEV2 Settings**:

<b>DPD Keep Alive</b>	Define the interval (or frequency) for IKE keep alive messages for dead peer detection. Options include <i>Seconds</i> (10 - 3,600), <i>Minutes</i> (1 - 60) and <i>Hours</i> (1). The default setting is 30 seconds.
<b>DPD Retries</b>	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.
<b>NAT Keep Alive</b>	Define the interval (or frequency) for NAT keep alive messages for dead peer detection. Options include <i>Seconds</i> (10 - 3,600), <i>Minutes</i> (1 - 60) and <i>Hours</i> (1). The default setting is 20 seconds.
<b>Cookie Challenge Threshold</b>	Use the spinner control to define the number of half open IKE <i>security associations</i> (SAs) (from 1 - 100) that, when exceeded, enables the cookie challenge mechanism. The is setting applies exclusively to IKEV2. The default setting is 5.
<b>Crypto NAT Pool</b>	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.

- 10 Select **OK** to save the updates made to the Global Settings screen. Selecting **Reset** reverts the screen to its last saved configuration.

## Auto IPSec Tunnel

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 the **Configuration** tab from the Web U.
- 2 Select **Profiles** from the Configuration tab.
- 3 Select **Manage Profiles** from the Configuration > Profiles menu.
- 4 Select **Security**.
- 5 Select **Auto IPsec Tunnel**.

The **Settings** field lists those Auto IPsec tunnel policies created thus far. Any of these policies can be selected and applied to a profile

<b>Group ID</b>	Define a 1 - 64 character identifier for an IKE exchange supporting auto IPsec tunnel secure peers.
<b>Authentication Type</b>	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
<b>Authentication Key</b>	Enter the 8 - 21 character shared key (password) used for auto IPsec tunnel secure peer authentication.
<b>IKE Version</b>	Use the drop-down menu to select the IKE version used for auto IPsec tunnel secure authentication with the IPsec gateway.
<b>Enable NAT after IPsec</b>	Select this option to enable internal source port NAT on the auto IPsec secure tunnel.
<b>Use Unique ID</b>	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.

- 6 Select **OK** to save the changes made to the auto IPsec tunnel configuration. Select **Reset** to revert to the last saved configuration.

## Setting the Profile's NAT 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.

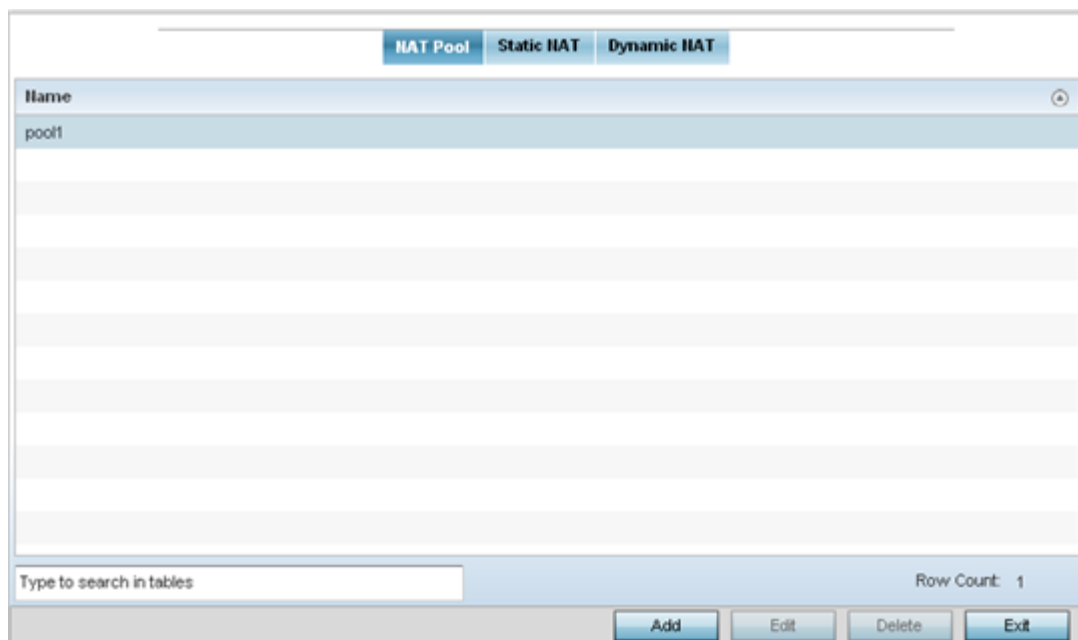
NAT is a process of modifying network address information in IP packet headers while in transit across a traffic routing device for the purpose of remapping one IP address to another. In most deployments NAT is used in conjunction with IP masquerading which hides RFC1918 private IP addresses behind a single public IP address.

NAT can provide an profile outbound Internet access to wired and wireless hosts connected to a controller, service platform or access point. Many-to-one NAT is the most common NAT technique for outbound Internet access. Many-to-one NAT allows a controller, service platform or access point 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.

### *NAT Pool*

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**.



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 an existing policy or select **Delete** to remove obsolete NAT policies from the list of those available to a profile

## Add

To add or edit 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**.
- 6 Select **Add** to create a new NAT policy that can be applied to a profile. Select **Edit** to modify the attributes of an existing policy or select **Delete** to remove obsolete NAT policies from the list of those available to a profile.

- 7 If adding a new NAT policy or editing the configuration of an existing policy, define the following parameters:

<b>Name</b>	If adding a new NAT policy, provide a name to help distinguish it from others with similar configurations. The length cannot exceed 64 characters.
<b>IP Address Range</b>	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.

## Static NAT

Static NAT maps a device's unregistered IP address to a registered IP address. It's useful when a device needs to be accessible from outside the network.

For more information, see:

- [Source](#)
- [Destination](#)

### Source

To define a static 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**.
- 6 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.

IAT Pool
Static IAT
Dynamic IAT

Source
Destination

Protocol	Source IP	Source Port	IAT IP	IAT Port	Network
Any	157.235.232.255	1	157.235.121.221	1	inside

Type to search in tables Row Count: 1

Add
Edit
Delete
Exit

- 7 Select **Add** to create a new static NAT configuration. Existing NAT source configurations are not editable.

Source ×

Add NAT Source ?

**Settings**

Protocol ★ Any ▼

Source IP ★ . . .

Source Port ★ 1 other ▼ (1 to 65,535)

NAT IP ★ . . .

NAT Port ★ 1 other ▼ (1 to 65,535)

Network ★ ▼

OK
Reset
Exit

- 8 Set or override the following Source configuration parameters:

<b>Protocol</b>	Select the protocol for use with static translation ( <i>TCP</i> , <i>UDP</i> and <i>Any</i> 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 <i>User Datagram Protocol</i> (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.
<b>Source IP</b>	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.
<b>Source Port</b>	Use the spinner control to set the local port number used at the origination of the static NAT configuration. The default source port is 1.
<b>NAT IP</b>	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.
<b>NAT Port</b>	Enter the port number of the matching packet to the specified value. This option is valid only if the direction specified is destination.
<b>Network</b>	Select <i>Inside</i> or <i>Outside</i> NAT as the network direction. Select <i>Inside</i> 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. <i>Inside</i> NAT is the default setting. <i>Inside</i> is the default setting.

- 9 Select **OK** to save the changes or overrides made to the static NAT configuration. Select **Reset** to revert to the last saved configuration.

## Destination

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.

To set a NAT destination 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**.
- 6 Select the **Static NAT** tab.
- 7 Select the **Destination** tab.

NAT Pool    Static NAT    Dynamic NAT					
Source			Destination		
Protocol	Destination IP	Destination Port	NAT IP	NAT Port	Network
Any	157.235.232.32	179	157.235.121.21	1	outside

Type to search in tables Row Count: 1

- 8 Select **Add** to create a new NAT destination configuration. Existing NAT destination configurations are not editable.

#### Adding and Editing Destination NAT

To add or edit a NAT destination 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**.
- 6 Select the **Static NAT** tab.
- 7 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.
- 8 Select **Add** to create a new NAT destination configuration, **Edit** to modify the attributes of an existing configuration or **Delete** to permanently remove a NAT destination.

**Destination** [x]

**Add Destination NAT** [?]

**Settings**

Protocol: Any

Destination IP: 157.235.232.32

Destination Port: 179 (1 to 65,535) [bgp]

NAT IP: 157.235.121.21

NAT Port: 1 (1 to 65,535) [other]

Network: Outside

[OK] [Reset] [Exit]

- 9 Set the following **Destination** configuration parameters:

Static NAT creates a permanent, one-to-one mapping between an address on an internal network and an external network. To share a Web server with the Internet, use static address translation to map the actual address to a registered IP address. Static address translation hides the actual server address 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.

<b>Protocol</b>	Select the protocol for use with static translation. <i>TCP</i> , <i>UDP</i> and <i>Any</i> 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 <i>User Datagram Protocol</i> (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.
<b>Destination IP</b>	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.
<b>Destination Port</b>	Use the spinner control to set the local port used at the (source) end of the static NAT configuration. The default port is 1.
<b>NAT IP</b>	Enter the IP address of the matching packet to the specified value. The IP address modified can be either <i>source</i> or <i>destination</i> based on the direction specified.
<b>NAT Port</b>	Set the port number of the matching packet to the specified value. This option is valid only if the direction specified is destination.
<b>Network</b>	Select <i>Inside</i> or <i>Outside</i> NAT as the network direction. Inside is the default setting.

- 10 Select **OK** to save the changes made to the static NAT configuration. Select **Reset** to revert to the last saved configuration.

## Dynamic NAT

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.

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**.
- 6 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.

	<b>NAT Pool</b>	<b>Static NAT</b>	<b>Dynamic NAT</b>			
<b>Source List ACL</b>	<b>Network</b>	<b>Interface</b>	<b>Overload Type</b>	<b>NAT Pool</b>	<b>Overload IP</b>	<b>ACL Precedence</b>
forrole	outside	wwan1	One Global Address		157.235.232.255	1
Type to search in tables				Row Count: 1		
				<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Exit"/>		

- 7 Refer to the following to determine whether a new Dynamic NAT configuration requires creation, edit or deletion:

<b>Source List ACL</b>	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.
<b>Network</b>	Displays <i>Inside</i> or <i>Outside</i> NAT as the network direction for the dynamic NAT configuration.
<b>Interface</b>	Lists the VLAN (between 1 - 4094) used as the communication medium between the source and destination points within the NAT configuration.



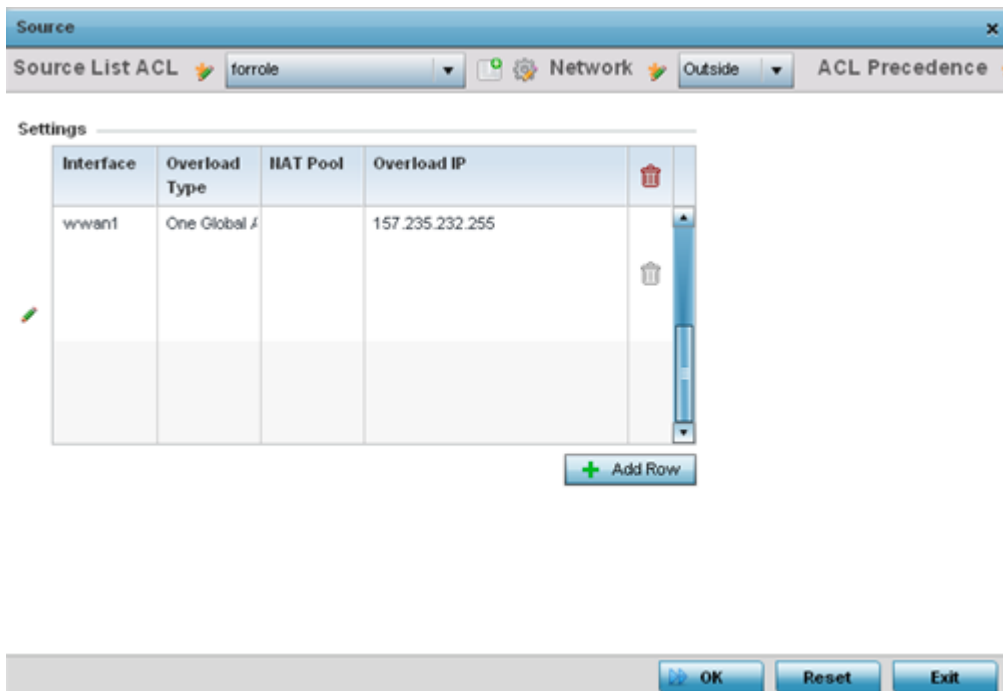
<b>Overload Type</b>	Lists the Overload Type used with the listed IP ACL rule. Options include <i>NAT Pool</i> , <i>One Global Address</i> and <i>Interface IP Address</i> . Interface IP Address is the default setting.
<b>NAT Pool</b>	Displays the name of an existing NAT pool used with the dynamic NAT configuration.
<b>Overload IP</b>	Enables the use of one global address for numerous local addresses.
<b>ACL Precedence</b>	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.

- 8 Select **Add** to create a new Dynamic NAT configuration, **Edit** to modify an existing configuration or **Delete** to permanently remove a configuration.

### Adding and Editing Dynamic NAT

To add or edit a dynamic 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**.
- 6 Select the **Dynamic NAT** tab.
- 7 Select **Add** to create a new Dynamic NAT configuration, **Edit** to modify an existing configuration or **Delete** to permanently remove a configuration.



- 8 Set the following to define the Dynamic NAT configuration:

<b>Source List ACL</b>	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.
<b>Network</b>	Select <i>Inside</i> or <i>Outside</i> NAT as the network direction for the dynamic NAT configuration. Inside is the default setting.
<b>ACL Precedence</b>	Set the priority (from 1 - 5000) for the source list ACL. The lower the value, the higher the priority assigned to these ACL rules.
<b>Interface</b>	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.
<b>Overload Type</b>	Select the check box of Overload Type used with the listed IP ACL rule. Options include <i>NAT Pool</i> , <i>One Global Address</i> and <i>Interface IP Address</i> . Interface IP Address is the default setting.
<b>NAT Pool</b>	Provide the name of an existing NAT pool for use with the dynamic NAT configuration.
<b>Overload IP</b>	Enables the use of one global address for numerous local addresses.

- 9 Select **OK** to save the changes made to the dynamic NAT configuration. Select **Reset** to revert to the last saved configuration.

## Bridge NAT 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, 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:

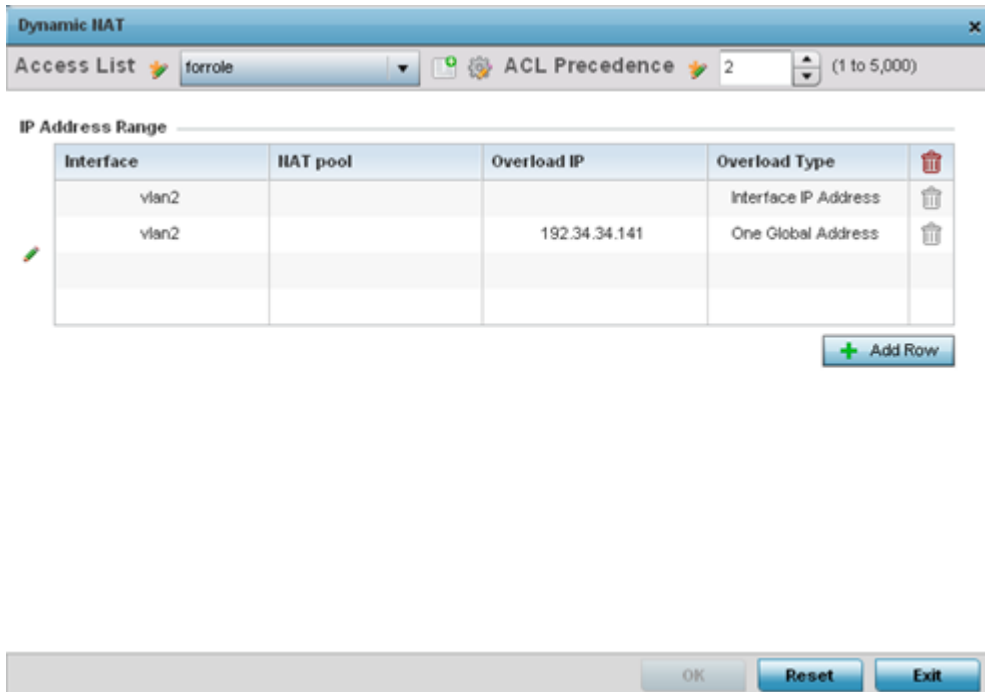
- 1 Select the **Configuration** tab from the Web UI
- 2 Select **Profiles** from the Configuration tab.
- 3 Select **Manage Profiles** from the Configuration > Profiles menu
- 4 Select **Security**.
- 5 Select **Bridge NAT**.



- 3 Select **Manage Profiles** from the Configuration > Profiles menu.
- 4 Select **Security**.
- 5 Select **Bridge NAT**.

**To Add Bridge NAT Configurations**

- 1 Select **Add** to create a new Bridge VLAN configuration, **Edit** to modify an existing configuration or **Delete** to remove a configuration.



- 2 Select the **ACL** 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.
- 3 Use the **IP Address Range** table to configure IP addresses and address ranges used to access the Internet.

<b>ACL Precedence</b>	Set the priority (from 1 - 5000) for the ACL. The lower the value, the higher the priority assigned to these ACL rules.
<b>Interface</b>	Lists the outgoing layer 3 interface on which traffic is re-directed. The interface can be an Access Point <i>wwan1</i> or <i>pppoe1</i> interface. Traffic can also be redirected to a designated VLAN.
<b>NAT Pool</b>	Displays the NAT pool used by this bridge NAT entry. A value is only displayed only when Overload Type has been set to <i>NAT Pool</i> .
<b>Overload IP</b>	Lists whether the single global address supports numerous local addresses.
<b>Overload Type</b>	Displays the overload type for this policy based forwarding rule.

- 4 Select **+ Add Row** to set IP address range settings for the bridge NAT configuration.

- 5 Select **OK** to save the changes made within the screen. Select **Reset** to revert to the last saved configuration.

## Profile Security Configuration and Deployment Considerations

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 RFS 4000 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 RFS 4000 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 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 RFS 6000 model wireless controller ships with a minimum baseline configuration without NAT enabled. A RFS 6000 wireless controller requires VLAN configuration, IP addressing and NAT rules be created before many-to-one NAT services can be defined.
- WiNG managed controllers and service platforms can provide outbound NAT services for hosts connected to multiple VLANs. For small deployments, VLANs should be terminated within a RFS 4000 wireless controller providing site routing services. For medium-scale deployments, VLANs are typically terminated on a L3 (IP layer) or L2 (Ethernet layer).

---

## 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.

## VRRP

To define the configuration of a VRRP group:

- 1 Select **Configuration > Profiles**.
- 2 Select **VRRP**.

		VRRP	Version		
Virtual Router ID	Description	Virtual IP Addresses	Interface	Priority	
1	lancelot	157.235.121.212	3	101	
Type to search in tables			Row Count: 1		
<b>Add</b>		<b>Edit</b>		<b>Delete</b>	
<b>Exit</b>					

- 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:

<b>Virtual Router ID</b>	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.
<b>Description</b>	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.
<b>Virtual IP Addresses</b>	Lists the virtual interface IP address used as the redundant gateway address for the virtual route.
<b>Interface</b>	Displays the device interfaces selected to supply VRRP redundancy failover support.
<b>Priority</b>	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 **Add** button to create a new VRRP configuration. Select **Edit** to update an existing VRRP configuration.

### *Adding and Editing VRRP Configurations*

To define the configuration of a VRRP group:

- 1 Select **Configuration > Profiles**.
- 2 Select **VRRP**.
- 3 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:

The screenshot shows the VRRP configuration window with the following settings:

- Virtual Router ID:** 1 (range 1 to 255)
- Description:** (empty text box)
- Priority:** 100 (range 1 to 254)
- Virtual IP Addresses:** A table with 4 rows, each containing '0 . 0 . 0 . 0' and a 'Clear' button.
- Advertisement Interval Unit:** seconds
- Advertisement Interval:** 1 (range 1 to 255) with a 'Seconds' dropdown and a secondary spinner for 250 (range 250 to 999 milliseconds).
- Preempt:**
- Preempt Delay:** 1 (range 1 to 65,535 seconds)
- Interface:** VLAN ID 1 (range 1 to 4,094)

Buttons at the bottom: OK, Reset, Exit.

- 4 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.
- 5 Define the following VRRP **General** parameters:

<b>Description</b>	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.
<b>Priority</b>	Use the spinner control to set a VRRP priority setting from 1 - 254. The defined setting is used 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.
<b>Virtual IP Addresses</b>	Provide up to 8 IP addresses representing Ethernet switches, routers or security appliances defined as virtual router resources.
<b>Advertisement Interval Unit</b>	Select either <i>seconds</i> , <i>milliseconds</i> or <i>centiseconds</i> as the unit used to define VRRP advertisements. Once an option is selected, the spinner control becomes enabled for that <i>Advertisement Interval</i> 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.
<b>Advertisement Interval</b>	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.



<b>Preempt</b>	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 <i>Preempt Delay</i> 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.
<b>Preempt Delay</b>	If the Preempt option is selected, use the spinner control to set the delay interval (in seconds) for pre-emption.
<b>Interface</b>	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.

- 6 Refer to the **Protocol Extension** field to define the following:

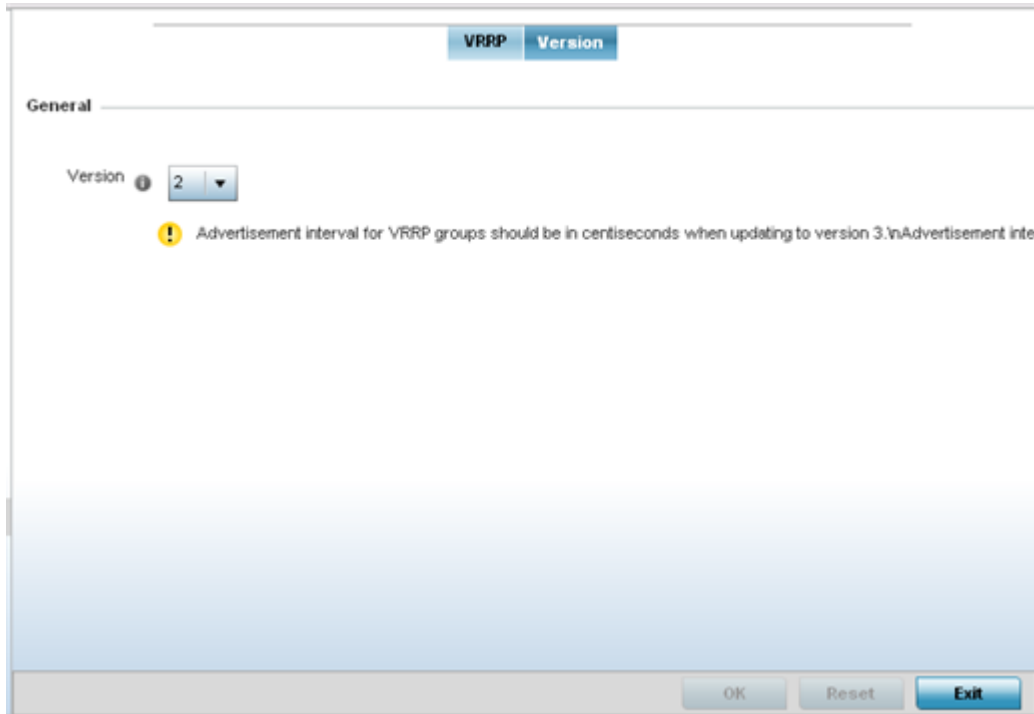
<b>Sync Group</b>	Select the option to assign a VRRP sync group to this VRRP ID's group of virtual IP addresses. This triggers VRRP failover if an advertisement is not received from the virtual masters that are part of this VRRP sync group. This setting is disabled by default.
<b>Network Monitoring: Local Interface</b>	Select the <i>wwan1</i> , <i>pppoe1</i> and <i>VLAN ID(s)</i> as needed to extend VRRP monitoring to these local interfaces. Once selected, these interfaces can be assigned an <i>increasing</i> or <i>decreasing</i> level or priority for virtual routing within the VRRP group.
<b>Network Monitoring: Critical Resource Name</b>	Assign the priority level for the selected local interfaces. Backup virtual routers can <i>increase</i> or <i>decrease</i> 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 <i>None</i> , <i>increment-priority</i> and <i>decrement priority</i> .
<b>Network Monitoring: Delta Priority</b>	Use this setting to decrement the configured priority (by the set value) when the monitored interface is down. When performing critical resource monitoring, the setting is incremented by the value defined.

- 7 Select **OK** to save the changes made to the VRRP configuration. Select **Reset** to revert to the last saved configuration.

## Version

To assess VRRP version information:

- 1 Select **Configuration > Profiles**.
- 2 Select **VRRP**.
- 3 Select the **Version** tab to define the VRRP version scheme used with the configuration.



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 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).

- 4 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.

## Critical Resources Configuration

*Critical resources* are device IP addresses or interface destinations on the network defined as critical to the health of the controller, service platform or access point managed 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 AP 8132 access point can be monitored by its IP address. However, a critical resource located on a VLAN must continue to be monitored on that VLAN.

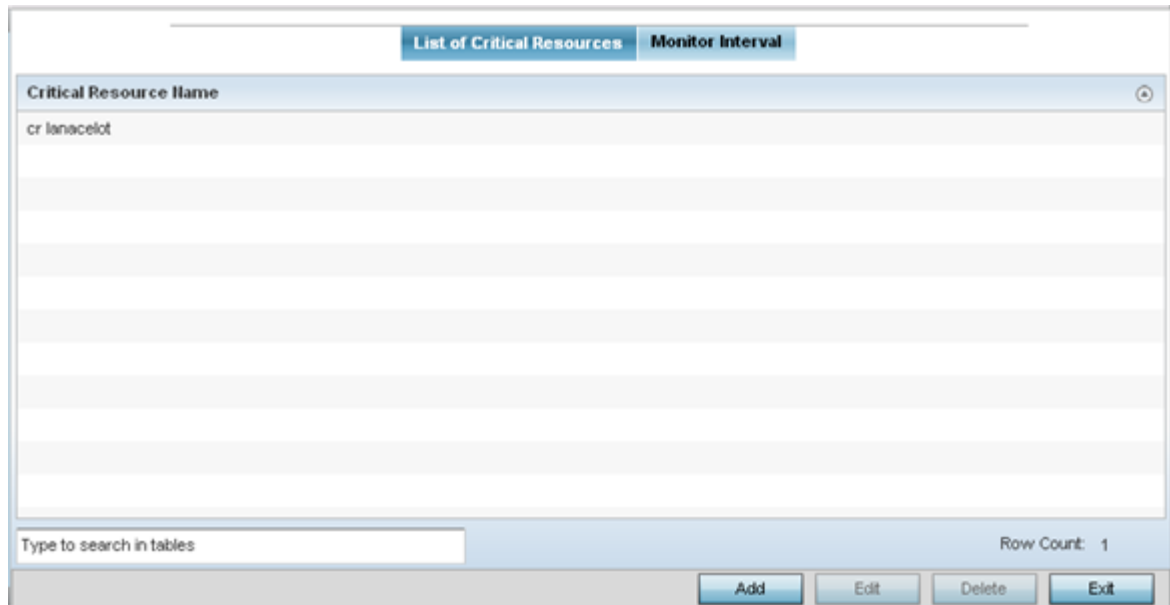
Critical resources can be configured for controllers, service platforms and access points using their respective device model profiles.

## List of Critical Resources

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.

To set a list of critical resources:

- 1 Select **Configuration > Profiles**.
- 2 Select **Critical Resources**.



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 access point or controller, whereas a VLAN, WWAN or PPPoE must be monitored behind an interface.

- 3 Select **Add** to add a new critical resource and connection method, or select an existing resource and select to update the resource's configuration.

### *Adding and Editing Critical Resources*

To add or edit a critical resource configuration:

- 1 Select **Configuration > Profiles**.
- 2 Select **Critical Resources**.
- 3 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.

Critical Resource Monitoring

Critical Resource Name \*

Settings

Use Flows  Sync Adoptees

Offline Resource Detection Any

Monitor Criteria cluster-master

Monitor Via  IP . . .  Interface vlan 1

Resources:

IP Address	Mode	Port	VLAN	

+ Add Row

OK Reset Exit

**Figure 224: Critical Resources Screen - Adding a Critical Resource**

- 4 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.
- 5 Select the **IP** checkbox (within the **Monitor Via** field at the top of the screen) to monitor a critical resource directly (within the same subnet) using the provided critical resource IP address as a network identifier.
- 6 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.
- 7 Use the **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.
- 8 Select **+ Add Row** to define the following for critical resource configurations:

<b>IP Address</b>	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.
<b>Mode</b>	Set the ping mode used when the availability of a critical resource is validated by the controller, service platform or access point. Select from: <ul style="list-style-type: none"> <li>•<i>arp-only</i> – Use the <i>Address Resolution Protocol</i> (ARP) for only pinging the critical resource. ARP is used to resolve hardware addresses when only the network layer address is known.</li> <li>•<i>arp-and-ping</i> – Use both ARP and <i>Internet Control Message Protocol</i> (ICMP) for pining the critical resource and sending control messages (device not reachable, requested service not available, etc.).</li> </ul>
<b>Port</b>	Use the drop-down menu to provide the physical port for each critical resource. The ports available depend on the device in use.
<b>VLAN</b>	Define the VLAN on which the critical resource is available using the spinner control.

- 9 Select **OK** to save the changes to the critical resource configuration. Select **Reset** to revert to the last saved configuration.

## Monitor Interval

To define a critical resource's monitoring interval:

- 1 Select **Configuration > Profiles**.
- 2 Select **Critical Resources**.
- 3 Select the **Monitor Interval** tab.
- 4 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.
- 5 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.
- 6 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.
- 7 Select **OK** to save the changes to the critical resource monitor interval. Select **Reset** to revert to the last saved configuration.

## Profile Services Configuration

A profile can contain specific captive portal, DHCP server and RADIUS server configurations supported by a controller, service platform or access point'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** tab from the Web UI.
- 2 Select **Profiles** from the Configuration tab.
- 3 Select **Manage Profiles** from the Configuration > Profiles menu.
- 4 Select **Services**.

**Profile\_Captive\_Portal**

Captive Portal Policies





**Create**




**RADIUS Server Application Policy**

Application Policy





**Create**

**DHCP Server**




DHCP Server Policy  <none>  

DHCPv6 Server Policy   




**Guest Management Policy**

Guest Management   




**RADIUS Server Policy**

Server Policy  <none>  

**Bonjour Gateway**

Forwarding Policy   

**Imagotag Policy**

Imagotag Policy  <none>  

**OK** **Reset** **Exit**

**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** 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 capture and redirect 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 more information, see, [Configuring Captive Portal Policies](#) on page 777.

- 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** 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).

Either select an existing captive portal policy or select the **Create** button to create a new captive portal configuration that can be applied to this profile. Existing policies can be modified by selecting the **Edit** icon. For more information, see [Setting the DHCP Configuration](#) on page 803.

- 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.

- 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 authentication data (usernames and passwords). When an client attempts to associate, an authentication request is sent to the RADIUS server.

If an existing RADIUS server policy does not meet your requirements, select the **Create** button to create a new policy configuration that can be applied to this profile. Existing policies can be modified by selecting the **Edit** icon. For more information, see [Setting the RADIUS Configuration](#) on page 829.

- 10 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.
- 11 From the **Forwarding Policy** drop-down, select the Bonjour Gateway forwarding policy.

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 Refer to the **Imagotag Policy** field to select or set a Imagotag Policy. Use the drop-down menu to select and apply an Imagotag Policy to the AP's profile. You can use the **Create** or **Edit** icons to create a new policy or edit an existing policy. The Imagotag feature is supported only on the AP 8432 model access point.

For information on enabling support for SES-imagotag's ESL tags on WiNG APs with USB interfaces, see [Setting the Imagotag Policy](#) on page 850.

- 13 Select **OK** to save the changes made to the profile's services configuration. Select **Reset** to revert to the last saved configuration.

## Profile Services Configuration and Deployment Considerations

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, since captive portals do increase the risk to the wireless network versus more secure access methods.
- 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.



---

## Profile Management Configuration

---

Controllers, service platforms and access points have mechanisms to *allow* or *deny* management access to the network for different 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 member, then propagated to each cluster member and onwards to the devices managed by each cluster member.

### Settings

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 a profile from those displayed in the right-hand pane.
- 5 Select **Management**.
- 6 Expand the Management menu item to display additional *Settings, Firmware* and *Heartbeat Management* options.
- 7 Select **Settings** from the Management menu.

**Figure 225: Profiles Management Settings Tab**

- 8 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.

- 9 Use to the **Critical Resource Policy** drop-down menu to set a critical resource policy for use with this profile. For more information on defining a critical resource policy, see [Overriding a Critical Resource Configuration](#) on page 270.
- 10 Refer to the **Message Logging** field to define how the profile logs system events. It's important to log individual events to determine an overall pattern that may be negatively impacting performance using the configuration defined for this profile.

<b>Enable Message Logging</b>	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.
<b>Remote Logging Host</b>	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 <i>Clear</i> as needed to remove an IP address.
<b>Facility to Send Log Messages</b>	Use the drop-down menu to specify the local server facility (if used) for the profile event log transfer.
<b>Syslog Logging Level</b>	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 - <i>Emergency</i> , 1 - <i>Alert</i> , 2 - <i>Critical</i> , 3 - <i>Errors</i> , 4 - <i>Warning</i> , 5 - <i>Notice</i> , 6 - <i>Info</i> and 7 - <i>Debug</i> . The default logging level is 4.
<b>Console Logging Level</b>	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 - <i>Emergency</i> , 1 - <i>Alert</i> , 2 - <i>Critical</i> , 3 - <i>Errors</i> , 4 - <i>Warning</i> , 5 - <i>Notice</i> , 6 - <i>Info</i> and 7 - <i>Debug</i> . The default logging level is 4.
<b>Buffered Logging Level</b>	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 - <i>Emergency</i> , 1 - <i>Alert</i> , 2 - <i>Critical</i> , 3 - <i>Errors</i> , 4 - <i>Warning</i> , 5 - <i>Notice</i> , 6 - <i>Info</i> and 7 - <i>Debug</i> . The default logging level is 4.
<b>Time to Aggregate Repeated Messages</b>	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 <i>Seconds</i> (0 - 60) or <i>Minutes</i> (0 -1). The default value is 0 seconds.
<b>Forward Logs to Controller</b>	Select the checkbox to define a log level for forwarding event logs. Log levels include <i>Emergency, Alert, Critical, Error, Warning, Notice, Info</i> and <i>Debug</i> . The default logging level is <i>Error</i> .

- 11 Refer to the **System Event Messages** section to set how system messages are logged and forwarded on behalf of the profile.

<b>Event System Policy</b>	Select an Event System Policy from the drop-down menu. If an appropriate policy does not exist click the <i>Create</i> button to make a new policy.
<b>Enable System Events</b>	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 determine an overall pattern that may be negatively impacting performance. This setting is enabled by default.
<b>Enable System Event Forwarding</b>	Select the Enable System Event Forwarding box to enable the forwarding of system events to another cluster member. This setting is enabled by default.

- 12 Refer to the **Events E-mail Notification** section to define how system event notification emails are sent.

<b>SMTP Server</b>	Specify either the <i>Hostname</i> or <i>IP Address</i> of the outgoing SMTP server where notification emails will be originated.
<b>Port of SMTP</b>	If a non-standard SMTP port is use on the outgoing SMTP server check this box and specify a port between 1 and 65,535 for the outgoing SMTP server to use.
<b>Sender Email Address</b>	Specify the 64 character maximum email address from which notification emails are originated. This is the from address on notification emails.
<b>Recipient's E-mail Address</b>	Specify up to 6 Email addresses to be the recipient's of event Email notifications.

<b>Username for SMTP Server</b>	Specify the username of the sender on the outgoing SMTP server. Many SMTP servers require users to authenticate with a <i>username</i> and <i>password</i> before sending email through the server.
<b>Password for SMTP Server</b>	Specify the password associated with the username of the sender on the outgoing SMTP server. Many SMTP servers require users to authenticate with a <i>username</i> and <i>password</i> before sending email through the server.

- 13 Refer to the **Persist Configurations Across Reloads** field to define how configuration settings are handled after reloads.

Use the drop-down menu to configure whether configuration updates should persist when the device configuration is reloaded. Available options are *Enabled*, *Disabled* and *Secure*.

- 14 Refer to the **External Analytics Engine** section to set 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 client 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.

<b>Controller</b>	Select this option to provide service platform analytics to a local device. This setting is enabled by default.
<b>URL</b>	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.
<b>User Name</b>	Enter the user name needed to access the external analytics engine
<b>Password</b>	Enter the password associated with the username on the external analytics engine.
<b>Update Interval</b>	Set the interval in either <i>Seconds</i> (1 - 3,600), <i>Minutes</i> (1 - 60) or <i>Hours</i> (1) to forward buffered information to an external server resource, even when the buffers are not full. The default setting is 1 minute.

- 15 Select **OK** to save the changes made to the profile's management settings. Select **Reset** to revert to the last saved configuration.

## Firmware

An administrator can provide a profile with unique device configuration file and firmware upgrade support. In a clustered environment, these operations can be performed on one device, then propagated to each member of a cluster and onwards to devices managed by each cluster member. The number of concurrent device upgrades and their start times can be customized to ensure a sufficient number of devices remain in duty while upgrades are administered to others. Additionally, AP71XX and AP650 legacy access points can be updated from their legacy WiNG 4.x firmware baseline to the most recent 5.x firmware baseline to ensure they're operating with the most recent feature set.

To define a profile's access point upgrade 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 additional *Settings*, *Firmware* and *Heartbeat Management* options.
- 6 Select **Firmware** from the Management menu.
- 7 Refer to the **Auto Install via DHCP Option** section to configure automatic configuration file and firmware updates.

<b>Enable Configuration Update</b>	Select the <i>Enable Configuration Update</i> 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.
<b>Enable Firmware Upgrade</b>	Select this option to enable automatic firmware upgrades (for this profile) from a user defined remote location. This value is disabled by default.
<b>Start Time (minutes)</b>	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.

- 8 Refer to the parameters within the **Legacy Device Firmware Management** field to set legacy access point firmware provisions:

<b>Migration Firmware from AP71xx 4.x path</b>	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.
<b>Legacy AP650 Auto Update</b>	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.

- 9 Use the parameters within the **Automatic Adopted AP Firmware Upgrade** section to define an automatic firmware upgrade from a local file.

<b>Enable Controller Upgrade of AP Firmware</b>	Select this radio button to enable adopted radios to upgrade to a newer firmware version using its associated controller's most recent resident firmware file for that access point model. This parameter is disabled by default.
<b>Number of Concurrent Upgrades</b>	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 and the access point rebooted.

- 10 Select the **Persist Image on Controller** button (from within the **Firmware Persistence for Adopted Devices** field) to enable a NX 4500, NX 6500, or NX 9000 series 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 Persist Image 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.

- 11 Select **OK** to save the changes made to the profile's Management Firmware configuration. Select **Reset** to revert to the last saved configuration.

## Profile Management Configuration and Deployment Considerations

Before defining a profile's management configuration, refer to the following deployment guidelines to ensure the profile configuration is optimally effective:

- Set profile management access configurations that provide 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.

## Overriding Management Heartbeat

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 Select **Management**.



#### 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

## Profile Mesh Point Configuration

Mesh points are WiNG managed access points dedicated to mesh network support. Mesh networking enables users to access broadband applications anywhere (including moving vehicles).

To set 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**.
- 5 Refer to the **Mesh Point** screen to review existing mesh point configurations and determine whether a new mesh point configuration requires creation or an existing mesh point configuration requires modification.

<b>MeshConnex Policy</b>	Lists the administrator assigned name for the MeshConnex Policy, defined upon its creation. The name cannot be edited later with other parameters.
<b>Is Root</b>	Displays whether the mesh point is the root node in the mesh network or not. A green checkmark defines the mesh point as a root, a red X does not.
<b>Preferred Root</b>	Lists the MAC address of a preferred root device.
<b>Preferred Neighbor</b>	Lists the MAC address of the preferred neighbor within the mesh point's mesh topology.
<b>Preferred Interface</b>	Displays either <i>2.4GHz</i> or <i>5 GHz</i> as the preferred band of operation for the mesh point.
<b>Monitor Critical Resources</b>	When enabled (as defined by a green checkmark) you allow the dynamic conversion of a mesh point from root to non-root when there is a critical resource failure. This option is disabled by default.

<b>Monitor Primary Port Link</b>	When enabled (as defined by a green checkmark) you allow the dynamic conversion of a mesh point from root to non-root during a link down event. This option is disabled by default.
<b>Path Method</b>	Lists the method used for path selection in a mesh network. Available options include: <i>None</i> – No criteria used in root path selection. <i>uniform</i> – Indicates the path selection method is uniform (two paths are considered equivalent if the average value is the same for these paths). <i>mobile-snr-leaf</i> – The access point is mounted on a vehicle or a mobile platform (AP 7161 models only). The path to the route is selected based on the <i>Signal To Noise Ratio</i> (SNR) with the neighbor device. <i>snr-leaf</i> – Indicates the path with the best signal to noise ratio is always selected.

**Note**

An AP 7161 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.

- 1 If an existing mesh point does not meet your requirements, select the **Add** button to create a new configuration or the **Edit** button to modify the parameters of an existing configuration.
- 2 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 when enabling VMM.
  - Set the RTS threshold value to 1 on all mesh devices. The default is 2347.
  - 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.
  - Consider setting 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 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:

```
nx9500-xxxxxx>enable
```

```
nx9500-xxxxxx #configure terminal
```



Enter configuration commands, one per line. End with CNTL/Z.

```
nx9500-xxxxxx (config)#profile ap71xx Non-Root AP71xx
```

```
nx9500-xxxxxx (config-profile-Non-Root-AP71xx)#misconfiguration-recovery-time 0
```

```
nx9500-xxxxxx (config-profile-Non-Root-AP71xx)
```

## MeshConnex Policy Settings

To set a mesh point's policy setting 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**.
- 5 Refer to the **Mesh Point** screen to review existing mesh point configurations and determine whether a new mesh point configuration requires creation or an existing mesh point configuration requires modification.
- 6 If an existing Mesh Point configuration does not meet your requirements, select the **Add** button to create a new configuration or **Edit** to modify the parameters of an existing configuration.

The **Settings** tab displays by default.

- 7 Set the following **General** parameters:

<b>MeshConnex Policy</b>	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.
<b>Is Root</b>	Select the root behavior of this mesh point. Select <i>True</i> to indicate this mesh point is a root node for this mesh network. Select <i>False</i> to indicate this mesh point is not a root node for this mesh network.
<b>Root Selection Method</b>	Use the drop-down menu to determine whether this meshpoint is the root or non-root meshpoint.
<b>Set as Cost Root</b>	Select this option to set the mesh point as the cost root for meshpoint root selection. This setting is disabled by default.
<b>Monitor Critical Resources</b>	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.
<b>Monitor Primary Port Link</b>	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.

<b>Wired Peer Excluded</b>	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.
<b>Path Method</b>	Use the drop-down menu to select the method (criteria) used for selecting the root path. <i>None</i> – Select this to indicate no criteria used in root path selection. <i>uniform</i> – 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. <i>mobile-snr-leaf</i> – Select this if this access point is mounted on a vehicle or a mobile platform (AP 7161 models only). When selected, the path to the route will be selected based on the Signal To Noise Ratio (SNR) to the neighbor device. <i>snr-leaf</i> – Select this to indicate that the path with the best signal to noise ratio is always selected.

**Note**

When using 4.9GHz, the root preferences selection for the radio's preferred interface still displays as 5GHz.

- 1 Set the following **Root Path Preferences**:

<b>Preferred Neighbor</b>	Specify the MAC address of a preferred neighbor within the mesh topology.
<b>Preferred Root</b>	Specify the MAC address of a preferred root device.
<b>Preferred Interface</b>	Use the drop-down menu to set the preferred mesh point interface to either <i>2.4GHz</i> , <i>4.9GHz</i> or <i>5.0GHz</i> .

- 2 Set the following **Root Method Hysteresis**:

<b>Minimum Threshold</b>	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 <i>Signal Strength Delta</i> and <i>Sustained Time Period</i> are used to dynamically select the next hop in a dynamic mesh network.
<b>Signal Strength Delta</b>	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 <i>Minimum Threshold</i> and <i>Sustained Time Period</i> are used to dynamically select the next hop in a dynamic mesh network.
<b>Sustained Time Period</b>	Enter the duration (in seconds or minutes) for the duration a signal must sustain the constraints specified in the <i>Minimum Threshold</i> and <i>Signal Strength Delta</i> path hysteresis values. These values are used to dynamically select the next hop in a dynamic mesh network.
<b>Root selection SNR Delta Range</b>	Select the root selection method hysteresis (from 1 - 100dB) Root Selection Delta Range. The device must sustain a signal strength within the delta range to be considered a candidate. The default setting is 10 dB.

- 3 Select **OK** to save the updates to the Settings screen. Select **Reset** to revert to the last saved configuration.

## Auto Channel Selection

The Auto Channel Selection screen is used to define the Dynamic Root Selection, Path Method SNR, and Path Method Root Path Metric.

Use the **Dynamic Root Selection** screen to refine channel scans, set the scan duration, whether scans are conducted off-channel, scan sample size and channel hold time.

Use the **Path Method SNR** screen to set a profile's mesh point channel width, mesh point priority and *signal to noise* (SNR) scan settings.

Use the **Path Method Root Path Metric** screen to set a profile's mesh point root path scan settings.

### Dynamic Root Selection

Use the **Dynamic Root Selection** screen to refine channel scans, set the scan duration, whether scans are conducted off-channel, scan sample size and channel hold time.

To define a profile's mesh point dynamic root selection:

- 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**.

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.

- 5 Select the **Auto Channel Selection** tab.

The Dynamic Root Selection screen displays by default.

- 6 Set the following values (common to both 2.4 GHz and 5.0/4.9 GHz):

<b>Channel Width</b>	Set the channel width the meshpoint's automatic channel scan assigns to the selected radio. Available options include: <i>Automatic</i> - Defines the channel width is calculated automatically. This is the default value. <i>20 MHz</i> - Sets the width between two adjacent channels as 20 MHz. <i>40 MHz</i> - Sets the width between two adjacent channels as 40 MHz. <i>80 MHz</i> - Sets the width between two adjacent channels as 80 MHz for 802.11ac access points.
<b>Priority Meshpoint</b>	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
<b>Off-channel Duration</b>	Set the duration (from 20 - 250 milliseconds) the scan dwells on each channel when performing an off channel scan. The default is 50 milliseconds
<b>Off-channel Scan Frequency</b>	Set the duration (from 1- 60 seconds) between two consecutive off channel scans. The default is 6 seconds.
<b>Meshpoint Root - Sample Count</b>	Configure the number of scan samples (from 1- 10) performed for data collection before a mesh channel is selected. The default is 5.
<b>Meshpoint Root - Channel Hold Time</b>	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.

- 7 Select **OK** to save the updates to the Mesh Point's dynamic root selection configuration. Select **Reset** to revert to the last saved configuration.

### Path Method SNR

Use the **Path Method SNR** screen to set a profile's mesh point channel width, mesh point priority and *signal to noise* (SNR) scan settings.

To define a profile's path method signal to noise ratio:

- 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**.

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.

- 5 Select the **Auto Channel Selection** tab.
- 6 Select the **Path Method SNR** tab.
- 7 Set the following values (common to both 2.4 GHz and 5.0/4.9 GHz):

<b>Channel Width</b>	Set the channel width the meshpoint's automatic channel scan assigns to the selected radio. Available options include: <i>Automatic</i> - Defines the channel width is calculated automatically. This is the default value. <i>20 MHz</i> - Sets the width between two adjacent channels as 20 MHz. <i>40 MHz</i> - Sets the width between two adjacent channels as 40 MHz. <i>80 MHz</i> - Sets the width between two adjacent channels as 80 MHz for 802.11ac access points.
<b>Priority Meshpoint</b>	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.
<b>SNR Delta</b>	Set the <i>signal to noise</i> (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.
<b>SNR Threshold</b>	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.
<b>Off-channel Duration</b>	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.

- 8 Select **OK** to save the updates to the Mesh Point's path method SNR configuration. Select **Reset** to revert to the last saved configuration.

### Path Method Root Path Metric

Use the **Path Method Root Path Metric** screen to set a profile's mesh point root path scan settings.

To define the path method root path metric:

- 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**.

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.

- 5 Select the **Auto Channel Selection** tab.
- 6 Select the **Path Method Root Path Metric** tab.
- 7 Set the following values (common to both 2.4 GHz and 5.0/4.9 GHz):

<b>Channel Width</b>	Set the channel width the mesh point's automatic channel scan assigns to the selected radio. Available options include: <i>Automatic</i> - Defines the channel width is calculated automatically. This is the default value. <i>20 MHz</i> - Sets the width between two adjacent channels as 20 MHz. <i>40 MHz</i> - Sets the width between two adjacent channels as 40 MHz. <i>80 MHz</i> - Sets the width between two adjacent channels as 80 MHz for 802.11ac access points.
<b>Priority Meshpoint</b>	Configure the mesh point monitored for automatic channel scans. This is the mesh point assigned priority over other available mesh points. When configured, a mesh connection is established with this mesh point. If not configured, a mesh point is automatically selected. This setting is disabled by default.
<b>Meshpoint: Path Minimum</b>	Set the minimum path metric (from 100 - 20,000) for mesh connection establishment. The default setting is 1000.
<b>Meshpoint: Path Metric Threshold</b>	Configure a minimum threshold (from 800 - 65535) for triggering an automatic channel selection for mesh point selection. The default is 1500.
<b>Meshpoint: Tolerance Period</b>	Configure a duration to wait before triggering an automatic channel selection for the next mesh hop. The default is one minute.
<b>Meshpoint Root: Sample Count</b>	Set the number of scans (from 1- 10) for data collection before a mesh point root is selected. The default setting is 5.
<b>Meshpoint Root: Off-channel Duration</b>	Define the duration (from 20 - 250 milliseconds) for scan dwells on each channel, when performing an off channel scan. The default setting is 50 milliseconds.
<b>Meshpoint Root: Channel Switch Delta</b>	Configure the delta (from 5 - 35 dBm) that triggers a mesh point root automatic channel selection when exceeded. The default setting is 10 dBm.
<b>Meshpoint Root Off-channel Scan Frequency</b>	Configure the duration (from 1 -60 seconds) between two consecutive off channel scans for mesh point root. The default is 6 seconds.
<b>Meshpoint Root Channel Hold Time</b>	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.

- 8 Select **OK** to save the updates to the Mesh Point's path method SNR configuration. Select **Reset** to revert to the last saved configuration.

## Environmental Sensor Configuration (AP 8132 Only)

An AP 8132 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 environmental conditions including temperature, humidity and light near the AP 8132's radio coverage area. The output of the sensor's detection mechanisms are viewable using either the Environmental Sensor screen.

To set an environmental sensor configuration for an AP 8132 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**.

- 5 Set the following **Light Sensor** settings for the AP 8132's sensor module:

<b>Enable Light Sensor</b>	Select this option to enable the light sensor on the module. This setting is enabled by default. The light sensor reports whether the <AP8132>'s deployment location has its lights powered on or off.
<b>Polling Time to Determine if Light is On/Off</b>	Define an interval in <i>Seconds</i> (10 - 201) or <i>Minutes</i> (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.
<b>Shutdown WLAN Radio at Low Limit of Light Threshold</b>	Select this option to power off the AP 8132's radio's fall below the set threshold. If enabled, select <i>All</i> (both radios), <i>radio-1</i> or <i>radio-2</i> .

<b>Low Limit of Light Threshold</b>	Set the low threshold limit (from 0 - 1,000 lux) to determine whether the lighting is off in the AP 8132'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.
<b>High Limit of Light Threshold</b>	Set the upper threshold limit (from 100 - 10,000 lux) to determine whether the lighting is on in the AP 8132'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 AP 8132 **Environmental Sensors**:

<b>Enable Temperature Sensor</b>	Select this option to enable the module's temperature sensor. Results are viewable in the access point's Environment screens within the Statistics node. This setting is enabled by default.
<b>Enable Motion Sensor</b>	Select this option to enable the module's motion sensor. Results are viewable in the access point's Environment screens within the Statistics node. This setting is enabled by default.
<b>Enable Humidity Sensor</b>	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 the following **Shared Configuration** settings:

Set a polling interval in either *Seconds* (1 - 100) or *Minutes* (1 - 2) for the time between environmental polling transmissions (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.

## Advanced Profile Configuration

A profile's advanced configuration is comprised its MINT protocol configuration, 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 controller, service platform or access point 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 Balancing](#)
- [Configuring MINT](#)
- [Advanced Profile Miscellaneous Configuration](#)

## Client Load Balancing

Set 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.

- 2 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.

- 3 Set the following **Neighbor Selection Strategies**:



<b>Using Probes from common clients</b>	Select this option to select neighbors (peer devices) using probes from common clients. This setting is enabled by default.
<b>Using Notifications from roamed clients</b>	Select this option to select neighbors (peer devices) using roam notifications from roamed clients. This setting is enabled by default.
<b>Using smart-rf neighbor detection</b>	Select this option to select neighbors (peer devices) using Smart RF. This setting is enabled by default.

- 4 Enable **Balance Band Loads by Radio** to distribute an access points client traffic load across both the 2.4 and 5 GHz radio bands.
- 5 Set the following **Channel Load Balancing** settings:

<b>Balance 2.4 GHz Channel Loads</b>	Select this option to balance an access point's 2.4 GHz client load across all channels. This setting is enabled by default.
<b>Balance 5 GHz Channel Loads</b>	Select this option to balance an access point's 5 GHz client load across all channels. This setting is enabled by default.

- 6 Enable **Balance AP Loads** to distribute client traffic evenly amongst neighbor access points.
- 7 Set the following **Band Control** values:

<b>Max. Band Load Difference Considered Equal</b>	Set the maximum load difference (from 1 - 100%) considered equal when comparing band loads. The default setting is 1%.
<b>Band Ratio (2.4 GHz)</b>	Set the relative load for the 2.4 GHz radio band as a leveled ratio from 1 - 10. The default setting is 0.
<b>Band Ratio (5 GHz)</b>	Set the relative load for the 5 GHz radio band as a leveled ratio from 1 - 10. The default setting is 0.
<b>5 GHz load at which both bands enabled</b>	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%.
<b>2.4 GHz load at which both bands enabled</b>	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%.

- 8 Define the following **Neighbor Selection** settings:

<b>Minimal signal strength for common clients</b>	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.
<b>Minimum number of clients seen</b>	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.
<b>Max confirmed neighbors</b>	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.
<b>Minimum signal strength for smart-rf neighbors</b>	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.

- 9 Set the following **Advanced Parameters** for client load balance values:

<b>Max. 2.4 GHz Difference Considered Equal</b>	Set the maximum load difference (from 1 - 100%) considered equal when comparing 2.4 GHz client loads. The default setting is 1%.
<b>Min. Value to Trigger 2.4 Ghz Channel Balancing</b>	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%.

<b>Weightage given to Client Count</b>	Set the weightage (from 1- 100%) applied to client count calculations in the 2.4 GHz radio band. The default setting is 90%.
<b>Weightage given to Throughput</b>	Set the weightage (from 1- 100%) applied to client throughput calculations in the 2.4 GHz radio band. The default setting is 10%.
<b>Max. 5 GHz Difference Considered Equal</b>	Set the maximum load difference (from 1 - 100%) considered equal when comparing 5 GHz client loads. The default setting is 1%.
<b>Min. Value to Trigger 5 Ghz Channel Balancing</b>	Set the threshold (from 1 - 100%) beyond which channel load balancing is triggered in the 5 GHz radio band. The default setting is 5%.
<b>Weightage given to Client Count</b>	Set the weightage (from 1- 100%) applied to client count calculations in the 5 GHz radio band. The default setting is 90%.
<b>Weightage given to Throughput</b>	Set the weightage (from 1- 100%) applied to client throughput calculations in the 5 GHz radio band. The default setting is 10%.

10 Define the following **AP Load Balancing** settings:

<b>Min. Value to Trigger Balancing</b>	Set a value (from 1 - 100%) used to trigger client load balancing when exceeded. The default setting is 5%.
<b>Max. AP Load Difference Considered Equal</b>	Set the maximum load balance differential (from 1 - 100%) considered equal when comparing neighbor access point client loads. The default setting is 1%.
<b>Weightage Given to Client Count</b>	Set the weightage (from 1- 100%) applied to client count in an access point's overall load calculation. The default setting is 90%.
<b>Weightage Given to Throughout</b>	Set the weightage (from 1- 100%) applied to client throughput in an access point's overall load calculation. The default setting is 10%.

11 Select **OK** to save the changes made to the profile's client load balance configuration. Select **Reset** to revert to the last saved configuration.

## Configuring MiNT

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.

For more information, see:

- [Settings](#)
- [IP](#)
- [VLAN](#)

## Settings

To define a profile's MiNT settings:

- 1 Select **MiNT Protocol** from the Advanced Profile's menu item.

- 2 The **Settings** tab displays by default.
- 3 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 the check box to enable a spinner control for setting the Level 1 Area ID between 1 - 4,294,967,295. The default value is disabled.

- 4 Define the following **Device Heartbeat Settings** 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.

- 5 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.
- 6 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, it can be another access point with a path to a controller.

**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, it can be another access point with a path to a controller.

- 7 Select **Tunnel Controller Load Balancing (Level 1)** (if available to your controller) to enable load balancing through a WLAN tunnel controller.



- 4 Set the following **Link IP** parameters to complete the MiNT network address configuration:

<b>IP</b>	Define the IP address used by peers for interoperation when supporting the MINT protocol.
<b>Port</b>	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.
<b>Routing Level</b>	Use the spinner control to define a routing level of either 1 or 2.
<b>Listening Link</b>	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.
<b>Forced Link</b>	Check this box to specify the MiNT link as a forced link.
<b>Link Cost</b>	Use the spinner control to set a link cost between 1 - 10,000. The default value is 100.
<b>Hello Packet Interval</b>	Set an interval in either <i>Seconds</i> (1 - 120) or <i>Minutes</i> (1 - 2) for the transmission of hello packets. The default interval is 15 seconds.
<b>Adjacency Hold Time</b>	Set a hold time interval in either <i>Seconds</i> (2 - 600) or <i>Minutes</i> (1 - 10) for the transmission of hello packets. The default interval is 46 seconds.
<b>IPSec Secure</b>	Enable this option to provide IPSec secure peer authentication on the MiNT connection (link). This option is disabled by default.
<b>IPSec GW</b>	Select the numerical IP address or administrator defined hostname of the IPSec gateway.

## VLAN

To set a profile's MiNT VLAN configuration:

- 1 Select **MiNT Protocol** from the Advanced Profile's menu item.
- 2 Select the **VLAN** tab to display the link IP VLAN information shared by the devices managed by the MiNT configuration.



<b>VLAN</b>	Define a VLAN ID between 1 - 4,094 used by peers for interoperation when supporting the MiNT protocol.
<b>Routing Level</b>	Use the spinner control to define a routing level of either 1 or 2.
<b>Link Cost</b>	Use the spinner control to set a link cost between 1 - 10,000. The default value is 100.
<b>Hello Packet Interval</b>	Set an interval in either <i>Seconds</i> (1 - 120) or <i>Minutes</i> (1 - 2) for the transmission of hello packets. The default interval is 15 seconds.
<b>Adjacency Hold Time</b>	Set a hold time interval in either <i>Seconds</i> (2 - 600) or <i>Minutes</i> (1 - 10) for the transmission of hello packets. The default interval is 46 seconds.

- 5 Select **OK** to save the updates to the MiNT Protocol configuration. Select **Reset** to revert to the last saved configuration.

## Advanced Profile Miscellaneous 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.

The screenshot shows the configuration interface for a device's RADIUS authentication parameters. The sections and their settings are as follows:

- Device RADIUS Authentication Parameters:**
  - NAS-Identifier Attribute: [Empty text field]
  - NAS-Port-Id Attribute: [Empty text field]
- LEDs (Light Emitting Diodes):**
  - Turn on LEDs:
    - Off (0)
    - On (1)
    - Flash Pattern (2)
- RF Domain Manager:**
  - Capable:
  - Priority: [Spinner set to 1] (1 to 255)
- MeshConnex Parameters:**
  - Root Path Monitor Interval: [Spinner set to 30] [Seconds] (1 to 65,535)
- RADIUS Dynamic Authorization:**
  - Additional Port: [Spinner set to 3800] (1 to 65,535) (Cisco ISE:1700)
- Client Bridge:**
  - Aging Time: [Spinner set to 10] [Minutes] (1 to 10,923)

Buttons at the bottom: OK, Reset, Exit.

- 2 Set a **NAS-Identifier Attribute** up to 253 characters in length.

This is the RADIUS NAS-Identifier attribute that typically identifies the device where a RADIUS request 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)** field) to enable the LEDs on an access point.

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 Set the **Meshpoint Behavior** as either an **External (Fixed)** unit or a mobile **Vehicle Mounted** unit.
- 8 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.
- 9 Set the **Additional Port** value for **RADIUS Dynamic Authorization** field. Set this value to 1700 to enable a CISCO Identity Services Engine (ISE) Authentication, Authorization and Accounting (AAA) server, when deployed in the network, to dynamically authenticate a client.

When a client requests access to the network, the CISCO ISE RADIUS server presents the client with a URL where the device's compliance to the networks security such as validity of anti-virus or anti-spyware software is checked for the validity for their definition files (this checking is called posture). If the client device complies, then it is allowed access to the network.

- 10 Set the **Aging Time** value for a dedicated Client Bridge. Use the spinner control to set a value in *Days* (1 -8), *Hours* (1 - 183), *Minutes* (1 - 10, 923) and *Seconds* (10 - 655, 350). The aging time represents the time this MAC address is allowed to remain on the network since its last update. The default setting is 10 minutes.
- 11 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

## Managing 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.

## Managing RF Domains

Managing RF Domains entails setting individual RF Domain configurations and administrating them as a collective set. Remember that access points, unlike controllers and service platforms, use only a single RF Domain shared among peer access points of the same model.

To review the configurations of existing RF Domains:

- 1 Select **Configuration > RF Domains** from the Web UI. Access points select RF Domains using a path of **Configuration > Devices > RF Domains**.

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.

RF Domain				
RF Domain	Location	Contact	Time Zone	Country
CN			Etc/UTC	China-cn
default			Asia/Calcutta	India-in
khepri			Etc/UTC	Algeria-dz
mesh domain			Etc/UTC	United States-us
rf 1			Etc/UTC	India-in
rf 2			Etc/UTC	United Kingdom-gb
rf 3			Etc/UTC	China-cn
rf 4			Etc/UTC	India-in
rf 4US			Etc/UTC	United States-us
rf US			Etc/UTC	United States-us
simba	munchen		Etc/UTC	Germany-de

Type to search in tables Row Count: 11

**Figure 226: 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 access point at one time.
Location	Displays the physical location assigned to the 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 devices are deployed using the policy's RF Domain configuration.
Contact	Lists the contact (administrator) assigned to respond to events created by, or impacting, each listed RF Domain.
Time Zone	Displays the geographic time zone set for each RF Domain policy. RF Domains can contain unique country codes and time zone information for controllers and access points deployed across different states or countries, thus making them ideal for managing device configurations across different geographical deployments.
Country Code	Display 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 an existing policy and review the members of that controller, service platform or access point RF Domain.



**Figure 227: 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](#) on page 692
  - [RF Domain Sensor Configuration](#) on page 695
  - [RF Domain Client Name Configuration](#) on page 697
  - [RF Domain Overrides](#) on page 698
  - [RF Domain Network Alias](#) on page 704

## RF Domain Basic Configuration

An administrator needs to set RD Domain deployment values, Smart RF policy and override settings, smart scan channel assignments, WIPS policy and stat fetching configuration as part of a RF Domain's unique basic configuration:

To set a RF 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 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**.

- 3 If you are adding or modifying an existing RF Domain, the **RF Domain Basic Configuration** screen displays by default.

**Basic Configuration**

Location: san jose

Contact: percy hilton

Time Zone: (GMT) Etc/UTC

Country: Algeria-dz

VLAN for Control Traffic:  1 (1 to 4,094)

Controller Managed:

**SMART RF**

SMART RF Policy: analytics Smart-rf policy

Override Channel List 2.4 GHz: Select

Override Channel List 5 GHz: Select

**Smart Scan**

Enable Dynamic Channel:

2.4 GHz Channels: 1,2,3,4,...

5 GHz Channels: 21,25,34,36,...

**Wireless IPS**

WPS Policy: <none>

**Statistics**

Update Interval: 0 (0,5-300 seconds)

Window Index	Sample Interval	Window Size
1	5	3

+ Add Row

OK Reset Exit

**Figure 228: RF Domain - Basic Configuration Screen**

- 4 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 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	Displays the geographic time zone set for each RF Domain policy. RF Domains can contain unique country codes and time zone information to controllers, service platforms and access points deployed across different states or countries, thus making them ideal for managing device configurations across different geographical deployments.

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.

- 5 Define the following **SMART RF** parameters for the RF Domain:

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. Manual detector radio selection can also be made using visualizations from the LANPlanner tool.

For an overview of Smart RF and instructions on how to create a Smart RF policy that can be used with an RF Domain, see [Smart RF Policies](#) on page 395.

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.

- 6 Define the following RF Domain **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.

- 7 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 760.

- 8 Refer to the **Statistics** field to define how RF Domain stats are updated.

Update Interval	Set an interval of 0 or from 5-3600 seconds for update retrievals.
Window Index	Use the spinner control to set a numerical index used as an identifier for each RF Domain statistic defined.
Sample Interval	Use the spinner control to define the interval (in seconds) to capture windowed statistics supporting a RF Domain configuration. The default is 5 seconds.
Window Size	Use the spinner control to set the number of samples used to represent a RF Domain statistic. The default value is 6 samples.

- 9 Select **OK** to save the changes or **Reset** to revert to the last saved configuration.

## RF Domain Sensor Configuration

The Wireless Intrusion Protection System (WIPS) protects clients and access point radio traffic from attacks and unauthorized wireless network 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 wired and wireless device lockdowns upon threat acknowledgement.

In addition to dedicated AirDefense sensors, an access point radio can function as a sensor and upload information to an external WIPS server. Unique WIPS server configurations can be used by RF Domains to ensure a WIPS server configuration 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 the 2.4 and 5.0 GHz radio bands. 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 AP 7522, AP 7532, AP 7562, AP 8432 and AP 8533 model access points can also function as ExtremeLocation sensors. ExtremeLocation 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 ExtremeLocation server should be up and running and the RF Domain Sensor configuration should point to the ExtremeLocation server.

To define a WIPS server 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 **Sensor** item from within the RF Domain screen.

**Sensor Policy**

Sensor Policy

**Note:** If the sensor is being used by ADSP for WIPS, any policy selected here will be discarded by the sensor. Please use ADSP channel settings instead to configure the sensor

**ExtremeLocation Appliance Configuration**

Server Id	IP Address/Hostname	Port	

**ExtremeLocation Tenant Account**

Tenant Account

**Sensor Appliance Configuration**

Server Id	IP Address/Hostname	Port	

**NSight Sensor**

Enable NSight Sensor

OK Reset Exit

**Figure 229: RF Domain - Sensor Screen**

- 3 Use the **Sensor Policy** drop-down menu to select a Sensor policy to send RSSI information to a dedicated system for device locationing calculations. If no Sensor policy exists, use the **Create** icon to create a new Sensor policy. Or, use the **Edit** icon to edit an existing Sensor policy if required.

Different policies can be created with either a default set of scanned channels or with custom channels, widths and weighted scan priorities. Specific channels can also be isolated and locked for specific channel scans.

If a dedicated sensor is utilized with ADSP 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.

- 4 Select the **+ Add Row** button to populate the **ExtremeLocation Appliance Configuration** table with up to one ExtremeLocation server credentials.



Server Id	Use the spinner control to assign a DNS hostname of the ExtremeLocation resource. As of now only one (1) ExtremeLocation sever can be configured.  <b>Note:</b> The ExtremeLocation sensor capabilities are supported only on the AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 8432, and AP 8533model access points.
IP Address/Hostname	Provide the ExtremeLocation server's hostname. When configured, access points within the RF Domain post location-related analytics to the specified ExtremeLocation server.  <b>Note:</b> Enter the server's hostname and not the IP address, as the IP address is likely to change periodically in order to balance load across multiple Location server instances.
Port	Use the spinner control to specify the port for the ExtremeLocation server. This is the port on which the ExtremeLocation server is reachable. The default port is 443.

- 5 Enter the ExtremeLocation Tenant's account number in the **Tenant Account** field.

Use this field to configure your ExtremeLocation Tenant account number. ExtremeLocation Tenants, at the time of registration, are communicated (via email) an account number uniquely identifying the Tenant. Configure this account number in the RF Domain context. When configured, RF Domain AP reports, pushed to the ExtremeLocation server, include the Tenant's account number along with the reporting AP's MAC address. Including the Tenant account number reinforces the Tenant's identity..

- 6 Select the **+ Add Row** button to populate the **Sensor Appliance Configuration** table with up to three rows for server credentials:

Server Id	Use the spinner control to assign a numerical ID for up to three ADSP 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 ADSP 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 ADSP sensor server utilized by RF member devices. The default port is 443.

- 7 Select the **Enable NSight Sensor** option, within the NSight Sensor field, to enable the sensor module. This option is disabled by default.
- 8 Select **OK** to save the changes to the Sensor configuration, or select **Reset** to Revert to the last saved configuration.

## RF Domain Client Name Configuration

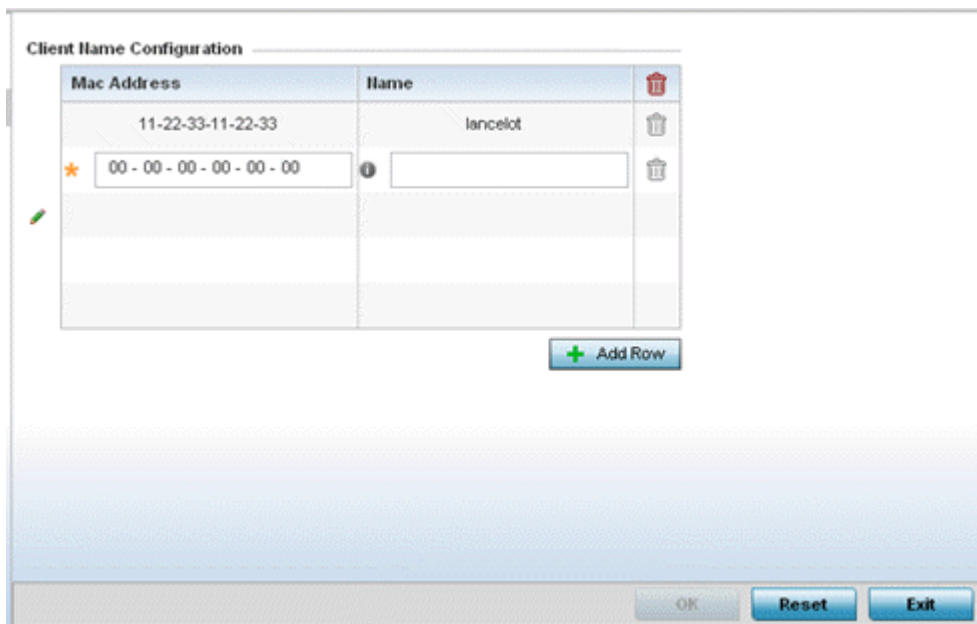
The **Client Name Configuration** screen displays clients connected to RF Domain member access points adopted by networked controllers or service platforms. Use the screen to associate administrator assigned client names to specific connected client MAC addresses for improved client management..

To define a client name configuration used with 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 **Client Name Configuration** item from within the **RF Domain** screen.



**Figure 230: 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.

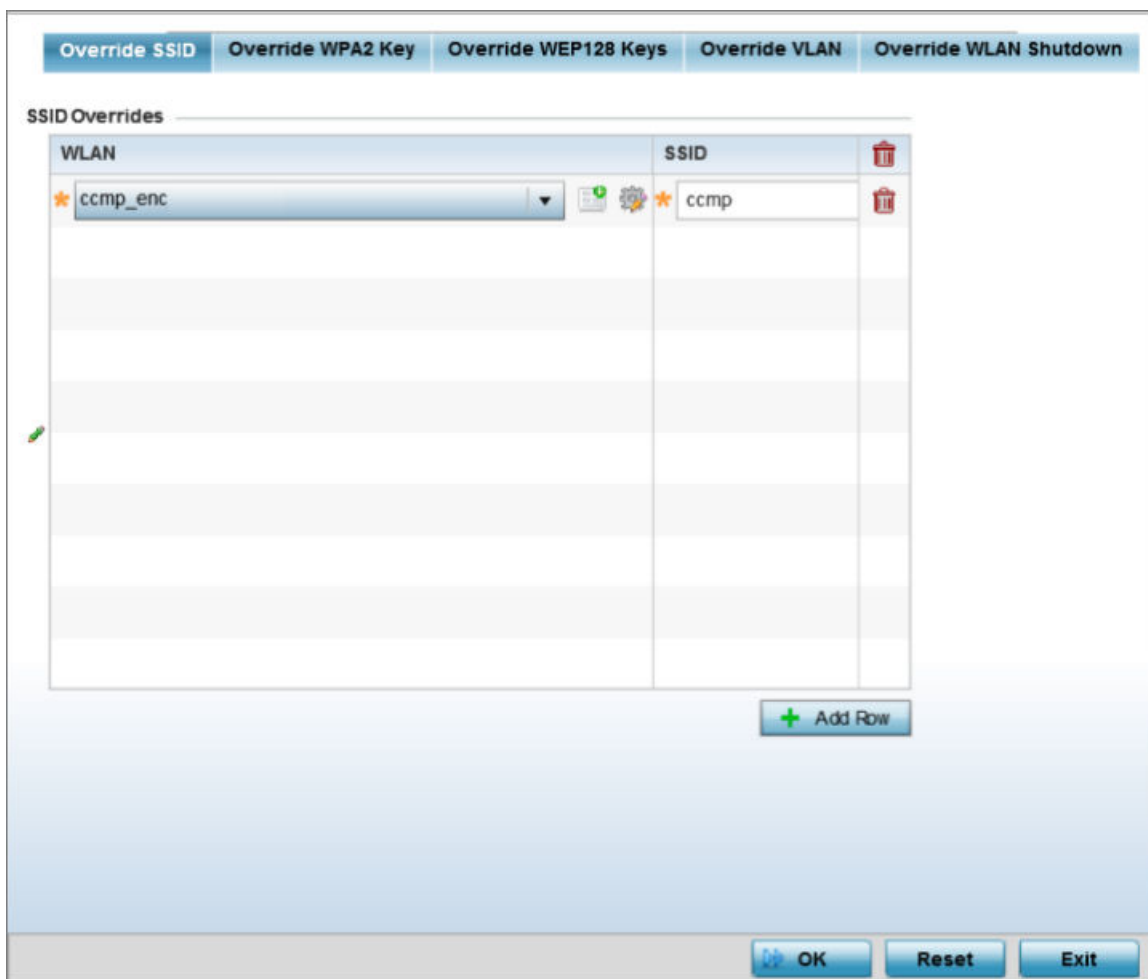
## RF Domain Overrides

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 231: RF Domain Override SSID Screen**

The **Overrides** screen is partitioned into two tabs, with the **Override SSID** screen displayed by default.

- 3 Select the **+ Add Row** button to create a new Override SSID configuration.  
To remove an existing Sensor Server Configuration from the table, highlight it and select the **Delete** icon.
- 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, 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](#).
- 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 232: 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 <b>Edit</b> 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 WEP 128 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 WLANs whose WEP 128 key configuration can be overridden at the RF Domain level. Either select **Add** to create a new WEP 128 key configuration, or select an existing WEP 128 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.

The screenshot shows the 'WEP128 Key Overrides' configuration window. It features a 'Transmit Key' dropdown menu at the top. Below it, there is a 'Generate Keys' section with a text input field and a 'Generate' button. The main configuration area contains four rows for 'WEP128 Key 1' through 'WEP128 Key 4'. Each row includes a text input field, a dropdown menu set to 'HEX', a 'Show' button, and a radio button labeled 'Transmit Key'. A 'Restore Default WEP Keys' button is located below the key rows. At the bottom of the window, there are 'OK', 'Reset', and 'Exit' buttons.

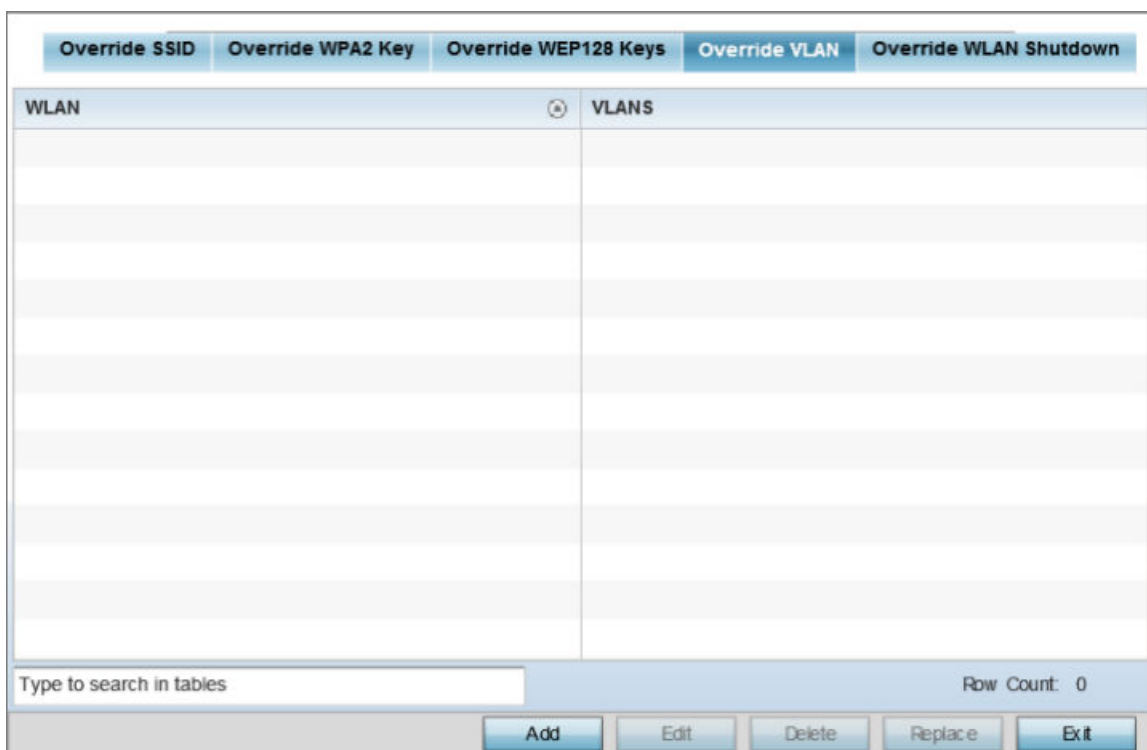
**Figure 233: RF Domain Override WEP128 Keys Screen**

- 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 <b>Generate</b> 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: <ul style="list-style-type: none"> <li>• Key 1 101112131415161718191A1B1C</li> <li>• Key 2 202122232425262728292A2B2C</li> <li>• Key 3 303132333435363738393A3B3C</li> <li>• Key 4 404142434445464748494A4B4C</li> </ul>

- 12 Select **OK** to save the changes to the Override WEP 128 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 234: RF Domain Override VLAN screen**

- 14 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

The screenshot shows the 'VLAN Overrides' configuration window for the WLAN 'ccmp\_enc'. The window title is 'VLAN Overrides'. Below the title bar, there is a dropdown menu for 'WLAN' set to 'ccmp\_enc'. The main area is titled 'Override VLAN Pool for WLAN' and contains a table with two columns: 'VLAN' and 'Wireless Client Limit'. The table has three rows. The first row has '2' in the 'VLAN' column and '10' in the 'Wireless Client Limit' column. The second row has '1' in the 'VLAN' column and '0' in the 'Wireless Client Limit' column, with orange asterisks next to the input fields. The third row is empty. To the right of each row is a red trash icon. Below the table is a '+ Add Row' button. At the bottom of the window are three buttons: 'OK', 'Reset', and 'Exit'.

VLAN	Wireless Client Limit	
2	10	
* 1	* 0	

**Figure 235: 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.

The screenshot displays a configuration window titled "WLAN Shutdown n Overrides". At the top, there are five tabs: "Override SSID", "Override WPA2 Key", "Override WEP128 Keys", "Override VLAN", and "Override WLAN Shutdown", with the last one being active. Below the tabs is a table with two columns: "WLAN" and "Shutdown". The "WLAN" column has a dropdown menu open, showing three options: "ccmp\_enc", "eapauth", and "open". The "Shutdown" column has a checkbox. Below the table is a "+ Add Row" button. At the bottom of the window are three buttons: "OK", "Reset", and "Exit".

**Figure 236: 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.

## 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 a 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](#)

### *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.

- 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**.

- Expand the **Network** menu item and select **Alias**.

The **Alias** screen displays with the Basic Alias tab displayed by default.

Basic Alias | Network Group Alias | Network Service Alias

Delete button is enabled only for entries created in this context.

**Vlan Alias**

Name	Vlan	
* \$lanelot	2	

+ Add Row

**Host Alias**

Name	Host	
* \$rudskipper	157.235.35.255	

+ Add Row

**Address Range Alias**

Name	Start IP	End IP	
* \$renegade	157.235.212	157.235.242	

+ Add Row

**Network Alias**

Name	Network	
* \$percival	157.235.242.42 / 42	

+ Add Row

OK Reset Exit

**Figure 237: RF Domain Network Basic Alias Screen**

- 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 you are adding a new VLAN Alias, give 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 you are adding a new Address Alias, give 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 you are adding a new Host Alias, give it a distinguishing name up to 32 characters. The alias name always starts with a dollar sign (\$).
Host	Lists 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 you are adding a new Network Alias, give 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 to its last saved configuration.

### *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 edit or delete a network alias configuration:

- 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.

Name	Host	Network
\$alias2	157.235.123.131	157.235.123.123/15

Type to search in tables Row Count: 1

**Figure 238: RF Domain Network Group Alias Screen**

Name	Displays the administrator assigned name assigned 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 239: RF Domain Network Group Alias Add Screen**

- 7 If adding a new Network Alias Rule, give 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 In 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 an existing alias range entry to edit it.
- 10 Select **OK** when completed to update the network alias rules. Select **Reset** to revert the screen to its last saved configuration.

### *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 two source port ranges and up

to two destination port ranges can be configured. A maximum of four 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:

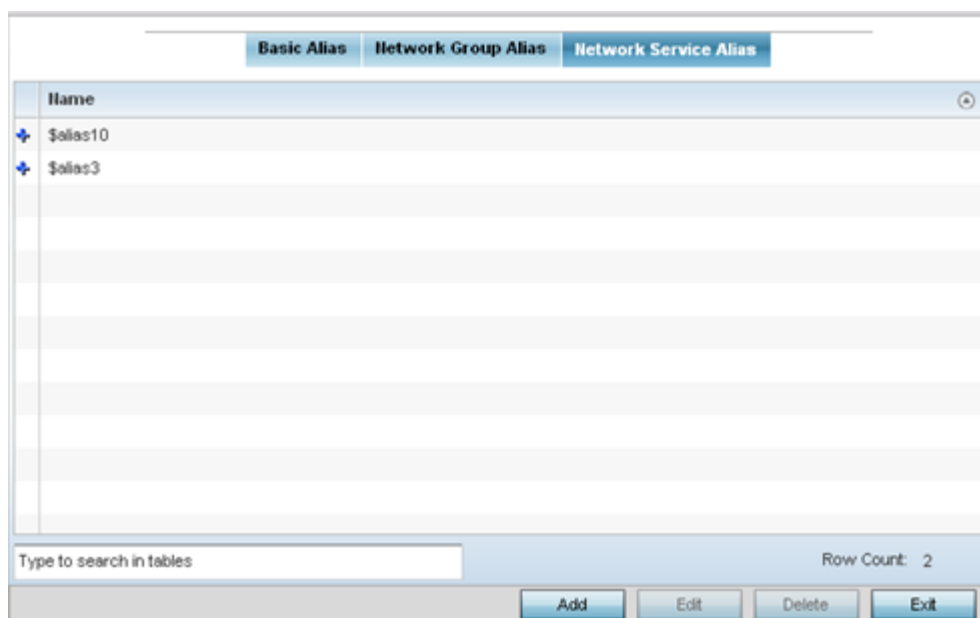
- 1 Select **Configuration** > **RF Domains** from the Web UI.

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 the attributes of existing network group alias configurations.



**Figure 240: 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 241: RF Domain Network Service Alias Add Screen**

- 7 If adding a new Network Service Alias Rule, give 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 <b>eigrp</b> , <b>gre</b> , <b>icmp</b> , <b>igmp</b> , <b>ip</b> , <b>vrrp</b> , <b>igp</b> , <b>ospf</b> , <b>tcp</b> , and <b>udp</b> . Select <b>other</b> 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 relevant only if the protocol is either <b>tcp</b> or <b>udp</b> . Specify the source ports for this protocol entry. A range of ports can be specified. Select the <b>Enter Ranges</b> 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 relevant only if the protocol is either <b>tcp</b> or <b>udp</b> . Specify the destination ports for this protocol entry. A range of ports can be specified. Select the <b>Enter Ranges</b> button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

- 9 In 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 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 to its last saved configuration.

## RF Domain Deployment Considerations

Before settings RF Domains for controllers, service platforms and access points, refer to the following deployment guidelines to ensure the configurations are optimally effective:



- Each controller 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, 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 controllers and access points assigned to the RF Domain.

# 10 Security Configuration

Wireless Firewall  
Configuring IP Firewall Rules  
Wireless Client Roles  
Device Fingerprinting  
Intrusion Prevention  
EX3500 Time Range

When taking precautions to secure wireless traffic between a client and an access point, the network administrator should not lose sight of the security solution in its entirety, because the network's chain is as weak as its weakest link. A WiNG-managed wireless 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. They are 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-and location-based secure access available to users based on identity and on the security posture of the client device.

When addressing the security of a WiNG-managed wireless network, consider each of the following:

- [Wireless Firewall](#)
- [Configuring IP Firewall Rules](#) on page 732
- [Wireless Client Roles](#)
- [Device Fingerprinting](#)
- [Intrusion Prevention](#)
- [EX3500 Time Range](#) on page 773

## Wireless Firewall

A Firewall enforces access control and is considered a first line of defense in protecting proprietary information within the access-point managed 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 in the network. Because firewalls implement uniquely defined access control policies, they are of little value unless you have a clear idea of what kind of access to allow or deny. In such an instance, in fact, a firewall could provide a false sense of security.

With WiNG 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 while permitting authorized users to communicate freely outside the network.

Firewalls can be implemented in both hardware and software, or a combination of both. All traffic entering or leaving a controller, service platform, or access point passes through the firewall, which examines each message and blocks those that do not meet 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 that a controller, service platform, or access point is processing, the firewall uses that rule's action to determine whether to allow or deny the traffic.

Rules have two parts:

- A *condition* describes a traffic packet stream. It defines constraints on source and destination devices, the service (protocols and ports), and the incoming interface.
- An *action* describes what happens to packets matching the conditions that have been set. For example, if the packet stream meets all conditions, then traffic is permitted, authenticated, and sent to the destination device.

Additionally, IP and MAC rule-based firewall filtering can be deployed to apply firewall policies to traffic bridged by centrally managed radios. IP and MAC filtering permits or restricts 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](#)

## Configuring a Firewall Policy

Firewall configurations can be defined as separate policies available to the administrator for specific controller, service platform or access point deployments.

To define a firewall configuration:

- 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 policies for review.

Firewall Policy	Status	Proxy ARP
default	Enabled	✓
policy2	Enabled	✓

Type to search in tables

Row Count: 2

Buttons: Add, Edit, Delete, Copy, Rename

**Figure 242: 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.

When adding a new firewall policy, begin by entering a name for the policy (not to exceed 64 characters). Then 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](#) on page 716 (displayed by default)
- [Firewall Policy Storm Control](#) on page 720
- [Firewall Policy Advanced Settings](#) on page 722

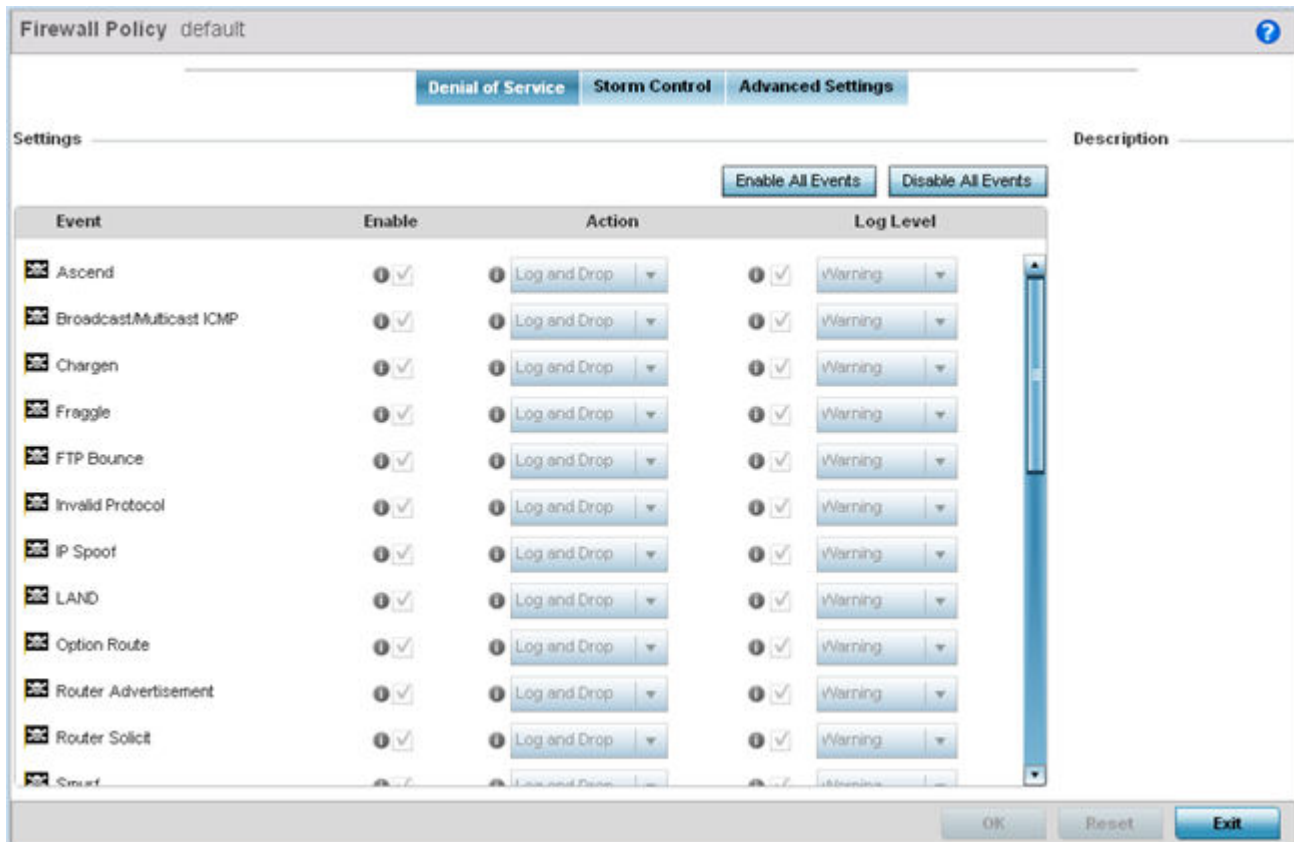
### *Firewall Policy Denial of Service*

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 243: Wireless Firewall - Add/Edit - Denial of Service Screen**

- 2 The **Settings** window contains a list of all of the Denial of Service (DoS) attacks for which the wireless controller's firewall has filters.

Each DoS filter contains the following items:

Event	Lists the name of each DoS attack.
Enable	Checking the <b>Enable</b> 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. <ul style="list-style-type: none"> <li>• Log and Drop - An entry for the associated DoS attack is added to the log and then the packets are dropped.</li> <li>• Log Only - An entry for the associated DoS attack is added to the log. No further action is taken.</li> <li>• Drop Only - The DoS packets are dropped. No further action is taken.</li> </ul>
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 <b>Log Level</b> drop-down menu.

## 3 Refer to the following for a summary of each Denial of Service attack the firewall can filter.

Ascend	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, called 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	<p>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.</p> <p>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.</p>
TCP Intercept	<p>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.</p> <p>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.</p> <p>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.</p>
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	<p>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.</p> <p>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.</p>
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 System (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	Enables the check for Hop Limit in IPv6 packets. If the value is zero, it is considered a DoS and is blocked.
Multicast ICMPv6	The Multicast ICMPv6 attack sends multicast ICMPv6 packets. This is applicable to only ICMPv6 Echo request/reply packets.
TCP Intercept Mobility	Enables the detection of IPv6 TCP packets with mobility option Home- Address- Option (HAO) or RH (Routing Header) type two and does not generate TCP syn cookies for these packets.

- 4 Events can be individually enabled or collectively enabled/disabled using the **Enable All Events** and **Disable All Events** buttons.
- 5 Select **OK** to update the Denial of Service settings.  
Select **Reset** to revert to the last saved configuration.

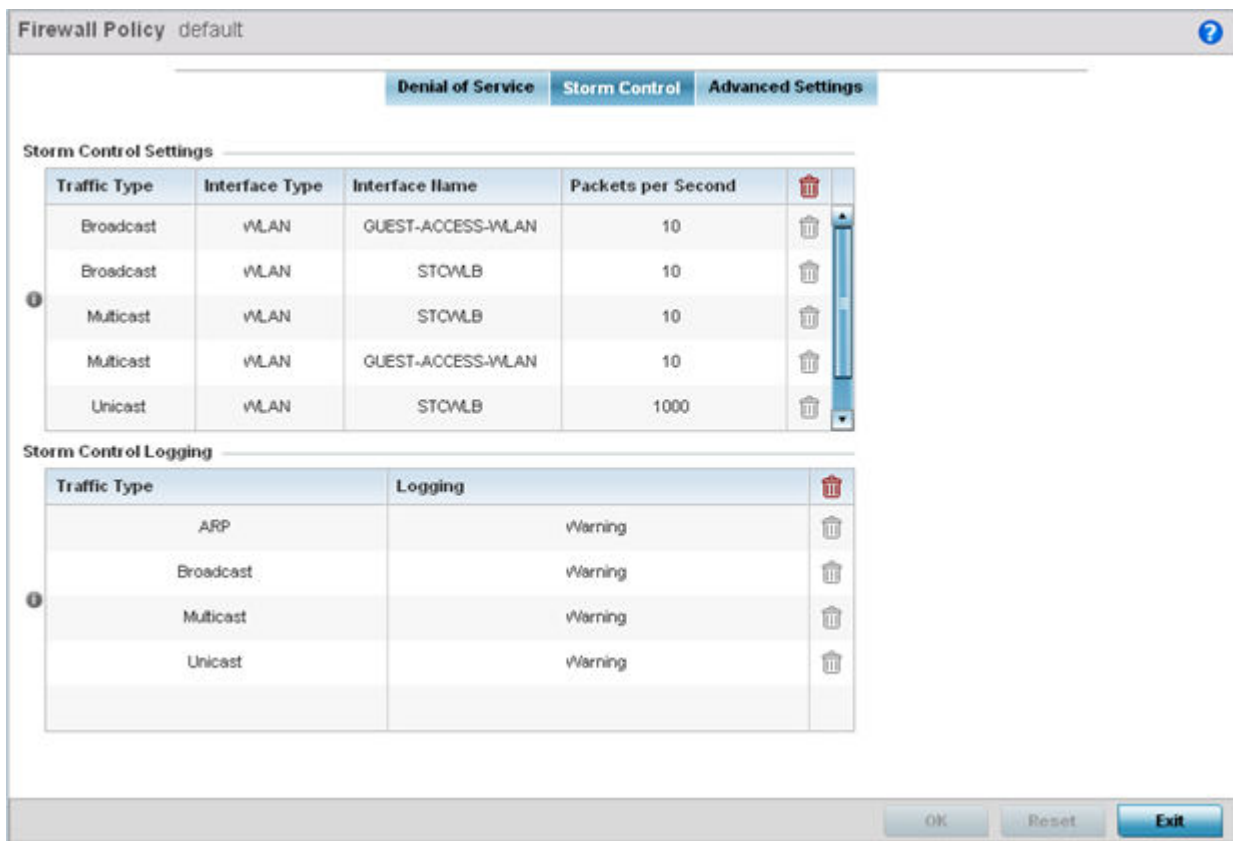
### *Firewall Policy Storm Control*

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 244: 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.

### Firewall Policy Advanced Settings

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 245: Wireless Firewall - Add/Edit - Advanced Settings - Common Tab**

- 2 Refer to the **Firewall Status** radio buttons to define the firewall as either enabled or disabled.

The firewall is enabled by default.

If you are disabling the firewall, a confirmation prompt displays stating NAT, wireless hotspot, proxy ARP, deny-staticwireless- 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	Select 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 <b>Seconds</b> (1 - 32,400), <b>Minutes</b> (1 - 540) or <b>Hours</b> (1 - 9). The default setting is 10 seconds.
TCP Established	Define a flow timeout value in either <b>Seconds</b> (1 - 32,400), <b>Minutes</b> (1 - 540) or <b>Hours</b> (1 - 9). The default setting is 90 minutes.
TCP Reset	Define a flow timeout value in either <b>Seconds</b> (1 - 32,400), <b>Minutes</b> (1 - 540) or <b>Hours</b> (1 - 9). The default setting is 10 seconds.

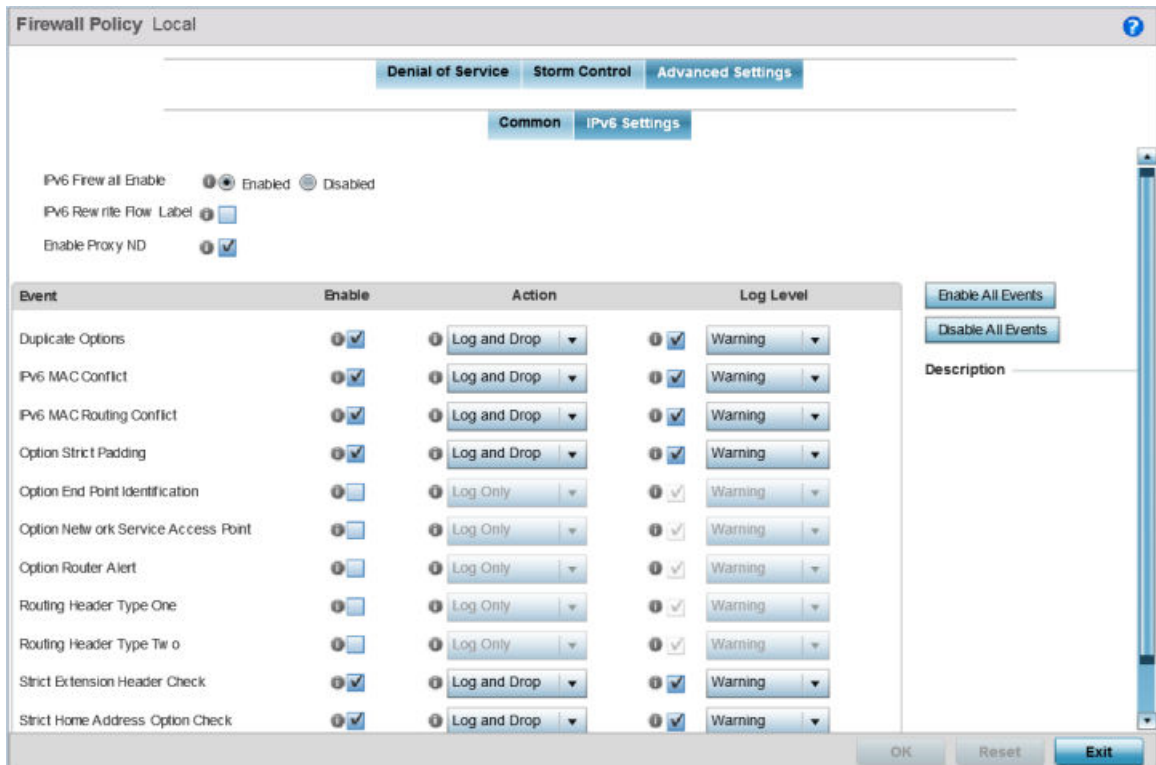
TCP Setup	Define a flow timeout value in either <b>Seconds</b> (1 - 32,400), <b>Minutes</b> (1 - 540) or <b>Hours</b> (1 - 9). The default setting is 10 seconds.
Stateless TCP Flow	Define a flow timeout value in either <b>Seconds</b> (1 - 32,400), <b>Minutes</b> (1 - 540) or <b>Hours</b> (1 - 9). The default setting is 90 seconds.
Stateless FIN/RESET Flow	Define a flow timeout value in either <b>Seconds</b> (1 - 32,400), <b>Minutes</b> (1 - 540) or <b>Hours</b> (1 - 9). The default setting is 10 seconds.
ICMP	Define a flow timeout value in either <b>Seconds</b> (1 - 32,400), <b>Minutes</b> (1 - 540) or <b>Hours</b> (1 - 9). The default setting is 30 seconds.
UDP	Define a flow timeout value in either <b>Seconds</b> (1 - 32,400), <b>Minutes</b> (1 - 540) or <b>Hours</b> (1 - 9). The default setting is 30 seconds.
Any Other Flow	Define a flow timeout value in either <b>Seconds</b> (1 - 32,400), <b>Minutes</b> (1 - 540) or <b>Hours</b> (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 246: Wireless Firewall - Add/Edit - Advanced Settings - IPv6 Settings Tab**

- 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 <b>Event</b> column lists the name of each IPv6 specific event subject to logging.
Enable	Checking <b>Enable</b> sets the firewall policy to filter the associated IPv6 event based on the selection in the Action column.
Action	If a filter is enabled, chose an action from the drop-down menu to determine how the firewall treats the associated IPv6 event. <ul style="list-style-type: none"> <li>• Log and Drop - An entry for the associated IPv6 event is added to the log and then the packets are dropped.</li> <li>• Log Only - An entry for the associated IPv6 event is added to the log. No further action is taken.</li> <li>• Drop Only - The packet is dropped. No further action is taken.</li> </ul>
Log Level	To enable logging to the system log, check the box in the <b>Log Level</b> column. Then select a standard Syslog level from the <b>Log Level</b> drop-down menu.

- 15 Select **OK** to update the firewall policy's advanced IPv6 settings.  
Select **Reset** to revert to the last saved configuration.

## Configuring MAC Firewall Rules

Access points can use MAC based firewalls like Access Control Lists (ACLs) to filter and 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.

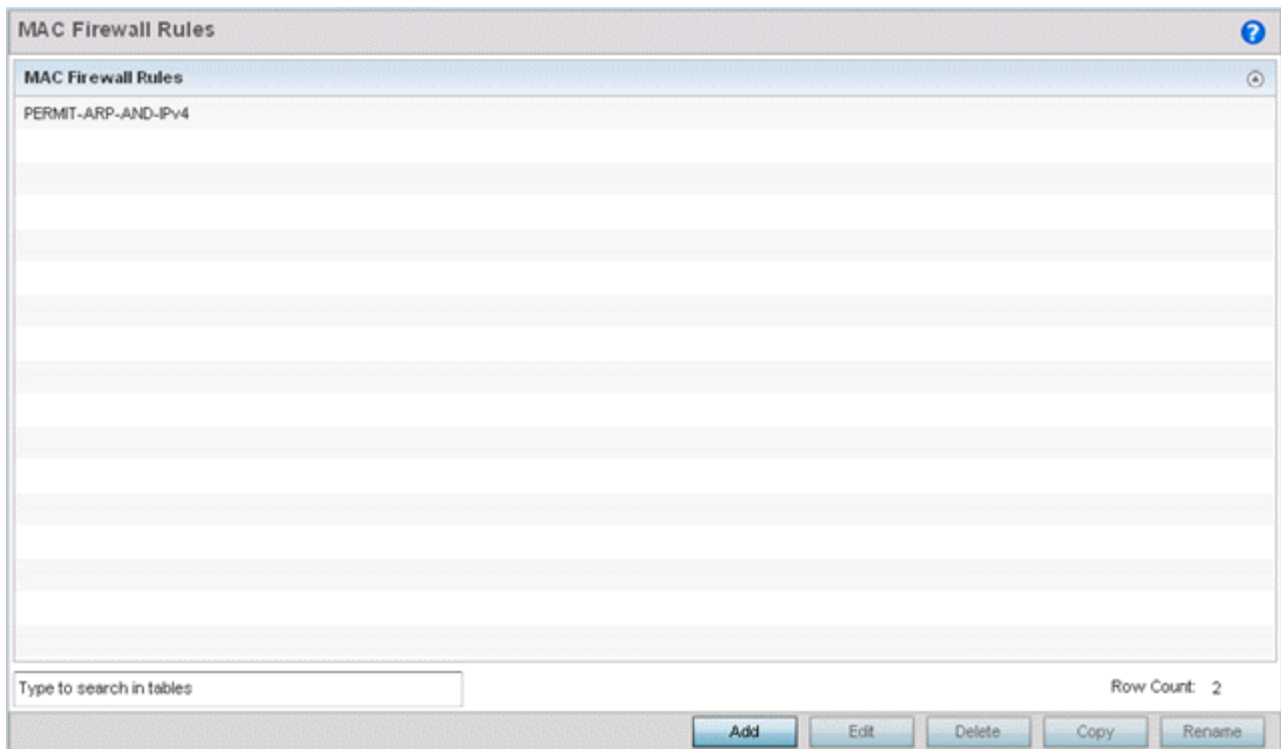


### Note

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 247: 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.

The screenshot displays the 'MAC Firewall Rules' configuration interface for 'EX3500 MAC ACL'. It features a table with two columns: 'Precedence' and 'Rules'. Rule 10 is selected and expanded, showing the following configuration:

- Allow:** Permit
- Source MAC:** Any
- Destination MAC:** Any
- Actions:** Log, Mark, Traffic Class 0, Ethertype: ipv4 (0x0800)
- Description:** "permit all IPv4 traffic"

At the bottom of the screen, there are buttons for '+ Add Row', '- Delete Row', 'OK', 'Reset', and 'Exit'.

**Figure 248: MAC Firewall Rules - Add/Edit screen**

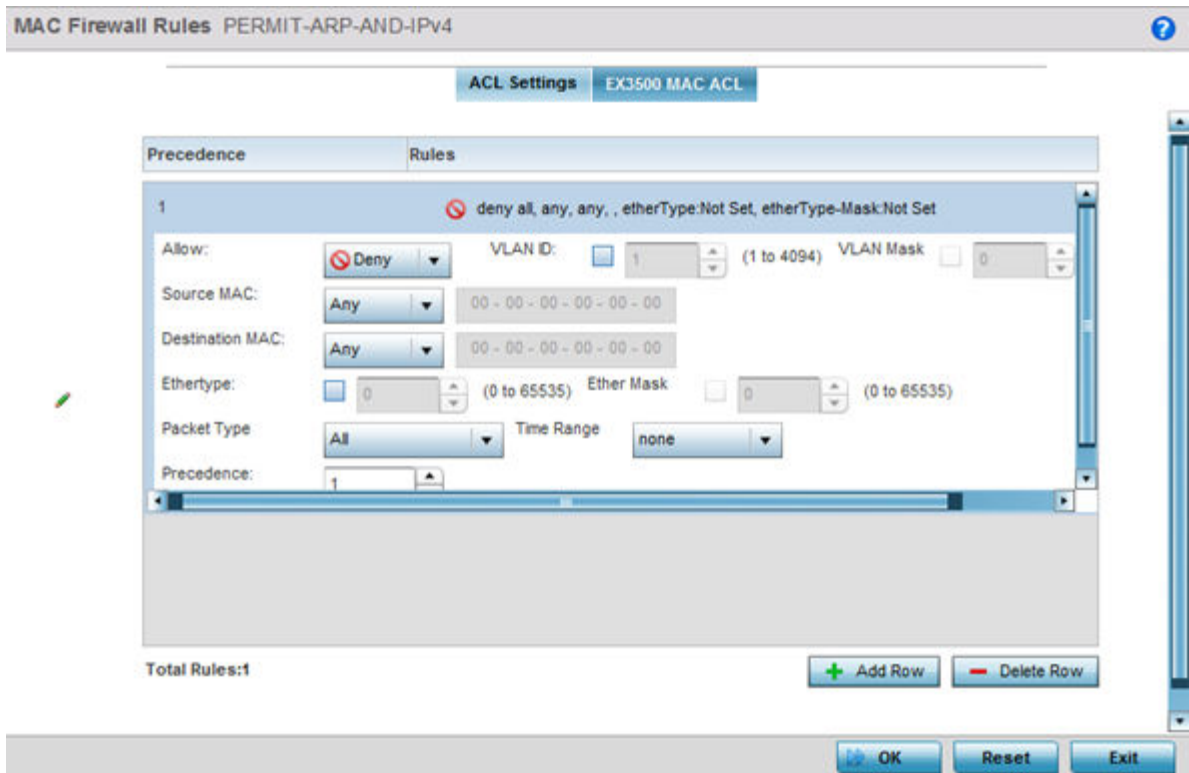
- 4 If adding a new **MAC Firewall Rule**, provide a name up to 32 characters to help describe its filtering configuration.
- 5 Select a rule to modify it.

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: <ul style="list-style-type: none"> <li>Deny - Instructs the firewall to prevent a packet from proceeding to its destination when filter conditions are met.</li> <li>Permit - Instructs the firewall to allow a packet to proceed to its destination when filter conditions are met.</li> </ul>
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 MAC 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: <ul style="list-style-type: none"> <li>Log - Events are logged for archive and analysis.</li> <li>Mark - Modifies certain fields inside the packet and then permits them. Therefore, mark is an action with an implicit permit. <ul style="list-style-type: none"> <li>VLAN 802.1p priority.</li> <li>DSCP bits in the IP header.</li> <li>TOS bits in the IP header.</li> </ul> </li> <li>Mark, Log - Conducts both mark and log functions.</li> </ul>
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 it from others with similar configurations.

- 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.
- Select the 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 249: EX3500 MAC ACL Add/Edit Screen**

## 8 Select a rule to modify it.

Define 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: <ul style="list-style-type: none"> <li>Deny - Instructs the firewall to prevent a packet from proceeding to its destination.</li> <li>Permit - Instructs the firewall to allow a packet to proceed to its destination.</li> </ul>
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 <a href="#">EX3500 Time Range</a> on page 773.
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.

## Firewall Deployment Considerations

Before defining a unique controller, service platform or access point Firewall access policy, 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 is 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 captive portal network access. Firewall policies should be applied to captive portal enabled WLANs to prevent guest user traffic from being routed to trusted networks and hosts.

## Configuring IP Firewall Rules

---

IP-based firewalls function like Access Control Lists (ACLs) to filter or mark packets, as opposed to filtering packets on Layer 2 ports.

IP-based Firewall rules are specific to *source* and *destination* IP addresses and the unique *rules* and *precedence* definitions 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 both IPv4 and IPv6, if you intend to deny specific types of packets, we recommend that you create access rules for traffic entering a controller, service platform, or access point interface before the controller, service platform, or access point spends time processing them. This is because 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:

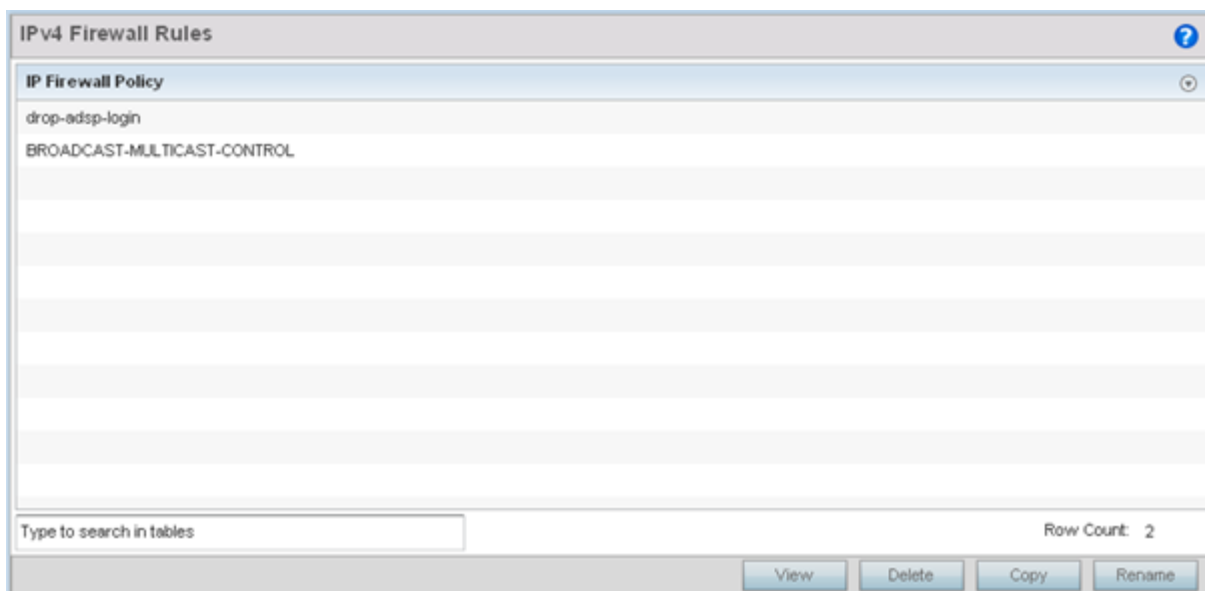
- [Setting an IP SNMP ACL Policy](#) on page 737
- [Setting a Network Service Alias](#) on page 740
- [EX3500 ACL Standard](#) on page 742

## 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**.

- Expand the **IP Firewall** menu item and select either the **IPv4 ACL** or **IPv6 ACL** menu option.  
Either the **IPv4 Firewall Rules** screen or the **IPv6 Firewall Rules** screen displays the existing policies defined thus far.



**Figure 250: IP Firewall Rules Screen**

- 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.

- Select the added row to expand it into configurable parameters for defining the IPv4 or IPv6 based firewall policy.

IP Firewall Policy BROADCAST-MULTICAST-CONTROL

	Precedence	Action	Source	Destination	Protocol	Mark	Log	Enable	Description
	10	Allow	0.0.0.0/	0.0.0.0/0	TCP	<input type="checkbox"/> Mark	<input type="checkbox"/> Log	<input checked="" type="checkbox"/> Enable	*permit all TCP
	11	Allow	0.0.0.0/	0.0.0.0/0	UDP SPort 67, DPort 68	<input type="checkbox"/> Mark	<input type="checkbox"/> Log	<input checked="" type="checkbox"/> Enable	*permit DHCP r
	20	Deny	0.0.0.0/	0.0.0.0/0	UDP SPort 137-138, DPort 13	<input type="checkbox"/> N/A	<input type="checkbox"/> Log	<input checked="" type="checkbox"/> Enable	*deny window
	21	Deny	0.0.0.0/	224.0.0.0/4	IP	<input type="checkbox"/> N/A	<input type="checkbox"/> Log	<input checked="" type="checkbox"/> Enable	*deny IP multic
	22	Deny	0.0.0.0/	255.255.25	IP	<input type="checkbox"/> N/A	<input type="checkbox"/> Log	<input checked="" type="checkbox"/> Enable	*deny IP local
	100	Allow	0.0.0.0/	0.0.0.0/0	IP	<input type="checkbox"/> Mark	<input type="checkbox"/> Log	<input checked="" type="checkbox"/> Enable	*permit all IP tr

Type to search in tables

Add Insert Remove

Edit Rule Drag and Drop

OK Reset Exit

Figure 251: IPv4 Firewall Rules - Add/Edit Screen

IPv6 Firewall Policy

	Precedence	Action	Source	Destination	Protocol	Mark	Log	Description
	1	Deny	Any	Any	other	<input type="checkbox"/> N/A	<input type="checkbox"/> Log	
	2	Allow	Any	Any	IPv6	<input checked="" type="checkbox"/> Traffic Class	<input checked="" type="checkbox"/> Log	

Type to search in tables

Add Remove

Edit Rule

OK Reset Exit

Figure 252: IPv6 Firewall Rules - Add/Edit 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.

The screenshot displays the 'Add Criteria' configuration screen for an IP firewall rule. The fields are as follows:

- Precedence:** 20
- Allow:**  Allow;  Deny
- Source:** network; 0 . 0 . 0 . 0 / 0
- Destination:** network; 0 . 0 . 0 . 0 / 0
- Network Service Alias:** \$
- Protocol:** UDP; 17
- Source Port:** range; Low 137; High 138
- Destination Port:** range; Low 137; High 138
- Show More Options

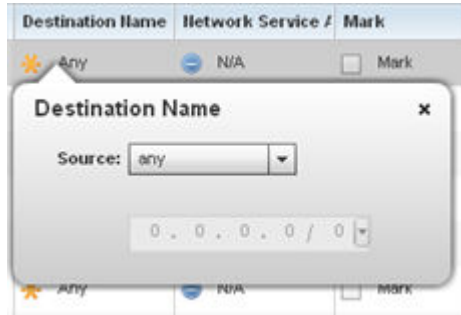
**Figure 253: IP Firewall Rules - Add Criteria Screen**

- 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.

The screenshot shows a 'Select columns' pop-up dialog with the following options:

- Source
- Destination Name
- Network Service Alias
- Source Port
- Destination Port
- ICMP Type
- ICMP Code
- Start Vlan

**Figure 254: IP Firewall Rules - Select Columns Pop-up**



**Figure 255: IP Firewall Rules - Add/Edit - Specific Criteria Pop-up**



**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: <ul style="list-style-type: none"> <li>Deny - Instructs the firewall to restrict a packet from proceeding to its destination.</li> <li>Permit - Instructs the firewall to allow a packet to proceed to its destination.</li> </ul>
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 <b>Mark</b> check box 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 <b>Log</b> check box 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 <b>Select Columns</b> 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 to its last saved configuration.

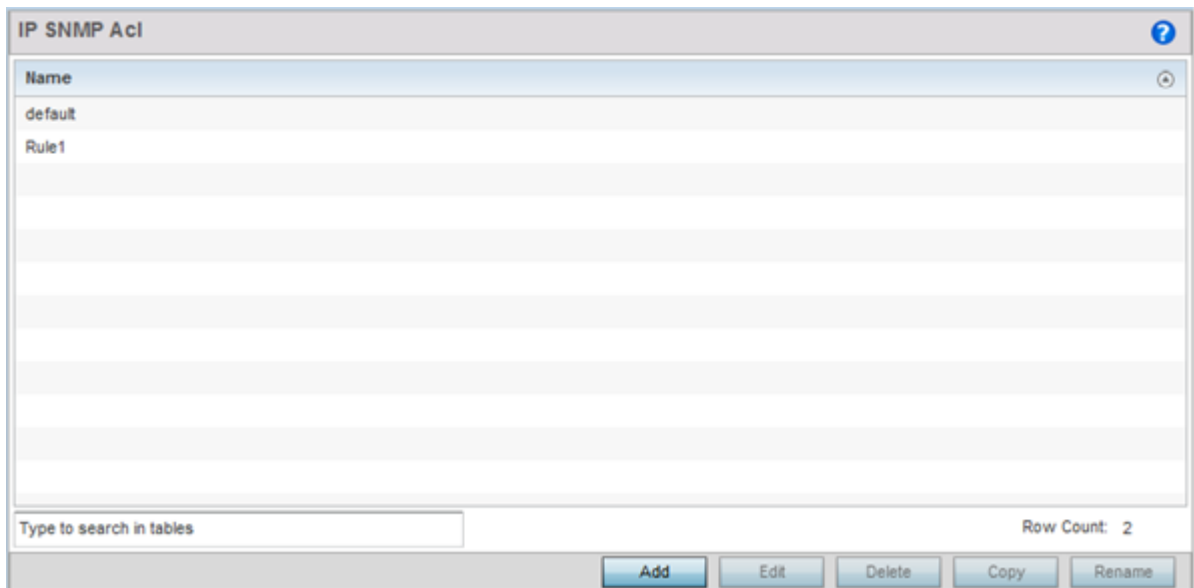
## Setting an IP SNMP ACL Policy

SNMP performs network management functions using a data structure called a Management Information Base (MIB). SNMP is widely implemented but not very secure, because 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:

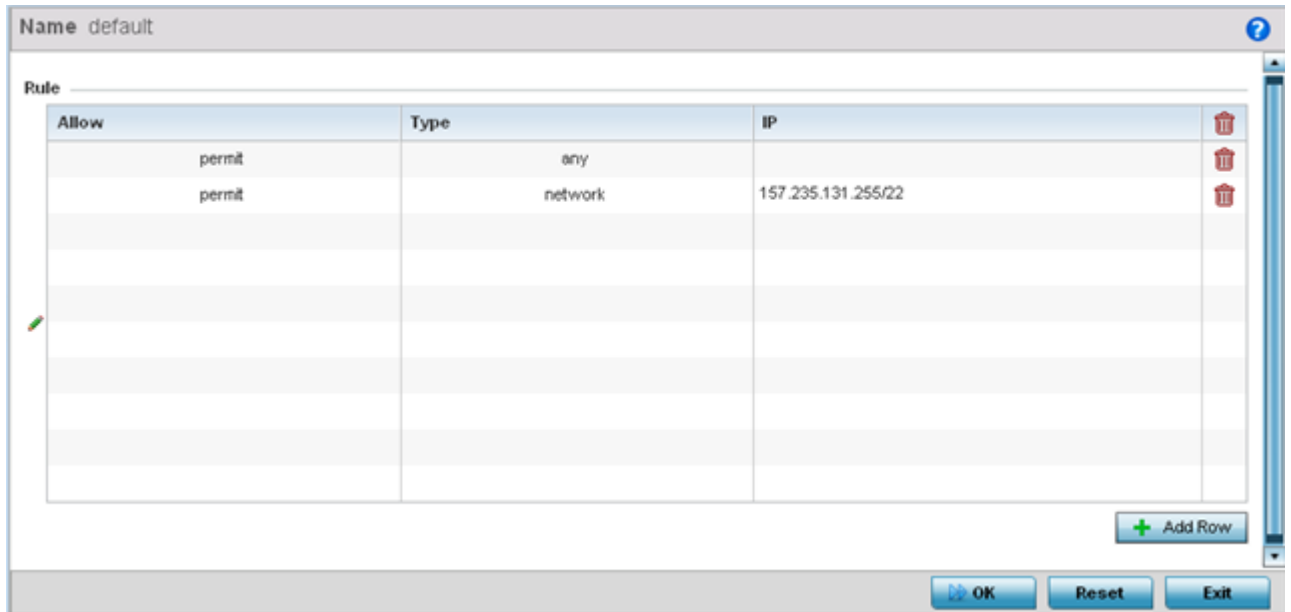
- 1 Select **Configuration > Security > IP Firewall**.
- 2 Expand the **IP Firewall** menu item and select **IP SNMP ACL**.



**Figure 256: IP SNMP ACL 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 257: IP SNMP ACL - Add/Edit screen**

- 4 Provide a new IP SNMP ACL **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 <b>Host</b> IP address, is applied to a <b>Network</b> address and subnet mask, or is applied to <b>Any</b> . The default setting is <b>Network</b> .

- 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 to its last saved configuration.

## Setting a 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 an IP firewall:

- 1 Select **Configuration > Security > IP Firewall > Network Group Alias** from the Web UI.
- 2 Select **Add**, or highlight an existing network group alias and select **Edit**.

Name	Host	Network
SNGA_IP_FW_HostList	10.233.89.93	10.233.88.0/24

Type to search in tables Row Count: 1

**Figure 258: 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.

- Click **Add** to create a new network group alias, or select an existing network group alias and click **Edit**.

**Figure 259: Network Group Alias - Add/Edit Screen**

If you are adding a new network alias rule, provide a name up to 32 characters. The network group alias name always starts with a dollar sign (\$).

- 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.

- 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 alias range entry to edit it.
- Select **OK** when completed to update the network group alias settings. Select **Reset** to revert the screen to its last saved configuration.

## Setting a Network Service Alias

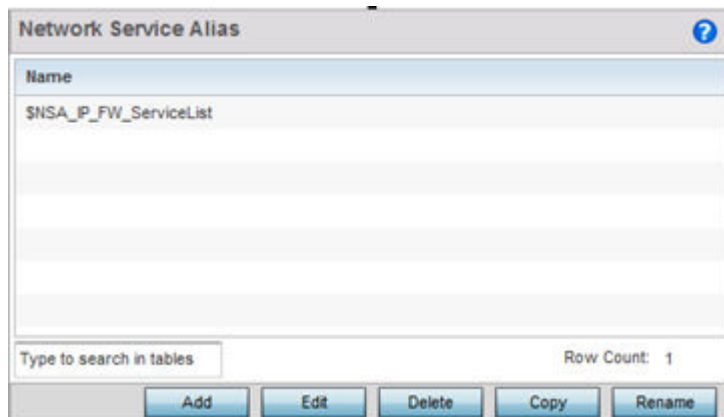
A network service alias is a set of configurations that consist of protocol and port mappings. Both source and destination ports are configurable. For each protocol, up to two source port ranges and up to two destination port ranges can be configured. A maximum of four protocol entries can be configured 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.



**Figure 260: IP Firewall Network Service Alias Screen**

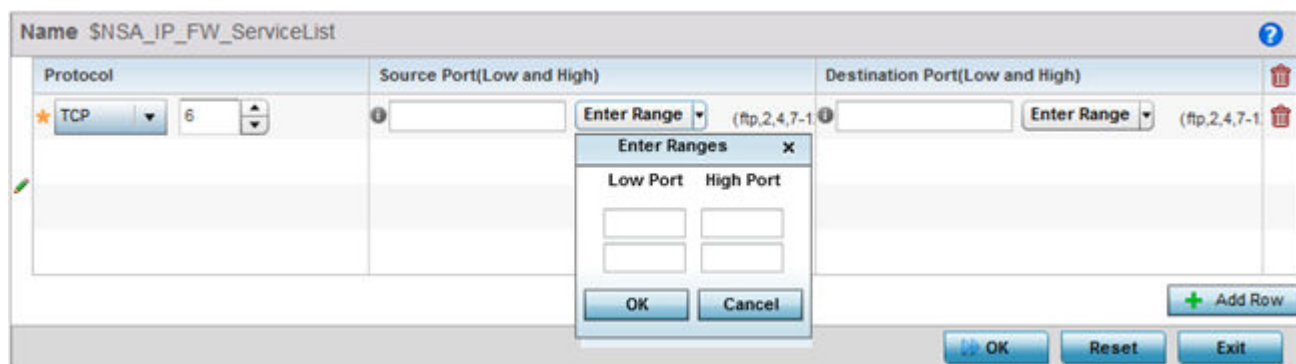
- 2 Select **Add** to create a new network service alias.

Select an existing network service alias and click **Edit** to modify it. Select **Delete** to remove an existing network service alias from those available in the list.

Use **Copy** to create a copy of the selected policy and modify it for further use. Use **Rename** to rename the selected policy.

- 3 If you are adding a new **Network Service Alias**, give it a **Name** up to 32 characters to distinguish this alias configuration from others with similar attributes.

The network group alias name always starts with a dollar sign (\$).



**Figure 261: IP Firewall Network Service Alias - Add/Edit Screen**

Select **Reset** to revert to the last saved configuration. Select **Exit** to exit without creating a network service alias.

- 4 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 <b>other</b> 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 relevant only if the protocol is tcp or udp. Specify the source ports for this protocol entry. A range of ports can be specified. Select the <b>Enter Ranges</b> 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 relevant only if the protocol is tcp or udp. Specify the destination ports for this protocol entry. A range of ports can be specified. Select the <b>Enter Ranges</b> button next to the field to enter a lower and higher port range value. Up to eight (8) such ranges can be specified.

- 5 In 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.
- 6 Select **OK** when completed to update the network service alias settings.  
Select **Reset** to revert the screen to its last saved configuration.

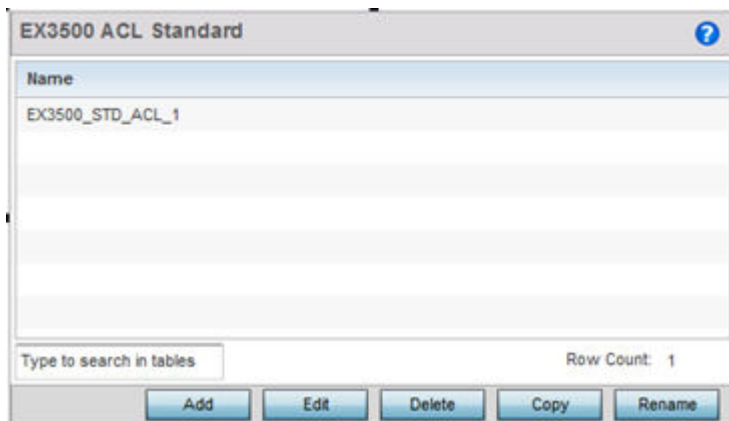
## EX3500 ACL Standard

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 262: 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 **Add** to create a new EX3500 Standard ACL, or select an existing ACL and click **Edit** to edit it.

The following screen displays.

Allow	Time Range	IP Address Type	Source IP Address
Permit	EX3500_TimeRange_01	Host	10.233.89.10/32

**Figure 263: EX3500 ACL Standard - Add/Edit Screen**

- 4 If you are adding a new **EX3500 ACL Standard**, provide it a name with up to 32 characters.
- 5 To add a new standard rule, click **Add Row**.

**Figure 264: EX3500 ACL Standard - Add/Edit - 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 <b>Permit</b> or <b>Deny</b> .
Time Range	From the drop-down menu select the preconfigured time range to use for this ACL. Select None to indicate no preference. For more information on time ranges, see <a href="#">EX3500 Time Range</a> on page 773.

- 7 Select **OK** when completed to update the EX3500 Standard ACL.  
Select **Reset** to revert the screen to its last saved configuration.

## EX3500 ACL Extended

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.

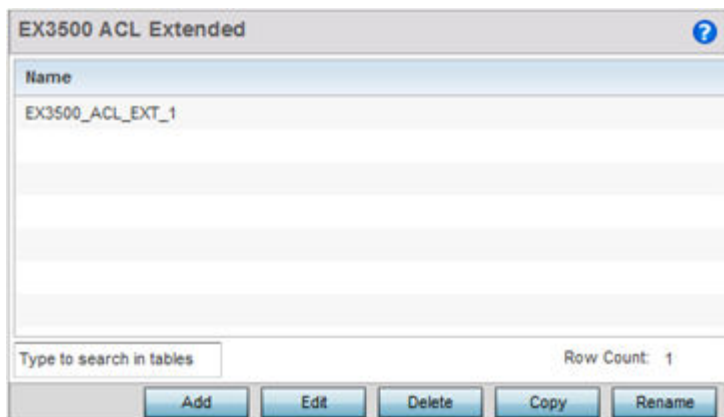
An ACL affords a system administrator the ability to grant or restrict client access by specifying that traffic from a specific host or a specific network to either be denied or permitted.

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 265: 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 **Add** to create a new EX3500 Extended ACL, or select an existing ACL and click **Edit** to edit it.

The following screen displays.



Name EX3500_ACL_EXT_1								
Precedence	Source	Destination	Action	Time Range	Protocol	DSCP	IP Header P	
1	Any	Any	Allow		other	Not Set	Not Set	

Type to search in tables

Add Remove

OK Reset Exit

**Figure 266: 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.

- Select the **Edit Rule** icon to the left of a particular IP firewall rule configuration to update its parameters collectively.

Precedence: 1

Allow:  Allow:  Deny:

Source: any 0 . 0 . 0 . 0 / 0

Destination: any 0 . 0 . 0 . 0 / 0

Protocol: IP 0

Show Less Options

Time Range: EX3500\_TimeRange\_01

DSCP  0

IP Precedence Header  0

**Figure 267: EX3500 ACL Extended - Add/Edit - Add Criteria Screen**

- 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.

Select Columns

- Source
- Destination
- Time Range
- Protocol
- Source Port
- Destination Port
- DSCP
- IP Header Precedence

**Figure 268: 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: <ul style="list-style-type: none"> <li>Deny - Instructs the firewall to restrict a packet from proceeding to its destination.</li> <li>Permit - Instructs the firewall to allow a packet to proceed to its destination.</li> </ul>
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 <a href="#">EX3500 Time Range</a> on page 773.
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 <b>DSCP</b> or <b>IP Header Precedence</b> can be configured. The two 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 <b>DSCP</b> or <b>IP Header Precedence</b> can be configured. The two fields cannot be configured together.

- 5 Select **OK** when completed to update the EX3500 Extended ACL.  
Select **Reset** to revert the screen to its last saved configuration.

## 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, service platform or access point compares the packet fields against applied matching policy rules to verify the packet has the required permissions to be forwarded. If a packet does not meet any of the criteria specified, the packet is dropped.

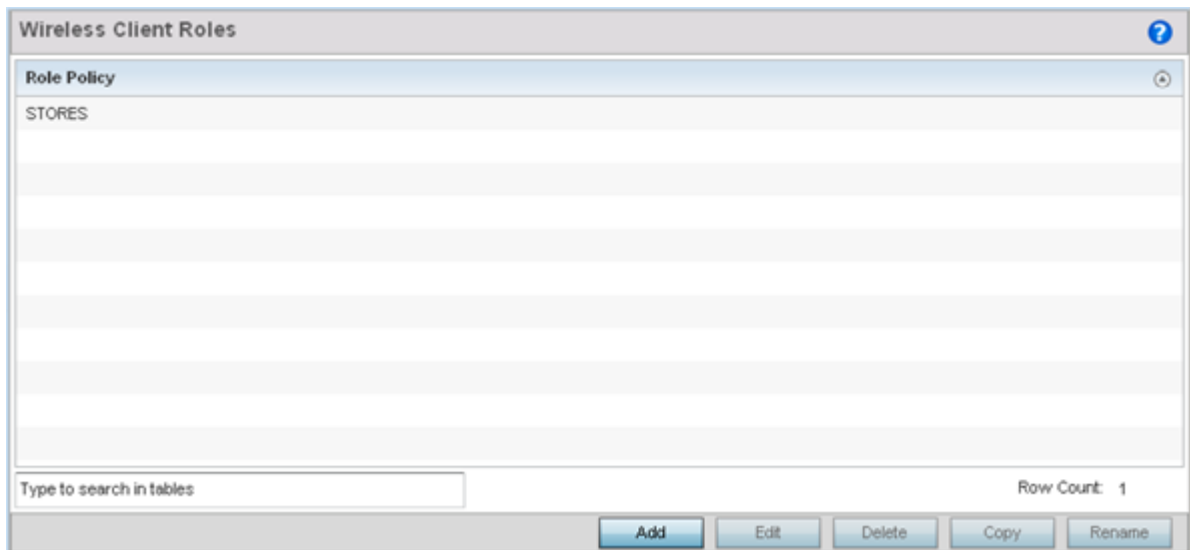
Additionally, wireless client connections are also managed by granting or restricting access by specifying a range of IP or MAC addresses to include or exclude from connectivity. These MAC or IP access control mechanisms are configured as Firewall Rules to further refine client filter and matching criteria.

## Configuring a Client's Role Policy

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.



**Figure 269: Wireless Client Roles Screen**

- 2 Select **Add** to create a new Wireless Client Role policy, **Edit** to modify an existing policy or **Delete** to remove a policy.

The **LDAP Settings** tab displays by default.

The screenshot shows the 'Role Policy STORES' configuration window with the 'LDAP Settings' tab selected. The 'Configuration' section includes:
 

- LDAP Query:** A checked checkbox and two radio buttons: 'Internal (Self)' (selected) and 'Through Wireless Controller'.
- Dead Period:** A spinner box set to 120, with a range of (60 to 300).
- Timeout:** A spinner box set to 2, with a range of (1 to 5).

 The 'LDAP Server Options' section contains a table with the following columns: ServerId, Host, Bind DN, Base DN, Bind Password, Port, and a delete icon. The table is currently empty. An 'Add Row' button is located at the bottom right of the table area. At the bottom of the window are 'OK', 'Reset', and 'Exit' buttons.

**Figure 270: Wireless Client Roles - Add/Edit - LDAP Settings Tab**

- 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.

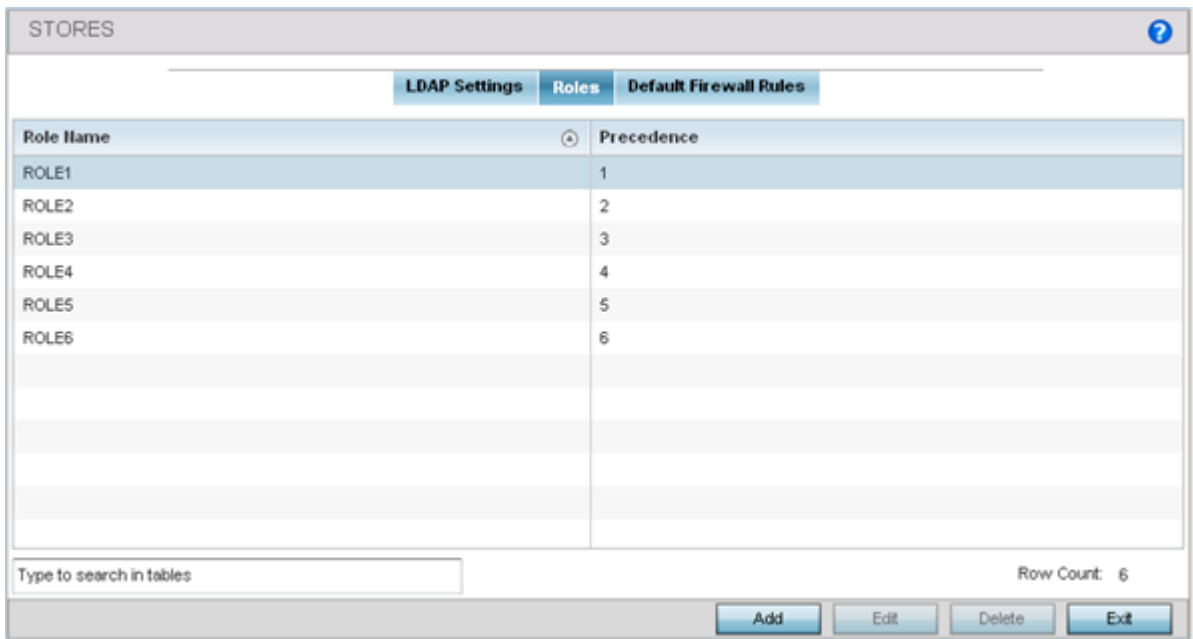
When adding or editing the LDAP server options, define the following parameters:

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 <b>Host</b> field.
Bind DN	When adding or editing an LDAP server entry, enter the LDAP server's bind distinguished name in the <b>Bind DN</b> field.

Base DN	When adding or editing an LDAP server entry, enter the LDAP server's base distinguished name in the <b>Base DN</b> field.
Bind Password	When adding or editing an LDAP server entry, enter the password for bind. Click the <b>Show</b> 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 271: Wireless Client Roles - Add/Edit - Roles Tab**

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 272: Wireless Client Roles - Add/Edit - Roles - Settings Tab**

- 8 If you are 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 In 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 In 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	<p>Use the drop-down menu to specify the location of an access point matched in an RF domain or the access point's resident configuration. Select one of the following filter options:</p> <ul style="list-style-type: none"> <li>• Exact - The role is applied only to access points with the exact location string specified in the role.</li> <li>• Contains - The role is applied only to access points whose location contains the location string specified in the role.</li> <li>• Does Not Contain - The role is applied only to access points whose location does not contain the location string specified in the role.</li> <li>• Any - The role is applied to any access point location. This is the default setting.</li> </ul>
SSID Configuration	<p>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:</p> <ul style="list-style-type: none"> <li>• Exact - The role is applied only when the exact SSID string is specified in the role..</li> <li>• Contains - The role is applied only when the SSID contains the string specified in the role.</li> <li>• Does Not Contain - The role is applied when the SSID does not contain the string specified in the role.</li> <li>• Any - The role is applied to any SSID Location. This is the default setting.</li> </ul>
Group Configuration	<p>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:</p> <ul style="list-style-type: none"> <li>• Exact - The role is applied only when the exact RADIUS Group Name string is specified in the role..</li> <li>• Contains - The role is applied when the RADIUS Group Name contains the string specified in the role.</li> <li>• Does Not Contain - The role is applied when the RADIUS Group Name does not contain the string specified in the role.</li> <li>• Any - The role is applied to any RADIUS Group Name. This is the default setting.</li> </ul>
RADIUS User	<p>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:</p> <ul style="list-style-type: none"> <li>• Exact - The role is applied only when the exact RADIUS user string is specified in the role..</li> <li>• Contains - The role is applied when the RADIUS user starts with the string specified in the role.</li> <li>• Does Not Contain - The role is applied when the RADIUS user does not contain the string specified in the role.</li> <li>• Any - The role is applied to any RADIUS user name. This is the default setting.</li> </ul>

- 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. Selecting **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 applied only when the authentication and encryption type matches the exact method(s) specified by the radio button selections.

**Not Equals** The role is applied only 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 apply to each LDAP attribute:

**Exact** The role is applied only 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 name 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.

The screenshot shows the 'Role Policy Roles' configuration window for role 'CAT1'. The 'Firewall Rules' tab is active. The configuration includes:

- Vlan ID:** A numeric input field set to '1' (range 1 to 4,094).
- URL Filter:** A dropdown menu.
- Application Policy:** A dropdown menu.
- IPv6 Inbound:** A table with columns 'IPv6 Firewall Rules Name', 'Precedence', and a delete icon.
- IPv6 Outbound:** A table with columns 'IPv6 Firewall Rules Name', 'Precedence', and a delete icon.
- IP Inbound:** A table with columns 'IP Firewall Rules Name', 'Precedence', and a delete icon.
- IP Outbound:** A table with columns 'IP Firewall Rules Name', 'Precedence', and a delete icon.
- MAC Inbound:** A table with columns 'MAC Firewall Rules Name', 'Precedence', and a delete icon.
- MAC Outbound:** A table with columns 'MAC Firewall Rules Name', 'Precedence', and a delete icon.

Buttons at the bottom: OK, Reset, Exit.

**Figure 273: Wireless Client Roles - Add/Edit - Roles - 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 Specify an **IPv6 Inbound** or **IPv6 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. Select the **+ Add Row** button or **Delete** icon as needed to add or remove IPv6 firewall rules. If no IPv6 Inbound or Outbound firewall ACL exist create the IPv6 firewall ACL and use here. For more information on creating IPv6 ACL, refer to [Setting an IPv4 or IPv6 Firewall Policy](#) on page 732.
- 23 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. Select the **+ Add Row** button or **Delete** icon as needed to add or remove IP firewall rules. If no IP Inbound or Outbound firewall ACL exist create the IP firewall ACL and use here. For more information on creating IP ACL, refer to [Setting an IPv4 or IPv6 Firewall Policy](#) on page 732.
- 24 Specify an **MAC Inbound** or **MAC 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. Select the **+ Add Row** button or **Delete** icon as needed to add or remove MAC firewall rules. If no MAC Inbound or Outbound firewall ACL exist create the MAC firewall ACL and use here. For more information on creating MAC ACL, refer to [Configuring MAC Firewall Rules](#) on page 727.
- 25 Select **OK** to save the Firewall Rules updates.  
Select **Reset** to revert to the last saved configuration.

## 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 networks 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

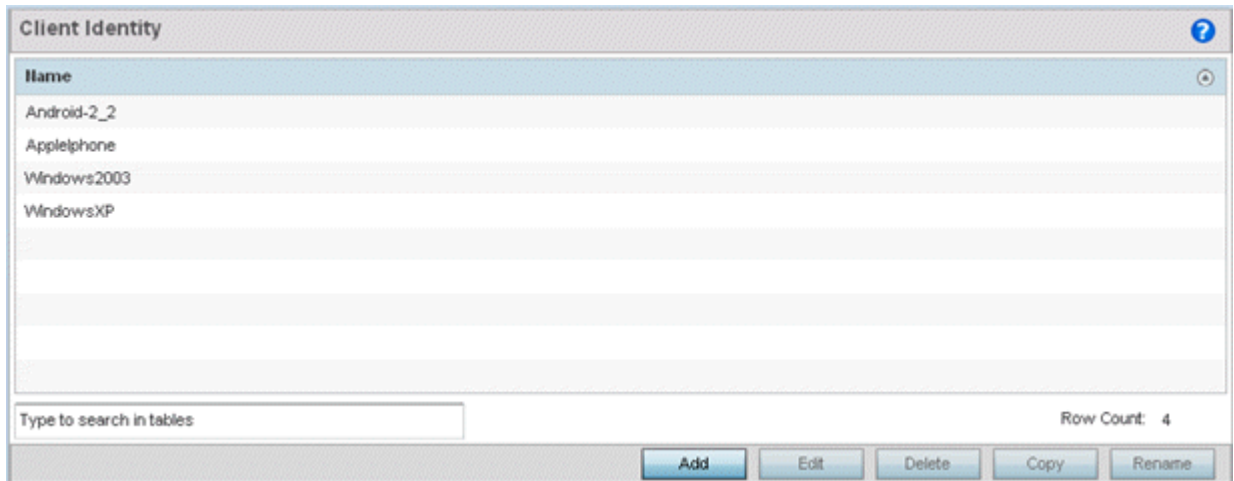
Ensure DHCP is enabled on the WLAN on which device fingerprinting is to be enabled.

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, populated by default with existing client identity configurations.



**Figure 274: 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.

Use **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 you are 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.

Index	Message Type	Match Option	Match Type	Value Format	Option Value
8	Request	55	Exact	Hex String	012103061c333a3b
9	Request	60	Starts With	ASCII	dhcpcd-5.2.10
10	Request	60	Starts With	ASCII	dhcpcd-5.2.10:Linux-3

**Figure 275: Device Fingerprinting - Add/Edit - Client Signature Screen**

- 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. <ul style="list-style-type: none"> <li>Request – Looks for a signature in DHCP request messages. This is the default value.</li> <li>Discover – Looks for a signature in DHCP discover messages.</li> </ul>

Match Option	Options are passed in DHCP discover and request messages as Option Code, Option Type, and Option Value sets. When <b>Option Codes</b> 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. <ul style="list-style-type: none"> <li>• 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.</li> <li>• Option Codes – Indicates the Option Code passed in the DHCP request and discover message is used for matching.</li> </ul>
Match Type	Use the drop-down menu to select how signatures are matched. Available options include: <ul style="list-style-type: none"> <li>• Exact – The complete signature string matches the string specified in the <b>Option Value</b> field.</li> <li>• Starts-with – The signature is checked if it starts with the string specified in the <b>Option Value</b> field.</li> <li>• Contains – The signature is checked if it contains the string specified in the <b>Option Value</b> field.</li> </ul>
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.

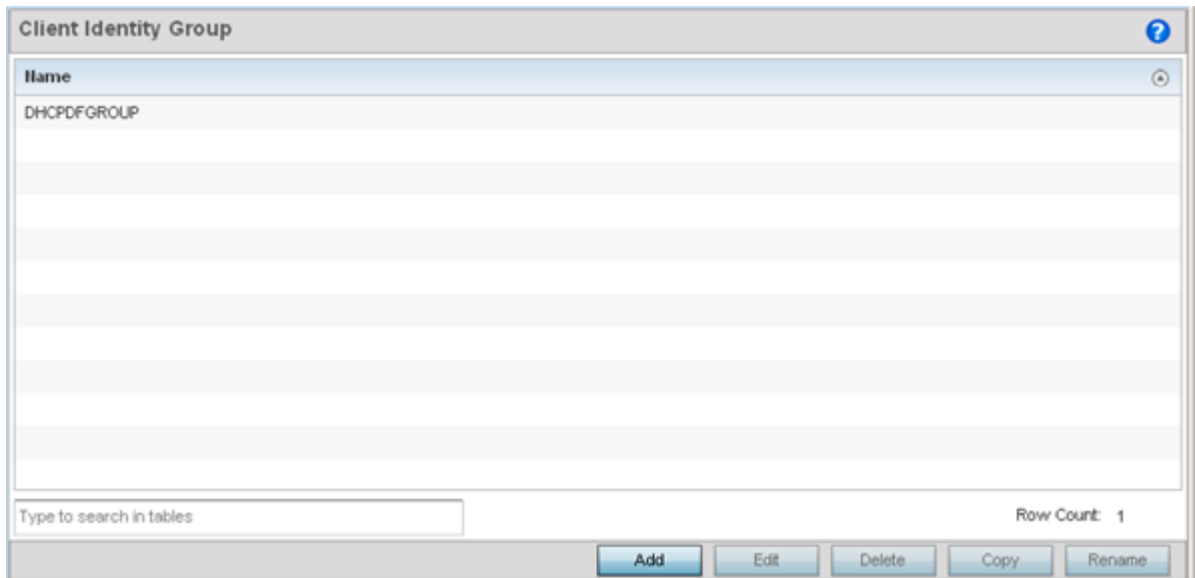
**Any** The fingerprint is checked with either the DHCP request or the DHCP discover message.

**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 276: Device Fingerprinting - Client Identity Group Screen**

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.

Use **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 you are 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's **Client Identity** and **Precedence** parameters.

The screenshot shows a window titled "Name androidgroup" with a "DHCP Match Criteria" section. It contains a table with the following data:

Client Identity	Precedence	
Android-2_2	1	[Delete]
Applephone	4	[Delete]
vWindows2003	2	[Delete]
vWindowsXP	3	[Delete]

At the bottom right of the table area is a "+ Add Row" button. At the bottom of the window are "OK", "Reset", and "Exit" buttons.

**Figure 277: Device Fingerprinting - Add/Edit - Client Identity Group Screen**

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

## Intrusion Prevention

The *Wireless Intrusion Protection System* (WIPS) provides continuous protection against wireless threats and acts as an additional layer of security complementing VPNs and encryption and authentication policies. WIPS is supported through the use of dedicated sensor devices (access point radios) designed to detect and locate unauthorized devices. After detection, unauthorized devices are blocked 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 controllers, service platforms and access points support unauthorized AP detection, location and containment natively. A WIPS server can alternatively be deployed as a dedicated solution

within a separate enclosure. 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 a controller, service platform or access point managed network.
- *Rogue Detection and Segregation* - WIPS 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 through 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.

## Configuring a WIPS Policy

Unauthorized device detection needs to be enabled for each WIPS policy (it's disabled by default). Whether currently enabled or disabled, A WIPS policy can have specific categorization policies defined and specific events enabled for detection. Once defined, a WIPS policy is available for use with controller, service platform or Access Point device profile.

To configure a WIPS policy:

- 1 Select **Configuration > Security > Intrusion Prevention**.



- Expand the Intrusion Prevention option within the **Configuration > Security** menu to display the **WIPS Policy, Advanced WIPS Policy** and **Device Categorization** items available.

The **Wireless IPS** screen displays by default. It lists existing WIPS policies if any are configured. Any of these existing WIPS policies can be selected and applied.

WIPS Policy	Status	Interval to Throttle Duplicates
tym	✓ Enabled	2m 0s

Type to search in tables Row Count: 1

**Figure 278: Wireless IPS Screen**

- 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 check mark if the listed WIPS policy is enabled and ready for use with a profile. A red "X" designates 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.

Use **Rename** to change the name of an existing policy or **Copy** a policy to a different location.

If you are adding or editing an existing WIPS policy, the **WIPS Policy** screen displays with the **Settings** tab displayed by default.

The screenshot shows the 'WIPS Policy' configuration window for 'ALPHANET-WIPS'. It has three tabs: 'Settings', 'WIPS Events', and 'WIPS Signatures'. The 'Settings' tab is selected. The configuration is organized into sections:

- Wireless IPS Status:** Status is set to 'Enabled' (radio button selected).
- Duplicate Events:** 'Interval to Throttle Duplicates' is set to 2 Minutes (range: 1 to 1,440).
- Rogue AP Detection:**
  - 'Enable Rogue AP Detection' is checked.
  - 'Wait Time to Determine AP Status' is 1 Minutes (range: 1 to 10).
  - 'Ageout for AP Entries' is 5 Minutes (range: 1 to 1,440).
  - 'Interferer Threshold' is -75 dBm (range: -100 to -10 dBm).
  - 'Recurring Event Interval' is 5 Minutes (range: 0 to 166).
  - 'Air Termination' is unchecked.
  - 'Air Termination Channel Switch' is unchecked.
  - 'Air Termination Mode' is set to 'manual'.
- Device Categorization:** 'Device Categorization Policy' is set to a dropdown menu.

Buttons for 'OK', 'Reset', and 'Exit' are visible at the bottom right.

**Figure 279: WIPS Policy Screen - Add/Edit - Settings Tab**

- 5 If you are 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 **Enabled** or **Disabled** to activate or deactivate 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 check box to enable the detection of unauthorized (unsanctioned) devices for this WIPS policy. The default setting is <b>Disabled</b> .
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 age out 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 an 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 disassociated 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.

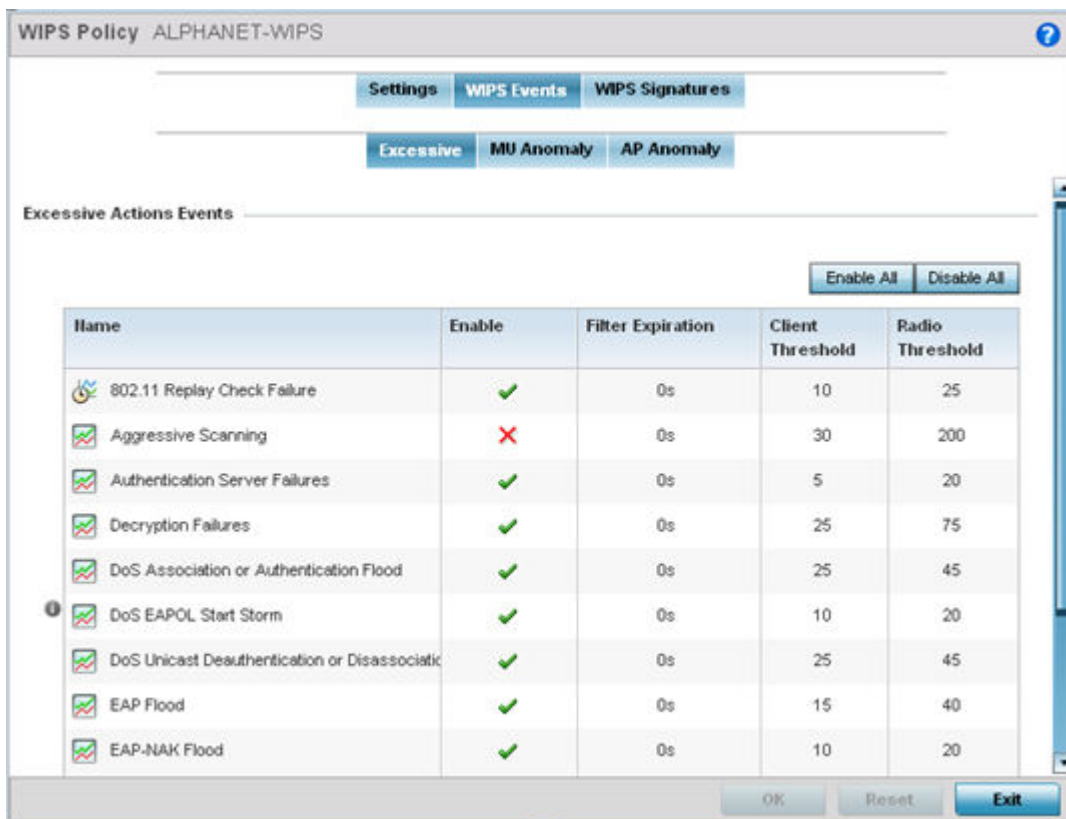
- 9 Use the **Device Categorization Policy** drop-down menu to select a policy describing whether a device is filtered as sanctioned, a client or access point, and the MAC and SSID addresses used as filtering mechanisms.

If a policy requires creation, select **Create**. If an existing policy requires modification, select **Edit** 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 280: WIPS Events Screen - Add/Edit - 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.

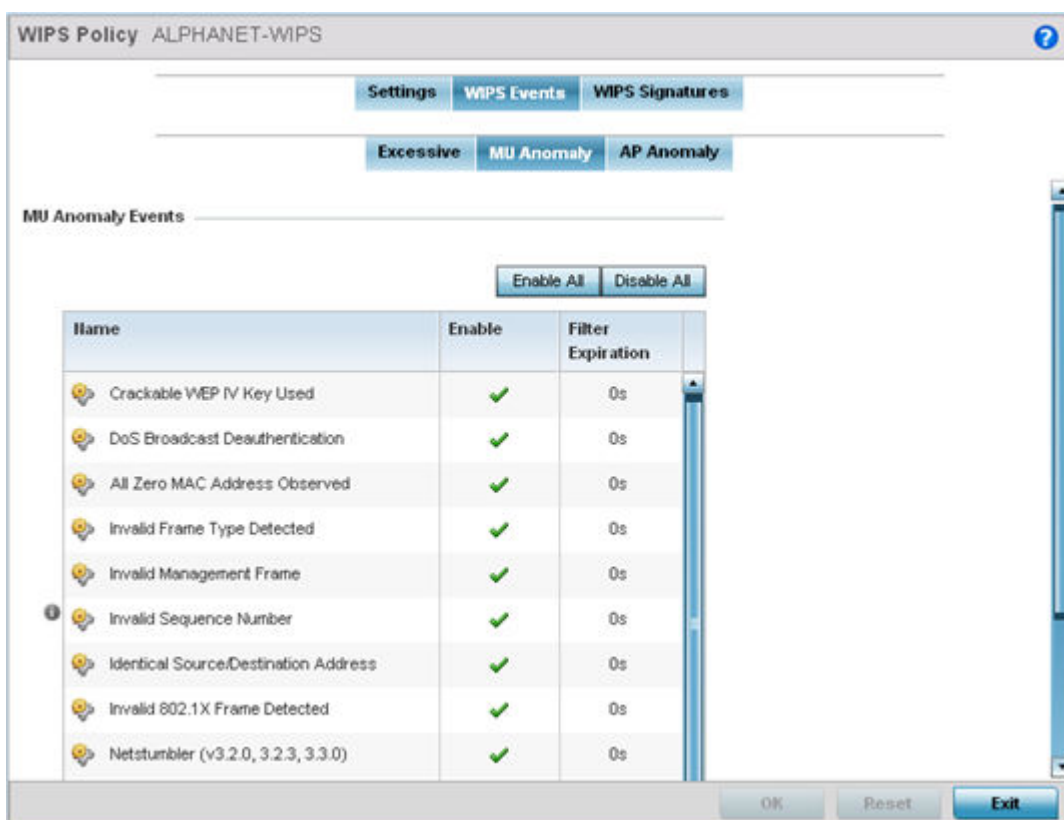
AP events can be globally enabled and disabled as required using the **Enable All** and **Disable All** buttons on the top-right-hand side of the screen.

- 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 check mark 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 <b>Enable All</b> and <b>Disable All</b> 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 281: WIPS Events Screen - Add/Edit - 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.

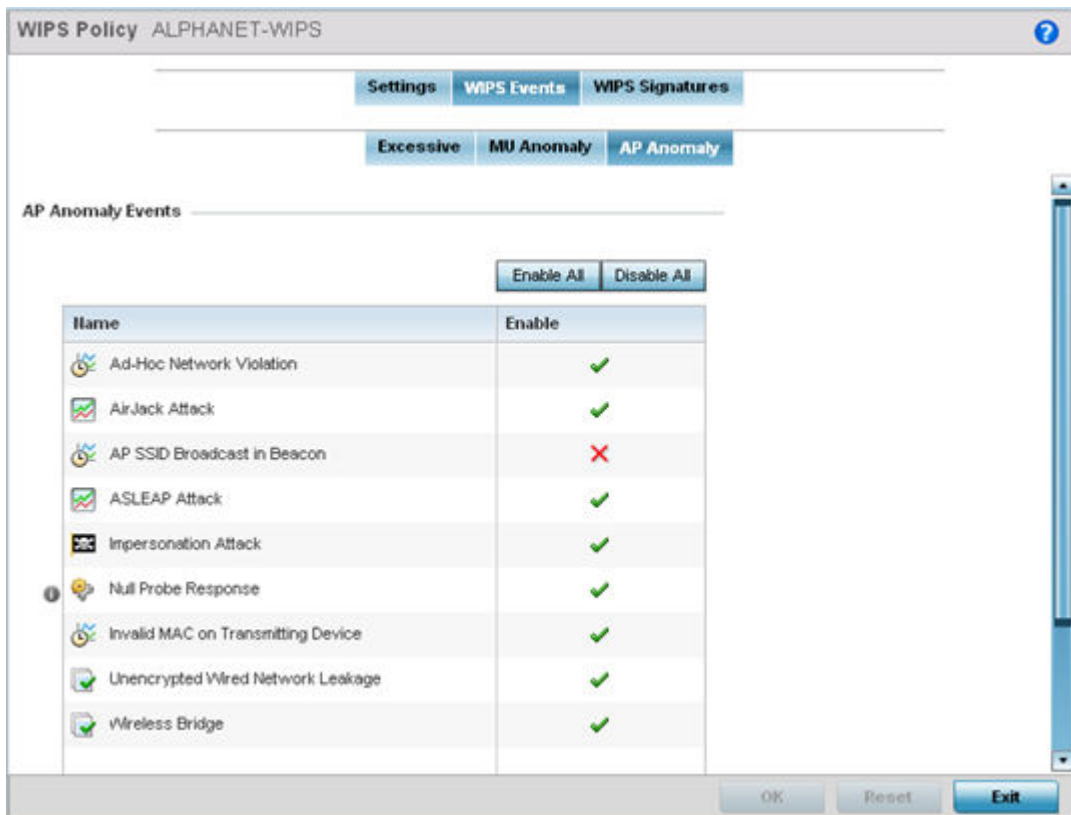
MU events can be globally enabled and disabled as required using the **Enable All** and **Disable All** buttons on the top-right-hand side of the screen.

- 15 Set the 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 check mark 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 <b>Enable All</b> and <b>Disable All</b> 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 282: WIPS Events screen - Add/Edit - 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** configurations:

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 check mark 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 <b>Enable All</b> and <b>Disable All</b> 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.

Name	Signature	BSSID MAC	Source MAC	Destination MAC	Frame Type to Match	Match on SSID
signature 1	✓	Not Set	Not Set	Not Set	All	Not Set
signature 2	✓	Not Set	Not Set	Not Set	Association	Not Set

**Figure 283: 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 check mark 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 284: WIPS Signatures Screen - Add/Edit - Signature Screen**

- 23 If you are 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 that it is specified properly, or the SSID will not 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 the **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 **Index**, **Pattern**, and **Offset** variables for the payload.

28 Select **OK** to save the updates to the WIPS Signature configuration.

Select **Reset** to revert to the last saved configuration.

## Configuring a Device Categorization Policy

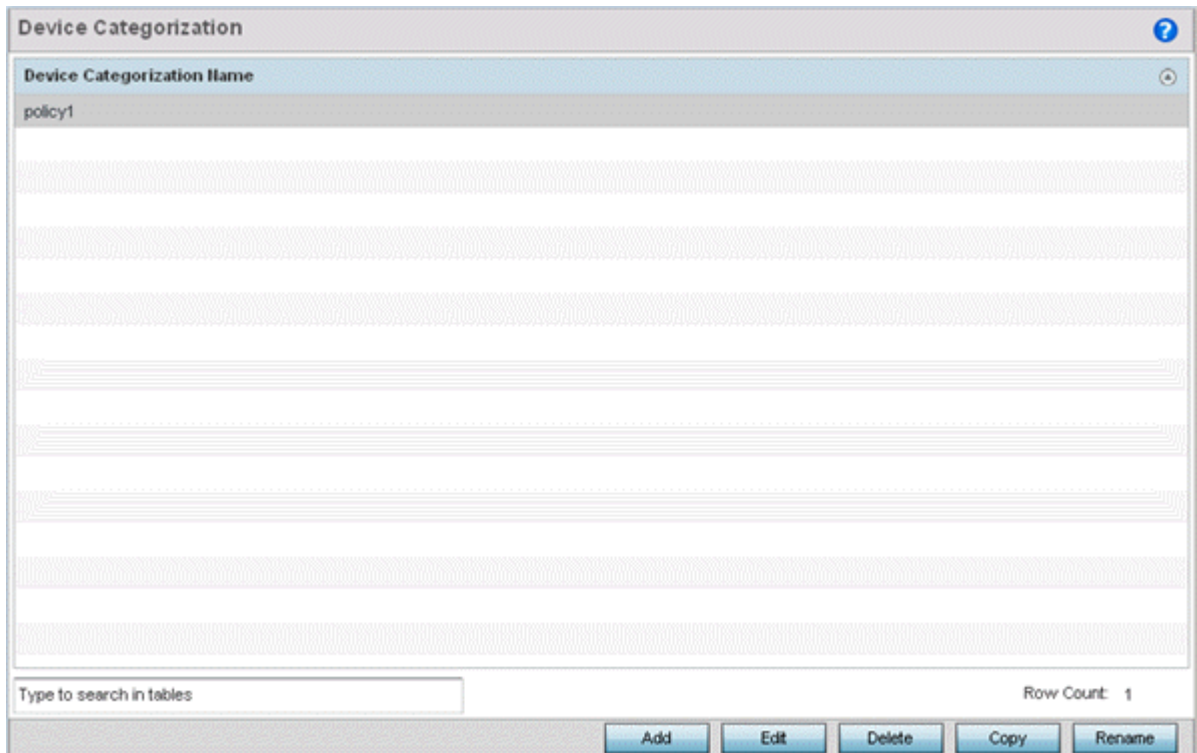
Having devices properly classified can help suppress unnecessary unsanctioned AP alarms and allow an administrator to focus on the alarms and devices actually behaving in a suspicious manner. An intruder with a device erroneously authorized could potentially perform activities that harm your organization 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**.

- Expand the Intrusion Prevention option within the **Configuration > Security** menu and select **Device Categorization**.



**Figure 285: 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 286: WIPS Device Categorization - Configuration Screen**

- 4 If you are 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 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 check mark 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 check mark 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.

## Intrusion Detection Deployment Considerations

Before configuring WIPS support on a controller, service platform or access point, 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 administration time. Vulnerability and activity reports should automatically run and be distributed to the appropriate administrators. These reports should highlight areas to be investigated and minimize the need for network monitoring.
- It is 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.

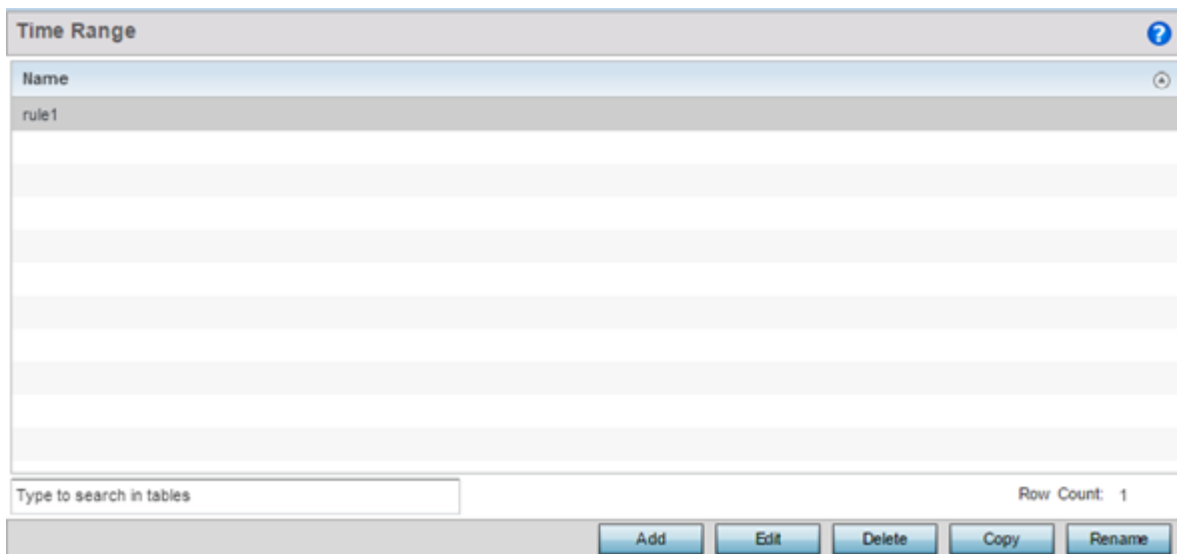
## EX3500 Time Range

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 727.

To set an EX3500 switch periodic or absolute time ranges:

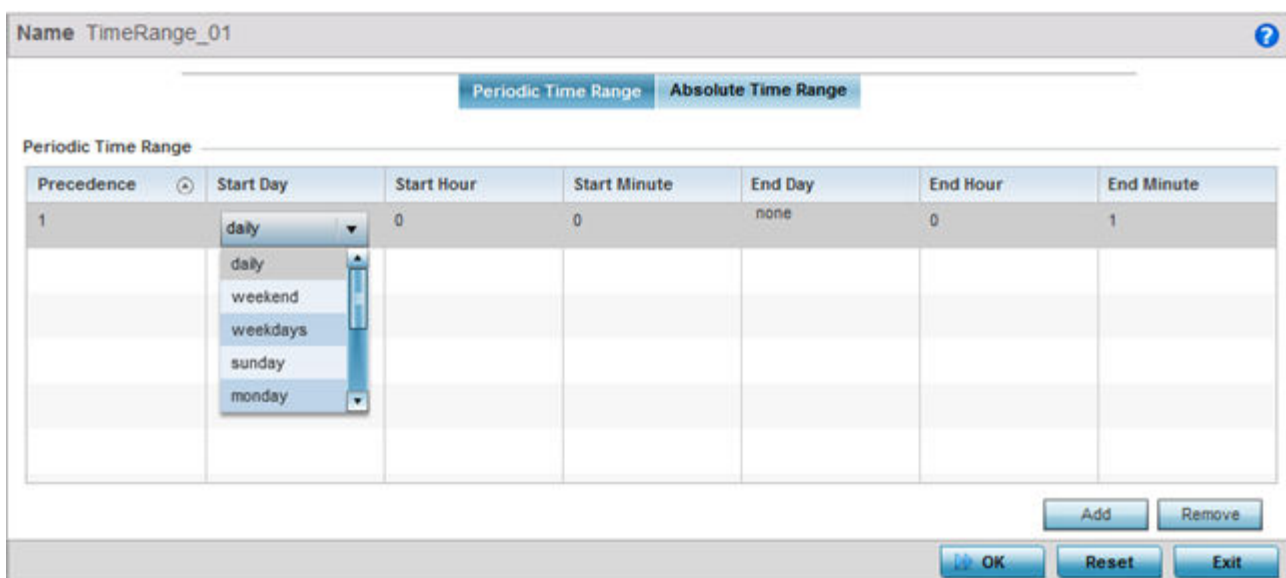
- 1 Select **Configuration** > **Security** > **EX3500 Time Ranges**.



**Figure 287: 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 288: EX3500 Time Range - Periodic Time Range Screen**

The **Periodic Time Range** tab displays by default.

- 4 If you are adding a new EX3500 time range, give 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 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 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 <b>Start Day</b> 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 <b>Start Hour</b> 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 <b>Start Minute</b> 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 289: EX3500 Time Range - Absolute Time Range Screen**

- 8 Select **Enable** to enable this feature.  
Absolute time range can be configured only 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 <b>Start Year</b> 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 <b>Start Day</b> 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 <b>Start Hour</b> 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 <b>Start Minute</b> field. Use the spinner to select the correct end.

10 Select **OK** when completed to update the EX3500 time range.

Select **Reset** to revert to the last saved configuration.



# 11 Services Configuration

[Configuring Captive Portal Policies](#)  
[Setting the Guest Management Configuration](#)  
[Setting the DHCP Configuration](#)  
[Setting the Bonjour Gateway Configuration](#)  
[Setting the DHCPv6 Server Policy](#)  
[Setting the RADIUS Configuration](#)  
[Setting the URL List](#)  
[Setting the ImagoTag Policy](#)

Controllers, service platforms and access points natively support guest and temporary user access policies, lease DHCP IP addresses to requesting clients and authenticate requesting clients.

For more information, refer to the following:

- [Configuring Captive Portal Policies](#)
- [Setting the Guest Management Configuration](#) on page 793
- [Setting the DHCP Configuration](#)
- [Setting the Bonjour Gateway Configuration](#) on page 819
- [Setting the DHCPv6 Server Policy](#) on page 823
- [Setting the RADIUS Configuration](#)
- [Setting the URL List](#) on page 849

## Configuring Captive Portal Policies

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](#) on page 791
- [Captive Portal Deployment Considerations](#) on page 792

## Configuring a Captive Portal Policy

To configure a captive portal policy:

- 1 Select **Configuration > Services**.

The upper left-hand side of the user interface displays a **Services** menu where **Captive Portal**, **DHCP**, and **RADIUS** configuration options can be selected.

- 2 Select **Captive Portals**.

The **Captive Portal** screen displays existing policies. New policies can be created, existing policies can be modified, or existing policies deleted.

Captive Portal Policy	Captive Portal Server Host	Captive Portal IPv6 Server	Captive Portal Server Mode	Hosting VLAN Interface	Connection Mode	Simultaneous Access	Web Page Source	AAA Policy
ALPHANET-GUEST	guestaccess.extre	Not Set	Centralized Contr	0	HTTP	Not Set	Advanced	EGUEST-AAA

**Figure 290: 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 <b>Internal (Self)</b> or <b>External (Fixed)</b> . If the mode is <b>Internal (Self)</b> , the controller or Access Point is maintaining the captive portal internally, while <b>External (Fixed)</b> means the captive portal is being hosted on an external server resource.
Hosting VLAN Interface	Lists the VLAN (from 1 - 4,094) a client utilizes for controller or service platform interoperation when the <b>Captive Portal Server Mode</b> is set to <b>Centralized Controller</b> .
Connection Mode	Lists each policy's connection mode as either <i>HTTP</i> or <i>HTTPS</i> . Both HTTP and HTTPS use the same Uniform Resource Identifier (URI) so that requesting clients can be identified. However, we recommend using HTTPS because it affords transmissions a measure of data protection HTTP cannot provide.
Simultaneous Users	Displays the number of users permitted at one time for each listed captive portal. A captive portal can support from 0-8192 users simultaneously.
Web Page Source	Displays whether the captive portal HTML pages are maintained <b>Internally</b> , <b>Externally</b> (on an external system you define), or are <b>Advanced</b> pages maintained and customized by the network administrator. <b>Internal</b> 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, an 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.

Select **Replace** to replace an existing captive portal policy with another captive portal policy.

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.

The screenshot shows the 'Captive Portal Policy' configuration window with the 'Basic Configuration' tab selected. The interface is organized into several sections:

- Settings:**
  - Captive Portal Server Mode:  Internal (Self),  Centralized,  Centralized Controller
  - Hosting VLAN Interface:  (0 to 4,096)
  - Captive Portal Server Host:
  - Captive Portal IPv6 Server:
  - Connection Mode:  HTTP,  HTTPS
  - Simultaneous Access:   (1 to 8,192)
- Security:**
  - AAA Policy:
- Access:**
  - Access Type:  No authentication required,  RADIUS Authentication,  Registration,  E-mail Access,  Mobile Access,  Other Access
  - Terms and Conditions page:
  - Frictionless Onboarding:
- Social Media Authentication:**
  - This feature requires access to the relevant websites. Please refer to the Help section for additional information.
  - Facebook:
  - Google:
- Bypass:**
  - Bypass Captive Portal Detection:

At the bottom right, there are three buttons: **OK**, **Reset**, and **Exit**.

**Figure 291: Captive Portal Policy - Add/Edit - Basic Configuration Tab**

## 5 Define the following settings for the captive portal policy:

Captive Portal Policy	If you are creating a new policy, assign a name representative of its access permissions, location or intended wireless client user base. If you are 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 <b>Centralized</b> is selected as the <b>Captive Portal Server Mode</b> , 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	When <b>Centralized</b> is selected as the <b>Captive Portal Server Mode</b> , set a numeric IP address (or DNS hostname) for the server validating guest user permissions for the captive portal policy. When <b>Centralized Controller</b> is selected, use this field to provide the hostname of the controller or controllers acting as the captive portal server host.
Captive Portal IPv6 Server	When using <b>Centralized</b> 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 <b>HTTP</b> or <b>HTTPS</b> to define the connection medium to the Web server. We recommend the use of <b>HTTPS</b> because it affords some additional data protection <b>HTTP</b> cannot provide. The default value, however, is <b>HTTP</b> .
Simultaneous Access	Select the check box 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 captive portal 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	<p>Select the authentication scheme applied to clients requesting captive portal guest access to the WiNG network. Within the WiNG UI there are six options. The WiNG CLI uses five options. User interface options include:</p> <ul style="list-style-type: none"> <li>• <b>No authentication required</b> - Requesting clients are redirected to the captive portal Welcome page without authentication.</li> <li>• <b>RADIUS Authentication</b> - A requesting client's user credentials require authentication before access to the captive portal is permitted. This is the default setting.</li> <li>• <b>Registration</b> - A requesting client's user credentials require authentication through social media credential exchange.</li> <li>• <b>Email Access</b> - Clients use E-mail username and passwords for authenticating their captive portal session. Optionally set whether E-mail access requests are RADIUS validated.</li> <li>• <b>Mobile Access</b> - Mobile clients use their device's access permissions for authenticating their captive portal session. Optionally set whether mobile access requests are RADIUS validated.</li> <li>• <b>Other Access</b> - 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.</li> </ul>
Terms and Conditions page	<p>Select this option (with any access type) 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 <b>No authentication required</b> is selected as the access type, otherwise the terms appear in the Login page. The default setting is disabled.</p>
Frictionless Onboarding	<p>Select this option to enable wireless clients, associated with guest WLANs, to self-register with the ExtremeGuest server. In other words, this feature enables frictionless on-boarding of guest users to the ExtremeGuest server. It also provides an integration API, as a means of on-boarding guest users through a loyalty application.</p> <p>In the captive portal, set access-type as 'Registration', enable 'Frictionless Onboarding', and provide the Localization 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.</p> <p><b>Note:</b> If enabling this feature, in the WLAN (using this captive-portal) set the following parameters: authentication-type as 'MAC' and registration-mode as 'device'. Enable the 'External Controller' and 'Follow AAA' options. Use the AAA Policy drop-down menu to specify the AAA policy. In the AAA policy, ensure that the authentication server configuration points to the ExtremeGuest server.</p>

- 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, how long clients are allowed captive portal access, and when clients are 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 <a href="#">Application</a> on page 495.

- 12 Use the **DNS Whitelist** parameter to create a set of allowed destination IP addresses for the captive portal.

These allowed DNS destination IP addresses are called a whitelist.

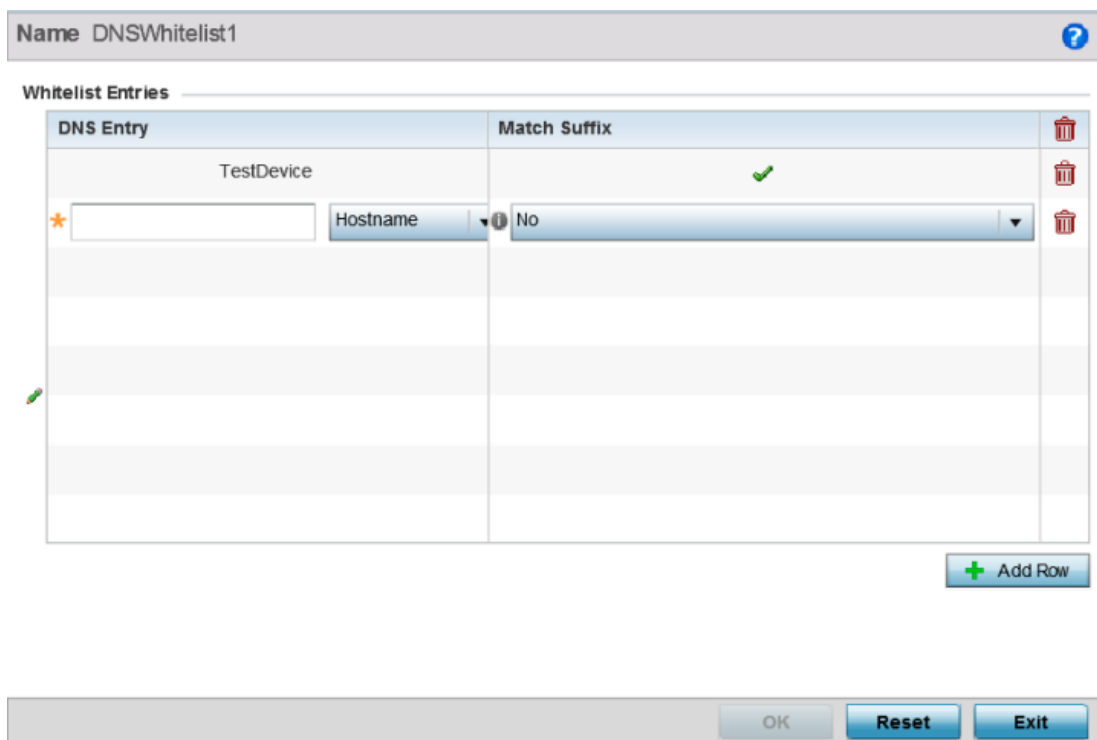
To effectively host captive portal pages on an external web server, the IP addresses of the destination web servers should be in the whitelist.

- a Refer to the drop-down menu of existing **DNS Whitelist** 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 do the following.

- b 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 292: Captive Portal Policy - Basic Configuration - Add DNS Whitelist Screen**

- c 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 underscores.
  - d Use the **Match Suffix** parameter to match any hostname or domain name as a suffix.  
The default setting is disabled.
  - e If necessary, select the radio button of an existing whitelist entry and select the **- Delete** icon to remove the entry from the whitelist.
- 13 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.

- 14 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. Choose from one of: <ul style="list-style-type: none"> <li>• <b>Log Only</b> - Logs the event</li> <li>• <b>log-and-disconnect</b> - Logs the event and disconnects the user</li> </ul> When <b>Log Only</b> is selected, an entry is added to the log file whenever a captive portal client exceeds the data limit. When <b>log-and-disconnect</b> 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.

- 15 Set the **Logout FQDN** as the fully qualified domain name (FQDN) of the domain where the user will be redirected after logging out of the captive portal.

Example: `logout.guest.com`

- 16 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, <code>local.guestaccess.com</code> ) used to obtain localization parameters for a client.
Response	Enter a response message (512-character maximum) directed back to the client for localization HTTP requests.

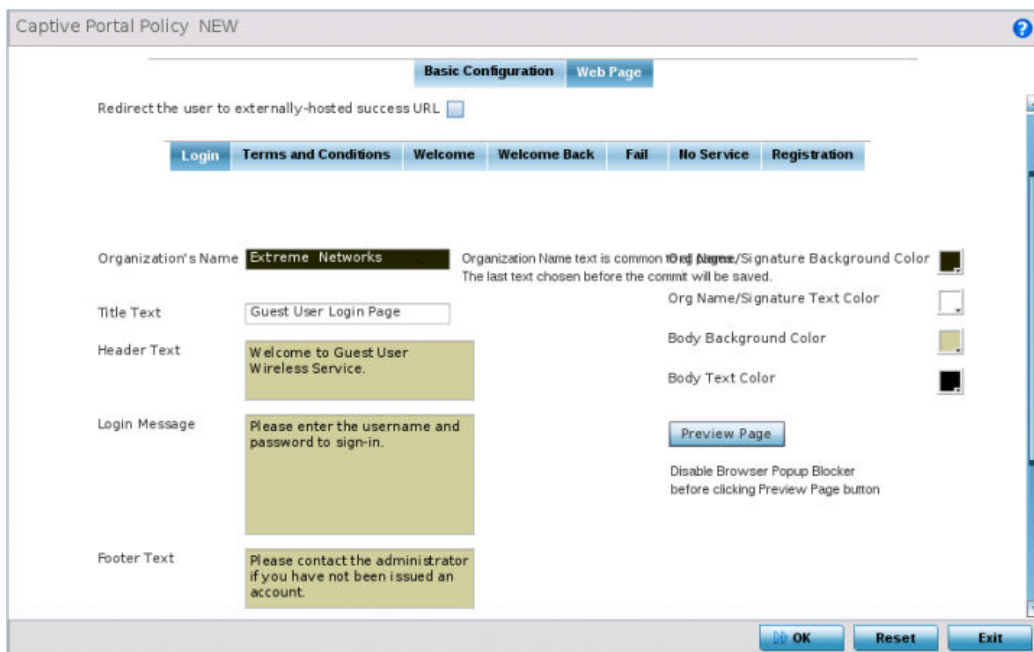
- 17 Refer to the **Destination Ports for Redirection** parameter (within the **Redirection Ports** field), and enter destination ports (separated by commas, or using a dash for a range) for consideration when re-directing client connections.

Standard ports 80 and 443 are always considered for client connections regardless of what's entered by the administrator.

- 18 Select **OK** to save the changes made within the **Basic Configuration** screen.  
Select **Reset** to revert to the last saved configuration.

- 19 Select the Web Page tab to create locally or externally hosted HTML pages.

The **Login** page displays by default.



**Figure 293: Captive Portal Policy - Web Page - Internal Option 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 page 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.

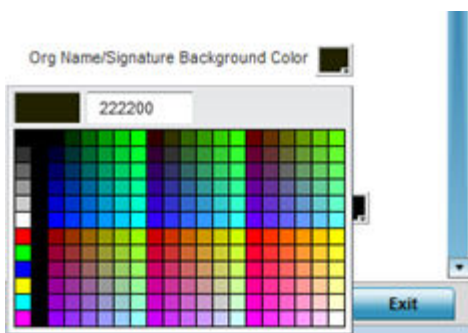
The No Service page asserts the captive portal service is temporarily unavailable for technical reasons. Once the services become available, the captive portal user is automatically connected back to the services available through the captive portal.

- 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.

Organization Name	Set any organizational specific name or identifier which clients see during login. This setting is available only 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 captive portal Web pages.
Main Logo URL	The Main Logo URL is the URL for the main logo image displayed on each of the pages. Use the <b>Browse</b> button to navigate to the location of the target file. Optionally select the <b>Use as banner</b> 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 <b>Browse</b> 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. This setting is available only for the Login page.

- 21 Refer to the right 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 294: Captive Portal Policy - Web Page - Color Palette Menu**

- 22 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.

The screenshot shows the configuration page for the Captive Portal Policy. The 'Web Page' tab is active, displaying the following configuration:

- Main Logo URL: wing-banner.png
- Small Logo URL: extr.png
- Signature: Extreme Networks. All Rights Reserved
- Registration Page Fields table:

Name	Type	Enabled	Mandatory	Label	Placeholder
age-range	dropdown-menu	✓	✗	Age Range	Age Range
city	text	✗	✗	City	Enter City
country		✗	✗		
disclaimer		✗	✗		
dob		✗	✗		

Buttons at the bottom include OK, Reset, and Exit.

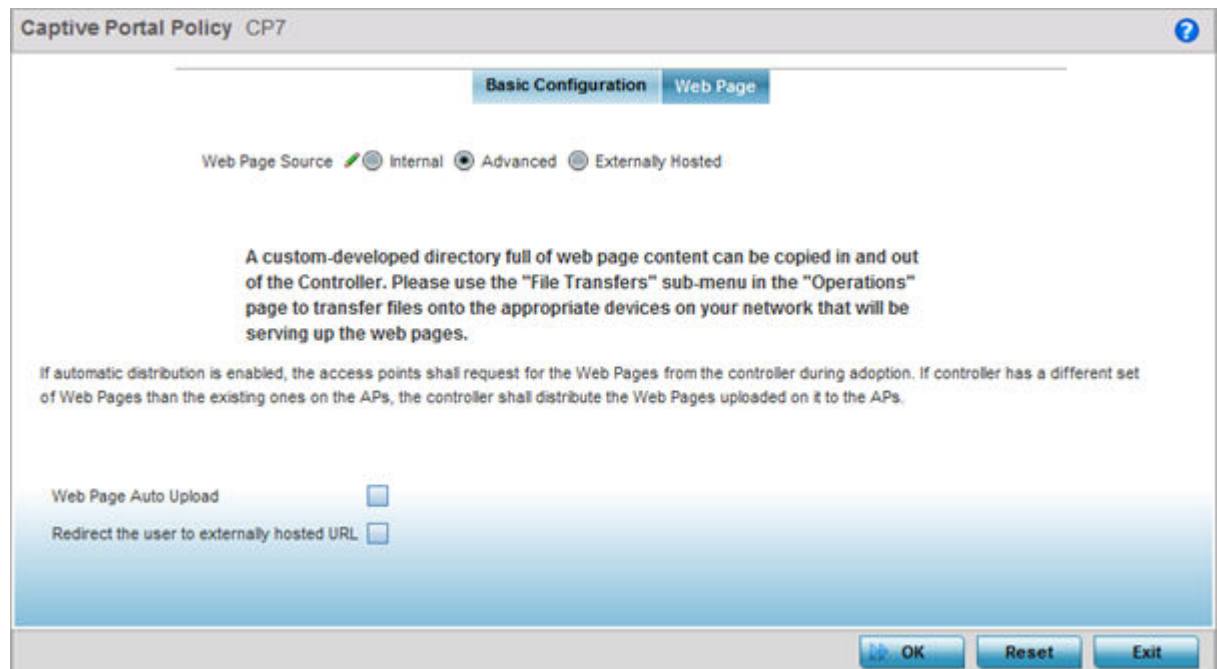
**Figure 295: Captive Portal Policy - Web Page - Internal - Registration - Registration Page Fields Table**

- 23 Click **OK** to save the changes made within any of the **Internal Page** screens.  
Click **Reset** to revert to the last saved configuration.

- 24 Select **Advanced** to use a custom-developed directory of web pages.

Web pages in the directory can be copied to and from the controller or service platform, to support the captive portal.

Use the File Transfers sub-menu in the **Operations** page to transfer files to the appropriate devices serving up the web pages.

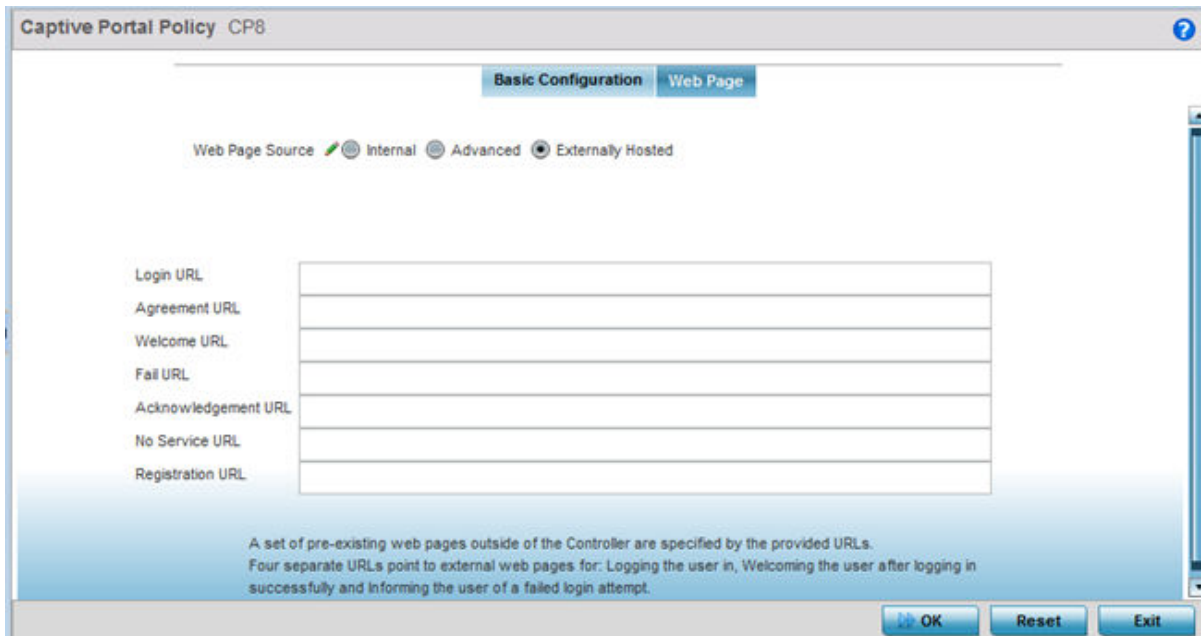


**Figure 296: Captive Portal Policy - Web Page Screen - Advanced Option**

- 25 Select the **Externally Hosted** radio button if hosting the captive portal on an external server resource.

Select 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 297: Captive Portal Policy - Web Page - Externally Hosted Option**

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.

26 Click **OK** when completed to update the captive portal's advanced configuration.

Click **Reset** to revert the screen back to its last saved configuration.

## Creating DNS Whitelists

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** .

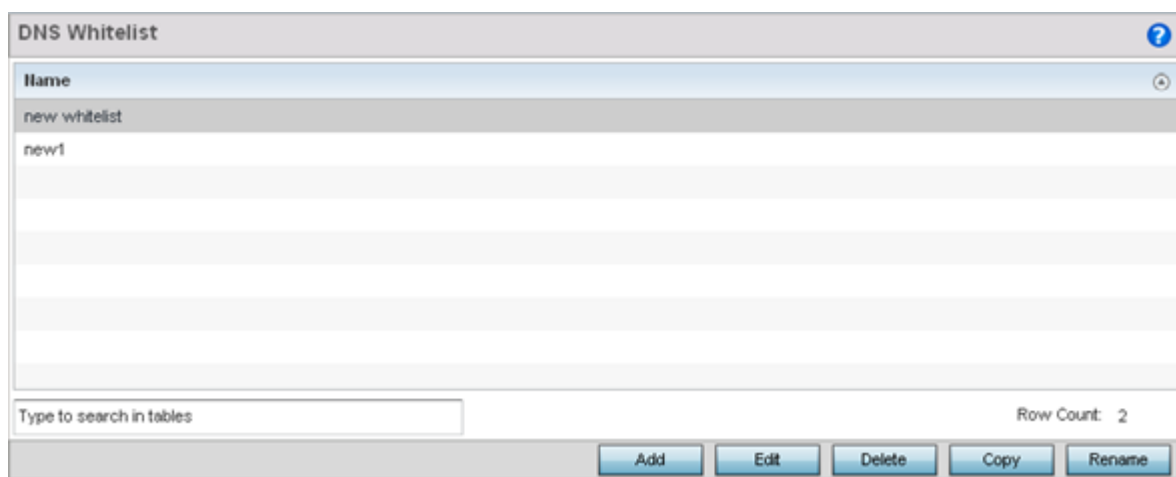
The upper, left-hand, side of the user interface displays a Services menu pane where Captive Portal, DHCP and RADIUS configuration options can be selected.

- 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**.

The **DNS Whitelist** screen displays.



**Figure 298: Captive Portal DNS Whitelist Screen**

- 4 Review the names of existing whitelists. 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 do the following:

- 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.

The screenshot displays a configuration window titled "Name DNSWhitelist1". Below the title bar, there is a section labeled "Whitelist Entries". This section contains a table with two main columns: "DNS Entry" and "Match Suffix".

DNS Entry	Match Suffix	
TestDevice		✓
* <input type="text"/>	Hostname	No

At the bottom right of the table area, there is a button labeled "+ Add Row". At the bottom of the window, there are three buttons: "OK", "Reset", and "Exit".

**Figure 299: Captive Portals - DNS Whitelist - Add DNS 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.

## Captive Portal Deployment Considerations

Before defining a captive portal configuration for a controller, service platform or access point, 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 be taken into consideration to meet each deployment's requirements.
- Captive portal authentication uses secure HTTPS to protect user credentials, but does not 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 does not 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.

## Setting the Guest Management Configuration

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 NX9000 series service platforms as an adopting controller with up to 2 million user identity entries. Guest registration is supported on NX 7500 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-databasebackup` command must be invoked using the CLI. For more information, refer to the *WiNG CLI Reference Guide*.

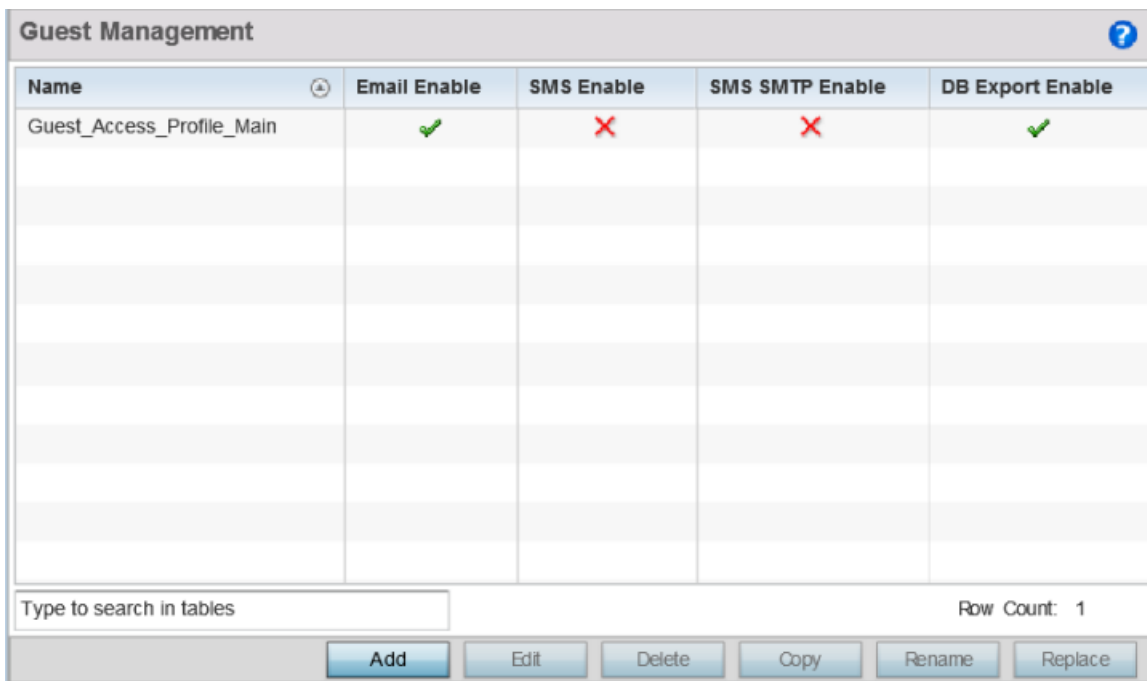
Refer to the following sections for configuring Guest Management parameters:

- [Email](#) on page 795
- [SMS](#) on page 797
- [SMS SMTP](#) on page 799
- [DB Export](#) on page 801

To set the guest management configuration:

- 1 Select **Configuration > Services > Guest Management**.

The **Guest Management** screen displays.



**Figure 300: 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 an existing configuration needs to be deleted.

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 the guest user’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 Click **Add** to create a new guest management configuration, choose an existing configuration and click **Edit** to modify its properties, or choose an existing guest management and click **Delete** to remove it from those available.

Click **Rename** to change the name of an existing guest management configuration or copy a configuration to a different location. Click **Replace** to replace an existing Guest Management policy with a new policy.

## Email

Guest users can register themselves with their email 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 email as the primary key for authentication:

- 1 Select **Configuration > Services > Guest Management**.

Review existing guest management configurations to determine whether new email configuration requires creation or an existing guest user configuration requires modification or deletion.

- 2 Select the **Email** tab.

**Figure 301: Guest Management - Add/Edit - Email Tab**

- 3 Set the following email guest user network address and message content information required for notifying a guest with a passcode using email:

Enable	Enable this option so guest users can register themselves with their email 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. 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 email 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 email credentials.

Security	Use the drop-down menu to select ssl or starttls as the email 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 email 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 email credentials.
Subject	Enter the 100 character maximum email subject for the email 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 email sent to the guest user along with the passcode. You can use the following tags in the message body. <ul style="list-style-type: none"> <li>• GM_NAME - indicates the guest user's name in the message. This tag is replaced by the guest user's name when the email is created.</li> <li>• GM_PASSCODE - indicates the password assigned to the user. The tag is replaced by the actual password when the email is created.</li> <li>• CR-NL - indicates a line break. When used, the word next to this tag starts on a new line when the email is created.</li> </ul>

4 Click **OK** to save the updates to the guest management Email configuration.

Click **Reset** to revert the screen back to its last saved configuration.

## SMS

SMS enables guest users to registers themselves with their email 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 email 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.

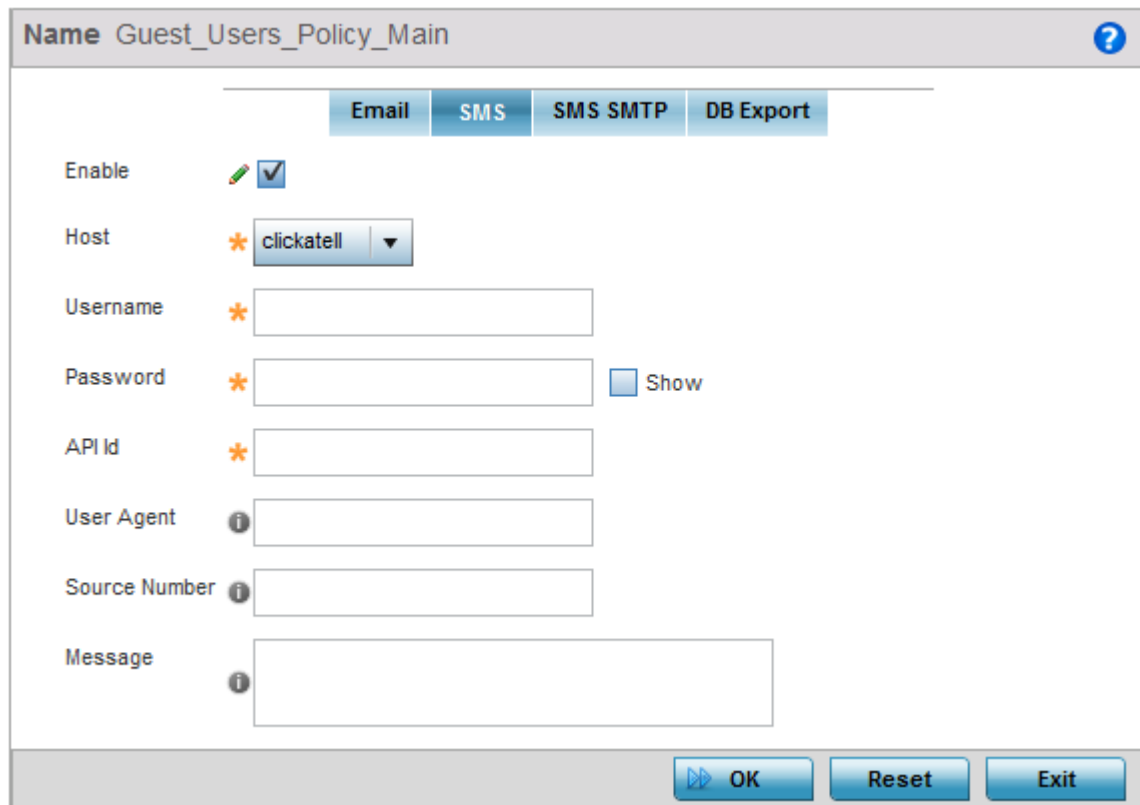
The default gateway used with SMS is Clickatell. A passcode can be sent with SMS to the guest user directly using Clickatell, or the passcode can be sent via email to the SMS Clickatell gateway server, and Clickatell sends the passcode SMS to the guest user.

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 302: Guest Management - Add/Edit - SMS Tab**

- 3 Set the following SMS guest user network address 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 email 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, <i>clickatell</i> is the only host SMS gateway server resource. Upon receiving the passcode email, 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 ( <a href="http://smtp_api_id">http/smtp api_id</a> ).

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 Click **OK** to save the updates to the guest management SMS configuration.  
Click **Reset** to revert the screen back to its last saved configuration.

## SMS SMTP

Optionally configure an email host server (for example: smtp.gmail.com) along with sender related credentials and the recipient gateway email address to which the message is emailed. The gateway server converts the email into SMS and sends the message to the guest user's mobile device.

When sending an email, the email 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 303: Guest Management - Add/Edit - 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 email host server (for example: smtp.gmail.com) along with sender related credentials and the recipient gateway Email address to which the message is emailed. 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 email 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 email credentials using SMTP.



Security	Use the drop-down menu to select <code>ssl</code> or <code>starttls</code> 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 <code>ssl</code> .
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 email address for the recipient of guest management email traffic.
Subject	Enter a 100 character maximum email subject for the email message sent to the guest user along with the required passcode.
Message	Enter a 1024 character maximum email message per the message format required by the gateway server. The sms-over-smtp message format is the required format from clickatell while sending email to the SMS gateway server.

- 4 Click **OK** to save the updates to the guest management SMS SMTP configuration.

Click **Reset** to revert the screen back to its last saved configuration.

## DB Export

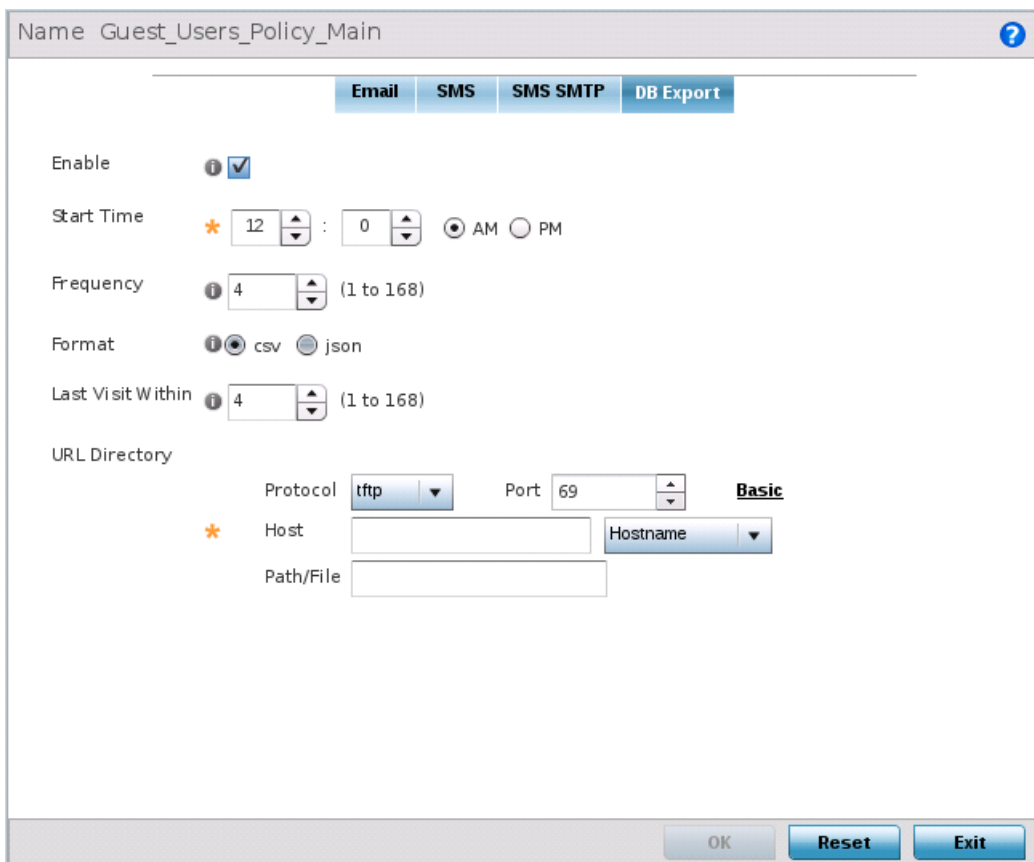
Optionally configure the guest user database export parameters. The guest user database can be periodically exported to an external server for backup and analysis.

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 304: Guest Management - Add/Edit - 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	The guest user database can be exported in the following formats: <ul style="list-style-type: none"> <li>• CSV</li> <li>• JSON</li> </ul> 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: <ul style="list-style-type: none"> <li>• tftp</li> <li>• ftp</li> <li>• sftp</li> <li>• http</li> <li>• cf</li> <li>• usb1-4</li> </ul>
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 Click **OK** to save the updates to the guest management DB Export configuration.  
Click **Reset** to revert the screen back to its last saved configuration.

## Setting the DHCP Configuration

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 a 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, [Profile Alias Configuration](#) on page 611.



**Note**

DHCP server updates are implemented only when the controller or service platform is restarted.

Refer to the following sections for more information on configuring DHCP parameters:

- [Defining DHCP Pools](#) on page 805
- [Defining DHCP Server Global Settings](#) on page 814
- [DHCP Class Policy Configuration](#) on page 816
- [DHCP Deployment Considerations](#) on page 818

To access and review the local DHCP server configuration:

- 1 Select **Configuration > Services > DHCP Server Policy**.

Review existing guest management configurations to determine whether new email configuration requires creation or an existing guest user configuration requires modification or deletion.

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.

DHCP Server Policy	Ignore BOOTP Requests	Ping Timeout
PrivateNetwork	<input checked="" type="checkbox"/>	10s

Type to search in tables Row Count: 1

**Figure 305: DHCP Server Policy Screen**

- 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 <b>DHCP Server Global Settings</b> 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 <b>DHCP Server Global Settings</b> screen.

- Click **Add** to create a new DHCP server policy, choose an existing policy and click **Edit** to modify the policy's properties, or choose an existing policy and click **Delete** to remove the policy from those available.

Adding or Editing a DHCP server policy displays the **DHCP Server Policy** screen by default. Click **Rename** to change the name of an existing policy or **Copy** a policy to a different location.

## Defining DHCP Pools

A *pool* (or range) of IP network addresses and DHCP options can be created for each IP interface configured. 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.

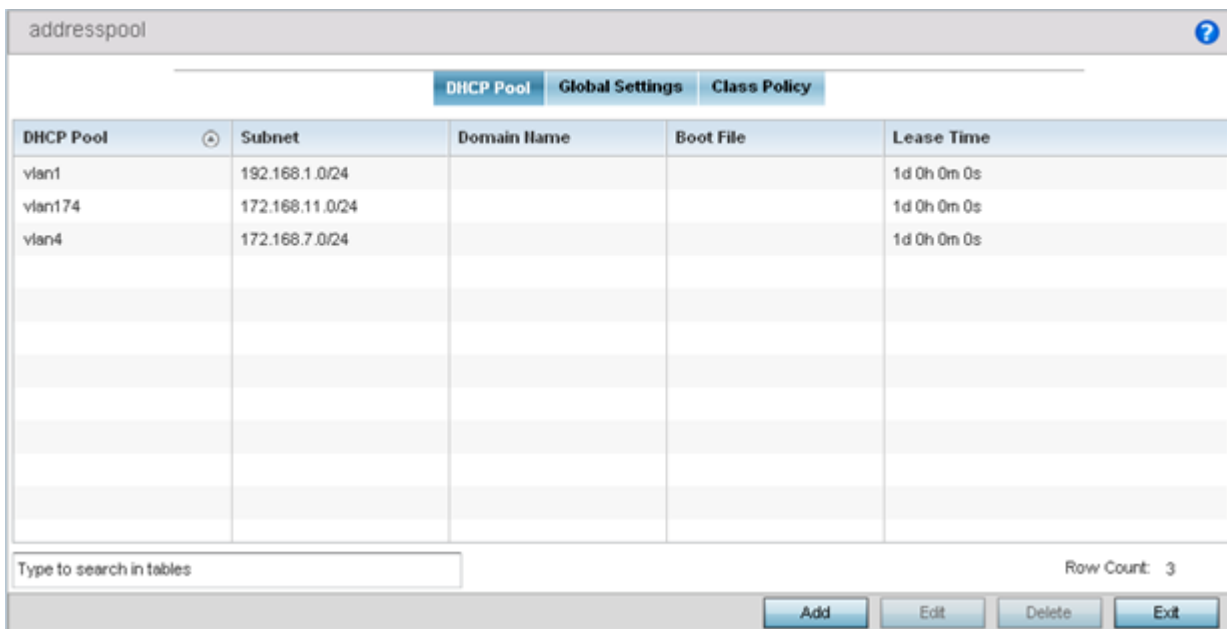
To define the parameters of a DHCP pool:

- 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 **DHCP Server Policy**.

The DHCP Server Policy screen displays the DHCP Pool tab by default.

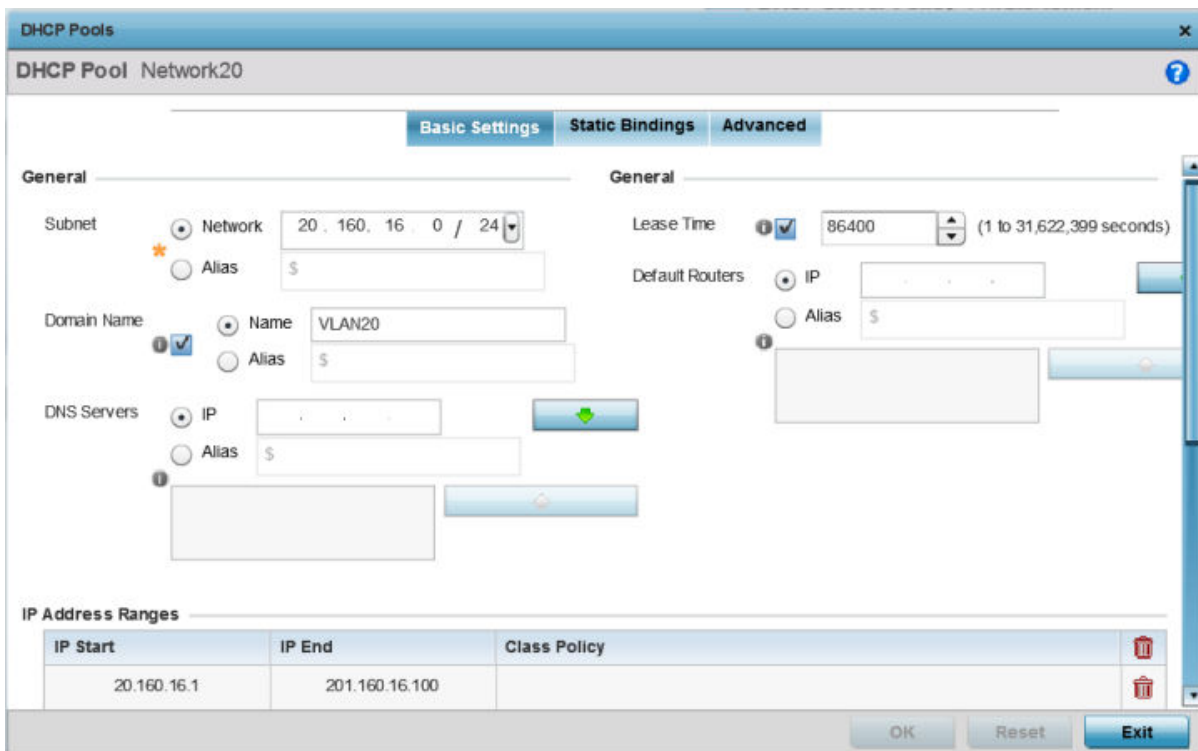


**Figure 306: DHCP Server Policy - Add/Edit - DHCP Pool Tab**

3 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 and mask used by clients requesting DHCP resources.
Domain Name	Displays the domain name defined used with this network pool. <i>Domain Name Services</i> (DNS) converts human-readable host names into IP addresses. Host names are not case sensitive and can contain alphabetic or numeric letters or a hyphen. A <i>fully qualified domain name</i> (FQDN) consists of a host name plus a domain name. For example, <i>computername.domain.com</i> .
Boot File	Boot files ( <i>Boot Protocol</i> ) 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 requesting DHCP client.

- 4 Select **Add** to create a new DHCP pool, **Edit** to modify an existing pool's properties or **Delete** to remove a pool from among those available.



**Figure 307: DHCP Pools - Add/Edit - Basic Settings Tab**

If you are 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.

- 5 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) are required to match the addresses of the layer 3 interface for the addresses to be supported through that interface. If you are setting a subnet IP alias, ensure that 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, <i>computername.domain.com</i> . If you are setting a domain name alias, ensure that it begins with a dollar sign (\$) and does not exceed 32 characters. A numeric IP address 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 you are setting a DNS IP alias, ensure that 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 eight 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. If you are setting a default router IP alias, ensure that it begins with a dollar sign (\$) and does not exceed 32 characters. An actual router IP address is the default setting, not an alias.

- 6 Define the range of included (starting and ending IP addresses) addresses for this particular pool. Use the **IP Address Ranges** field for this operation.
  - 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 the **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.
- 7 Refer to the **Excluded IP Address Range** field and select the **+Add Row** button.

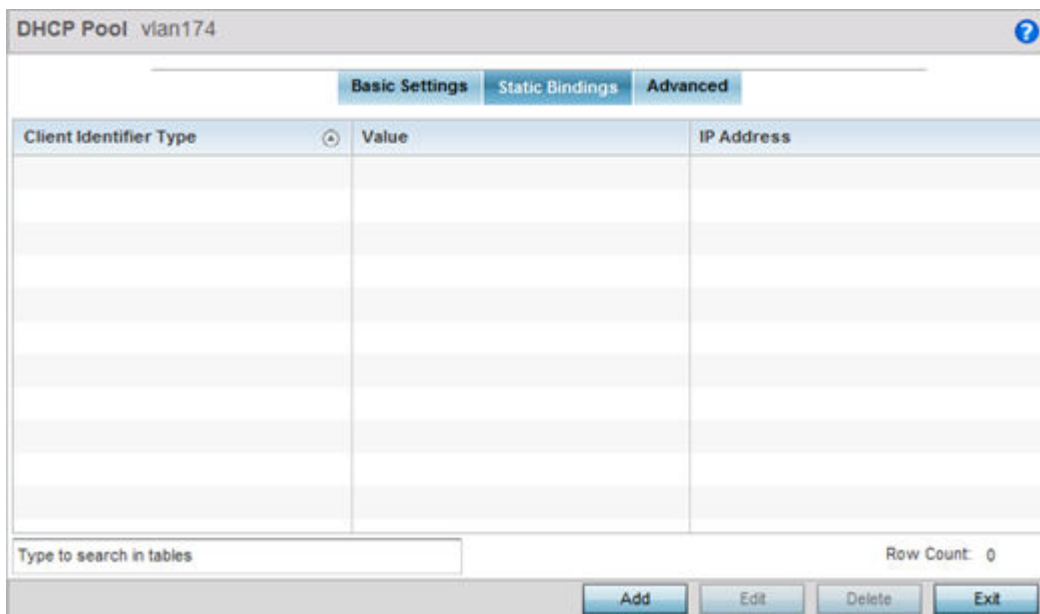
Add ranges of IP address to exclude from lease to requesting clients. Having ranges of unavailable addresses is a good practice to ensure IP address resources are in reserve. Select the **Delete** icon as needed to remove an excluded address range.
- 8 Click **OK** to save the updates to the DHCP Pool Basic Settings tab.

Click **Reset** to revert to the last saved configuration.



- 9 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.

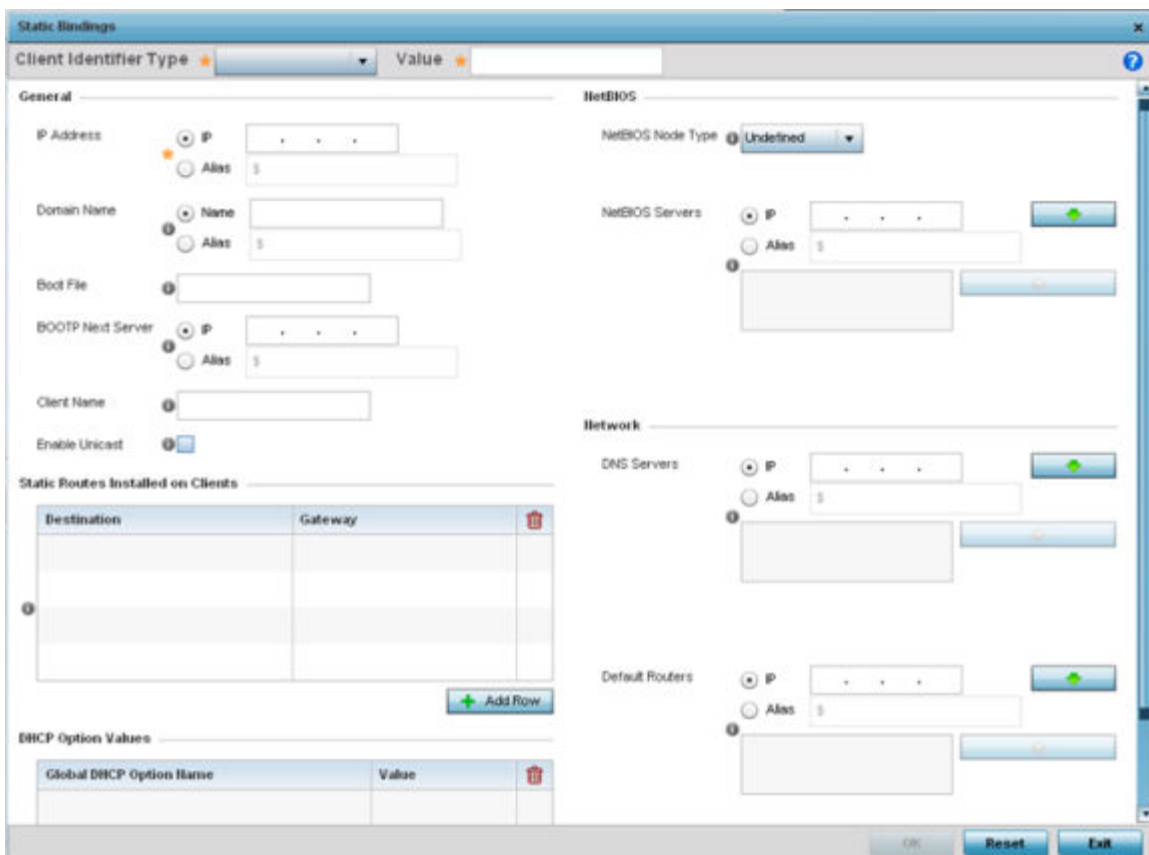


**Figure 308: DHCP Pools - Add/Edit - Static Bindings Tab**

- 10 Review existing DHCP pool static bindings to determine if a static binding can be used as is, if a new binding requires creation or edit, or if a binding requires deletion:

Client Identifier Type	Whether the reporting client is using a hardware address or client identifier as its identifier type within requests to the DHCP server.
Value	The hardware address or client identifier assigned to the client when added or last modified.
IP Address	The IP address of the client on this interface that's currently using the pool name listed.

- Click **Add** to create a new static binding configuration, **Edit** to modify an existing static binding configuration or **Delete** to remove a static binding from among those available.



**Figure 309: DHCP Pools - Add/Edit - Static Bindings - Add Screen**

- 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 <b>Alias</b> to provide an IP alias beginning with a dollar sign (\$) and not exceeding 32 characters.
Domain Name	Provide a domain name for the current interface. Domain names are not case sensitive and can contain letters, numbers, and hyphens. A fully qualified domain name (FQDN) consists of a host name plus a domain name. For example, <i>computername.domain.com</i> . The Name option is selected by default. Optionally select <b>Alias</b> 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 <b>Alias</b> 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 is just one sender and one receiver). Select this option to forward unicast messages to just a single device within this network pool. This setting is disabled by default.

- 13 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: <ul style="list-style-type: none"> <li>• Broadcast - Uses broadcasting to query nodes on the network for the owner of a NetBIOS name.</li> <li>• 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.</li> <li>• Mixed - A mixed node using broadcast queries to find a node, and failing that, queries a known p-node name server for the address.</li> <li>• Hybrid - A combination of two or more nodes.</li> <li>• Undefined - No node type is applied.</li> </ul>
NetBIOS Servers	Specify a numerical IP address of a single NetBIOS WINS server or a group of servers available to requesting clients. A maximum of eight 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.

- 14 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.

- 15 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 one a **Global DHCP Option Name** to help differentiate it from others with similar configurations. Select the radio button for 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 through 254.
 

A vendor-specific option definition only applies to the vendor class for which it is defined.



- 16 In the **Network** field, define one or more of DNS Servers and Default Routers to translate domain names to IP addresses.

Up to eight IP addresses can be provided. The IP option is selected by default for both DNS Servers and Default Routers. foo

Optionally, select **Alias** to provide an IP alias beginning with a dollar sign (\$) and not exceeding 32 characters.

- 17 Click **OK** when completed to update the static bindings configuration.

Click **Reset** to revert the screen back to its last saved configuration.

- 18 Select the Advanced tab to define additional NetBIOS and Dynamic DNS parameters.

The screenshot shows the 'Advanced' tab of the DHCP Pools configuration window. The window title is 'DHCP Pools' and the specific pool is 'vlan174'. The 'Basic Settings' tab is selected. The 'General' section contains fields for 'Boot File', 'BOOTP Next Server' (with radio buttons for 'IP' and 'Alias'), and 'Enable Unicast'. The 'NetBIOS' section includes 'NetBIOS Node Type' (set to 'None') and 'NetBIOS Servers' (with radio buttons for 'IP' and 'Alias'). The 'Dynamic DNS' section, noted as 'Not Applicable for Static Bindings', includes 'DNS Domain Name' (with radio buttons for 'Name' and 'Alias'), 'DDNS TTL' (set to 1), 'DDNS Multi User Class', 'Update DNS' (set to 'Do Not Update'), and 'DNS Server' (with radio buttons for 'IP' and 'Alias'). The 'DHCP Option Values' section features a table with columns 'Global DHCP Option Name' and 'Value', and an 'Add Row' button. The 'Static Routes Installed on Clients' section features a table with columns 'Destination' and 'Gateway', and an 'Add Row' button. At the bottom of the window are 'OK', 'Reset', and 'Exit' buttons.

**Figure 310: DHCP Pools - Add/Edit - Advanced Tab**

19 To add or modify the DHCP pool's advanced settings, set the following General parameters:

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 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.

20 Set the following **NetBIOS** parameters for the network pool:

NetBIOS Node Type	Set the NetBIOS Node Type used with this particular pool. The following options are available: <ul style="list-style-type: none"> <li>• Broadcast - Uses broadcasting to query nodes on the network for the owner of a NetBIOS name.</li> <li>• 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.</li> <li>• Mixed - Mixed uses broadcast queries to find a node, and failing that, queries a known p-node name server for the address.</li> <li>• Hybrid - A combination of two or more nodes.</li> <li>• Undefined - No NetBIOS node type is applied.</li> </ul>
NetBIOS Servers	Specify a numerical IP address of a single NetBIOS WINS server or a group of servers available to requesting clients. A maximum of eight 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.

21 Refer to the **DHCP Option Values** table to set Global DHCP options applicable to all clients, whereas a set of subnet options applies only to 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 through 254.

A vendor-specific option definition applies only to the vendor class for which it is defined.

22 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, <i>test.net</i> . The <b>Name</b> option is selected by default. Optionally select <b>Alias</b> 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 <b>Do Not Update</b> , <b>Update from Server</b> , or <b>Update from Client</b> . The default setting is <b>Do Not Update</b> , 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 <b>Alias</b> to provide a DDNS server IP alias beginning with a dollar sign (\$) and not exceeding 32 characters.

23 Refer to the **Static Routes Installed on Clients** table to set fixed routes for client destination and gateways.

Select the **+ Add Row** button to add individual options for Destination and Gateway addresses.

24 Click **OK** to save updates to the DHCP pool's Advanced settings.

Click **Reset** to revert the screen to its last saved configuration.

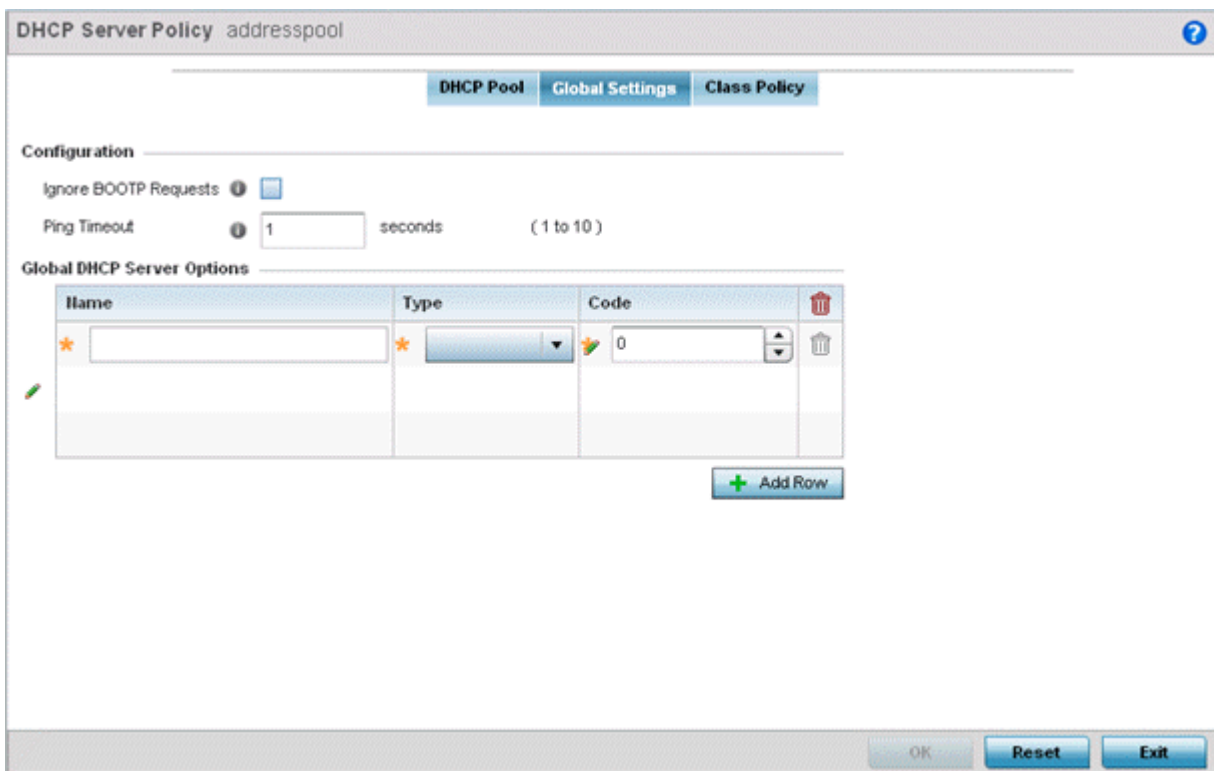
## Defining DHCP Server Global Settings

Set a DHCP server global configuration by defining whether BOOTP requests are ignored and by defining DHCP global server options.

To define DHCP server global settings:

- 1 Select **DHCP Server Policy** from within the Services menu pane.  
**Add** or **Edit** an existing policy.

- 2 Select the **Global Settings** tab.



**Figure 311: DHCP Server Policy - Add/Edit - Global Settings Tab**

- 3 Set the following parameters within the **Configuration** field:

Ignore BOOTP Requests	Select the check box 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 determine whether a client requested IP address is already used.

- 4 Set the **Activation Criteria** for the DHCP server policy:

Select the **Criteria** option to invoke a drop-down menu to determine when the DHCP daemon is invoked. Options include **vrrp-master**, **cluster-master** or **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, an ASCII string, or a hex string.  
Highlight an entry from within the **Global Options** screen and click the **Remove** button to delete the name and value.
- 6 Click **OK** to save the updates to the DHCP server global settings.  
Click **Reset** to revert the screen to its last saved configuration.

## DHCP Class Policy Configuration

A controller, service platform or Access Point's local DHCP server assigns IP addresses to requesting DHCP clients based on user class option names. The DHCP server can assign IP addresses from as many IP address ranges as defined by an 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.

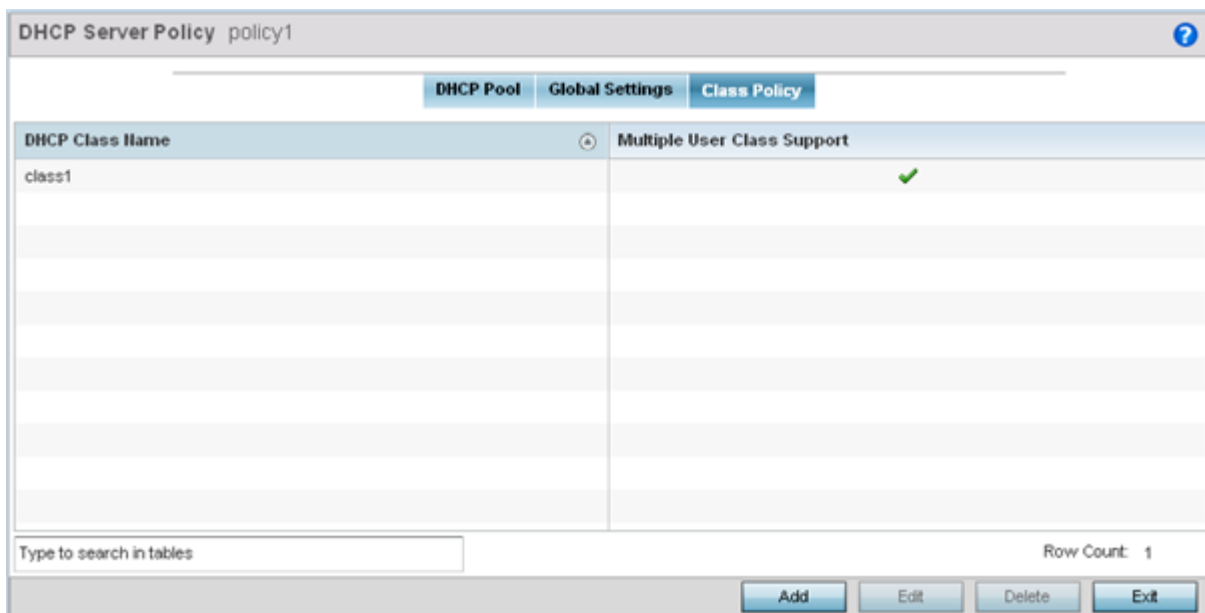
Refer to the **DHCP Class Policy** screen to review existing DHCP class names and their current multiple user class designations. Multiple user class options enable a user class to transmit option values to DHCP servers supporting multiple user class options. Either add a new class policy, edit the configuration of an existing policy or permanently delete a policy as required.

To review DHCP class policies:

- 1 Select **DHCP Server Policy** from within the Services menu pane.  
**Add** or **Edit** an existing policy.



- 2 Select the **Class Policy** tab.



**Figure 312: DHCP Server Policy - 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	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 <i>enabled</i> or <i>disabled</i> for existing class names by editing the class name's configuration.

- Click **Add** to create a new DHCP class policy, **Edit** to update an existing policy or **Delete** to remove an existing policy.

**DHCP Class** x

DHCP Class Name class 3 ?

**Settings**

User Class

Option	Value
Option 1	101
Option 2	
Option 3	
Option 4	
Option 5	
Option 6	
Option 7	
Option 8	

Multiple User Class Support

OK Reset Exit

**Figure 313: DHCP Class Name Add Screen**

- If you are 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.
- Select a row within the **Value** column to enter a 32-character maximum value string.
- Select **Multiple User Class** 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.
- Click **OK** to save the updates to this DHCP class policy.  
Click **Reset** to revert the screen to its last saved configuration.

## DHCP Deployment Considerations

Before defining an DHCP server configuration, refer to the following deployment guidelines to ensure the configuration is optimally effective:

- DHCP option 189 is required when AP650 model 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 that traffic can pass on UDP ports 67 and 68 for clients receiving DHCP information.

## Setting the Bonjour Gateway Configuration

---

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](#)

## Configuring a Bonjour Discovery Policy

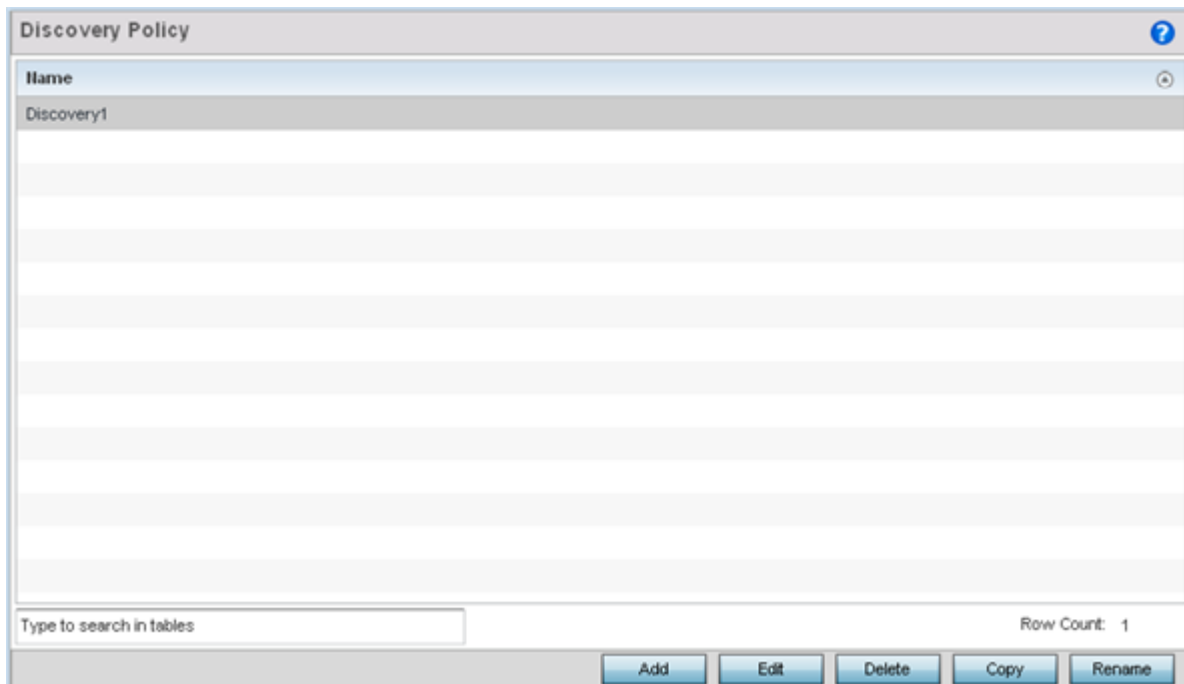
The Bonjour discovery policy configures how Bonjour services are located. It configures the VLANs on which these services can be found.

To display Bonjour discovery policy information:

- 1 Select **Configuration**.
- 2 Select **Services**.
- 3 Select **Bonjour Gateway** to expand its submenu.

- 4 Select **Discovery Policy**.

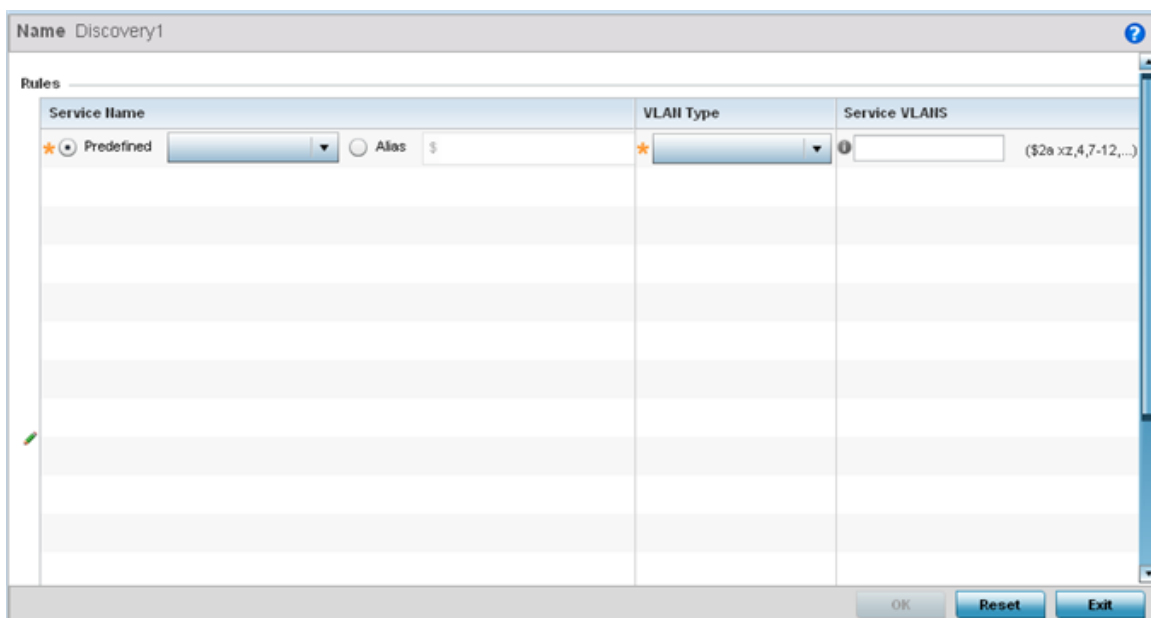
The **Discovery Policy** screen displays the name of the configured Bonjour discovery policies.



**Figure 314: Bonjour Gateway - Discovery Policy Screen**

- 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 315: Bonjour - Discovery Policy - Add/Edit Policy Screen**

- 6 Select the **+ Add Row** button to add a rule to the Bonjour discovery policy.

These are the services discoverable by the Bonjour gateway.

- 7 Set the following discovery attributes for the discovery policy configuration:

Service Name	<p>Define the service that can be discovered by the Bonjour gateway.</p> <ul style="list-style-type: none"> <li>• <b>Predefined</b> - Use the drop-down menu to select from a list of predefined Apple services (Scanner, Printer, HomeSharing etc.).</li> <li>• <b>Alias</b> - Use an existing alias to define a service that is not available in the predefined list.</li> </ul>
VLAN Type	<p>Use the drop-down menu to select the VLAN type.</p> <ul style="list-style-type: none"> <li>• <b>local</b> - The VLAN(s) defined in the <b>Service VLAN</b> field use a local bridging mode.</li> <li>• <b>tunneled</b> - The VLAN(s) defined in the <b>Service VLAN</b> field are shared tunnel VLANs.</li> </ul>
Service VLANs	<p>Provide a VLAN or a list of VLANs on which the selected service is discoverable.</p>
Instance Name	<p>Optionally, specify the selected Bonjour service's instance name. When specified, the Bonjour service discovery queries contain the instance name. of the service to be discovered. You can either directly specify the string value to be used as a match criteria, or use a string alias (for example, \$BONJOURSTRING) to identify the string to match. If using a string alias, ensure that it is existing and configured. For information on configuring a string alias, see <a href="#">Network Basic Alias Configuration</a> on page 487.</p> <p>This option is useful especially in large distributed, enterprise networks. Use it to create different instances of a Bonjour service for the different organizations or departments (VLANs) within your network. Creating instances allows you to advertise specific service instances for a specific set of VLANs, instead of advertising top-level Bonjour Services to various allocated VLAN(s).</p>

- 8 Click **OK** to save updates to this Bonjour Discovery policy.

Click **Reset** to revert the screen to its last saved configuration.

## Configuring a Bonjour Forwarding Policy

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

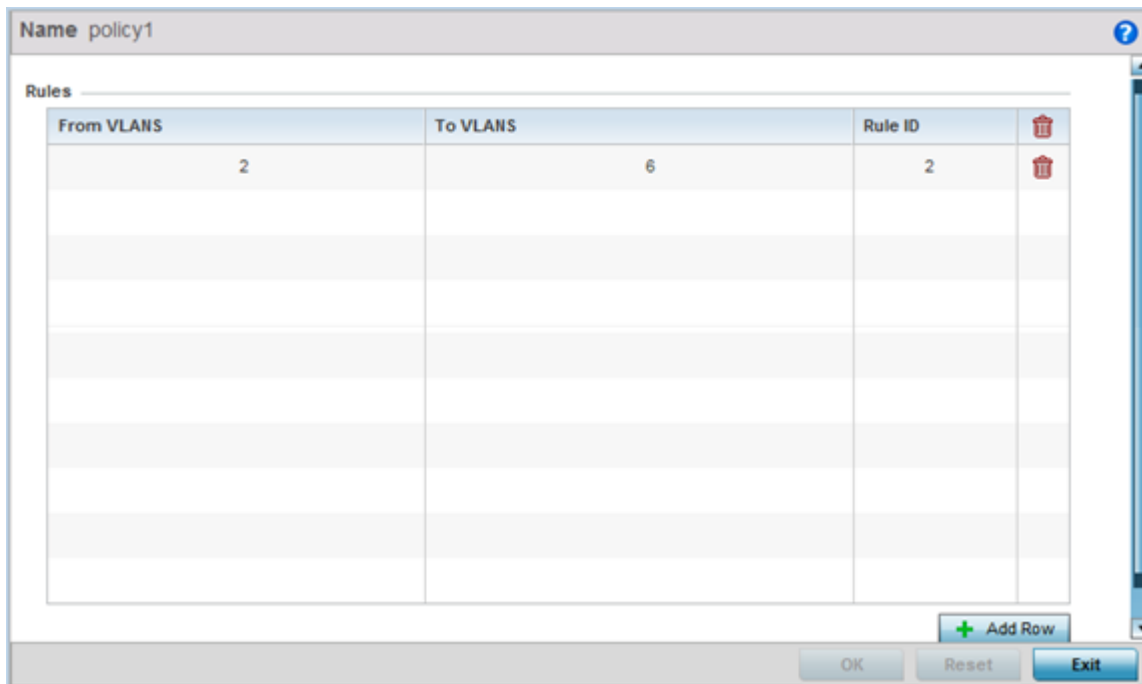
There must be Layer 2 connectivity between devices for forwarding to work.

To display Bonjour forwarding policy information:

- 1 Select **Configuration**.
- 2 Select **Services**.
- 3 Select **Bonjour Gateway** to expand its submenu.

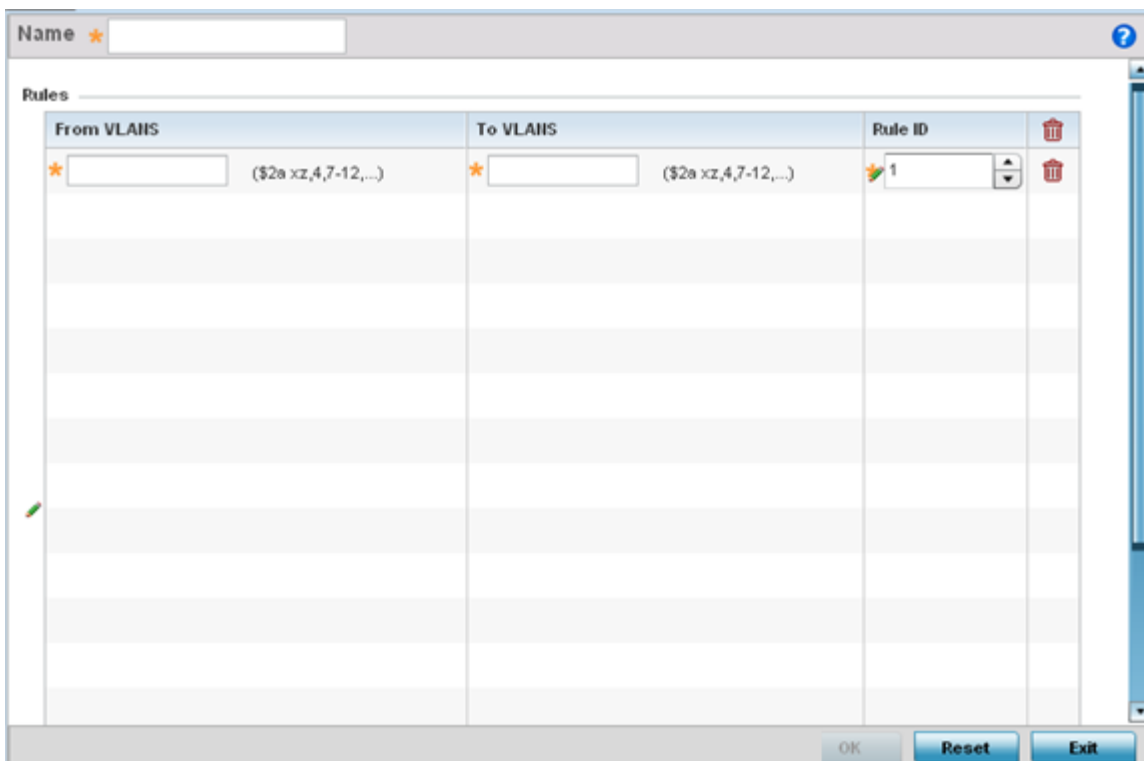
4 Select **Forwarding Policy**.

The screen displays the name of existing Bonjour forwarding policies.



**Figure 316: Bonjour Gateway - Forwarding Policy Screen**

- Select an existing policy and select **Edit** to modify its configuration or select **Add** to create a new configuration..



**Figure 317: Bonjour Gateway - Forwarding Policy - Add Screen**

- 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.

- Click **OK** to save updates to this Bonjour Gateway Forwarding policy. Click **Reset** to revert the screen to its last saved configuration.

## Setting the DHCPv6 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.

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.

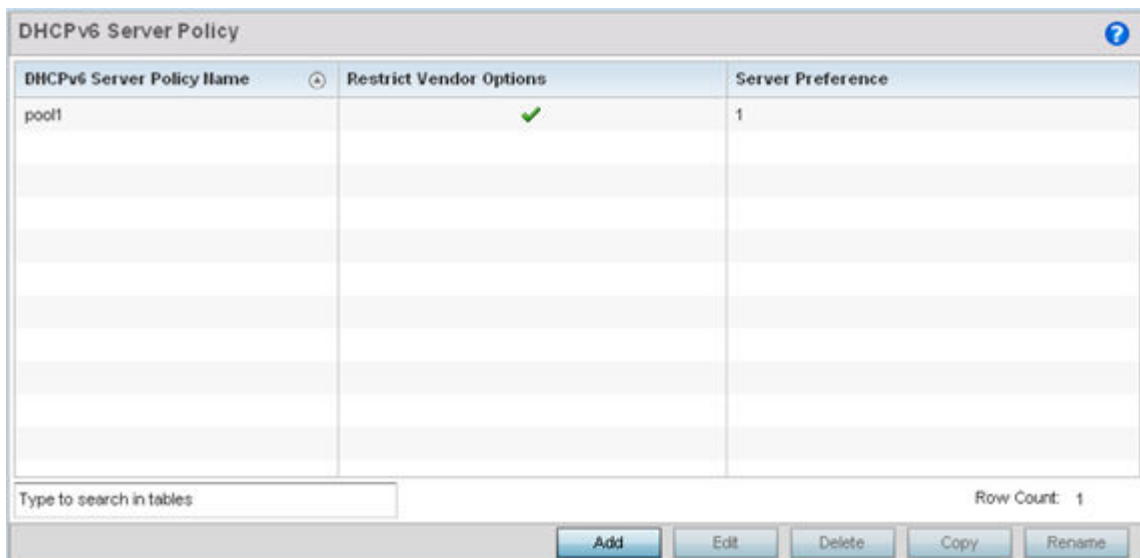
Refer to the following for more information on configuring the DHCPv6 Server Policy parameters:

- [Defining DHCPv6 Options](#) on page 825
- [DHCPv6 Pool Configuration](#) on page 827

To access and review the local DHCPv6 server configuration:

- 1 Select **Configuration > Services > DHCPv6 Server Policy**.

The DHCPv6 Server Policy screen displays.



**Figure 318: 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	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 apply only to the vendor class defined.
Server Preferences	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.

## Defining DHCPv6 Options

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 properties of a selected DHCPv6 server policy.

Select **+ Add Row** to populate the screen with editable rows for DHCPv6 option configuration.

**Figure 319: DHCPv6 Server 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.

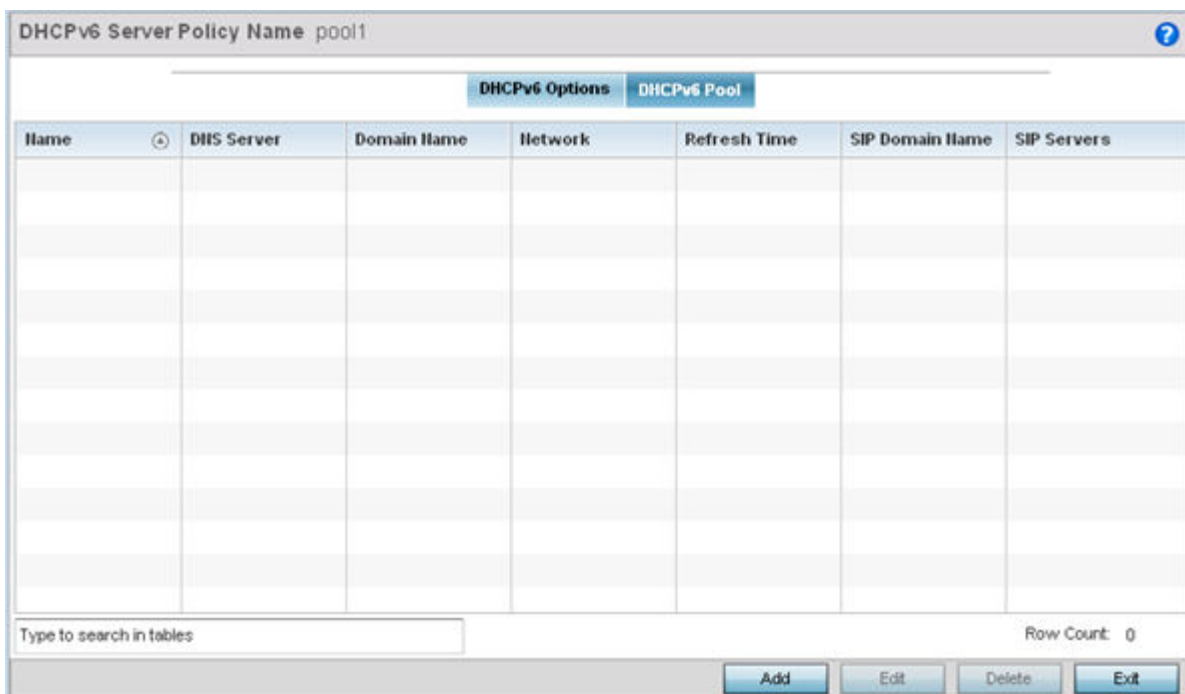
- Click **OK** to save the updates to the DHCPv6 options.  
Click **Reset** to revert the screen to its last saved configuration.

## DHCPv6 Pool Configuration

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:

- Select **Configuration > Services > DHCPv6 Server Policy**.  
The DHCPv6 Options tab displays by default.
- Select **Add** to create a new policy or **Edit** to modify the properties of a selected DHCPv6 server policy.  
Select **+ Add Row** to populate the screen with editable rows for DHCPv6 option configuration.
- Select the DHCPv6 Pool tab.



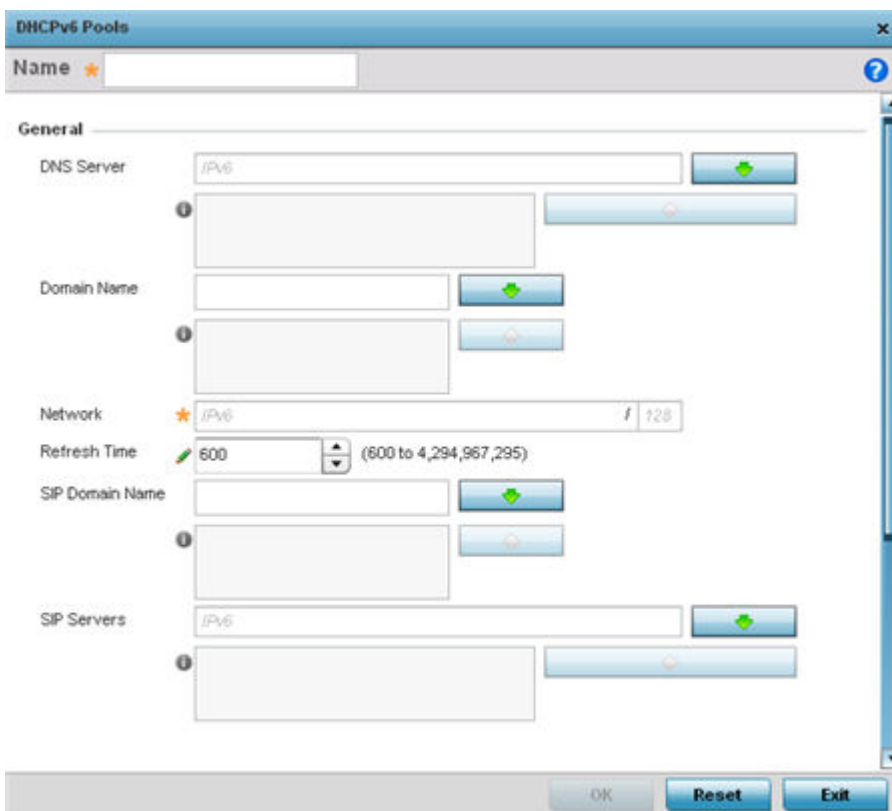
**Figure 320: DHCP Server Policy - DHCPv6 Pool Tab**

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 <b>Add/Edit</b> screen.
Refresh Time	Displays the time, in seconds, between refreshes of the DHCPv6 address pool.
SIP DomainName	Displays the domain name associated with the Session Initiation Protocol (SIP) server that 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 321: 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 DomainName	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 you are 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.  
Click **Reset** to revert to the last saved configuration.

## Setting the RADIUS Configuration

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 controller, service platform or access point's 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 controller, service platform or access point, 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 access point's 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.

Controllers and service platforms have full internal RADIUS resource capability. Additionally, all access points maintain a local RADIUS resource.

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 the 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](#) on page 830
- [Defining User Pools](#) on page 833
- [Configuring RADIUS Server Policies](#) on page 838
- [RADIUS Deployment Considerations](#)

## Creating RADIUS Groups

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 the RADIUS Groups menu:

- 1 Select **Configuration > Services > RADIUS** from the main menu.

2 Select **Groups**.

The browser displays a list of the existing groups.

RADIUS Group Policy	Guest User Group	Management Group	Role	VLAN	Time Start	Time Stop
group1	X	X		Not Set	12:00 am	11:59 pm
GUEST-USERS	✓	X		Not Set	12:00 am	11:59 pm
guestgroup	✓	X		Not Set	12:00 am	11:59 pm

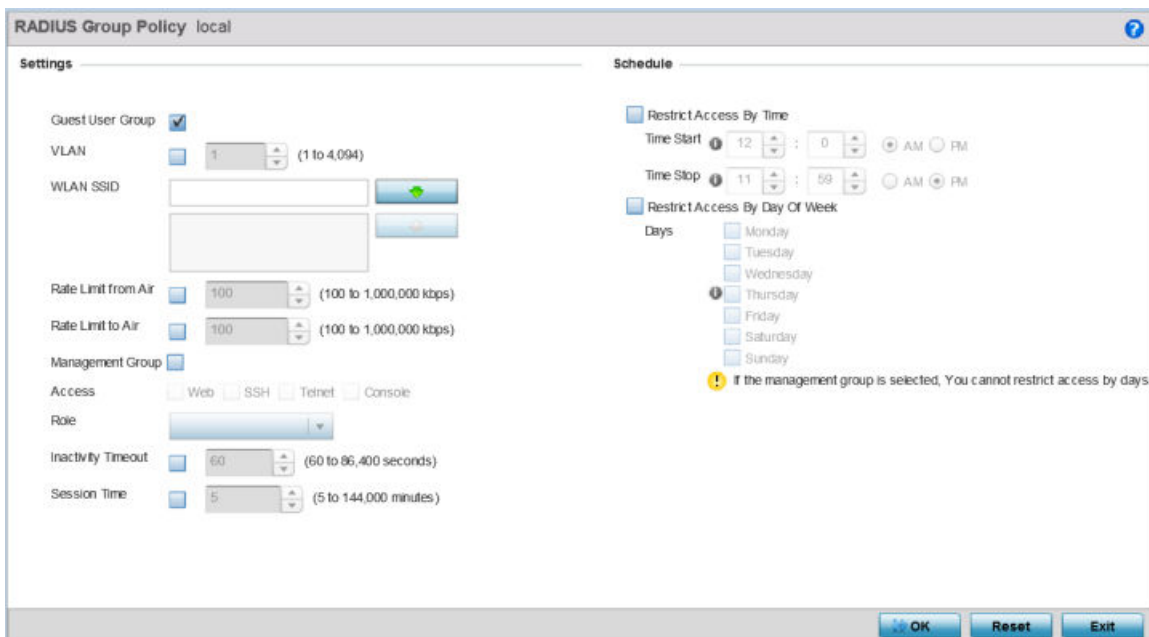
Type to search in tables Row Count: 3

**Figure 322: RADIUS Group Screen**

3 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: <ul style="list-style-type: none"> <li>• <b>monitor</b> - Read-only access</li> <li>• <b>helpdesk</b> - Helpdesk/support access</li> <li>• <b>network-admin</b> - Wired and wireless access</li> <li>• <b>security-admin</b> - Full read/write access</li> <li>• <b>system-admin</b> - System administrator access</li> </ul>
VLAN	Displays the group'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.

- Click **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 323: RADIUS Group Policy - Add/Edit Screen**

- Define the following settings to define the user group configuration:

RADIUS Group Policy	If you are 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. If set as management group, assign member roles (System-Admin, Help Desk etc.) using the <b>Role</b> drop-down menu. This feature is disabled by default.



Access	<p>If a group is listed as a management group, assign how the devices can be accessed. Available access types are:</p> <ul style="list-style-type: none"> <li>• <b>Web</b> - Web access through browser is permitted.</li> <li>• <b>SSH</b> - SSH access through command line is permitted.</li> <li>• <b>Telnet</b> - Telnet access through command line is permitted.</li> <li>• <b>Console</b> - Console access to the device is permitted.</li> </ul> <p>The conditions defined within the policy are applied to authentication requests on these interfaces only.</p>
Role	<p>If a group is listed as a management group, it may also have a unique role assigned. Available roles include:</p> <ul style="list-style-type: none"> <li>• <b>monitor</b> - Read-only access</li> <li>• <b>helpdesk</b> - Helpdesk/support access</li> <li>• <b>network-admin</b> - Wired and wireless access</li> <li>• <b>security-admin</b> - Full read/write access</li> <li>• <b>system-admin</b> - System administrator access</li> </ul>
Inactivity Timeout	<p>Select the option to enable inactivity timeout. Use the drop-down menu to specify an interval in Seconds (60 - 86,400). When, for this duration no frame is received, the session is timed out.</p>
Session Time	<p>Select the option to enable session timeout. Use the drop-down menu to set a client session time in Minutes (5 - 144,000). This is the session time a client is granted upon successful authentication. When this time expires, the RADIUS session is terminated.</p>

- 6 Set the **Schedule** to configure access times and dates.

Select **Restrict Access By Time** to enable time-based access.

Time Start	<p>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 <b>AM</b> or <b>PM</b> radio button to set the time as morning or evening.</p>
Time Stop	<p>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 <b>AM</b> or <b>PM</b> radio button to set the time as morning or evening. If already logged in, the RADIUS group user is deauthenticated from the WLAN.</p>
Days	<p>Optionally select the <b>Restrict Access by Day Of Week</b> option, and select the days on which RADIUS group members can access RADIUS resources. This is an additional means of refining the access permissions of RADIUS group members.</p>

- 7 Click **OK** to save the changes.

Click **Reset** to revert to the last saved configuration.

## Defining User Pools

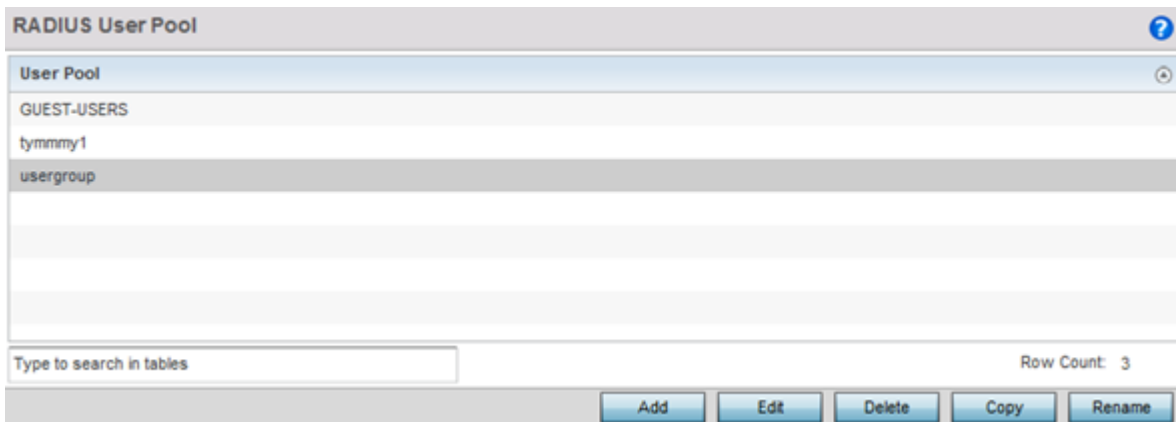
A user pool defines policies for individual user access to local (controller, service platform or Access Point managed) RADIUS resources. User pools are a convenient means of providing RADIUS resources based on the pool's unique permissions (temporary or permanent). A pool can contain a single user or group of users.

To configure a RADIUS user pool and unique user IDs:

- 1 Select **Configuration > Services > RADIUS** from the main menu.

2 Select **User Pools**.

The **RADIUS User Pool** screen lists the default pool along with any other admin created user pool.

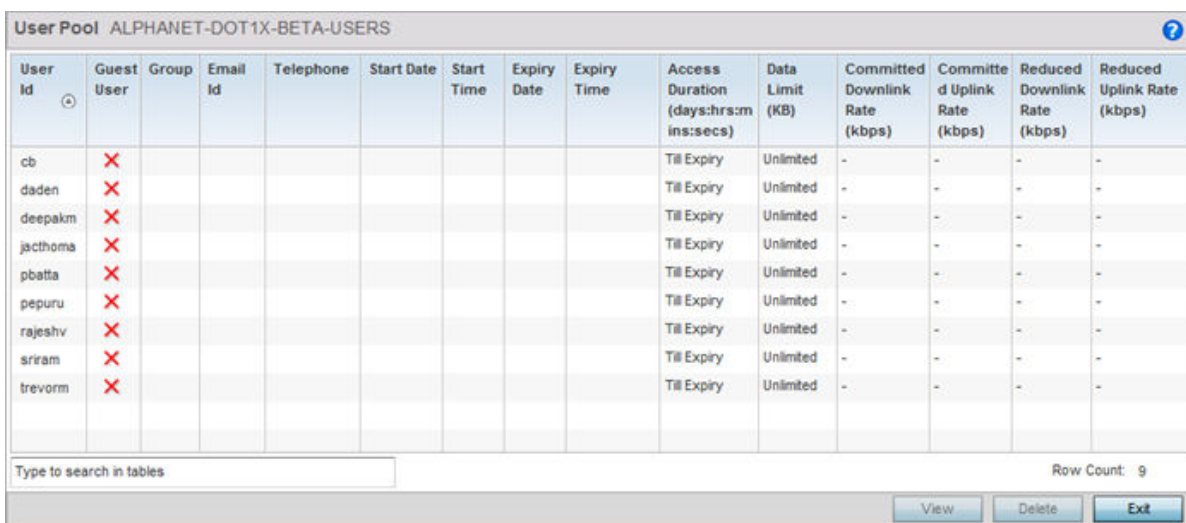


**Figure 324: RADIUS User Pool Screen**

3 Click **Add** to create a new RADIUS user pool, **Edit** to modify the configuration of an existing pool, or **Delete** to permanently remove a selected pool.

4 If you are creating a new pool, assign it a name up to 32 characters and click **Continue**.

The name should be representative of the users comprising the pool and/or the temporary or permanent access privileges assigned.



**Figure 325: RADIUS User Pool - User Pools - Details Screen**

5 Refer to the following **User Pool** configurations.

They define when specific user IDs have access to RADIUS resources.

User ID	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	The group name each configured user ID is a member.
Email ID	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	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	The month, day and year the listed user ID can access local RADIUS server resources.
Start Time	The time the listed user ID can access local RADIUS server resources. The time applies only to the range defined by the start and expiry date.
Expiry Date	The month, day and year the listed user ID can no longer access local RADIUS server resources.
Expiry Time	The time the listed user loses access to RADIUS server resources. The time applies only to the range defined by the start and expiry date.
Access Duration (days:hrs:mins:secs)	The amount of time a user is allowed access when time-based access privileges are applied. The duration cannot exceed 365 days.
Data Limit (KB)	The total amount of bandwidth (in kilobytes) consumable by each guest user.
Committed Downlink Rate (kbps)	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 <b>Reduced Downlink Rate</b> .
Committed Uplink Rate (kbps)	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 <b>Reduced Uplink Rate</b> .
Reduced Downlink Rate (kbps)	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 <b>Reduced Downlink Rate</b> .
Reduced Uplink Rate (kbps)	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 <b>Reduced Uplink Rate</b> .

- Click **Add** to add a new RADIUS user, **Edit** to modify the configuration of an existing user or **Delete** to remove an existing user ID.

**Figure 326: RADIUS User Pool - Add/Edit - Users Screen**

- Refer to the following settings to create a new user 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 <b>Show</b> checkbox to expose the password’s actual character string. Otherwise the password displays as a string of asterisks (*).
Guest User	Select the check box 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 has been defined as a guest, use the <b>Group</b> drop-down menu 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 no groups are relevant to the user’s intended access, select the <b>Create</b> link (or icon for guests) and create a new group configuration suitable for the user’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	Specify 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.

- 8 Refer to 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 <b>AM</b> and <b>PM</b> 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 <b>Till Expiry</b> radio button.
Expiry Time	If you are using the <b>Till Expiry</b> option, enter an end time, or use the spinner controls to select an ending time for the user's credentials to expire. Use the <b>AM</b> and <b>PM</b> 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 <b>Till Expiry</b> 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.

- 9 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 <b>Reduced Downlink Rate</b> .
Reduced Downlink Rate	Use the spinner control to specify a reduced speed for guest operation when they have 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 <b>Reduced Downlink Rate</b> . 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 <b>Reduced Uplink Rate</b> .
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 <b>Reduced Uplink Rate</b> . Once a value is configured, select the measurement as either MBPS (Megabytes per second) or KBPS (Kilobytes per second).

- 10 Click **OK** to save the user's group membership configuration.

Click **Reset** to revert to the last saved configuration.

## Configuring RADIUS Server Policies

A RADIUS server policy is a unique authentication and authorization configuration for client 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 controller, service platform or Access Point's local RADIUS server has 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 or manage the modification of existing policies:

- 1 Select **Configuration > Services** from the main menu.
- 2 Select **RADIUS > Server Policy**.

The Server Policy Browser lists existing server policies by group or randomly. A policy can be selected and modified from the browser.

- 3 Refer to the **RADIUS Server** screen to review high-level server policy configuration data:

RADIUS Server	RADIUS User Pools	Default Source	Default Fallback	Authentication Type	CRL Validation
INTERNAL-AAA	GUEST-USERS	Local	✗	All	✗
ldap		LDAP	✗	All	✗
policy1	usergroup	Local	✗	All	✗

Type to search in tables Row Count: 3

**Figure 327: RADIUS Server Policy Screen**

- 4 Select a server policy from the Server Policy Browser.  
You can add a new policy, modify an existing policy, or delete 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	<p>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:</p> <ul style="list-style-type: none"> <li>• All - Enables both TTLS and PEAP</li> <li>• TLS - Uses TLS as the EAP type</li> <li>• TTLS and MD5 - The EAP type is TTLS with default authentication using MD5</li> <li>• TTLS and PAP - The EAP type is TTLS with default authentication using PAP</li> <li>• TTLS and MSCHAPv2 - The EAP type is TTLS with default authentication using MSCHAPv2</li> <li>• PEAP and GTC - The EAP type is PEAP with default authentication using GTC</li> <li>• PEAP and MSCHAPv2 - The EAP type is PEAP with default authentication using MSCHAPv2</li> </ul> <p>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.</p>
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.

- 5 Click **Copy** 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 click **Copy** to initiate the configuration copy operation. This feature streamlines the creation of RADIUS server policies using the attributes of existing server policies.

- 6 An existing RADIUS server policy can be renamed at any time by selecting it from among the listed policies and clicking **Rename**.

This allows an administrator to simply rename a server policy without having to create (or edit) a new policy with all the same settings.

- 7 Select either **Add** to create a new RADIUS server policy, **Edit** to modify an existing policy, or **Delete** to permanently remove a policy.

The Server Policy tab displays by default.

**RADIUS Server**

Activate RADIUS Server Policy

Server Policy Client Proxy LDAP

**Settings**

RADIUS User Pools

- RADIUSUserPool01
- [Create](#)

LDAP Server Dead Period 5 Minutes ( 0 to 10 )

LDAP Groups <none>

LDAP Group Verification

LDAP Chase Referral

Local Realm

**Authentication**

Default Source  Local  LDAP

Default Fallback

Source	FallBack	SSID	Precedence	

OK Reset

**Figure 328: RADIUS Server Policy - Add/Edit - Server Policy Tab**

- 8 If creating a new policy, assign it a **RADIUS Server Policy** name up to 32 characters.



- 9 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.

- 10 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	<p>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:</p> <ul style="list-style-type: none"> <li>• All - Enables both TTLS and PEAP</li> <li>• TLS - Uses TLS as the EAP type</li> <li>• TTLS and MD5 - The EAP type is TTLS with default authentication using MD5</li> <li>• TTLS and PAP - The EAP type is TTLS with default authentication using PAP</li> <li>• TTLS and MSCHAPv2 - The EAP type is TTLS with default authentication using MSCHAPv2</li> <li>• PEAP and GTC - The EAP type is PEAP with default authentication using GTC</li> <li>• PEAP and MSCHAPv2 - The EAP type is PEAP with default authentication using MSCHAPv2</li> </ul> <p>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.</p>
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 CRL	Select this option to allow the use of an expired CRL. This option is enabled by default

- 11 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.

- 12 If you are 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 setting 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.

- 13 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 entries.

- 14 Click **OK** to save the settings to the server policy configuration.  
Click **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](#) on page 843
- [Configuring a RADIUS Proxy](#) on page 844
- [Configuring an LDAP Server Configuration](#) on page 846

### *Configuring RADIUS Clients*

A RADIUS client is a mechanism to communicate with a central server to authenticate users and authorize access to the controller, service platform or access point managed network.

The client and server share a secret (a password). That shared secret followed by the request authenticator is put through a MD5 hash algorithm 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.

The screenshot shows the 'RADIUS Server Policy' window for 'policy1'. It has four tabs: 'Server Policy', 'Client', 'Proxy', and 'LDAP'. The 'Client' tab is selected. Below the tabs is a section titled 'RADIUS Clients' containing a table with two columns: 'IP Address' and 'Shared Secret'. The 'IP Address' column has a text input field with a mask and a dropdown menu. The 'Shared Secret' column has a text input field with a show/hide checkbox. There is a '+ Add Row' button at the bottom right of the table. At the bottom of the window are 'OK', 'Reset', and 'Exit' buttons.

**Figure 329: RADIUS Server Policy Screen - Add/Edit - 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 a RADIUS enabled-device configured with the same shared secret. Select the **Show** checkbox to expose the shared secret's actual character string. Otherwise, the shared secret is displayed as a string of asterisks (\*).

- 5 Click **OK** to save the server policy's client configuration. Click **Reset** to revert to the last saved configuration.

### Configuring a RADIUS Proxy

A user's access request is sent to a proxy server if it cannot be authenticated by a controller, service platform or access point's 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.

The screenshot shows the 'RADIUS Server Policy' configuration window for 'INTERNAL-AAA'. The 'Proxy' tab is selected. Under 'Proxy Retries', there are two fields: 'Proxy Retry Delay' set to 5 seconds (range 5 to 10) and 'Proxy Retry Count' set to 3 (range 3 to 6). Below is a table with columns: Realm Name, IP Address, Port Number, Shared Secret, and a Delete icon. The table is currently empty. An 'Add Row' button is at the bottom right of the table. At the bottom of the window are 'OK', 'Reset', and 'Exit' buttons.

Realm Name	IP Address	Port Number	Shared Secret	

**Figure 330: RADIUS Server Policy Screen - Add/Edit - 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 the number of retries (from 3 - 6) sent to 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 In the **Port Number** field, enter the TCP/IP port number for the server used as a data source for the proxy server. Use the spinner to select a value from 1024 and 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 **OK** to save the changes. Click **Reset** to revert to the last saved configuration.

### Configuring an LDAP Server Configuration

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 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 controller, service platform or access point 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.

Redundancy	IP Address	Port
Primary	157.235.233.232	389

Type to search in tables

Row Count: 1

Add Edit Delete Exit

**Figure 331: RADIUS Server Policy Screen - LDAP Tab**

#### Note



If you are using LDAP for external authentication, PEAP-MSCHAPv2 can be used only 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 <i>primary</i> or <i>secondary</i> 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.

- Click **Add** 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 332: LDAP Server Add Screen**

- 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. The default port value for start-tls is 389. The 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 exceed 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:

GroupAttribute	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	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	The group member attribute sent to the LDAP server when authenticating users.

- 7 Click **OK** to save the changes to the LDAP server configuration. Click **Reset** to revert to the last saved configuration.

## RADIUS Deployment Considerations

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 (password). 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.

## Setting the URL List

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.

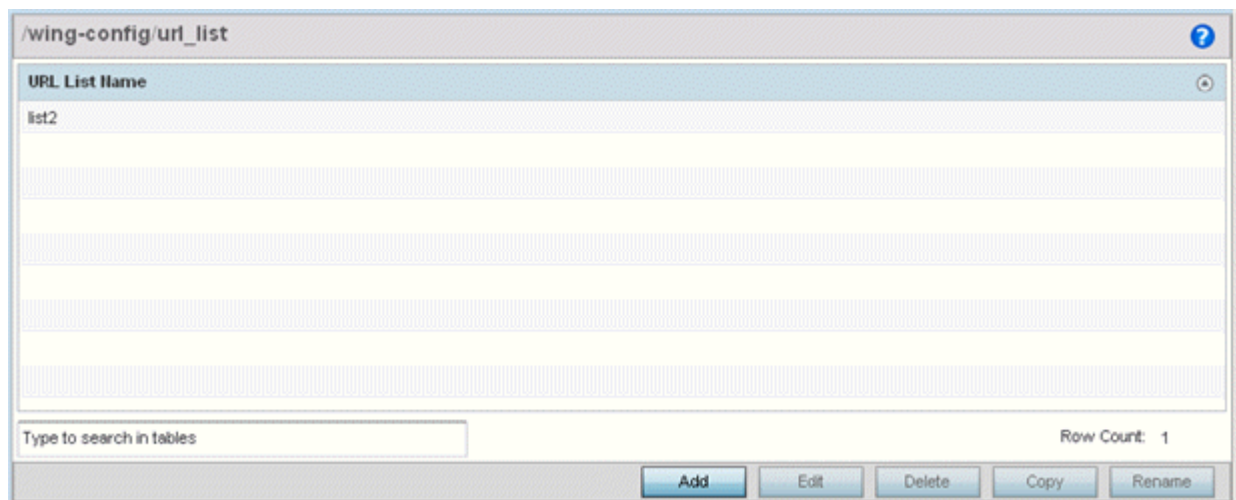
To configure a URL lists policy:

- 1 Select the **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.

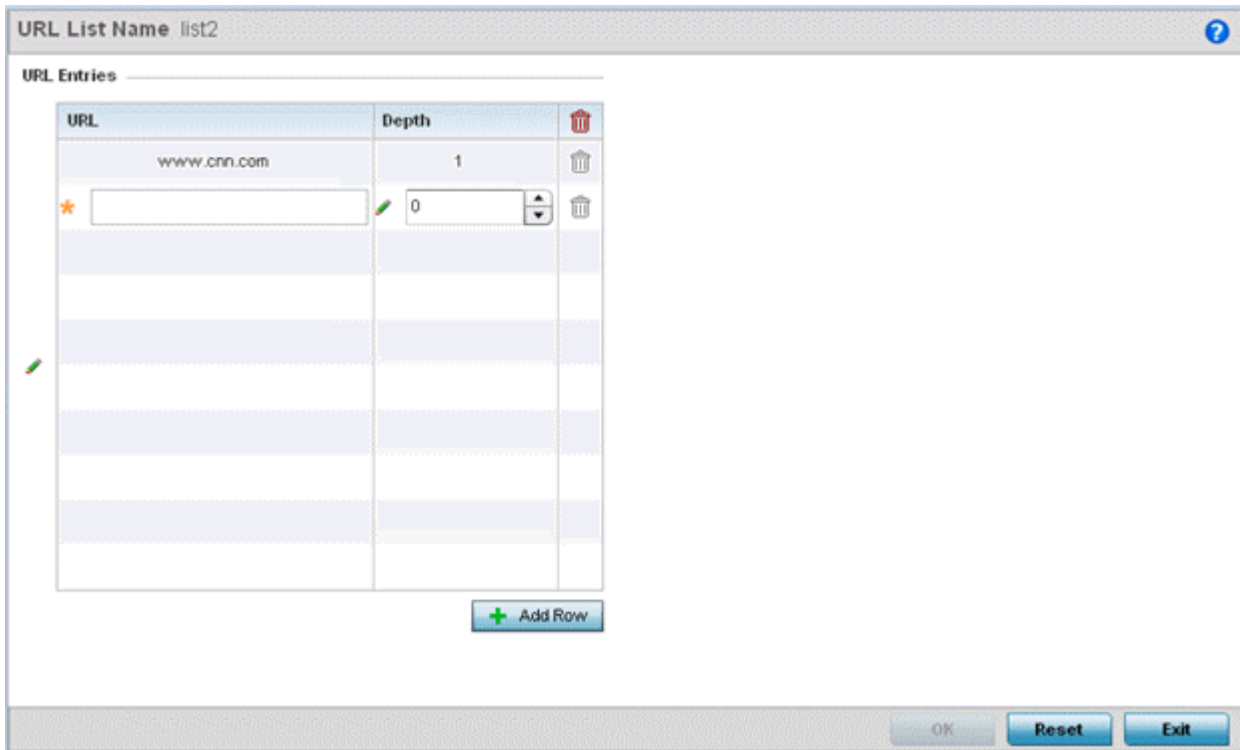
- 3 Select **URL Lists**.

The URL Lists screen displays existing policies. New policies can be created. Existing policies can be modified, deleted or copied.



**Figure 333: 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.



**Figure 334: URL List Name - Add/Edit Screen**

- 6 Select **+ Add Row** to display configurable parameters for defining a URL and its depth.
- 7 If you are creating a new URL lists policy, assign a name to it. The name cannot exceed 32 characters.

If you are editing an existing URL lists policy, the policy name cannot be modified.

- 8 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. Because 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.

- 9 Select **OK** to save the URL Entries list configuration. Select **Reset** to revert to the last saved configuration.

## Setting the Imagotag Policy

SES-imagotag’s ESL (Electronic Shelf Label) tags are small, battery-powered devices used by retail businesses to display information, such as product code, pricing, etc. These tags are activated, configured, and managed through an SES-Imagotag provided server. The tags and server communicate through an ESL communicator (a USB dongle), connected to the USB port on the WiNG AP. This communication is over the 2.4 GHz band using a proprietary RF protocol. The ESL communicator acts as a bridge between the tags and the server, using WiNG AP as an infrastructure device.

Use this option to enable support for SES-imagotag’s ESL tags on WiNG APs with USB interfaces. In case of standalone AP’s, apply the policy to the AP’s self. In case of adopted APs, the policy is pushed to the AP through the adopting controller. In the latter case, apply the policy on the AP’s profile.

An Imagotag-enabled AP recognizes the ESL communicator, and facilitates communication between communicator and tags.



**Note**

This feature is supported only on the AP 8432 model access point.

To navigate to the **Imagotag Policy** screen:

- 1 Select the **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**, **DNS Whitelist**, **DHCP Server Policy**, **RADIUS** , **Guest Management**, etc. configuration options can be selected.

- 3 Select the **Imagotag Policy** option.

Imagotag Name	Enable	Channel	Window Size	Payload Size	Output Power	SSL	FCC-Mode
ImagoTagPolicy	✓	9	12	25	Level-B	✗	✗

Type to search in tables Row Count: 1

**Figure 335: Configuration - Services - Imagotag Policy screen**

- 4 Review the following existing Imagotag Policy settings, to determine whether a new policy requires creation, an existing policy requires modification or an existing policy requires deletion:

Imagotag Name	Displays the Imagotag policy name.
Enable	Displays the status of the policy: Enabled/Disabled. A green check mark indicates that the policy is enabled. A red cross mark indicates that the policy is disabled.
Channel	Displays the channel assigned for ESL communicator to tag communication in the 2.4 GHz band.
Window Size	Displays the transmission window size for messages exchanged between ESL communicator and tags.



Payload Size	Displays the maximum payload size in packets exchanged between ESL communicator and tags.
Output Power	Displays the maximum output power set for the ESL communicator.
SSL	Displays if SSL (Secure Socket Layer) encryption mode of communication is enabled or not. A green check mark indicates that this option is enabled. A red cross mark indicates that this option is disabled.
FCC-Mode	Displays if the FCC compatibility mode is enabled or not on the ESL communicator. A green check mark indicates that this option is enabled. A red cross mark indicates that this option is disabled.

## Adding/Editing Imagotag Policy Settings

To add/edit an Imagotag policy:

- 1 Select **Add** and create a new policy. To modify, remove, copy or rename an existing policy, select the policy from those listed on the screen and click the **Edit**, **Delete**, **Copy** or **Rename** button.

The Imagotag Policy add/edit screen displays.

**Figure 336: Add/Edit Imagotag Policy screen**

- 2 If adding a new Imagotag policy, in the **Imagotag Name** field, enter the policy name.

## 3 Configure or edit the following Imagotag policy settings:

Enable	Select to enable the policy.
Channel	Use the Channel drop-down menu to configure the channel assigned for ESL communicator to tag communication in the 2.4 GHz band. The option are: <ul style="list-style-type: none"> <li>ACS (Auto-Channel Selection) - Enables auto channel selection mode. This is the default setting.</li> <li>0 - 10 - Sets the RF channel of operation within the 0-10 range.</li> </ul>
Window Size	Use the spinner control to set the transmission window size for messages exchanged between ESL communicator and tags. <ul style="list-style-type: none"> <li>1-14 - Set a value between 1-14 bytes. The default value is 14 bytes.</li> </ul> <p><b>Note:</b> SES-Imagotags recommends NOT to change the default setting.</p>
Payload Size	Use the spinner control to set the maximum size of the payload in packets exchanged between ESL communicator and tags. <ul style="list-style-type: none"> <li>1-32 - Specify the value from 1 - 32 bytes. The default setting is 32 bytes.</li> </ul> <p><b>Note:</b> SES-Imagotags recommends NOT to change the default setting.</p>
Output Power	Use the spinner control to configure the maximum output power for the ESL communicator. The options are: <ul style="list-style-type: none"> <li>Level-A - 1 dBm. This is the default setting.</li> <li>Level-B - -4 dBm</li> <li>Level-C - -6 dBm</li> <li>Level-D - -12 dBm</li> <li>Level-E - 0 dBm</li> <li>Level-F - -2 dBm</li> <li>Level-G - -8 dBm</li> <li>Level-H - -10 dBm</li> </ul> <p><b>Note:</b> SES-Imagotags recommends NOT to change the default setting, which is in conformance to various country/region specific RF regulations.</p>
SSL	Select to enable secure, encrypted communication over the SSL (Secure Socket Layer) between the AP and SES-imagotag server. This option is disabled by default.
FCC-Mode	Select to enable the FCC (Federal Communications Commission) compatibility mode on the ESL communicator. This option is disabled by default.

4 Select **OK** to save the configurations. Select **Reset** to revert to the last saved configuration.

# 12 Management Access

Viewing Management Access Policies  
Adding or Editing a Management Access Policy  
Creating an Administrator Configuration  
Setting an Allowed Location Configuration  
Setting the Access Control Configuration  
Setting the Authentication Configuration  
Setting the SNMP Configuration  
SNMP Trap Configuration  
T5 PowerBroadband SNMP  
EX3500 Management Policies  
Configuring a Hierarchical Tree  
Management Access Deployment Considerations

Controllers, service platforms and access points have mechanisms to *allow* or *deny* device access for separate interfaces and protocols (*HTTP,HTTPS, Telnet, SSH* or *SNMP*). Management access can be *enabled* or *disabled* as required for unique policies. The Management Access functionality is not meant to function as an ACL (in routers or other firewalls), where administrators specify and customize specific IP addresses 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.

---

## Note



Access points utilize a single Management Access policy, so ensure all the intended administrative roles, permissions, authentication and SNMP settings are correctly set. If an access point is functioning as a Virtual Controller AP, these are the access settings used by adopted access points of the same model as the Virtual Controller AP.

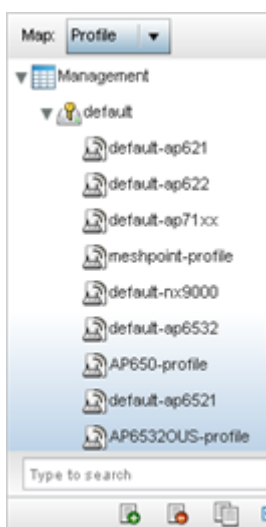
---

## Viewing Management Access Policies

Management Access policies display in the lower left-hand side of the controller, service platform or access point UI. 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.



The **Management Policy** screen displays existing management policies and their unique protocol support configurations.

Management Policy	Telnet	SSHv2	HTTP	HTTPS	SIIMPv1	SIIMPv2	SIIMPv3	FTP
default	✓	✓	✓	✓	✗	✓	✓	✓

Row Count: 1

Buttons: Add, Edit, Delete, Copy, Rename

- 3 Refer to the following **Management** access policy configurations to determine whether these existing policies can be used as is, require modification or a new policy requires creation:

A green check mark indicates controller, service platform or access point access is allowed using the listed protocol. A red X indicates device access is denied using the listed protocol.

<b>Management Policy</b>	Displays the name of the Management Access policy assigned when initially created. The name cannot be updated when modifying a policy.
<b>Telnet</b>	Telnet provides a command line interface to a remote host over TCP. Telnet provides no encryption, but it does provide a measure of authentication.
<b>SSHv2</b>	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.
<b>HTTP</b>	HTTP (Hypertext Transfer Protocol) provides access to the device's UI using a Web browser. This protocol is not very secure.
<b>HTTPS</b>	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.
<b>SNMPv1</b>	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.
<b>SNMPv2</b>	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.
<b>SNMPv3</b>	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.
<b>FTP</b>	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](#). If necessary, select an existing Management Access policy and select **Delete** to permanently remove it from the list of those available.

## Adding or Editing a Management Access Policy

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 the Management Browser.
  - To modify an existing policy, select **Management Browser > Edit**.
  - To add a new policy, click **Add** on the bottom right-hand side of the Management screen.
- 2 Name the new policy to enable the **Access Control**, **SNMP**, **SNMP Traps** and **Administrators** tabs and define the policy configuration.

The name cannot exceed 32 characters.
- 3 Click **OK** to commit the new policy name.

Once the new name is defined, the screen's 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:



<b>Creating an Administrator Configuration</b>	Use the Administrators tab to create specific users, assign them permissions to specific protocols and set specific administrative roles for the network.
<b>Setting an Allowed Location Configuration</b>	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.
<b>Setting the Access Control Configuration</b>	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.
<b>Setting the Authentication Configuration</b>	Refer to the Authentication tab to set the authentication scheme used to validate user credentials with this policy.
<b>Setting the SNMP Configuration</b>	Refer to the SNMP tab to enable SNMPv2, SNMPv3 or both and define specific community strings for this policy.
<b>SNMP Trap Configuration</b>	Use the SNMP Traps tab to enable trap generation for the policy and define trap receiver configurations.
<b>T5 PowerBoadband SNMP</b>	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 888.

## Creating an Administrator Configuration

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 RADIUS using 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.

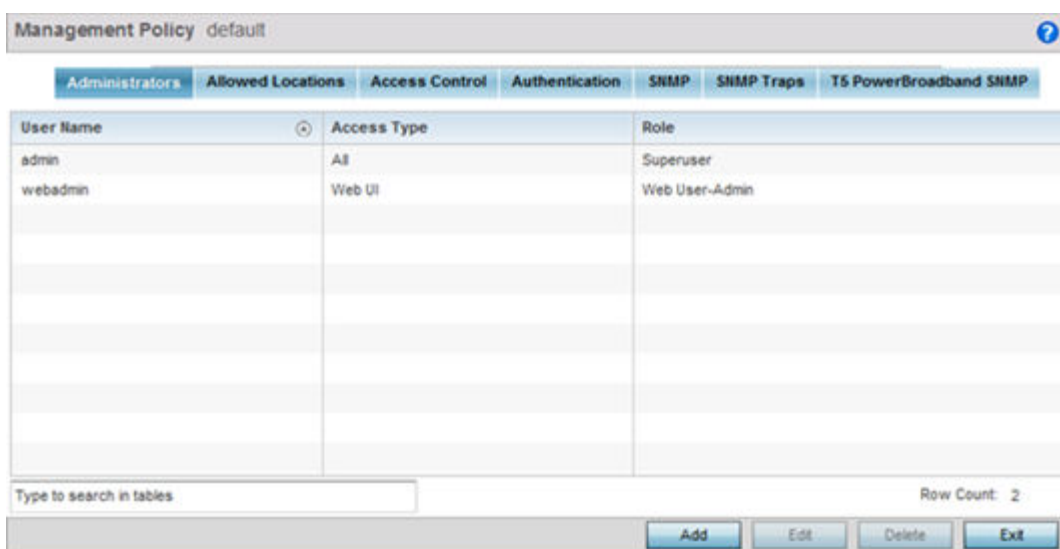
The controller or service platform authenticates users using the integrated local database. When user credentials are presented the controller or service platform validates the username and password against the local database and assigns permissions based on the associated roles assigned. The controller 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 (type) and administrative role within the controller, service platform or access point managed network. New administrators can be added, and existing administrative configurations modified or deleted as required.

To create administrators and assign them access types and roles:

- 1 Go to **Configuration > Management > Administrators**.

The **Administrators** screen displays.



User Name	Access Type	Role
admin	All	Superuser
webadmin	Web UI	Web User-Admin

Type to search in tables Row Count: 2

Add Edit Delete Exit

- 2 Refer to the following 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.

- 3 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.

- 4 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.
- 5 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.
- 6 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.

Option	Description
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.

- 7 Select the **Administrator Role** for the administrator using this profile. Only one role can be assigned.

Option	Description
Superuser	Select this option to assign complete administrative rights to the user. This entails all the roles listed for all the other administrative roles.

Option	Description
<b>System</b>	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.
<b>Network</b>	The Network role provides privileges to configure all wired and wireless parameters like IP configuration, VLANs, L2/L3 security, WLANs, radios, and captive portal.
<b>Security</b>	Select Security to set the administrative rights for a security administrator allowing configuration of all security parameters.
<b>Monitor</b>	Select Monitor to assign permissions without any administrative rights. The Monitor option provides read-only permissions.
<b>Help Desk</b>	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 and retrieves logs. Help Desk personnel are <i>not</i> allowed to conduct controller or service platform reloads.
<b>Web User</b>	Select Web User to assign the administrator privileges needed to add users for authentication.
<b>Device Provisioning</b>	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.
<b>Vendor Admin</b>	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 onboarding 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.

- Click **OK** to save the administrator's configuration, or click **Reset** to revert to the last saved configuration.

## Setting an Allowed Location Configuration

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, securityadmin, 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.

The Allowed Location screen lists existing users and their permitted locations.

Name	Locations
help-desk user 1	location1,location2

Type to search in tables Row Count: 1

Add Edit Delete Exit

- 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.

**Allowed Locations** x

Name help-desk user ?

Locations

Locations

location 1

OK Reset Exit

- 3 Set the following allowed location parameters:

**Name** Define a 32 character maximum user name whose access is 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 revert to the last saved configuration.

## Setting the Access Control Configuration

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. Consider disabling unused interfaces 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

Access Type	Encrypted	Authenticated	Default State
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.

The screenshot displays the 'Management Policy - Test' configuration interface. The 'Access Control' tab is selected. On the left, there are sections for Telnet, SSH, HTTP/HTTPS, Rest Server, FTP, and General settings. On the right, the 'Access Restrictions' section is expanded, showing 'Filter Type' as 'None', 'IP Access List' as '<none>', and a list of 'Source Hosts' with IP addresses '0.0.0.0'. Below this is the 'Source Subnets' field and the 'Logging Policy' set to 'None'. At the bottom right, the 'User Lockout Settings' table is visible, with columns for 'Role', 'Lockout Time', and 'Number of Password Attempts'. An 'Add Row' button is located at the bottom right of the table.

- 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 check box to enable HTTP device access. HTTP provides limited authentication and no encryption.
Enable HTTPS	Select the check box to enable HTTPS device access. HTTPS (Hypertext Transfer Protocol Secure) is more secure than plain HTTP. HTTPS provides both authentication and data encryption as opposed to just authentication.



#### 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 check box 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 on the controller. 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 connects (in seconds) between 1 - 4,320. The default setting is 12.0
Message of the Day	Enter message of the day text (no longer than 255 characters) displayed at login for clients connecting via Telnet or SSH.

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 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.
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 **Add Row** to configure the following role-based user-account lockout and unlock criteria:

Role	<p>Specify the user-role for which account lockout is to be enabled. The options are:</p> <ul style="list-style-type: none"> <li>• device-provisioning-admin</li> <li>• helpdesk</li> <li>• monitor</li> <li>• network-admin</li> <li>• security-admin</li> <li>• system-admin</li> <li>• vendor-admin</li> <li>• web-user-admin</li> </ul> <p><b>Note:</b> You can enable account lockout for multiple roles. After specifying the role/roles, set the Lockout Time and Number of Password Attempts.</p> <p>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.</p>
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 Click **OK** to save the Access Control configuration or click **Reset** to revert to the last saved configuration.

## Setting the Authentication Configuration

Refer to the **Authentication** tab to define how user credential validation is conducted on behalf of a Management Access policy. Setting up an authentication scheme by policy allows for policy member credential validation collectively, as opposed to authenticating users individually.

To configure an external authentication resource:



- 1 Select **OK** to update the authentication configuration. Select **Reset** to the last saved configuration.
- 1 Select the **Authentication** tab from the Management Policy screen.

- 2 Define the following settings to authenticate management access requests:

<b>Local</b>	Select whether the authentication server resource is centralized (local), or whether an external authentication resource is used for validating user access requests. Only AP 6511 and AP 6521 model access points lack local RADIUS resources.
<b>RADIUS</b>	If local authentication is disabled, define whether the RADIUS server is <i>External</i> and or <i>Fallback</i> . Select fallback to revert to local RADIUS resources should a dedicated external server be unreachable.
<b>AAA Policy</b>	Define the AAA policy used to authenticate user validation requests to the controller or service platform managed network. Select the <i>Create</i> icon as needed to define a new AAA policy or select the <i>Edit</i> icon to modify the configuration of an existing policy.
<b>TACACS</b>	If local authentication is disabled, optionally select <i>Authentication</i> or <i>Fallback</i> (only one authentication or fallback option can be selected) or <i>Accounting</i> and <i>Authorization</i> . TACACS policies control user access to devices and network resources while providing separate accounting, authentication, and authorization services.
<b>AAA TACACS Policy</b>	Select an existing AAA TACACS policy (if available), or select <i>Create</i> to define a new policy or <i>Edit</i> to modify an existing one.

- 3 Use the drop-down menu to specify to select the AAA Policy to use with an external RADIUS resource. An AP6521 model access point (or a model that is not using its local RADIUS resource) will need to interoperate with a RADIUS and LDAP Server (AAA Servers) to provide user database information and user authentication data. If there is no AAA policy suiting your RADIUS authentication requirements, either select the Create icon to define a new AAA policy or select an existing policy from the drop-down menu and select the Edit icon to update its configuration. For more information on defining the configuration of a AAA policy, see “AAA Policy” on page 663.

- 4 Set the following AAA TACACS configuration parameters:

Authentication	Select to enable TACACS authentication on login. This option is not available when the Local field is set to enabled. Also, this option cannot be selected when Fallback is selected.
Fallback	Select to enable fallback to use local authentication if TACACS authentication fails. This option is not available when the Local field is set to enabled. Also, this option cannot be selected when Authentication is selected.
Accounting	Select to enable TACACS accounting on login. This option is not available when the Local field is set to enabled. When selected, the AAA TACACS Policy field is enabled.
Authorization	Select to enable TACACS authorization on login.
Authorization Fallback	Select to enable fallback on TACACS authorization failure. This option is only available when Authorization is selected.

- 5 Configure the **AAA TACACS Policy** to use with this authentication policy. Use the drop-down to select a configured AAA TACACS policy.
- 6 Click **OK** to update the authentication configuration, or click **Reset** to revert to the last saved configuration.

## Setting the SNMP Configuration

Optionally use the *Simple Network Management Protocol* (SNMP) to communicate with controllers, service platforms and access points within the wireless network. SNMP is an application layer protocol that facilitates the exchange of management information to and from a managed device. SNMP enabled devices listen on port 162 (by default) for SNMP packets from the 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 Trap Configuration

Controller, service platform and access point managed networks use SNMP trap receivers for fault notifications. SNMP traps are unsolicited notifications triggered by thresholds (or actions), and are an important fault management tool.

A SNMP trap receiver is the defined destination for SNMP messages (external to the controller, service platform or access point). 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 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.

Management Policy policy1

Administrators Access Control Authentication SNMP **SNMP Traps**

Trap Generation

Enable Trap Generation

Trap Receivers

IP Address	Port	Version	

+ Add Row

OK Reset Exit

- 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 receive trap information. Select **Add Row +** as needed to add additional trap receivers. Select the **Delete** icon to permanently remove a trap receiver.

<b>IP Address</b>	Sets the IP address of an external server resource dedicated to receive SNMP traps on behalf of the controller, service platform or access point.
<b>Port</b>	Set the virtual port of the server resource dedicated to receiving SNMP traps. The default port is port 162.
<b>Version</b>	Sets the SNMP version to use to send SNMP traps. SNMPv2 is the default.

- 4 Select **OK** to update the SNMP Trap configuration. Select **Reset** to revert to the last saved configuration.

## T5 PowerBroadband SNMP

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.

- 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.

## 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, NX5500 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.



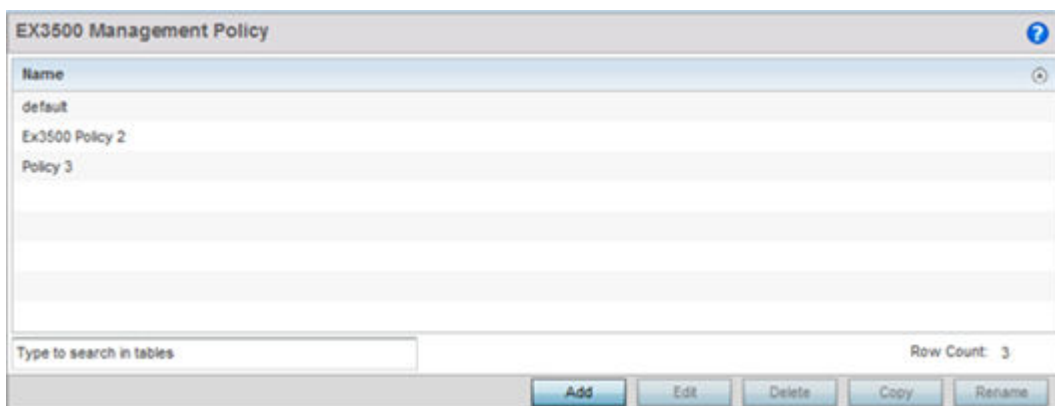
### Note

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:

Go to **Configuration > Management > EX3500 Management Policy**.



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](#) on page 872
- [EX3500 Authentication](#) on page 873
- [EX3500 Exec Password Management](#) on page 875
- [EX3500 System Settings](#) on page 876
- [EX3500 SNMP Management](#) on page 877

## 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 passwords to provide administrative priority.

To set an EX3500 user group configuration:

- 1 Go to **Configuration > Management > EX3500 Management Policy**.

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.

- 2 If creating a new EX3500 user group, assign it a **Name** up to 32 characters. Select **Continue**.

User Name	Access Level	Hash Type
group5	1	0

Type to search in tables Row Count: 1



- 3 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:

Access Level  (0 to 15)

Hash Type

Admin Password  Enter 1-32 ASCII Characters

OK Reset Exit

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.

- 4 Select **OK** when completed to update the EX3500 user group configuration. Select **Reset** to revert the screen back to its last saved configuration.

## 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 Go to **Configuration > Management > EX3500 Management Policy**.  
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.

- 2 Select the **Authentication** tab.

- 3 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.

- 4 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.

- 5 Select **OK** when completed to update the EX3500 authentication configuration. Select **Reset** to revert the screen back to its last saved configuration.

## EX3500 Exec Password Management

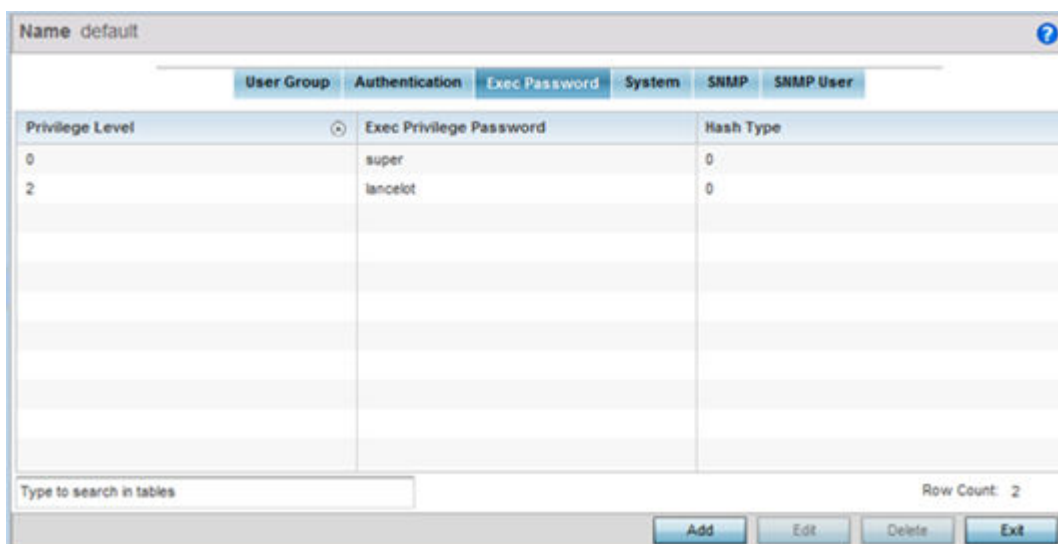
Each EX3500 management policy can have a unique exec password with its own privilege level assigned. Utilize these passwords as specific EX3500 management sessions require priority over others.

To administrate EX3500 management passwords and their privileges:

- 1 Go to **Configuration > Management > EX3500 Management Policy**.

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.

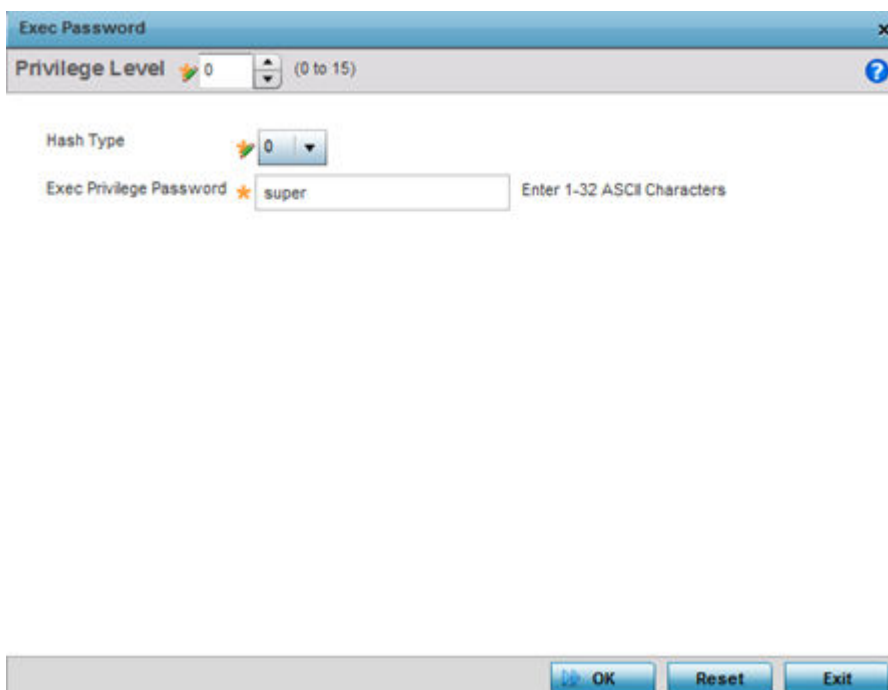
- 2 Select the **Exec Password** tab.



Privilege Level	Exec Privilege Password	Hash Type
0	super	0
2	lancelot	0

Row Count: 2

- 3 Select **Add** to create a new EX3500 exec password, **Edit** to modify an existing password configuration or **Delete** to remove an obsolete password.



**Exec Password**

Privilege Level: 0 (0 to 15)

Hash Type: 0

Exec Privilege Password:  Enter 1-32 ASCII Characters

OK Reset Exit

- 4 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.
- 5 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.

- 6 Select **OK** when completed to update the EX3500 exec password. Select **Reset** to revert the screen back to its last saved configuration.

## 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 Go to **Configuration > Management > EX3500 Management Policy**.

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.

- 2 Select the **System** tab.

The screenshot shows the configuration interface for the EX3500 System settings. The 'System' tab is active, displaying alarm configuration for both Memory and CPU. The Memory section has a Falling Threshold of 90 and a Rising Threshold of 95. The CPU section has a Falling Threshold of 70 and a Rising Threshold of 90. The interface includes a top navigation bar with tabs for User Group, Authentication, Exec Password, System, SNMP, and SNMP User. At the bottom, there are buttons for OK, Reset, and Exit.

- 3 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.

- 4 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.

- 5 Select **OK** when completed to update the EX3500 system threshold settings. Select **Reset** to revert the screen back to its last saved configuration.

## 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.

- 1 Go to **Configuration > Management > EX3500 Management Policy**.

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.

- 2 Select the **SNMP** tab.

The screenshot shows the SNMP configuration page with the following details:

- SNMP Section:**
  - Enable:
  - Contact:
  - Local Engine ID:
  - Location:
- Community String Table:**

Name	Access
private	rw
public	ro
- Group Table:**

Group Name	Authentication	Version	Notify View	Read View	Write View
lanelot	none	v2c			

- 3 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.

- 4 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.

- 5 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.

- 6 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).

- 7 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.

- 8 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.

- 9 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.



10 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.

## 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 Go to **Configuration > Management > EX3500 Management Policy**.

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.

- 2 Select the **SNMP User** tab.

User Name	Version	Remote IP Address	Group Name
lancelot	SNMPv3	157.235.121.21	percival

- 3 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.

- Select **Add** to create a new user configuration or **Edit** to modify the attributes of an existing EX3500 SNMP user configuration.

- 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.

- 6 Select **OK** when completed to update the EX3500 SNMP user settings. Select **Reset** to revert the screen back to its last saved configuration.

## Configuring a 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 ADSPlike 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

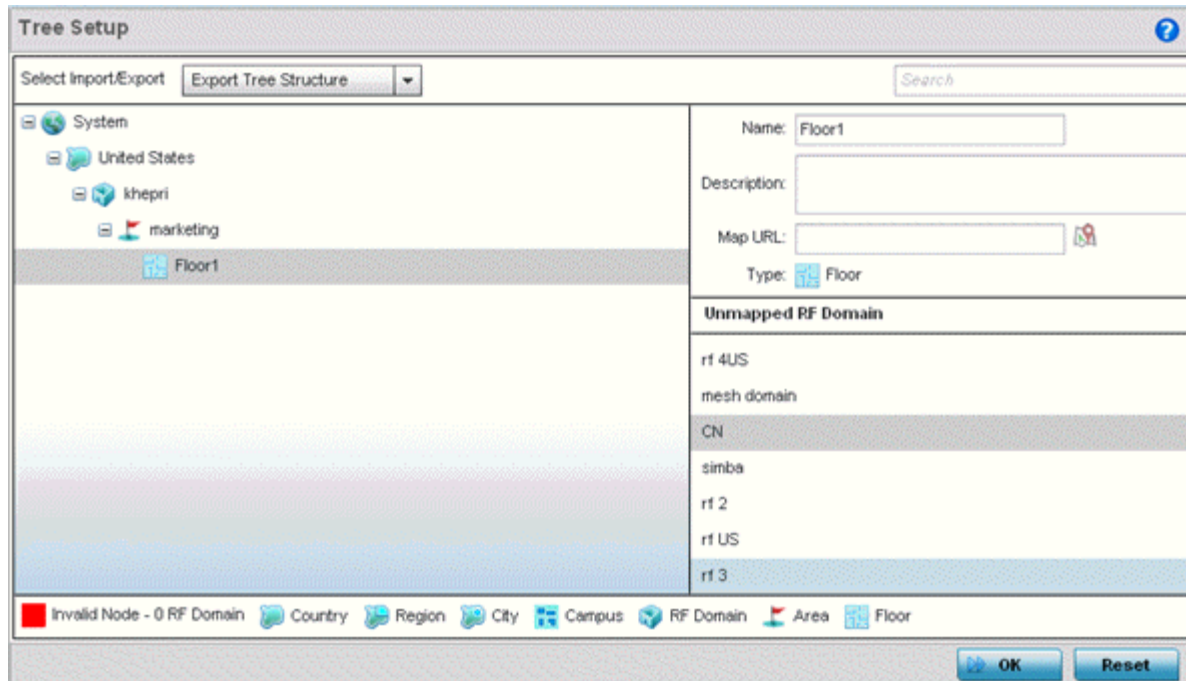
- City
- Campus

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 hierarchical tree to use with ADSP:

- 1 Select **Configuration > Management**.
- 2 Click **Tree Setup** on the top left-hand corner of the UI.

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.



- 3 To add a Country, Region, City or Campus to the tree, select **System** from the upper, left-hand, portion of the **Tree Setup** screen.

**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.

An **Add Child** link displays on the right-hand side of the display.

- 4 If adding a country, go to **Type > Name** 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.

- 5 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.

- 6 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.

- 7 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.

- 8 Select the **add RF Domain** link at the right-hand side of any container to display an **Unmapped RF Domain** screen.

- 9 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.

- 10 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 defined, select **Add** to populate the tree with the Area and Floor.

- 11 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

- 12 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.
- 13 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.

- 14 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.
- 15 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.
- 16 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.

## Management Access Deployment Considerations

Before defining an 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 (as opposed to HTTP which does not).
- 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 device management, as it provides both encryption and authentication (both unavailable together in HTTP).
- 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 be enabled. This provides better management and control of user names and passwords, and allows administrators to quickly change credentials in the event of a security breach.



# 13 Diagnostics

---

## Fault Management Crash Files Advanced

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 allow event filtering, some enable log views and some allow you to manage files generated when hardware or software issues are detected.

Diagnostic capabilities include:

- [Fault Management](#)
- [Crash Files](#)
- [Advanced](#)

## 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 a controller, service platform, access point or wireless client.

### Filter Events

To conduct fault management on an access point:

- 1 Select **Diagnostics > Fault Management > Filter Events**.

The 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 337: Fault Management - Filter Events screen**

- 2 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.
- 3 Define the following **Customize Event Filters** parameters for the Fault Management configuration:

<b>Severity</b>	Set the filtering severity. Select from the following: <i>All Severities</i> – All events are displayed, irrespective of their severity <i>Critical</i> – Only critical events are displayed <i>Error</i> – Only errors and above are displayed <i>Warning</i> – Only warnings and above are displayed <i>Informational</i> – Only informational and above events are displayed
<b>Module</b>	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 <i>TEST</i> , <i>LOG</i> , <i>FSM</i> etc.) or all modules can be tracked by selecting <i>All Modules</i> .
<b>Source</b>	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.
<b>Message Substring</b>	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.

- 4 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.
- 5 Refer to the **Active Event Filters** table to set the following parameters:



<b>Source</b>	Displays the MAC address of the source device tracked by the selected module.
<b>Hostname</b>	Displays the Hostname/IP address of the source device tracked by the selected module.

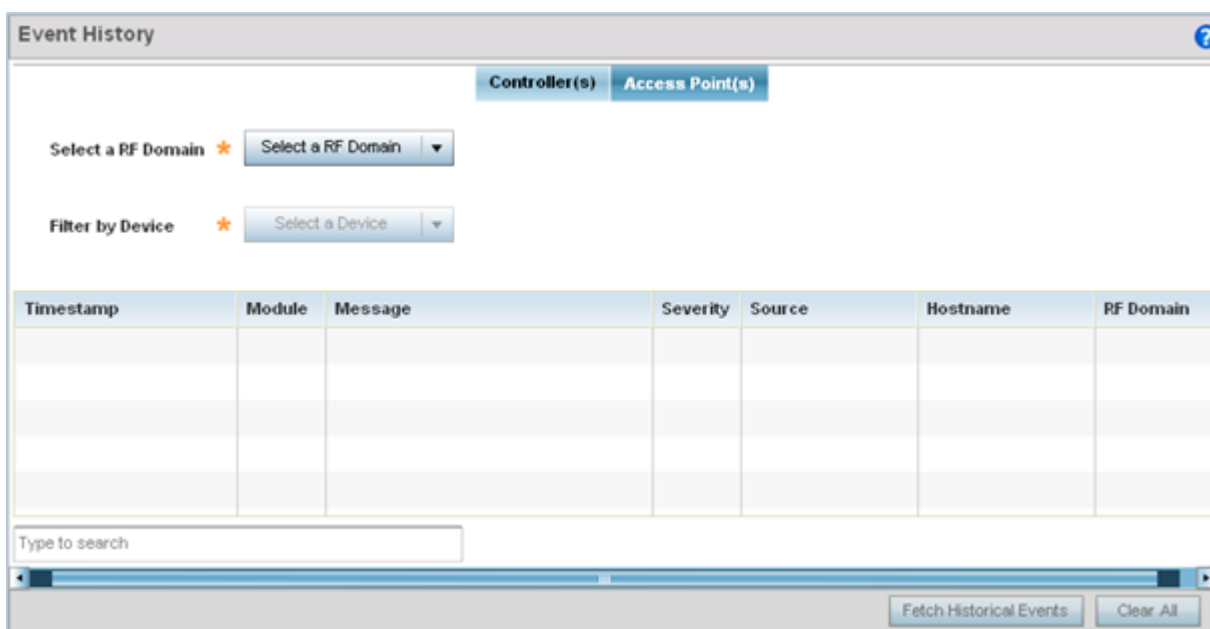
- 3 Select **Clear All** to clear the events displayed on this screen and begin a new event data collection.

## Event History

The Event History screen displays events for both wireless controllers and access points. The Controller(s) tab displays by default. Information on this tab can be filtered by controllers and then further by the RF Domains on the selected controller. 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.

To review the Event History:

- 1 Select **Diagnostics > Fault Management > Event History**



**Figure 339: Fault Management - Event History screen**

- 2 In 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.
- 3 In 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.
- 4 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:

<b>Timestamp</b>	Displays the timestamp (time zone specific) each listed event occurred.
<b>Module</b>	Displays the module tracking the listed event. Events detected by other modules are not tracked.
<b>Message</b>	Displays error or status messages for each event.



<b>File Name</b>	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.
<b>Size</b>	Lists the size of the crash file, as this information is often needed when copying files to an external location.
<b>Last Modified</b>	Displays the time stamp of the most recent update to the file.
<b>Actions</b>	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.

## Advanced

Use Advanced diagnostics to review and troubleshoot potential issues with the access point's User Interface (UI). The UI Diagnostics screen contains tools to effectively identify and correct access point UI issues. Diagnostics can also be performed at the device level for connected clients.

The following options are available under the Advanced menu:

- [UI Debugging](#) on page 894
- [Viewing UI Logs](#) on page 895
- [View Sessions](#) on page 897

## UI Debugging

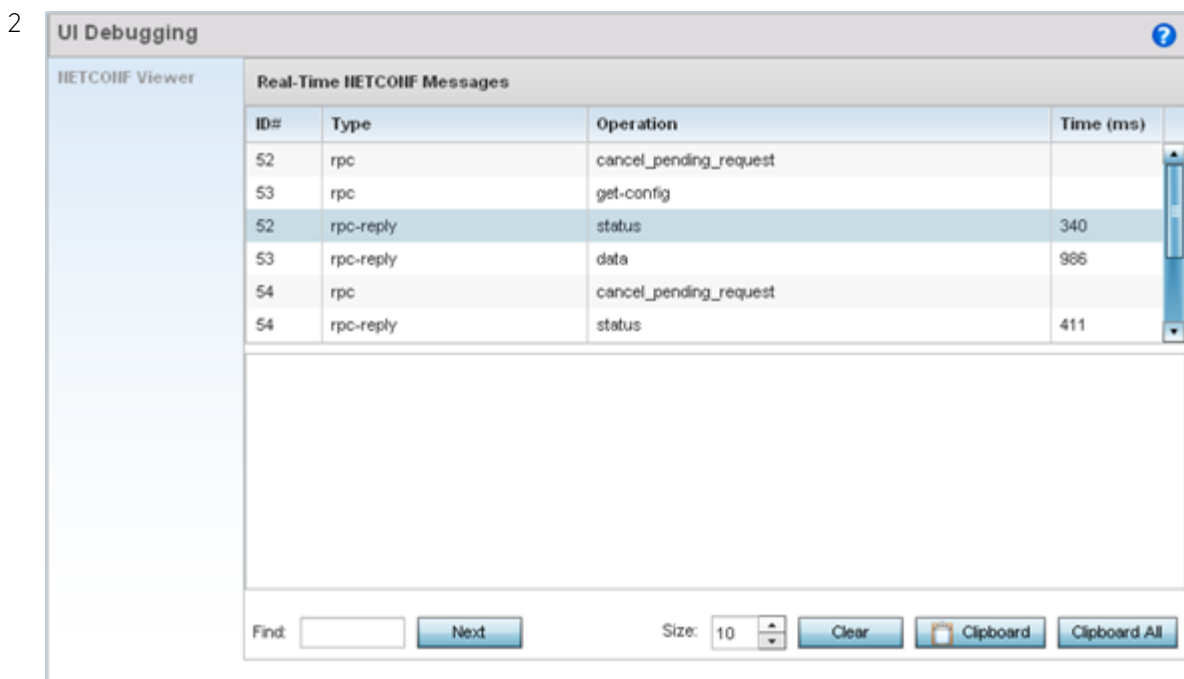
Use the **UI Debugging** screen to view debugging information for a selected device.

To review device debugging information:

- 1 Select **Diagnostics > Advanced > UI Debugging**

By default, **NETCONF Viewer** is selected.

Once a target ID is selected, its debugging information displays within the **NETCONF Viewer** screen.



**Figure 341: UI Debugging screen - NETCONF Viewer**

- 3 Use **NETCONF Viewer** to review NETCONF information. NETCONF is a tag-based configuration protocol. Messages are exchanged using XML tags.

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 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.

Use the **Clipboard** button to copy the current selected message to the clipboard memory of the device used to access the user interface. Use the **Clipboard All** button to copy all the displayed messages to the clipboard memory.

## Viewing UI Logs

Use the **View UI Logs** screen to view the log messages generated by the device. Logs are classified as Flex Logs and Error Logs. These logs provide a real-time look into the state of the device and provide useful information for debugging and trouble shooting issues.

To display the logs:

- 1 Select **Diagnostics > Advanced > Viewing UI Logs**.

By default, the Flex Logs screen displays.

2

Sequ	Date/Time	Type	Category	Message
0	7/7/2015 09:20:2	INFO	mx.messaging.Producer	'81753119-31A7-3D21-1B05-66A2D4B8F36F' producer set des
1	7/7/2015 09:20:2	INFO	mx.messaging.Channel	'direct_http_channel' channel endpoint set to http://192.168.13.;
2	7/7/2015 09:20:2	INFO	mx.messaging.Producer	'81753119-31A7-3D21-1B05-66A2D4B8F36F' producer sendin
3	7/7/2015 09:20:2	DEBU	mx.messaging.Channel	'direct_http_channel' channel sending message:
4	7/7/2015 09:20:2	INFO	mx.messaging.Producer	'81753119-31A7-3D21-1B05-66A2D4B8F36F' producer connec
5	7/7/2015 09:20:2	INFO	mx.messaging.Producer	'81753119-31A7-3D21-1B05-66A2D4B8F36F' producer acknow
6	7/7/2015 09:20:2	INFO	mx.rpc.http.HTTPService	Decoding HTTPService response
7	7/7/2015 09:20:2	DEBU	mx.rpc.http.HTTPService	Processing HTTPService response message:
8	7/7/2015 09:20:2	INFO	mx.messaging.Producer	'9FF86B74-412E-EDEA-D663-66A2D6EBD4C6' producer set de
9	7/7/2015 09:20:2	INFO	mx.messaging.Producer	'81753119-31A7-3D21-1B05-66A2D4B8F36F' producer sendin
10	7/7/2015 09:20:2	DEBU	mx.messaging.Channel	'direct_http_channel' channel sending message:
11	7/7/2015 09:20:2	INFO	mx.messaging.Producer	'81753119-31A7-3D21-1B05-66A2D4B8F36F' producer acknow

**Figure 342: View UI Logs - Flex Logs tab**

The sequence (order of occurrence), Date/Time, Type, Category and Message items display for each application log, flex log or error log selected.

Use the **Clear All** button to clear all logs shown in this screen.

- 3 Select the **Error Logs** tab to display the error logs for this device.



View UI Logs <span style="float: right;">?</span>				
		<span style="border: 1px solid black; padding: 2px;">Flex Logs</span> <span style="border: 1px solid black; padding: 2px; background-color: #0070C0; color: white; margin-left: 10px;">Error Logs</span>		
Sequer	Date/Time	Type	Category	Message
0	7/3/2015 11:37:05.42	ERROR	com.motorola.wing.error.error	MEC0000E: UNKNOWN
1	7/3/2015 11:37:05.42	ERROR	com.motorola.wing.error.error	MEC0000E: UNKNOWN
2	7/3/2015 11:37:05.59	ERROR	com.motorola.wing.error.error	MEC0000E: UNKNOWN
3	7/3/2015 11:37:05.59	ERROR	com.motorola.wing.error.error	MEC0000E: UNKNOWN

**Figure 343: View UI Logs - Error Logs tab**

The Sequence (order of occurrence), Date/Time, Type, Category and Message items display for each log option selected.

## View Sessions

The **View Sessions** displays a list of all sessions associated with this device. A session is created when a user name/password combination is used to access the device to interact with it for any purpose. Use the following to view a list of sessions associated with this device:

- 1 Select **Diagnostics > Advanced > View Sessions**
- 2

View Sessions <span style="float: right;">?</span>					
<input type="checkbox"/>	Cookie	From	Role	Start Time	User
<input checked="" type="checkbox"/>	16	192.168.100.210(web)	superuser	2015-07-07 09:59:07	admin
<input type="checkbox"/>	5	127.0.0.1	superuser	2015-07-06 12:36:21	snmp
<input type="checkbox"/>	6	127.0.0.1	superuser	2015-07-06 12:36:21	snmp2
<input type="checkbox"/>	15	192.168.13.30(web)	superuser	2015-07-07 09:32:13	admin

Delete

**Figure 344: Advanced - View Sessions screen**

- 3 Refer to the following table for more information on the fields displayed in this screen:

<b>Cookie</b>	Displays the number of cookies created by this session.
<b>From</b>	Displays the IP address of the device/process initiating this session.
<b>Role</b>	Displays the role assigned to the user name as displayed in the User column.
<b>Start Time</b>	Displays the start time of this session. This is the time at which the user successfully created this session.
<b>User</b>	Displays the user name of the account used to initiate this session.

- 4 To remove a listed session, select the check box before session, then select **Delete**.

# 14 Operations

## Device Operations Certificates Smart RF

The functions supported within the **Operations** menu allow the administration of firmware, configuration files and certificates for managed devices.

A certificate links identity information with a public key enclosed in the certificate. Device certificates can be imported and exported 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.

On controllers and service platforms, 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](#)

## 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 900
- [Adopted Device Upgrades](#) on page 902
- [Using the File Management Browser](#) on page 909
- [Restarting Adopted Devices](#) on page 911
- [Captive Portal Configuration](#) on page 913
- Crypto CMP Certificate

- RAID on page 916
- Re-Elect Controller

## Operations Summary

The **Summary** screen displays by default when the **Operations** is selected from the main menu bar. The **Summary** screen displays firmware information for a controller, service platform or access point selected from either the RF Domain or Network tabs on the left-hand side of the screen.

	Primary	Secondary
<b>Version</b>	5.5.0.0-038B	5.5.0.0-036B
<b>Build Date</b>	04:18:2013 20:59:03	04:11:2013 20:24:57
<b>Install Date</b>	04:22:2013 12:29:27	04:12:2013 18:18:06

FallBack Enabled  
 Current Boot primary  
 Upgrade Status Successful  
 2013-04-22 12:29:27

Firmware Upgrade    Reload

Device Type	Is Controller	Online	Offline	Total
rx9000	✓ Yes	1	1	2
ap81xx	✗ No	2	0	2
ap6532	✗ No	13	0	13
ap6521	✗ No	1	0	1
ap622	✗ No	2	0	2
ap6511	✗ No	1	0	1
ap650	✗ No	3	0	3

- 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 previous settings.

<b>Version</b>	Displays the primary and secondary firmware image version defined for the selected device. Keep in mind, secondary images with an older build version have a reduced feature and may limit the device.
<b>Build Date</b>	Displays the date the primary and secondary firmware image was built for the selected device.
<b>Install Date</b>	Displays the date the firmware was installed for the selected device.
<b>Fallback</b>	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.
<b>Current Boot</b>	Lists firmware image for the device on the current boot.

<b>Upgrade Status</b>	Displays the status of the last firmware upgrade performed for each listed device managed by this controller, service platform or Virtual Controller mode access point.
<b>Firmware Upgrade</b>	Select this option to display the firmware upgrade window for the selected device. Select the <i>Apply</i> button to perform the function.
<b>Reload</b>	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 <i>Reload</i> button to perform the function.

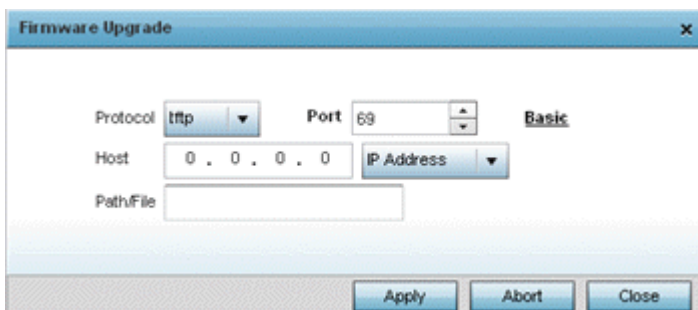
- 2 Refer to the device table for basic information for known device types. The device table displays the **Device Type**, **Controller** status, **Online**, **Offline** and **Total** device counts.

### Upgrading Device Firmware

Controllers, service platforms and access points has can conduct firmware updates for their managed or peer devices. access points can only update the firmware of peer access point models of the same type.

To update the firmware of a managed device:

- 1 Select **Operations** tab.
- 2 Select a device from the browser.
- 3 Select the **Firmware Upgrade** button.



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

- 4 Enter the complete path to the firmware file for the target controller, service platform or access point in the **Path/File** field.
- 5 Provide the following information to accurately define the location of the target firmware file:

<b>Protocol</b>	Select the connection protocol used for updating device firmware. Available options include: <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1-4</i></li> </ul>
<b>Port</b>	Use the spinner control or manually enter the value to define the port used for firmware updates. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
<b>IP Address</b>	Enter IP address of the server used to update the firmware. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
<b>Hostname</b>	Provide the hostname of the server used to update the firmware. This option is not valid for <i>cf</i> and <i>usb1-4</i> .

<b>User Name</b>	Define the user name used to access either a <i>FTP</i> or <i>SFTP</i> server.
<b>Password</b>	Specify the password for the user account to access a <i>FTP</i> or a <i>SFTP</i> server.
<b>Path / File</b>	Specify the path to the firmware file. Enter the complete relative path to the file on the server.

- 6 Select **Apply** to start the firmware update. Select **Abort** to terminate an in process firmware update. Select **Close** to close the upgrade pop up screen. The upgrade continues in the background.

## Adopted Device Upgrades

An administrator can designate controllers, service platforms or access points as RF Domain managers capable of receiving firmware files from the NOC (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.

### Device Upgrade List

- 1 Ensure **Devices** is selected from the Operations menu on the top, left-hand, side of the screen.
- 2 Expand the System node, select a RF Domain and one of its member devices.
- 3 Select **Adopted Device Upgrade**. The screen displays with the **Device Upgrade List** selected by default.

The screenshot shows the 'Adopted Device Upgrade' configuration page. At the top, there are tabs for 'Summary', 'Adopted Device Upgrade', 'File Management', 'Adopted Device Restart', 'Captive Portal Pages', and 'RAID'. Below the tabs, there are sub-tabs for 'Device Upgrade List', 'Device Image File', 'Upgrade Status', and 'Upgrade History'. The 'Device Upgrade List' sub-tab is active.

Configuration options include:

- Device Type List: NX9000
- Scheduled Upgrade Time:  Now, 10/04/2013, 0:00 (HH:MM)
- Scheduled Reboot Time:  Now, 10/04/2013, 0:00 (HH:MM)
- Reboot options:  No Reboot,  Staggered Reboot

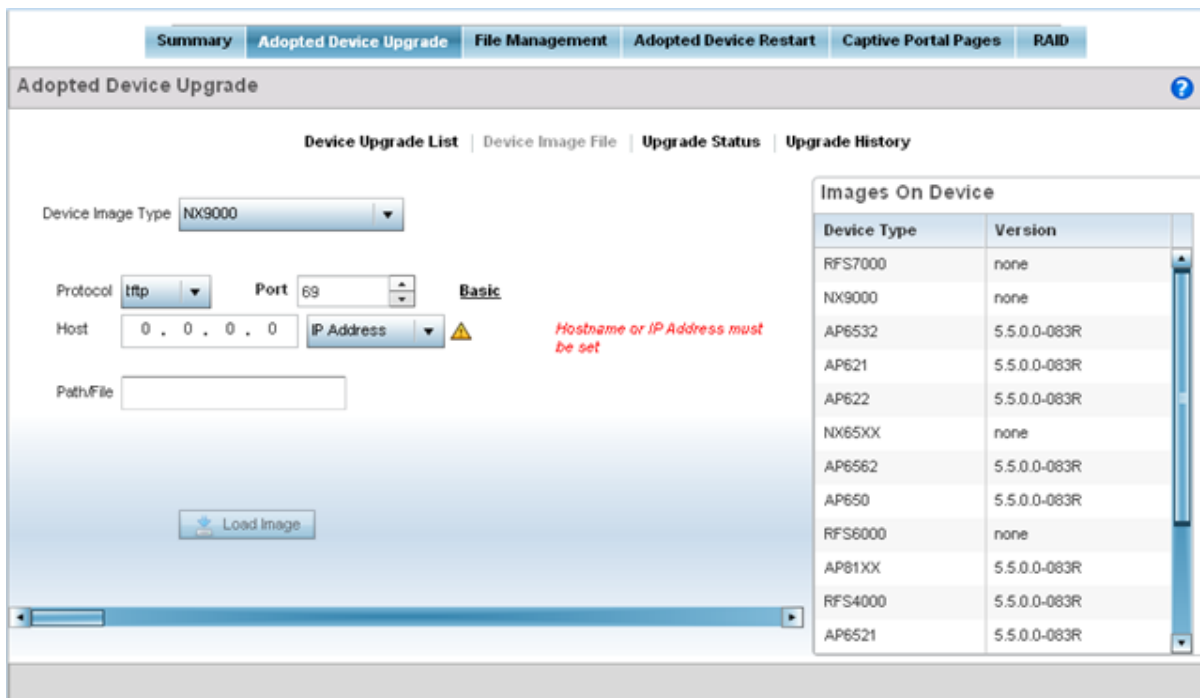
Below the configuration options is a table titled 'All Devices' with the following data:

Hostname	MAC Address	Device Type	Version	Upload Version
<input type="checkbox"/> AN-10-0F41C8	00-23-68-0F-41-C8	ap71xx	5.5.0.0-083R	5.5.0.0-083R
<input type="checkbox"/> AN-19-311779	00-23-68-31-17-79	ap650	5.5.0.0-083R	5.5.0.0-083R
<input type="checkbox"/> AN-18-3119E4	00-23-68-31-19-E4	ap650	5.5.0.0-083R	5.5.0.0-083R
<input type="checkbox"/> AN-17-311AC0	00-23-68-31-1A-C0	ap650	5.5.0.0-083R	5.5.0.0-083R
<input type="checkbox"/> AN-20-858F84	00-23-68-85-8F-84	ap650	5.5.0.0-083R	5.5.0.0-083R
<input type="checkbox"/> AN-21-859290	00-23-68-85-92-80	ap650	5.5.0.0-083R	5.5.0.0-083R
<input type="checkbox"/> AN-26-864484	00-23-68-86-44-84	ap650	5.5.0.0-083R	5.5.0.0-083R
<input type="checkbox"/> AN-11-8644B8	00-23-68-86-44-B8	ap650	5.5.0.0-083R	5.5.0.0-083R
<input type="checkbox"/> AN-15-864538	00-23-68-86-45-38	ap650	5.5.0.0-083R	5.5.0.0-083R
<input type="checkbox"/> AN-12-86455C	00-23-68-86-45-5C	ap650	5.5.0.0-083R	5.5.0.0-083R

At the bottom right of the interface is an 'Update Firmware' button.

- 4 Select **Device Image File**.

Use the **Device Image File** screen to select device image types for firmware updates and set the transfer protocol used for staging the firmware to the device itself prior to its update.



- 5 Select the controller, service platform or access point model from the **Device Type List** drop-down menu. This is the device model used to provision firmware to the devices selected within the All Devices table below. Selecting **All** makes each controller, service platform and access point model images available for updates on those specific models.
- 6 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).
- 7 Selecting **Advanced** lists additional options for the device's firmware image file location:

<b>Protocol</b>	Select the protocol for device firmware file management and transfer. Available options include: <ul style="list-style-type: none"> <li>•tftp</li> <li>•ftp</li> <li>•sftp</li> <li>•http</li> <li>•cf</li> </ul>
<b>Port</b>	Designate the port for transferring the firmware files used in the upgrade operation. Enter the port number directly or use the spinner control.
<b>Host</b>	Specify a numerical IP address or textual Hostname of the resource used to transfer files to the devices designated for a firmware update.
<b>Path / File</b>	Define the path to the file on the file repository resource. Enter the complete relative path to the file.

- 8 Select the **Load Image** button to upload the device firmware.

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.

## Device Image File

Use the **Device Image File** screen to select device image types for firmware updates and set the transfer protocol used for staging the firmware to the device itself prior to its update.

To define an upgrade configuration for a controller, service platform or access point:

- 1 Select **Operations**.
- 2 Ensure **Devices** is selected from the Operations menu on the top, left-hand, side of the screen.
- 3 Expand the System node, select a RF Domain and one of its member devices.
- 4 Select the **Adopted Device Upgrade** tab.
- 5 Select **Device Image File**.

**Adopted Device Upgrade**

Device Upgrade List | Device Image File | Upgrade Status | Upgrade History

Device Image Type: NX9000

Protocol: tftp | Port: 69 | Basic

Host: 0 . 0 . 0 . 0 | IP Address | Warning: Hostname or IP Address must be set

Path/File:

Device Type	Version
RFS7000	none
NX9000	none
AP6532	5.5.0.0-083R
AP621	5.5.0.0-083R
AP622	5.5.0.0-083R
NX65XX	none
AP6562	5.5.0.0-083R
AP650	5.5.0.0-083R
RFS6000	none
AP81XX	5.5.0.0-083R
RFS4000	5.5.0.0-083R
AP6521	5.5.0.0-083R

- 6 Select the controller, service platform or access point model from the **Device Type List** drop-down menu. This is the device model used to provision firmware to the devices selected within the All Devices table below. Selecting **All** makes each controller, service platform and access point model images available for updates on those specific models.
- 7 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).
- 8 Selecting **Advanced** lists additional options for the device's firmware image file location:

<b>Protocol</b>	Select the protocol for device firmware file management and transfer. Available options include: <ul style="list-style-type: none"> <li>•tftp</li> <li>•ftp</li> <li>•sftp</li> <li>•http</li> <li>•cf</li> </ul>
<b>Port</b>	Designate the port for transferring the firmware files used in the upgrade operation. Enter the port number directly or use the spinner control.



<b>Host</b>	Specify a numerical IP address or textual Hostname of the resource used to transfer files to the <i>devices</i> designated for a firmware update.
<b>Path / File</b>	Define the path to the file on the file repository resource. Enter the complete relative path to the file.

- 9 Select the **Load Image** button to upload the device firmware.

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.

### Upgrade Status

Once an upgrade operation has been started or schedules, an administrator can assess whether the upgrade was successful, the number of times the operation was attempted before completed and the upgraded device's current status.

To assess the administration, scheduling and progress of device firmware updates:

- 1 Select **Operations**.
- 2 Ensure **Devices** is selected from the Operations menu on the top, left-hand, side of the screen.
- 3 Expand the System node, select a RF Domain and one of its member devices.
- 4 Select the **Adopted Device Upgrade** tab.
- 5 Select **Upgrade Status**.

The screenshot shows the 'Adopted Device Upgrade' interface. At the top, there are tabs: Summary, Adopted Device Upgrade (selected), File Management, Adopted Device Restart, Captive Portal Pages, and RAID. Below the tabs is the title 'Adopted Device Upgrade' with a help icon. Underneath, there are links for 'Device Upgrade List', 'Device Image File', 'Upgrade Status' (selected), and 'Upgrade History'. The main section is titled 'Upgrade Status' and contains summary statistics:
 

- Number of devices currently being upgraded: 0
- Number of devices waiting in queue to be upgraded: 0
- Number of devices marked for cancellation: 0
- Number of devices currently being rebooted: 0
- Number of devices waiting in queue to be rebooted: 0

 Below the statistics is a table with the following columns: Device Type (with a checked checkbox), Hostname, MAC Address, Result, Upgrade Time, Reboot Time, Progress, Retries, Last Status (with a dropdown arrow), and Upgraded By. The table is currently empty. At the bottom right of the interface is a 'Cancel' button.

- 6 Refer to the **Upgrade Status** field to assess the completion of in-progress upgrades.

<b>Number of devices currently being upgraded</b>	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.
<b>Number of devices currently being booted</b>	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 <i>Device Upgrade List</i> , reboots can be staggered or placed on hold to ensure device remains in service.
<b>Number of devices waiting in queue to be upgraded</b>	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.
<b>Number of devices waiting in queue to be upgraded</b>	Lists the number of devices waiting to reboot before actively utilizing its upgraded image. The <i>Device Upgrade List</i> 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 be scheduled for periods of reduced load
<b>Number of devices marked for cancelation</b>	Lists the number of upgrades that have been manually canceled during the upgrade operation.

- 7 Refer to the following status reported for each current or scheduled upgrade operation:

<b>Device Type</b>	Displays the model number of devices pending an upgrade. Each listed device is provisioned an image file unique to that model.
<b>Hostname</b>	Lists the factory encoded MAC address of a device either currently upgrading or in the queue of scheduled upgrades.
<b>MAC Address</b>	Lists the factory encoded MAC address of a device either currently upgrading or in the queue of scheduled upgrades.
<b>Result</b>	Lists the state of an upgrade operation ( <i>downloading, waiting for a reboot etc.</i> ).
<b>Upgrade Time</b>	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.
<b>Reboot Time</b>	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.
<b>Progress</b>	Lists the number of specific device types currently upgrading.
<b>Retries</b>	Displays the number of retries, if any, needed for an in-progress firmware upgrade operation.
<b>Last Status</b>	Lists the last reported upgrade and reboot status of each listed in progress or planned upgrade operation.
<b>Upgraded By</b>	Lists the model of the controller, service platform or access point RF Domain manager that's provisioning an image to a listed device.

- 8 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 cancelation.
- 9 Select **Upgrade History**.

Once an upgrade operation has completed, an administrator can assess whether the upgrade was successful, the number of times the operation was attempted before completed and any errors encountered while upgrading.

Adopted Device Upgrade							
Device Upgrade List   Device Image File   Upgrade Status   Upgrade History							
Upgrade History							
Hostname	Device Type	MAC Address	Result	Time	Retries	Upgraded By	Last Status
AN-27-7033F4	ap81xx	B4-C7-99-70-33	done	Tue Oct 1 2013 11:10:00	1	SJCALPHAWLC	Update error: Unable to get update
AN-21-859290	ap650	00-23-68-85-92	done	Tue Oct 1 2013 11:10:00	0	SJCALPHAWLC	-
AN-20-858F84	ap650	00-23-68-85-8F	done	Tue Oct 1 2013 11:10:00	0	SJCALPHAWLC	-
AN-04-703464	ap81xx	B4-C7-99-70-34	done	Tue Oct 1 2013 11:10:00	0	SJCALPHAWLC	-
AN-19-311779	ap650	00-23-68-31-17	done	Tue Oct 1 2013 11:10:00	0	SJCALPHAWLC	-
AN-12-86455C	ap650	00-23-68-86-45	done	Tue Oct 1 2013 11:10:00	0	SJCALPHAWLC	-
AN-14-8647BC	ap650	00-23-68-86-47	done	Tue Oct 1 2013 11:10:00	0	SJCALPHAWLC	-
AN-03-7034DC	ap81xx	B4-C7-99-70-34	done	Tue Oct 1 2013 11:10:00	0	SJCALPHAWLC	-
AN-24-4A5FB8	ap622	B4-C7-99-4A-5F	done	Tue Oct 1 2013 11:10:00	0	SJCALPHAWLC	-
AN-17-311AC0	ap650	00-23-68-31-1A	done	Tue Oct 1 2013 11:10:00	0	SJCALPHAWLC	-
AN-22-4A3824	ap622	B4-C7-99-4A-3E	done	Tue Oct 1 2013 11:10:00	0	SJCALPHAWLC	-
AN-28-435766	ap622	B4-C7-99-43-57	done	Tue Oct 1 2013 11:10:00	0	SJCALPHAWLC	-

Clear History

10 Refer to the following **Upgrade History** status:

<b>Hostname</b>	Displays the administrator assigned Hostname for each listed controller, service platform or access point that's received an update.
<b>Device Type</b>	Displays the controller, service platform or access point model upgraded by a firmware update operation.
<b>MAC Address</b>	Displays the device <i>Media Access Control</i> (MAC) or hardware address for a device that's received an update.
<b>Result</b>	Displays the upgrade result for each listed device.
<b>Time</b>	Displays the time and date of the last status received from an upgraded device.
<b>Retries</b>	Displays the number of retries, if any, needed for the firmware upgrade operation.
<b>Upgraded By</b>	Displays the administrator credentials responsible for initiating each listed upgrade operation.
<b>Last Status</b>	Displays the last status update received for devices that have been upgraded.

11 Select the **Clear History** button to clear the current update information for each listed device and begin new data collections.

### Device Upgrade History

Once an upgrade operation has completed, an administrator can assess whether the upgrade was successful, the number of times the operation was attempted before completed and any errors encountered while upgrading.

To assess the administration, scheduling and progress of device firmware updates:

- 1 Select **Operations**.
- 2 Ensure **Devices** is selected from the Operations menu on the top, left-hand, side of the screen.

- 3 Expand the System node, select a RF Domain and one of its member devices.
- 4 Select the **Adopted Device Upgrade** tab.
- 5 Select **Upgrade History**.

Adopted Device Upgrade							
Device Upgrade List   Device Image File   Upgrade Status   Upgrade History							
Upgrade History							
Hostname	Device Type	MAC Address	Result	Time	Retries	Upgraded By	Last Status
AN-27-7033F4	ap81xx	B4-C7-99-70-33	done	Tue Oct 1 2013 11:00:00	1	SJCALPHAWLC	Update error: Unable to get update
AN-21-859290	ap650	00-23-68-85-92	done	Tue Oct 1 2013 11:00:00	0	SJCALPHAWLC	-
AN-20-858F84	ap650	00-23-68-85-8F	done	Tue Oct 1 2013 11:00:00	0	SJCALPHAWLC	-
AN-04-703464	ap81xx	B4-C7-99-70-34	done	Tue Oct 1 2013 11:00:00	0	SJCALPHAWLC	-
AN-19-311779	ap650	00-23-68-31-17	done	Tue Oct 1 2013 11:00:00	0	SJCALPHAWLC	-
AN-12-86455C	ap650	00-23-68-86-45	done	Tue Oct 1 2013 11:00:00	0	SJCALPHAWLC	-
AN-14-8647BC	ap650	00-23-68-86-47	done	Tue Oct 1 2013 11:00:00	0	SJCALPHAWLC	-
AN-03-7034DC	ap81xx	B4-C7-99-70-34	done	Tue Oct 1 2013 11:00:00	0	SJCALPHAWLC	-
AN-24-4A5FB8	ap622	B4-C7-99-4A-5F	done	Tue Oct 1 2013 11:00:00	0	SJCALPHAWLC	-
AN-17-311AC0	ap650	00-23-68-31-1A	done	Tue Oct 1 2013 11:00:00	0	SJCALPHAWLC	-
AN-22-4A3824	ap622	B4-C7-99-4A-3E	done	Tue Oct 1 2013 11:00:00	0	SJCALPHAWLC	-
AN-28-435766	ap622	B4-C7-99-43-57	done	Tue Oct 1 2013 11:00:00	0	SJCALPHAWLC	-

[Clear History](#)

- 6 Refer to the following **Upgrade History** status:

<b>Hostname</b>	Displays the administrator assigned Hostname for each listed controller, service platform or access point that's received an update.
<b>Device Type</b>	Displays the controller, service platform or access point model upgraded by a firmware update operation.
<b>MAC Address</b>	Displays the device <i>Media Access Control</i> (MAC) or hardware address for a device that's received an update.
<b>Result</b>	Displays the upgrade result for each listed device.
<b>Time</b>	Displays the time and date of the last status received from an upgraded device.
<b>Retries</b>	Displays the number of retries, if any, needed for the firmware upgrade operation.
<b>Upgraded By</b>	Displays the administrator credentials responsible for initiating each listed upgrade operation.
<b>Last Status</b>	Displays the last status update received for devices that have been upgraded.

- 7 Select the **Clear History** button to clear the current update information for each listed device and begin new data collections.

## Using the File Management Browser

Controllers, service platforms and access points can utilize a File Browser allowing an administrator to review the files residing on a 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 needed.

### 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**.

File Name	Size (Kb)	Last Modified	File Type
startup.3.log	905772	2013-04-22 17:00:31	binary
startup.5.log	901375	2013-04-12 18:23:18	binary
startup.2.log	908719	2013-04-22 17:14:36	binary
startup.4.log	901928	2013-04-22 12:57:19	binary
startup.1.log	912059	2013-04-23 13:26:44	binary

- 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:

<b>File Name</b>	Displays the name of the file residing on the selected <i>flash</i> , <i>system</i> , <i>nvram</i> or <i>usb1-4</i> location. The name cannot be modified from this location.
<b>Size (Kb)</b>	Displays the size of the file in kb. Use this information to help determine whether the file should be moved or deleted.
<b>Last Modified</b>	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.
<b>File Type</b>	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.
- 5 Optionally, use the **Delete Folder** or **Delete File** buttons to remove a folder or file from within the current memory resource.

### Managing File Transfers

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.

The screenshot shows a 'File Transfer' dialog box with the following configuration:

- Source:**
  - Radio buttons:  Server,  Local
  - Protocol: **tftp** (dropdown)
  - Port: **69** (spin box)
  - Host: **0 . 0 . 0 . 0** (IP Address dropdown)
  - Path/File:
- Target:**
  - Radio buttons:  Server,  Local
  - File: **flash:/** (text box)
  - Storage options:  flash,  system,  nvram,  cf,  usb1,  usb2
  - File list (File Name):
    - upgrade
    - crashinfo
    - log
    - cache
    - hotspot
    - floorplans
    - startuplog
    - radiusd.conf
    - nsm\_11\_1366\_13602399638\_AP7131\_!
    - MainApp.swf
    - nsm\_11\_1393\_1360239769\_AP7181\_5.
    - users
    - nwadmconf

Buttons: **OK** and **Cancel**

- 3 Set the following file management source and target directions and the configuration parameters of the required file management activity:

<b>Source</b>	Select the source of the file transfer. Select <i>Server</i> to indicate the source of the file is a remote server external to the controller or access point. Select <i>Local</i> to indicate the source of the file is the local device.
<b>File</b>	If the source is <i>Local</i> , enter the name of the file to be transferred.

<b>Protocol</b>	Select the protocol for file management. Available options include: <ul style="list-style-type: none"> <li>• <i>tftp</i></li> <li>• <i>ftp</i></li> <li>• <i>sftp</i></li> <li>• <i>http</i></li> <li>• <i>cf</i></li> <li>• <i>usb1-4</i></li> </ul> This parameter is required only when <i>Server</i> is selected as the Source.
<b>Port</b>	Specify the physical port for transferring files. This option is not available for <i>cf</i> and <i>usb1-4</i> . Enter the port number directly or use the spinner control. This parameter is required only when <i>Server</i> is selected as the Source.
<b>Host</b>	If needed, specify a hostname or numeric IP address of the server transferring the file. This option is <i>not</i> valid for <i>cf</i> and <i>usb1-4</i> . If a hostname is provided, an IP Address is not needed. This field is only available when <i>Server</i> is selected in the From field.
<b>User Name</b>	Provide a user name to access a FTP or a SFTP server. This parameter is required only when <i>Server</i> is selected as the Source, and the selected protocol is <i>ftp</i> or <i>sftp</i> .
<b>Password</b>	Provide a password to access the FTP or SFTP server. This parameter is required only when <i>Server</i> is selected as the Source, and the selected protocol is <i>ftp</i> or <i>sftp</i> .
<b>Path / File</b>	Define the path to the file on the server. Enter the complete relative path to the file. This parameter is required only when <i>Server</i> is selected as the Source.
<b>Target</b>	Select the target destination to transfer the file. <ul style="list-style-type: none"> <li>• Select <i>Server</i> if the destination is a remote server, provide a URL to the location of the server resource or select <i>Advanced</i> and provide the same network address information described above.</li> <li>• Select <i>Local</i> if the destination is the controller, service platform or access point.</li> </ul>

- 4 Select **Copy** to begin the file transfer. Selecting **Reset** reverts the screen to its last saved configuration.

## Restarting Adopted Devices

Controllers and service platforms can restart their adopted access points as needed for firmware upgrades or other administrative activities. access points set in Controller AP mode also have the ability to restart adopted peer model access points.

### 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 one or more adopted access points:

- 1 Select the **Operations > Devices > Adopted AP Restart**.

Adopted Device Restart									
	Hostname	MAC Address	Type	Version	Reason	<input type="checkbox"/> Force Reload	Delay (Seconds)	Message	Reload Status
<input type="checkbox"/>	ap6532-311E	00-23-68-83	ap6532	5.5.0.0-038B	reload by user	<input type="checkbox"/>	2		Status
<input type="checkbox"/>	ap650-3129C	00-23-68-83	ap650	5.5.0.0-038B	reload by user	<input type="checkbox"/>	2		Status
<input type="checkbox"/>	ap650-3129E	00-23-68-83	ap650	5.5.0.0-038B	reload by user	<input type="checkbox"/>	2		Status
<input type="checkbox"/>	ap650-312A	00-23-68-83	ap650	5.5.0.0-038B	reload by user	<input type="checkbox"/>	2		Status
<input type="checkbox"/>	ap7131-8A4	00-23-68-8E	ap71xx	5.5.0.0-038B	reload by user	<input type="checkbox"/>	2		Status
<input type="checkbox"/>	ap7131-0E3C	5C-0E-8B-83	ap71xx	5.5.0.0-038B	reload by user	<input type="checkbox"/>	2		Status
<input type="checkbox"/>	ap6532-345C	5C-0E-8B-83	ap6532	5.5.0.0-038B	reload by user	<input type="checkbox"/>	2		Status
<input type="checkbox"/>	ap6532-3471	5C-0E-8B-83	ap6532	5.5.0.0-038B	reload by user	<input type="checkbox"/>	2		Status
<input type="checkbox"/>	ap6532-3475	5C-0E-8B-83	ap6532	5.5.0.0-038B	reload by user	<input type="checkbox"/>	2		Status
<input type="checkbox"/>	ap6532-347E	5C-0E-8B-83	ap6532	5.5.0.0-038B	reload by user	<input type="checkbox"/>	2		Status
<input type="checkbox"/>	ap6532-3477	5C-0E-8B-83	ap6532	5.5.0.0-038B	reload by user	<input type="checkbox"/>	2		Status
<input type="checkbox"/>	ap6532-347E	5C-0E-8B-83	ap6532	5.5.0.0-038B	reload by user	<input type="checkbox"/>	2		Status
<input type="checkbox"/>	ap6532-347E	5C-0E-8B-83	ap6532	5.5.0.0-038B	reload by user	<input type="checkbox"/>	2		Status
<input type="checkbox"/>	ap6532-347E	5C-0E-8B-83	ap6532	5.5.0.0-038B	reload by user	<input type="checkbox"/>	2		Status

2 The Adopted AP Restart table displays the following information for each Adopted AP:

<b>Hostname</b>	Displays the administrator assigned hostname for each known access point.
<b>MAC Address</b>	Displays the factory assigned <i>Media Access Control</i> (MAC) or hardware address for each known access point.
<b>Type</b>	Displays the access point model number for each adopted access point.
<b>Version</b>	Displays the current firmware version for each adopted access point.
<b>Reason</b>	Lists the administrator defined reason an adopted device has been queued for a restart.

3 To restart one or more access points, select the checkbox to the left of each AP and set the following options:

<b>Force Reload</b>	To force a reload of an access point (or multiple access points), select the <i>Force Reload</i> checkbox next to the target AP.
<b>Delay (Seconds)</b>	Specify the amount of time, in seconds, before the access point restart is executed. Setting a delay time is recommended when an access point load cannot be assumed by a neighbor AP until a known time in the near future.
<b>Message</b>	Displays a message relating to the access point's current adoption.
<b>Reload Status</b>	Click the <i>Reload Status</i> button next to each adopted access point to display each device's current status information.



## Captive Portal Configuration

For information moving captive portal configurations to managed access points and making captive portals available to requesting clients, see:

- [AP Upload](#)
- [CP Page Image File](#)
- [Status](#)

### AP Upload List

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.

To upload captive portal pages to connected access points:

- 1 Select the **Operations** menu item.

Select **Devices** and select the **Captive Portal Pages** tab. The **AP Upload List** tab displays by default.

The screenshot displays the 'Captive Portal Pages' configuration page. The 'AP Upload List' sub-tab is active. The 'Captive Portal List' dropdown is set to 'CP8'. The 'Scheduled Upload Time' is set to 'Now' on '04/23/2013' at '00:00'. The 'All Devices' table contains the following data:

Hostname	MAC
ap6532-3118E0	00-23-68-31-18-E0
ap650-3129D8	00-23-68-31-29-D8
ap650-3129EC	00-23-68-31-29-EC
ap650-312A10	00-23-68-31-2A-10
ap7131-8A4848	00-23-68-8A-48-48
ap7131-0E3C40	5C-0E-8B-0E-3C-40
ap6532-34503C	5C-0E-8B-34-50-3C
ap6532-347110	5C-0E-8B-34-71-10

The 'Upload List' table is currently empty. Navigation buttons (>>, >, <<, <) are located between the two tables. At the bottom right, there are 'Cancel' and 'Upload' buttons.

- 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 for captive portal access.

### CP Page Image File

Use the **CP Pages Image File** screen to set the way managed access points receive captive portal images files required to provision captive portal access to requesting clients. Captive portal image files are the login, welcome and conditions pages specifically

To set the captive portal for upload and define the transfer configuration:

- 1 Select the **Operations** menu item.
- 2 Select **Devices** and select the **Captive Portal Pages** tab.
- 3 Select the **CP Pages Image File** tab.

<b>Captive Portal List</b>	Use the 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.
<b>Protocol</b>	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 <i>ftp</i> , <i>http</i> , <i>tftp</i> and <i>sftp</i> . A protocol parameter is required only when Server is selected as the Source and the Advanced option is used.
<b>Host</b>	If needed, specify a Hostname or numeric IP address of the server transferring the file. If a hostname is provided, an <i>IP Address</i> is not needed. This field is only available when Server is selected in the <i>From</i> field.
<b>Port</b>	Specify the port for transferring files. Enter the port number directly or use the spinner control..
<b>User Name</b>	Provide a user name to access the FTP or SFTP server. This parameter is required only when the selected protocol is ftp or sftp.
<b>Password</b>	Provide the password for the user name used to log in to the FTP/SFTP server. Only required when the protocol is ftp or sftp.
<b>Path/File</b>	Define the path to the file on the server. Enter the complete relative path to the file.

- 1 Select **Load Image** to upload the image file. Optionally, refer to the **Load Image Status** field to review the status of the current upload.

## Status

Use the **Status** screen to review those devices targeted for captive portal image uploads, their operational state and image upload completion status:

To assess the progress and completion status of captive portal image uploads:

- 1 Select the **Operations** menu item.
- 2 Select **Devices** and select the **Captive Portal Pages** tab.
- 3 Select the **Status** tab.

The screenshot shows a web interface window titled "Captive Portal Pages". At the top, there are three tabs: "AP Upload List", "CP Page Image File", and "Status", with "Status" being the active tab. Below the tabs is a section labeled "Upload History" containing a table with the following columns: Hostname, MAC, State, Progress, Retries, and Last Status. The table is currently empty. At the bottom right of the window, there are two buttons: "Clear History" and "Cancel".

<b>Hostname</b>	Displays the administrator defined hostname for the device receiving the captive portal page upload.
<b>MAC</b>	Displays the hardware encoded <i>Media Access Control</i> (MAC) address of the unit performing the captive portal page upload.
<b>State</b>	Displays the target device's current operational state within the controller or service platform managed network.
<b>Progress</b>	Displays the current upload progress for each captive portal page upload.
<b>Retries</b>	Lists the number of retries needed to upload the captive portal files to each listed device.
<b>Last Status</b>	Displays the last known status of the captive portal page upload to each listed device.

- 1 Select **Clear History** to clear the history displayed in the Status tab and begin new data collections.

## Crypto CMP Certificate

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.

Use the Crypto CMP Certificate menu item to manage these certificates:

- 1 Refer to the following for more information on **Crypto CMP Certificates**:  
:

<b>Hostname</b>	Lists the administrator assigned hostname of the CMP resource requesting a certificate renewal from the CMP CA server.
<b>MAC Address</b>	Lists the hardware encoded MAC address of the CMP server resource.
<b>Trust Point Name</b>	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.
<b>Trust Point Valid Until</b>	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.

- 2 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.
- 3 Select **Refresh** to update the screen to the last saved configuration.

## RAID

An administrator can configure a NX 95XX series RAID controller in respect to both its collective drive array as well as individual drive behavior and diagnostics. The service platform's array alarm can silenced, drive LEDs can be illuminated and stopped, drive consistency (integrity) checks can be made and the array can be prepared for drive replacements.

RAID controller drive arrays are available within the NX 95XX models only. However, they can be administrated on behalf of a NX 95XX profile by a different model service platform or controller.

## 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 locally with the controller, service platform or access point, while the private portion remains on a secure local area of the client.

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

- [Certificate Management](#) on page 917
- [RSA Key Management](#) on page 925
- [Certificate Creation](#) on page 70
- [Generating a Certificate Signing Request](#) on page 72

## Certificate Management

If not wanting to use an existing key or certificate, a *stored* certificate can be leveraged from a peer controller, service platform or access point. Device certificates can be imported and exported 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.

[Manage Certificates](#)
[RSA Keys](#)
[Create Certificate](#)
[Create CSR](#)

---

**Manage Certificates** ?

All Certificates Details			Certificate Details	
Certificates Name	RSA Keys	Valid	Subject Name :	<input style="width: 95%;" type="text"/>
default-trustpoint	CN=NX9000-B4-C7-99	02:02:2013 18:31:49 UT	Alternate Subject Name :	<input style="width: 95%;" type="text"/>
			Issuer Name :	<input style="width: 95%;" type="text"/>
			Serial Number :	<input style="width: 95%;" type="text"/>
			RSA Key Used :	<input style="width: 95%;" type="text"/>
			Is Self Signed :	
			RSA Key Used :	
			CRL Present :	
			Is CA :	

**Validity**

Valid From :	Valid Until :
--------------	---------------

The **Manage Certificates** screen displays for the selected MAC address.

- 3 Select a device from amongst those displayed to review its certificate.
- 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.

### *Import Certificates and Trustpoints*

A certificate links identity information with a public key enclosed in the certificate. 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.

To import trustpoints, certificate authorities, CRLs and signed 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.

- 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.

- To optionally import a CA certificate, 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.

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

<b>Trustpoint Name</b>	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.
<b>URL</b>	Provide the complete URL to the location of the trustpoint. If needed, select <i>Advanced</i> 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.
<b>Advanced / Basic</b>	Click the <i>Advanced</i> or <i>Basic</i> link to switch between a basic URL and an advanced location to specify trustpoint location.
<b>Protocol</b>	Select the protocol used for importing the target CA certificate. Available options include: <i>tftp</i> <i>ftp</i> <i>sftp</i> <i>http</i> <i>cf</i> <i>usb1-4</i>
<b>Port</b>	Use the spinner control to set the port. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
<b>Host</b>	Provide the hostname or numeric IP address of the server used to export the trustpoint. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
<b>Path/File</b>	Specify the path or filename of the CA certificate. Enter the complete relative path to the file on the server.
<b>Cut and Paste</b>	Select the <i>Cut and Paste</i> radio button to simply copy an existing CA into the cut and paste field. When pasting, no additional network address information is required.



- 6 Select **OK** to import the defined CA certificate. Select **Cancel** to revert the screen to its last saved configuration.
- 7 Select the **Import CRL** button from the **Import New Trustpoint** screen to optionally import a CRL to the controller, service platform or access point.

If a certificate displays with a CRL, that CRL can be imported into the controller, service platform or access point. 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 Certificate Revocation List \(CRL\) Configuration](#).

- 8 Define the following configuration parameters required for the **Import** of the CRL:

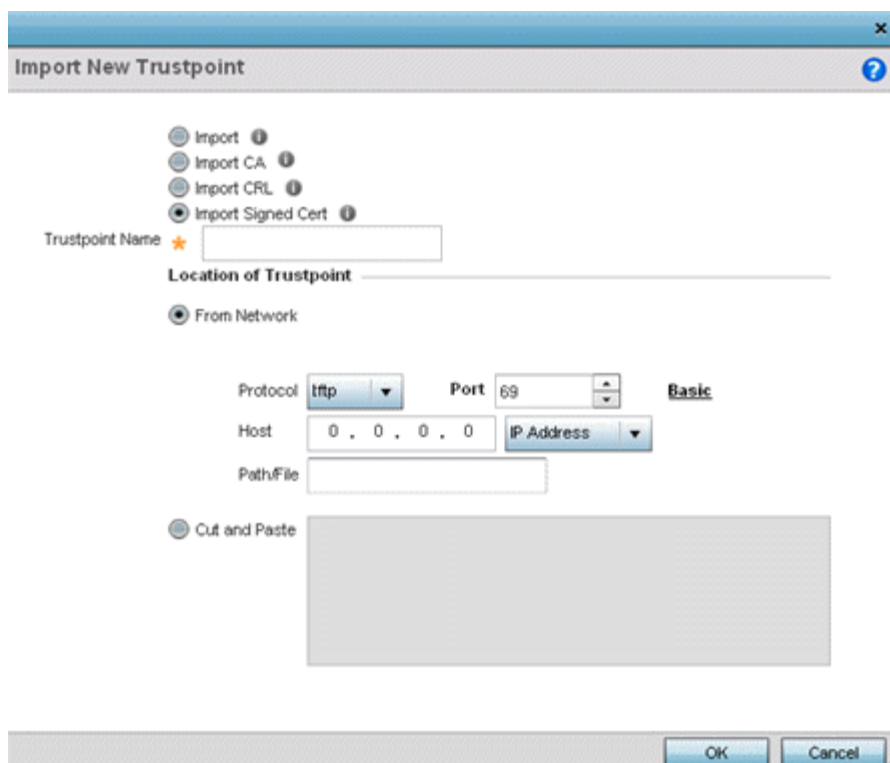
<b>Trustpoint Name</b>	Enter the 32 character maximum name assigned to the target trustpoint signing the certificate. A trustpoint represents a CA/identity pair containing the identity of the CA, CA-specific configuration parameters, and an association with an enrolled identity certificate.
<b>From Network</b>	Select the <i>From Network</i> 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.
<b>URL</b>	Provide the complete URL to the location of the CRL. If needed, select <i>Advanced</i> 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.

<b>Protocol</b>	Select the protocol used for importing the CRL. Available options include: <i>tftp</i> <i>ftp</i> <i>sftp</i> <i>http</i> <i>cf</i> <i>usb1-4</i>
<b>Port</b>	Use the spinner control to set the port. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
<b>Host</b>	Provide the hostname or numeric IP address of the server used to export the trustpoint. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
<b>Path/File</b>	Specify the path to the CRL. Enter the complete relative path to the file on the server.
<b>Cut and Paste</b>	Select the <i>Cut and Paste</i> radio button to simply copy an existing CRL into the cut and paste field. When pasting, no additional network address information is required.

- 9 Select **OK** to import the CRL. Select **Cancel** to revert the screen to its last saved configuration.
- 10 To import a signed certificate, select the **Import Signed Cert** button 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 controller 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.



- 11 Define the following parameters required for the **Import** of the Signed Certificate:

<b>Trustpoint Name</b>	Enter the 32 character maximum trustpoint name with which the certificate should be associated.
<b>From Network</b>	Select the <i>From Network</i> 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.
<b>URL</b>	Provide the complete URL to the location of the signed certificate. If needed, select <i>Advanced</i> 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.
<b>Protocol</b>	Select the protocol for importing the signed certificate. Available options include: <i>tftp</i> <i>ftp</i> <i>sftp</i> <i>http</i> <i>cf</i> <i>usb1-4</i>
<b>Port</b>	Use the spinner control to set the port. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
<b>Host</b>	Provide the hostname or numeric IP address of the server used to export the signed certificate. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
<b>Path/File</b>	Specify the path to the signed certificate. Enter the complete relative path to the file on the server.
<b>Cut and Paste</b>	Select the <i>Cut and Paste</i> radio button to simply copy an existing certificate into the cut and past cut and paste field. When pasting, no additional network address information is required.

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

### Export Trustpoints

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.

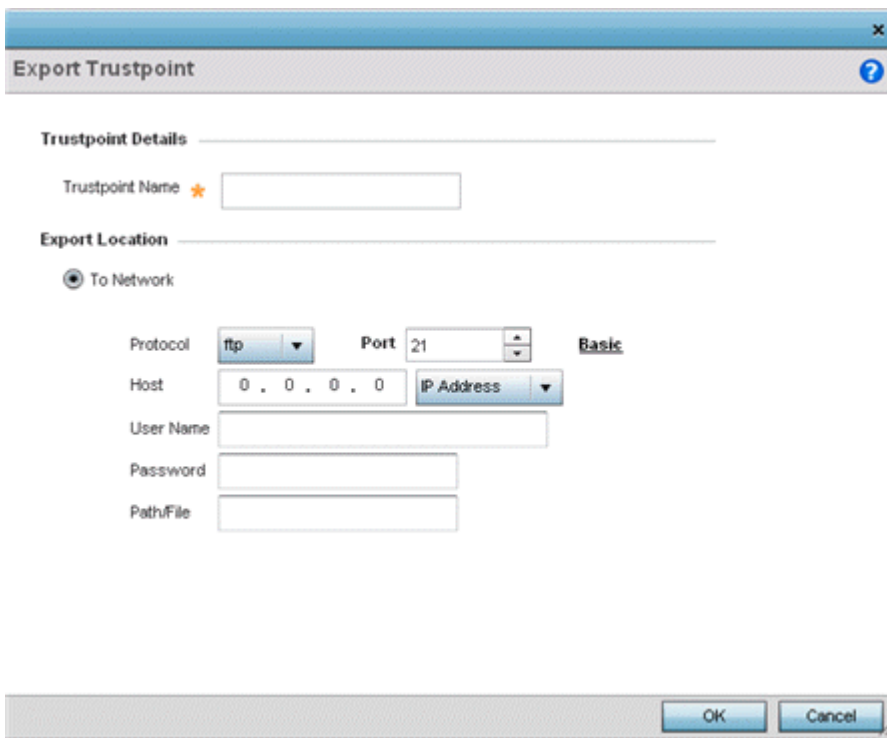
The trustpoints utilized by a controller, service platform or access point can be exported to an external resource for archive.

To export trustpoints:

- 1 Select **Operations > Manage Certificates**.
- 2 Select the **Export** button from the Certificate Management screen.

Once a certificate has been generated on the local 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.

- 3 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.



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

<b>Trustpoint Name</b>	Enter the 32 character maximum name assigned to the trustpoint. The trustpoint signing the certificate can be a certificate authority, corporation or individual.
<b>URL</b>	Provide the complete URL to the location of the trustpoint. If needed, select <i>Advanced</i> 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.
<b>Protocol</b>	Select the protocol used for exporting the target trustpoint. Available options include: <i>tftp</i> <i>ftp</i> <i>sftp</i> <i>http</i> <i>cf</i> <i>usb1-4</i>
<b>Port</b>	Use the spinner control to set the port. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
<b>Host</b>	Provide the hostname or numeric IP address of the server used to export the trustpoint. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
<b>Path/File</b>	Specify the path to the trustpoint. Enter the complete relative path to the file on the server.
<b>Cut and Paste</b>	Select the <i>Cut and Paste</i> radio button to simply copy an existing trustpoint into the cut and past field. When pasting, no additional network address information is required.

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



## RSA Key Management

Refer to the RSA Keys screen to review existing RSA key configurations applied to controller, service platform or access point 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.

The screenshot shows the 'RSA Keys' management interface. At the top, there are four tabs: 'Manage Certificates', 'RSA Keys', 'Create Certificate', and 'Create CSR'. Below the tabs is a header 'RSA Keys' with a help icon. The main content area is titled 'All Certificates Details' and contains a table with the following data:

RSA Name	Size (Kb)	RSA Public Key
default_rsa_key	1024	-----BEGIN PUBLIC KEY----- MIG1MA0GCsqGSib3DQEBAQUAA4GNADCBgQDA5yUm7WYz4M2Vgsh3qbdMmF3 0v2tURptgT3y8ra4eWzCX5QPE2jwq9yM2mpGmYVq3RPVEr+FAA4tkoXWROsX7Q/ 6pnXBS5evxxG1Paq4+LLXvJ+RUlpm7D5POLYrWICIZ+DwZJrOwdeRa09RBVAvocY76 ZgEibeNf8M0pMURWGIDAQAB -----END PUBLIC KEY-----

Below the table is a 'Certificate Details' section with the following information:

RSA Name: default\_rsa\_key  
Size: 1024  
RSA Public Key: -----BEGIN PUBLIC KEY-----  
MIG1MA0GCsqGSib3DQEBAQUAA4GNADCBgQDA5yUm7WYz4M2Vgsh3qbdMmF3  
0v2tURptgT3y8ra4eWzCX5QPE2jwq9yM2mpGmYVq3RPVEr+FAA4tkoXWROsX7Q/  
6pnXBS5evxxG1Paq4+LLXvJ+RUlpm7D5POLYrWICIZ+DwZJrOwdeRa09RBVAvocY76  
ZgEibeNf8M0pMURWGIDAQAB  
-----END PUBLIC KEY-----

At the bottom of the interface, there are four buttons: 'Generate Key', 'Import', 'Export', and 'Delete'.

- 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 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.
- 4 Define the following configuration parameters required for the Import of the key:

<b>Key Name</b>	Enter the 32 character maximum name assigned to the RSA key.
<b>Key Size</b>	Use the spinner control to set the size of the key (from 1,024 - 2,048 bits). Consider leaving this value at the default setting to ensure optimum functionality.

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

### Import an RSA Key

Controllers, service platforms and access point can import RSA keys utilized by other devices.

To Import an RSA Key:

- 1 Select **RSA Keys** tab from the Certificate Management screen.
- 2 Select the **Import** button from the **RSA Keys** tab.

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

<b>Key Name</b>	Enter the 32 character maximum name assigned to identify the RSA key.
<b>Key Passphrase</b>	Define the key (password) used by both the controller, service platform or access point and the server (or repository) of the target RSA key. Select <i>Show</i> to expose the actual characters used in the passphrase. Leaving the Show unselected displays the passphrase as a series of asterisks "***".
<b>URL</b>	Provide the complete URL to the location of the RSA key. If needed, select <i>Advanced</i> 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.
<b>Advanced / Basic</b>	Select either the <i>Advanced</i> or <i>Basic</i> link to switch between a basic URL and an advanced location to specify key location.

<b>Protocol</b>	Select the protocol used for importing the target key. Available options include: <i>tftp</i> <i>ftp</i> <i>sftp</i> <i>http</i> <i>cf</i> <i>usb1-4</i>
<b>Port</b>	Use the spinner control to set the port. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
<b>Host</b>	Provide the hostname or numeric IP address of the server used to import the RSA key. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
<b>Path/File</b>	Specify the path to the RSA key. Enter the complete relative path to the key on the server.

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

### Export an RSA Key

The keys utilized by a controller, service platform or access point can be exported to an external resource for archive and future use.

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.

To Export an RSA Key:

- 1 Select **RSA Keys** tab from the Certificate Management screen.
- 2 Select the **Export** button from the **RSA Keys** tab .
- 3 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.

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

<b>Key Name</b>	Enter the 32 character maximum name assigned to the RSA key.
<b>Key Passphrase</b>	Define the key passphrase used by both the controller, service platform or access point and the server. Select <i>Show</i> to expose the actual characters used in the passphrase. Leaving the Show unselected displays the passphrase as a series of asterisks <i>***</i> .
<b>URL</b>	Provide the complete URL to the location of the key. If needed, select <i>Advanced</i> 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.
<b>Protocol</b>	Select the protocol used for exporting the RSA key. Available options include: <i>tftp</i> <i>ftp</i> <i>sftp</i> <i>http</i> <i>cf</i> <i>usb1-4</i>
<b>Port</b>	Use the spinner control to set the port. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
<b>Host</b>	Provide the hostname or numeric IP address of the server used to export the RSA key. This option is not valid for <i>cf</i> and <i>usb1-4</i> .
<b>Path/File</b>	Specify the path to the key. Enter the complete relative path to the key on the server.

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

### Delete an RSA Key

As keys become obsolete they can be deleted from their managing controller, service platform or access point.

To delete an RSA Key:

- 1 Select **RSA Keys** tab from the Certificate Management screen.
- 2 Select the **Delete** button from within the **RSA Keys** tab.
- 3 Provide the key name within the **Delete RSA Key** screen and select **Delete Certificates** to remove the certificate.
- 4 Select **OK** to proceed with the deletion, or **Cancel** to revert back to the Certificate Management screen.

## Certificate Creation

Use the **Certificate Management** screen to create 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 In the **Certificate Management** screen, select **Launch Manager** from either the SSH RSA Key, RADIUS Certificate Authority, or RADIUS Server Certificate parameters.
- 2 Select **Create Certificate** from the upper, left-hand, side of the **Certificate Management** screen.



**Figure 345: 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 <b>Use Existing</b> 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 <b>Create New</b> to enter a 32-character maximum name used to identify the RSA key. Set the size of the key to either 1,024 or 2,048 bits. We recommend leaving this value at the default setting of 2,048 to ensure optimum functionality.

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



Certificate Subject Name	Select either <b>auto-generate</b> to automatically create the certificate's subject credentials or <b>user-configured</b> to manually enter the credentials of the self-signed certificate. The default setting is <b>auto-generate</b> .
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 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 the organization represented in the certificate. This is a required field.
Organizational Unit (OU)	Enter the organization unit represented in the certificate. This is a required field.
Common Name (CN)	If there is 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): an unambiguous domain name that absolutely specifies the node's position in the DNS tree hierarchy. To distinguish an FQDN from a regular domain name, a trailing period is added – for example, <i>somehost.example.com</i> . 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. IPv6 formatted addresses are not permitted.

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

## Generating a Certificate Signing Request

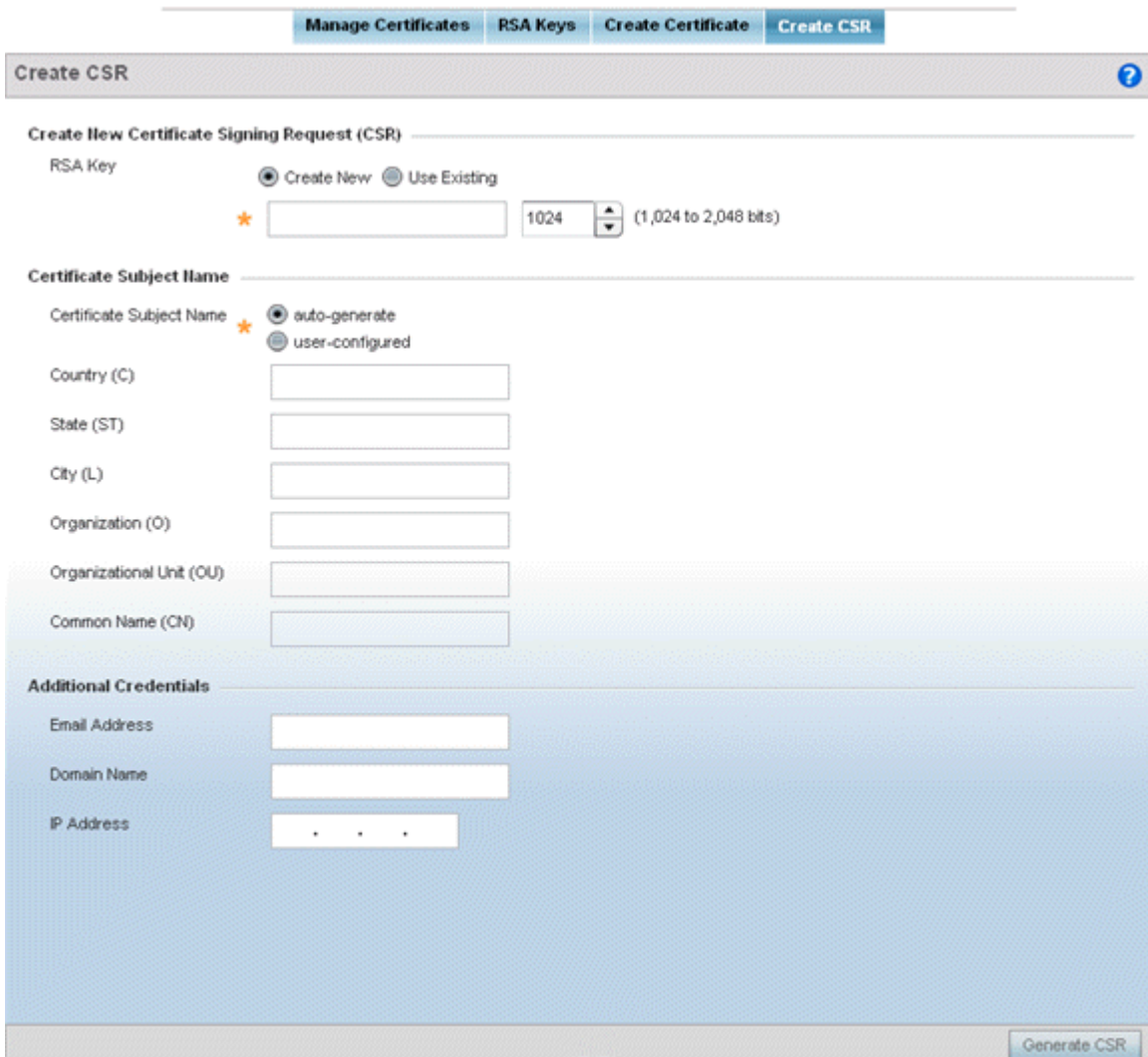
A certificate signing request (CSR) is a message from a requestor to a certificate authority to apply for a digital certificate. The CSR is composed of a block of encrypted text generated on the server where the certificate will be used. It contains the organization name, common name (domain name), locality, and country.

An 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 it 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 In the **Certificate Management** screen, select **Launch Manager** from either the SSH RSA Key, RADIUS Certificate Authority, or RADIUS Server Certificate parameters.
- 2 Select **Create CSR** from the upper, left-hand, side of the **Certificate Management** screen.



**Figure 346: Certificate Management - Create CSR Screen**

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

RSA Key	Select <b>Use Existing</b> 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 <b>Create New</b> to enter a 32-character maximum name used to identify the RSA key. Set the size of the key to either 1,024 or 2,048 bits. We recommend leaving this value at the default setting of 2,048 to ensure optimum functionality.
---------	--

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

Certificate Subject Name	Select either <b>auto-generate</b> to automatically create the certificate's subject credentials or <b>user-configured</b> to manually enter the credentials of the self-signed certificate. The default setting is <b>auto-generate</b> .
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 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 organization unit represented in the CSR. This is a required field.
Common Name (CN)	If there is 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): an unambiguous domain name that absolutely specifies the node's position in the DNS tree hierarchy. To distinguish an FQDN from a regular domain name, a trailing period is added – for example, <i>somehost.example.com</i> . 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. IPv6 formatted addresses are not permitted.

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

## 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 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, an individual controller, service platform or access point manages the calibration and monitoring phases. In clustered environments, a Smart Scan master is elected, 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.

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.

## Managing Smart RF for an RF Domain

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 a controller, service platform or access point RF Domain:

- 1 Select **Operations**.
- 2 Select **Smart RF**.
- 3 Expand the System mode in the upper, left-hand, side of the user interface to display the RF Domains available for Smart RF calibration.
- 4 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.

Hostname	AP MAC Address	Radio MAC Address	Radio Index	Old Channel	Channel	Old Power	Power	Smart Sensor	State	Type
ap622-57F:	B4-C7-99-E	B4-C7-99-E	0		1	0 dBm	13 dBm	✗	Normal	802.11bgn
ap622-57F:	B4-C7-99-E	B4-C7-99-E	1		52w	0 dBm	10 dBm	✗	Normal	802.11an
ap622-586:	B4-C7-99-E	B4-C7-99-E	1		44w	0 dBm	17 dBm	✗	Normal	802.11an
ap622-586:	B4-C7-99-E	B4-C7-99-E	0		8	0 dBm	10 dBm	✗	Normal	802.11bgn

Type to search in tables Row Count: 4

- 5 Refer to the following to determine whether a Smart RF calibration or an interactive calibration is required:

<b>Hostname</b>	Displays the administrator assigned Hostname for each member of the RF Domain.
<b>AP MAC Address</b>	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.
<b>Radio MAC Address</b>	Displays the hardware encoded MAC address assigned to each access point radio within the selected RF Domain. This value cannot be modified as part of a calibration activity.

<b>Radio Index</b>	Displays a numerical index assigned to each listed access point radio when it was added to the 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.
<b>Old Channel</b>	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.
<b>Channel</b>	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.
<b>Old Power</b>	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.
<b>Power</b>	This column displays the transmit power level for the listed access point MAC address after an Interactive Calibration resulted in a power adjustment. This is the new power level defined by Smart RF to compensate for a coverage hole.
<b>Smart Sensor</b>	Defines whether a listed access point is smart sensor on behalf of the other access point radios comprising the RF Domain.
<b>State</b>	Displays the current state of the Smart RF managed access point radio. Possible states include: <i>Normal</i> , <i>Offline</i> and <i>Sensor</i> .
<b>Type</b>	Displays the radio type (802.11an, 802.11bgn etc.) of each listed access point radio within the selected RF Domain.

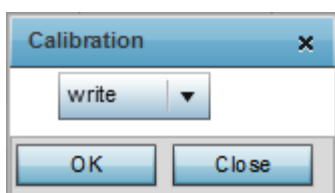
- 6 Select the **Refresh** button to (as needed) to update the contents of the Smart RF screen and the attributes of the devices within the selected RF Domain.



#### Note

Smart RF is not able to detect a voice call in progress, and will switch to a different channel resulting in voice call reconnections.

- 7 Select the **Interactive Calibration** button to initiate a Smart RF calibration using the access points within the selected RF Domain. The results of the calibration display within the Smart RF screen. Of particular interest are the channel and power adjustments made by the controller's Smart RF module. Expand the screen to display the Event Monitor to track the progress of the Interactive Calibration.
- 8 Select the **Calibration Result Actions** button to launch a sub screen used to determine the actions taken based on the results of the Interactive Calibration. The results of an Interactive calibration are not applied to radios directly, the administrator has the choice to select one of following options:



<b>Replace</b>	Overwrites the current channel and power values with new channel power values the Interactive Calibration has calculated.
<b>Write</b>	Writes the new channel and power values to the radios under their respective device configurations.
<b>Discard</b>	Discards the results of the Interactive Calibration without applying them to their respective devices.

- 9 Select the **Run Calibration** option to initiate a calibration. New channel and power values are applied to radios, they are not written to the running-configuration.

These values are dynamic and may keep changing during the course of the run-time monitoring and calibration the Smart RF module keeps performing to continually maintain good coverage. Unlike an Interactive Calibration, the Smart RF screen is not populated with the changes needed on access point radios to remedy a detected coverage hole. Expand the screen to display the Event Monitor to track the progress of the calibration.

- 10 The calibration process can be stopped by selecting the **Stop Calibration** button.

# 15 Statistics

System Statistics  
RF Domain Statistics  
Controller Statistics  
EX3500 Interface Extended IF  
Access Point Statistics  
Wireless Client Statistics  
Guest Access Statistics  
Analytics Developer Interface

This chapter describes statistics displayed by the GUI (graphical user interface). 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 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.

**System** wide statistics are available to review the health of the entire wireless network, including all its RF Domains and member devices.

**RF Domain** statistics are available to administrate specific device groups (domains) created in respect to their shared deployment objective.

**RFS controller** and **NX series service platform** statistics (both available under Wireless Controller statistics) display detailed information about 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](#) on page 937
- [RF Domain Statistics](#) on page 950
- [Controller Statistics](#) on page 1001
- [Wireless Client Statistics](#) on page 1276
- [Guest Access Statistics](#) on page 1288



#### Note

NOC controllers (VX 9000, NX 96XX, NX 95XX, and NX 7510) 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 1298.

## System Statistics

The **System** screen displays information supporting managed devices (wireless controllers, service platforms, access points and their connected wireless clients). Use this information to assess the overall state of the devices comprising the system. Systems data is organized as follows:

The data is organized as follows:

- [Health](#)
- [Inventory](#)
- [Adopted Devices](#)
- [Pending Adoptions](#)
- [Offline Devices](#)
- [Device Upgrade](#)
- [Licenses](#)
- [WIPS Summary](#) on page 948

The following devices can report system data:

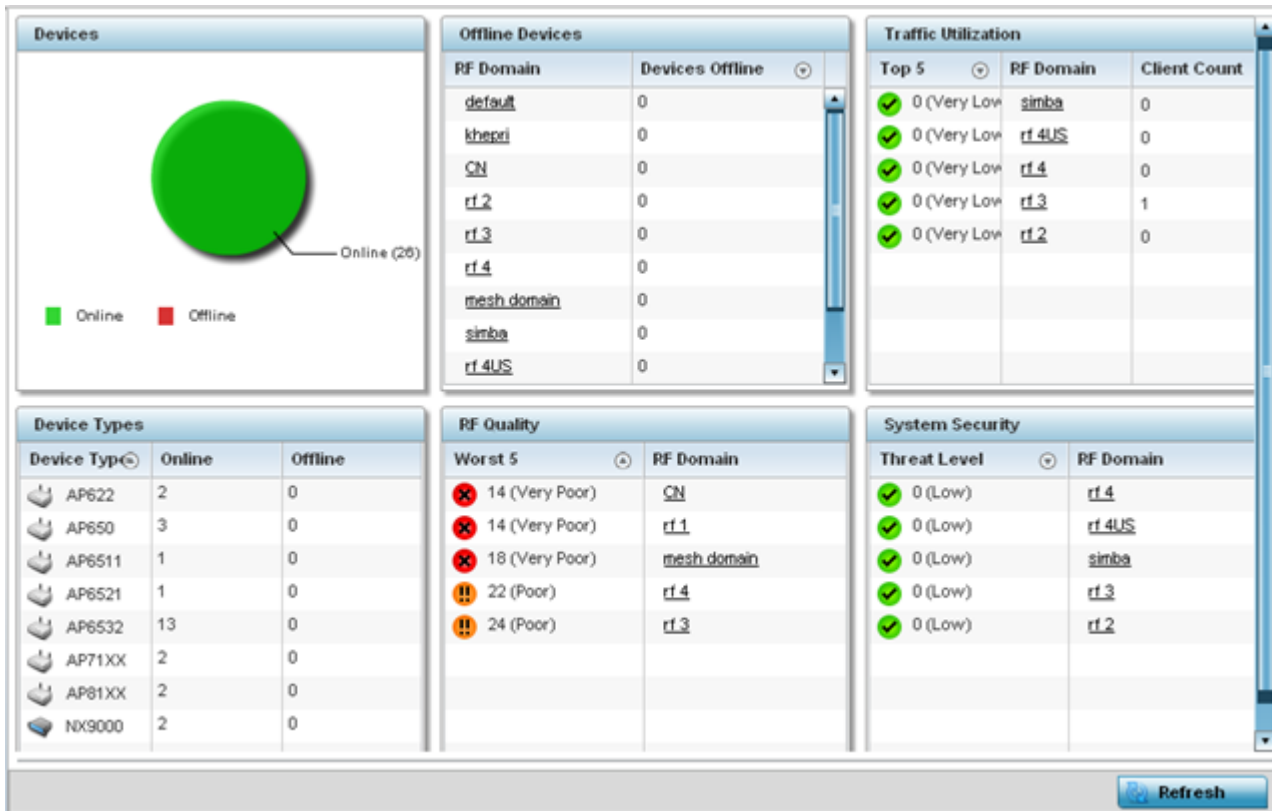
- Access Points - AP 6522, AP 6562, AP 7161, AP 7502, AP 7522, AP 7532, AP 7562, AP 7602, AP 7612, AP 7622, AP 7632, AP 7662, AP 8163, AP 8432, AP 8533
- Wireless Controllers - RFS 4000
- Service Platforms - NX 5500, NX 7510, NX 95XX, NX 96XX, VX 9000

## Health

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 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 347: Statistics - System - Health Screen**

- 4 The **Devices** table 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 managed network.
- 5 The **Offline Devices** table displays a list of devices in the controller managed network that are currently offline.

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.

<b>Top 5</b>	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: <ul style="list-style-type: none"> <li>• 0-20 – Very low utilization</li> <li>• 20-40 – Low utilization</li> <li>• 40-60 – Moderate utilization</li> <li>• 60 and above – High utilization</li> </ul>
<b>RF Domain</b>	Displays the name of the RF Domain. Each listed RF Domain can be selected to display device membership and performance data in greater detail.
<b>Client Count</b>	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 controller managed 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.

Refer to the following table for details:

Worst 5	Displays five RF Domains with the lowest quality indices in the wireless controller managed network. The value can be interpreted as: <ul style="list-style-type: none"> <li>• <b>0-50</b> – Poor Quality</li> <li>• <b>50-75</b> – Medium Quality</li> <li>• <b>75-100</b> – Good Quality</li> </ul>
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 is an average of the threat indices of all the RF Domains managed by the wireless controller or service platform.

Threat Level	Displays the threat perception value. This value can be interpreted as: <ul style="list-style-type: none"> <li>• <b>0-2</b> – Low threat level</li> <li>• <b>3-4</b> – Moderate threat level</li> <li>• <b>5</b> – High threat level</li> </ul>
RF Domain	Displays the name of the target RF Domain for which the threat level is displayed.

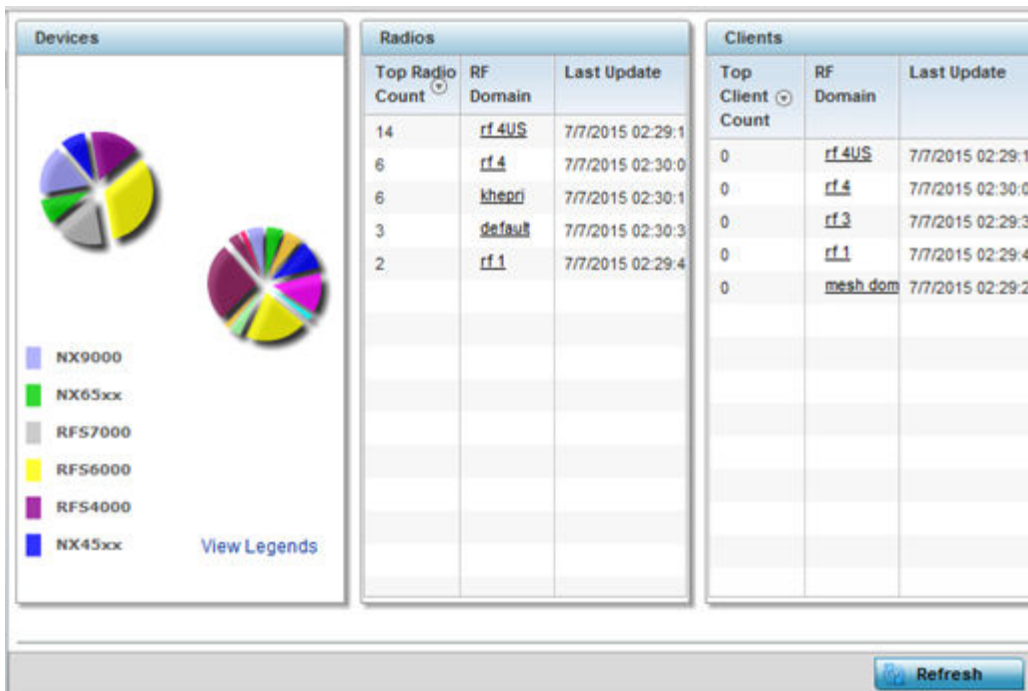
- 10 Select **Refresh** at any time to update the statistics counters to their latest values.

## Inventory

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 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.



- The **Devices** table displays an exploded pie chart depicting the 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 system's deployment objective.
- The **Radios** table displays radios deployed within the wireless controller or service platform managed network. This area displays the total number of managed radios and the top 5 RF Domains in terms of radio count. The **Total Radios** value is the total number of radios in this system.

Top Radio	Displays the radio index for each listed top performing radio.
RF Domain	Displays the name of the RF Domain where the listed radios reside as device members. The RF Domain displays as a link that can be selected to display specific RF Domain member radio configuration information in greater detail.
Last Update	Displays the UTC timestamp when each listed radio was last reported.

- The **Clients** table displays the total number of wireless clients managed by the wireless 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	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.





- Select **Refresh** to update the statistics counters to their latest values.

## Adopted Devices


The **Adopted Devices** screen displays a list of devices adopted to the wireless controller or service platform managed network. Use this screen to view a list of devices and their current status.

To view adopted device 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.

Adopted Device	Type	RF Domain Name	Model Number	Config Status	Config Errors	Adopter Hostname	Adoption Time	Startup Time
 <a href="#">RFS6K-SITE1</a>	 RFS60	<a href="#">default</a>	RFS6000	version-m		NOC-NX950	Mon Jan 8 2	Tue Jan 2 2018
 <a href="#">RFS6K-SITE2</a>	 RFS60	<a href="#">default</a>	RFS-6010	version-m		NOC-NX950	Mon Jan 8 2	Tue Jan 2 2018

Type to search in tables Row Count: 2



The **Adopted Devices** screen displays the following information:

Adopted Device	Displays the 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. Select the RF Domain link to display configuration and network address information in greater detail for member devices.
Model Number	Lists the model number of each AP that has been adopted 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.
Adopter Hostname	Lists the administrator hostname assigned to the adopting controller, service platform or access point.
Adoption Time	Displays a timestamp for each listed device reflecting when the device was adopted.
Startup Time	Provides a date stamp when the adopted device was restarted post adoption



- 4 Click **Refresh** to update the statistics counters to their latest values.

## Pending Adoptions

The **Pending Devices** screen displays those devices detected within a controller or service platform managed coverage area, but have yet to be adopted. Review these devices to assess whether they are good available resources to provide services to requesting clients and peer radio devices.

To view pending adoptions:

- 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.

	MAC Address	Type	IP Address	VLAN	Reason	Discovery Option	Last Seen
	00-23-68-8D-FE-4C	AP71xx	172.168.1.102	5	Auto-Provisioning	fqdn: ap7181-8Df	5/15/2013 08:31:23 PM 

Type to search in tables Row Count: 1

[Add to Devices](#) [Refresh](#)

The **Pending Adoptions** screen displays the following information:

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 device’s model type.
IP Address	Displays the current IP address of the device pending adoption.
VLAN	Displays the VLAN the pending device uses as a virtual interface once adopted.
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 <b>Add to Devices</b> button to begin the adoption process for this detected AP.

- 4 Click **Refresh** to update the statistics counters to their latest values.

## Offline Devices

The **Offline Devices** screen displays a list of devices within the wireless controller or service platform managed network or RF Domain that are currently off line. Review the contents of this screen to help determine whether an offline devices requires administration.

To view offline devices potentially available for adoption:

- 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.

Hostname	MAC Address	Type	RF Domain Name	Reporter	Area	Floor	Connected To	Last Update
ap622-57F5F	B4-C7-99-57	AP622	simba	nx9500-0C				8/16/2013 12:28:18 PM
ap622-5864A	B4-C7-99-58	AP622	simba	nx9500-0C				8/16/2013 12:28:18 PM
ap650-3129C	00-23-68-31	AP650	rf_4	nx9500-0C				8/16/2013 12:28:18 PM
ap650-3129E	00-23-68-31	AP650	rf_4	nx9500-0C				8/16/2013 12:28:18 PM
ap650-312A1	00-23-68-31	AP650	default	nx9500-0C				8/16/2013 12:28:18 PM
ap6511-8A4E	5C-0E-8B-8A	AP6511	rf_3	nx9500-0C				8/16/2013 12:28:18 PM
ap6521-970C	5C-0E-8B-97	AP6521	CN	nx9500-0C				8/16/2013 12:28:18 PM
ap6522-5A84	B4-C7-99-5A	AP6522	default	nx9500-0C				8/16/2013 12:28:18 PM
ap6532-3118	00-23-68-31	AP6532	rf_2	nx9500-0C				8/16/2013 12:28:18 PM
ap6532-3450	5C-0E-8B-34	AP6532	rf_1	nx9500-0C				8/16/2013 12:28:18 PM
ap6532-3471	5C-0E-8B-34	AP6532	rf_4US	nx9500-0C				8/16/2013 12:28:18 PM
ap6532-3475	5C-0E-8B-34	AP6532	rf_4US	nx9500-0C				8/16/2013 12:28:18 PM
ap6532-3476	5C-0E-8B-34	AP6532	rf_4US	nx9500-0C				8/16/2013 12:28:18 PM
ap6532-3477	5C-0E-8B-34	AP6532	rf_4US	nx9500-0C				8/16/2013 12:28:18 PM
ap6532-3478	5C-0E-8B-34	AP6532	rf_4US	nx9500-0C				8/16/2013 12:28:18 PM

Type to search in tables Row Count: 27

[Refresh](#)

The **Offline Devices** screen lists the following information:

Hostname	Lists the administrator assigned hostname provided when the device was detected within the controller, service platform or access point managed network.
MAC Address	Displays the factory encoded MAC address of each listed offline device.
Type	Displays the AP model type.
RF Domain Name	Displays the name of the offline device's RF Domain membership, if applicable. Select the RF Domain link to display configuration and network address information in greater detail.
Reporter	Displays the administrator assigned hostname of the device reporting a device as offline. Select the reporting device link to display configuration and network address information in greater detail.
Area	Lists the administrator assigned deployment area where the offline device is detected.
Floor	Lists the administrator assigned deployment floor where the offline device is detected.

Connected To	Lists the offline 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. Select the arrow next to the date and time to toggle between standard time and UTC.

- 4 Click **Refresh** to update the statistics counters to their latest values.

## Device Upgrade

The **Device Upgrade** screen displays available licenses for devices within a cluster. It displays the total number of AP licenses.

To view upgrade statistics at a system level:

- 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.

Upgraded By Device	Type	Device Hostname	History Id	Last Update Status	Time Last Upgraded	Retries Count	State
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 04:05:51 AM	1	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:05:32 AM	0	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:05:30 AM	0	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 04:05:31 AM	1	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 04:00:42 AM	1	done
nx9500-0C9848	ap622	ap622-5864	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 03:59:45 AM	1	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:04:47 AM	0	done
nx9500-0C9848	ap6532	ap6532-311	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:04:50 AM	0	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	Update error:	Mon May 13 2013 04:05:02 AM	1	done
nx9500-0C9848	ap81xx	ap8132-73B	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 04:05:18 AM	0	done
nx9500-0C9848	ap6532	ap6532-A65	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:57:23 AM	0	done
nx9500-0C9848	ap650	ap650-3129	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:57:38 AM	0	done
nx9500-0C9848	ap6511	ap6511-8A4	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:57:48 AM	0	done
nx9500-0C9848	ap6532	ap6532-347	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:57:55 AM	0	done
nx9500-0C9848	ap6521	ap6521-970	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:58:22 AM	0	done
nx9500-0C9848	ap650	ap650-312A	B4-C7-99-0C-98-48.1368	-	Mon May 13 2013 03:58:47 AM	0	done
nx9500-0C9848	ap81xx	ap8132-73B	B4-C7-99-0C-98-48.1368	Start Upgrade	Mon May 13 2013 03:58:58 AM	3	failed

Type to search in tables Row Count: 720

The **Device Upgrade** screen displays the following information:

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 of the access point.
Device Hostname	Displays the administrator-assigned hostname of the access point or the device receiving the 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	Displays the date and time of the last upgrade operation.
Retries Count	Displays the number of retries made in an update operation.
State	Displays the <b>done</b> or <b>failed</b> state of an upgrade operation.

- 4 Click **Clear History** to clear the screen of its current status and begin a new data collection.
- 5 Click **Refresh** to update the statistics counters to their latest values.

## Licenses

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.

The **Native Summary** tab displays by default.



### Note

For more information on the **Native License Summary** screen, click [here](#).

- 4 Select **Native Details** to view detailed license information.



### Note

For more information on the **Native > License > Details** screen, click [here](#).

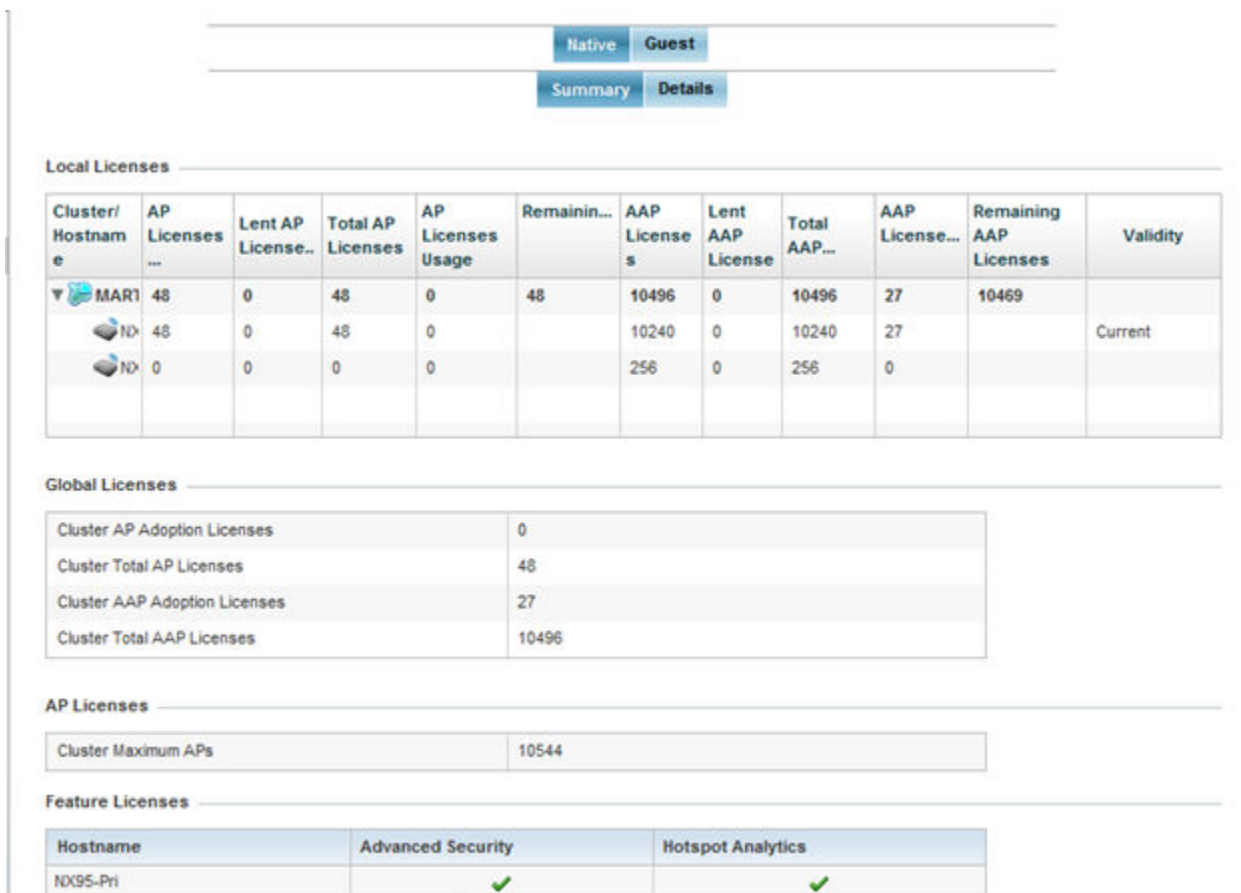
### *Native/Guest Summary Screen*

The **Native/Guest Summary** tab displays available licenses for cluster member devices. It displays the total number of AP (Access Point) and AAP (Adaptive Access Point) licenses that can be utilized amongst members.



### Note

The **Summary** page for the **Native** and **Guest** tabs display same set of information for local and guest devices respectively. Therefore, the following information applies to both.



**Figure 348: Statistics - Licenses Screen**

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 AP connections available to this controller or service platform under the terms of the current license.
Lent AP Licenses	Displays the number of AP licenses lent (from this controller or service platform) to a cluster member to compensate for an AP's license deficiency.
Total AP Licenses	Displays the total number of AP connection licenses currently available to this controller or service platform.
AP License Usage	Lists the number of AP 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 access point licenses available from the pooled license capabilities of all the members of the cluster.
AAP Licenses Installed	Lists the number of AAP connections available to this controller or service platform under the terms of the current license.
Lent AAP Licenses	Displays the number of AAP licenses lent (from this controller or service platform) to a cluster member to compensate for an AP licenses deficiency.
Total AAP Licenses	Displays the total number of AAP connection licenses currently available to this controller or service platform.

AAP Licenses Usage	Lists the number of AAP 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.

The **Global Licenses** area provides the following information:

<b>Cluster AP Adoption Licenses</b>	Displays the current number of AP adoption licenses utilized by controller or service platform connected APs within a cluster.
<b>Cluster Total AP Licenses</b>	Displays the total number of AP adoption licenses available to controller or service platform connected APs within a cluster.
<b>Cluster AAP Adoption Licenses</b>	Displays the current number of AAP adoption licenses utilized by controller or service platform connected APs within a cluster.
<b>Cluster Total AAP Licenses</b>	Displays the total number of AAP adoption licenses available to controller or service platform connected APs within a cluster.

The **AP Licenses** table provides the following information:

Cluster Maximum APs	Lists the maximum number of APs permitted in a cluster under the terms of the current license.
---------------------	--

The **Featured Licenses** area provides the following information:

Hostname	Displays the administrator assigned hostname of the controller, service platform or AP 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.
Advanced WIPS	Displays whether a separately licensed Advanced WIPS application is installed (separately licensed) for each listed hostname.
Hotspot Analytics	Displays whether a separately licensed Analytics application is installed for supported NX 95XX service platforms.

### *Native/Guest Details Screen*

Refer to the **Native/Guest 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.



**Note**

The **Details** page for the **Native** and **Guest** tabs display same set of information for local and guest devices respectively. Therefore, the following information applies to both.

Refer the following table for 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 AP.
AP Licenses Installed	Lists the number of AP connections available to this controller or service or peer AP under the terms of the current license.
Borrowed AP Licenses	Displays the number of AP licenses temporarily borrowed from a cluster member to compensate for an AP license deficiency.
Total AP Licenses	Displays the total number of AP connection licenses currently available to clustered devices.
AP License Usage	Lists the number of AP 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 (AAP) connections available under the terms of current licenses.
Borrowed AAP Licenses	Displays the number of AAP licenses temporarily borrowed from a cluster member to compensate for an AAP license deficiency.
Total AAP Licenses	Displays the total number of AAP connection licenses currently available to clustered devices.
AAP Licenses Usage	Lists the number of AAP 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.

## WIPS Summary

The WIPS (Wireless Intrusion Protection System) 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 lock down 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 APs, as well as the occurrence of WIPS events within the 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.

RF Domain	Number Of Rogue APs	Number Of Interfering APs	Number Of WIPS Events
7502	0	57	54
all			
CN	0	0	0
default			
khepri	0	153	1,024
mesh domain	0	58	1,024
Oak	0	331	17
rf 1	0	387	911
rf 2			
rf 3	0	70	270
rf 4	0	358	1,024
rf 4US	0	219	1,024
rf US			
simba			
sitecon			

Type to search in tables Row Count: 15

[WIPS Report](#) [Refresh](#)

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 AP 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 APs versus the other RF Domains within the controller, service platform or AP 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 an administrator as a known and approved controller, service platform or AP 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 <i>noise</i> value, it is 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 <b>enable</b> or <b>disable</b> 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.



- 6 Select one of the following options to refine event reporting to a specific type of WIPS activity.
  - **Only Rogue APs**
  - **Only Interferer APs**
  - **All APs**
- 7 Click **Generate Report** to compile and archive the results of the query.
- 8 Click **Refresh** to update the screen's statistics counters to their latest values.

## RF Domain Statistics

The **RF Domain** screens display status for a selected controller, service platform or access point RF Domain. This includes the RF Domain *health* and *device inventory*, *wireless clients* and *Smart RF* functionalities. 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.

Unlike controllers and service platforms, access point RF Domains are comprised of just other APs.

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](#)
- [Device Upgrade](#) on page 958
- [Wireless Clients](#)
- [Wireless LANs](#)
- [Radios](#)
- [Bluetooth](#) on page 967
- [Mesh](#)
- [Mesh Point](#)
- [SMART RF](#)
- [WIPS](#)
- [Captive Portal](#)
- [Application Visibility](#) on page 995
- [Coverage Hole Detection](#) on page 998

## Health

The **Health** screen displays general status information for a selected RF Domain, including data polled from all its members.

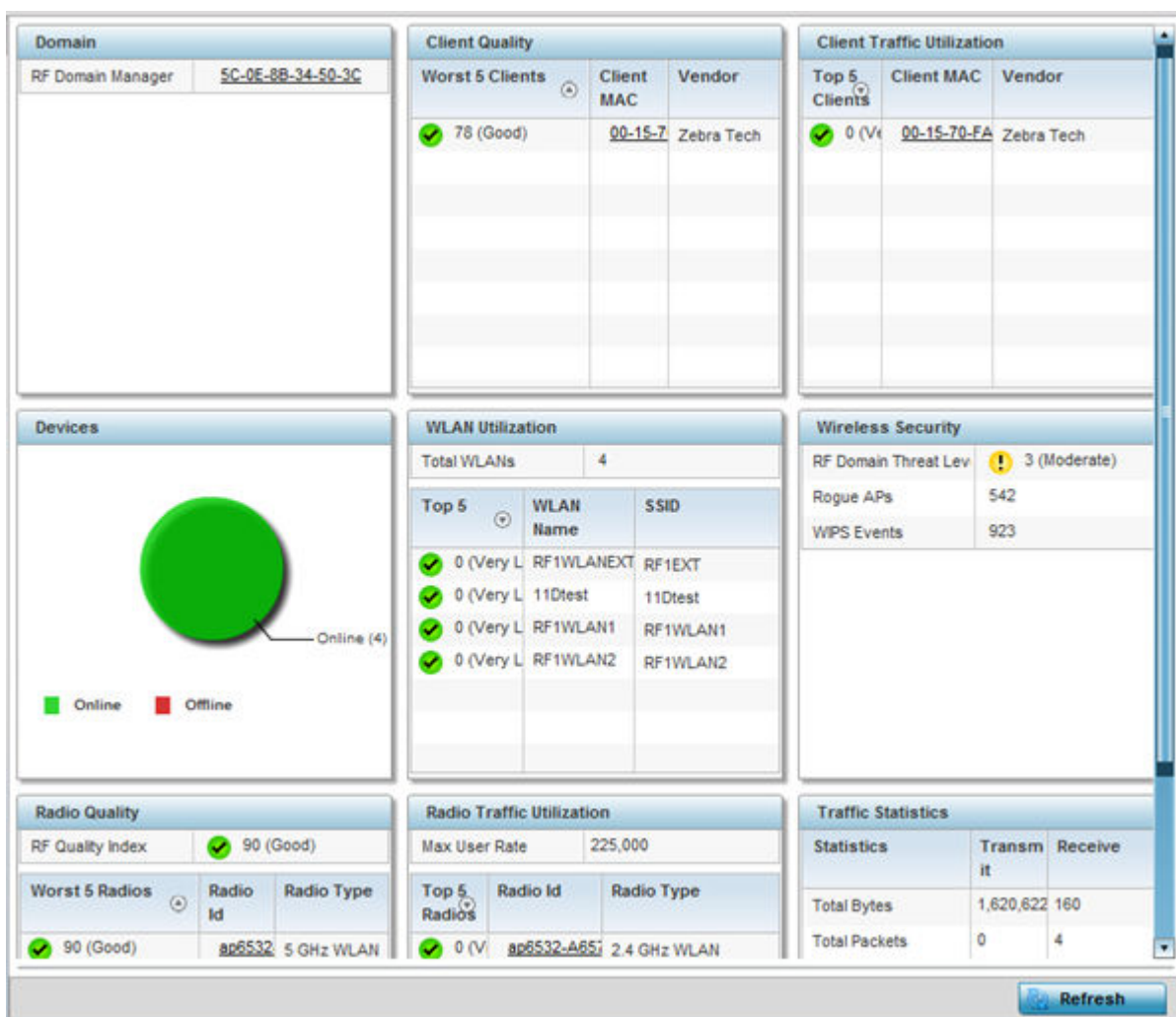
To display the collective device membership health of a controller, service platform or AP RF Domain:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.



- 4 Review the different fields displayed on the **RF Domain > Health** screen:

- **Domain** - 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.
- **Devices** - Displays the total number of online versus offline devices in the RF Domain, and an exploded pie chart depicts their status.
- **Radio Quality** - 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 amongst all the RF Domain device member radios.

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

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.

- **Client Quality** - Refer to the table below 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 hard coded radio MAC of the wireless client.
Vendor	Displays the vendor name of the wireless client.

- **WLAN Utilization** - Refer to the table below to assess WLAN related information:

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	Displays the SSID for the WLAN.

- **Radio Traffic Utilization** - Refer to the following table to identify radios requiring administration to improve performance:

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.





- **Client Traffic Utilization** - Refer to the following table for wireless client related information:

Top 5 Clients	Displays the five clients having the highest average quality indices.
Client MAC	Displays the client's hard coded MAC address used a hardware identifier.
Vendor	Lists each client's manufacturer.

- **Wireless Security** - 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 wireless clients trying to find network vulnerabilities within the RF Domain. The threat level is represented by an integer.
Rogue APs	Lists the number of unauthorized APs detected by RF Domain member devices.
WIPS Events	Lists the number of WIPS events generated by RF Domain member devices.

- **Traffic Statistics** - Displays the following information for transmitted and received packets:

Total Bytes	Displays the total bytes of data transmitted and received within the RF Domain.
Total Packets	Lists the total number of data packets transmitted and received within the RF Domain.
User Data Rate	Lists the average user data rate within the RF Domain.
Bcast/Mcast Packets	Displays the total number of broadcast/multicast packets transmitted and received within the RF Domain.
Management Packets	Displays the total number of management packets processed within the RF Domain.
Tx Dropped Packets	Displays the total number of dropped data packets within the RF Domain.
Rx Errors	Displays the number of errors encountered during data transmission within the RF Domain. The higher the error rate, the less reliable the connection or data transfer.

- **SMART RF Activity** - Refer to the table below for details:

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 RF Domain.
Channel Changes	Displays the total number of radio transmit channel changes that have been made using SMART RF within the RF Domain.
Coverage Changes	Displays the total number of radio coverage area changes that have been made using SMART RF within the RF Domain.

5 Periodically click **Refresh** to update the contents of the screen to their latest values.



## Inventory

The **Inventory** screen displays an inventory of RF Domain member APs, connected wireless clients, wireless LAN utilization and radio availability. Use this screen to evaluate if the inventory adequately supports client needs within the wireless network radio coverage area.

To display RF Domain inventory statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

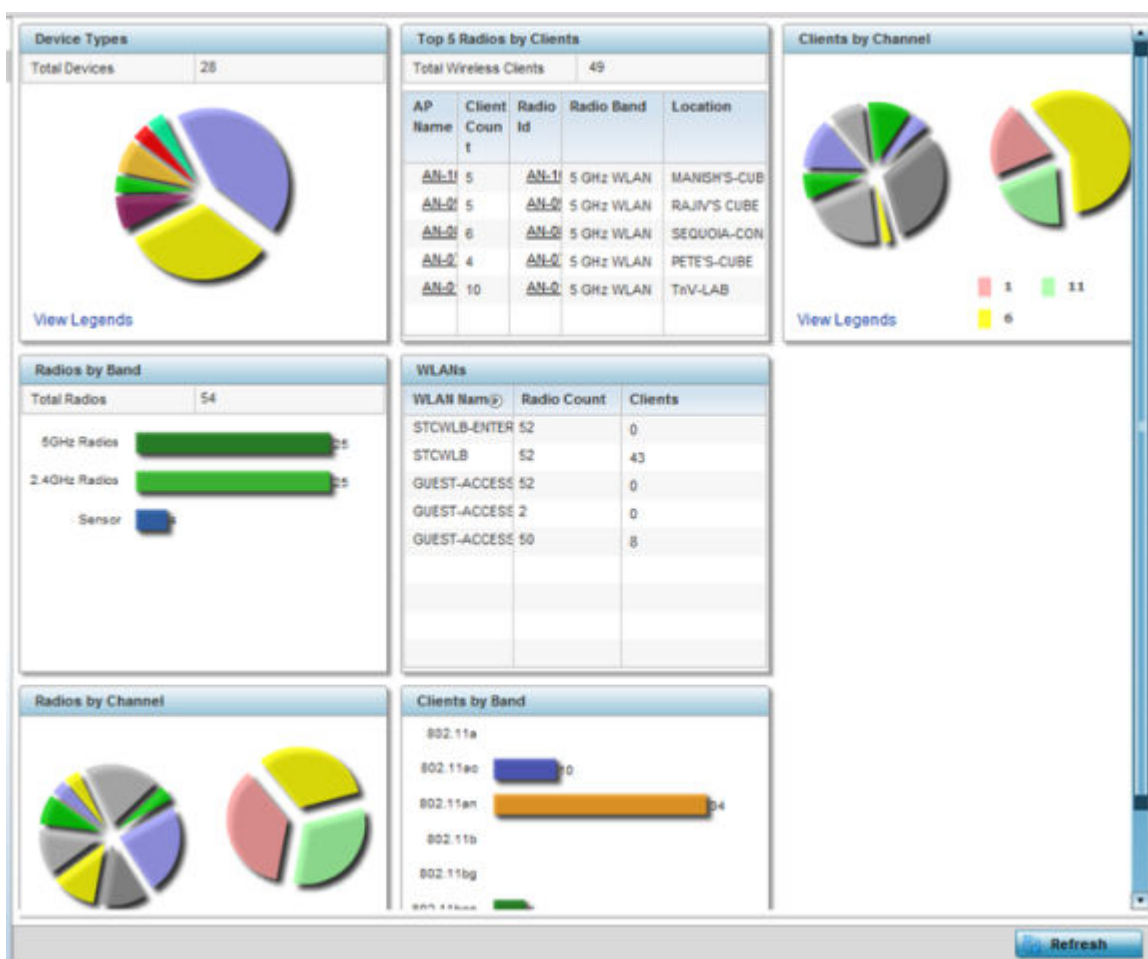
The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Select **Inventory** from the RF Domain menu.

The **Inventory** screen displays.



- 5 Review the different fields displayed on the **RF Domain > Inventory** screen:

- **Device Types** - Displays the total members in the RF Domain. The exploded pie chart depicts the distribution of RF Domain members by controller, service platform and AP model type.
- **Radios by Band** - 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, to reflect available sensor resources for intrusion detection.
- **Radios by Channel** - 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
- **Top 5 Radios by Clients** - Refer the following table, which displays the highest 5 performing wireless clients connected to RF Domain members:

<b>Total Wireless Clients</b>	Displays the total number of clients connected to RF Domain members.
AP Name	Displays the clients connected and reporting APs. The AP's name displays as a link that can be clicked to display AP data in greater detail.
Client Count	Displays the number of connected clients to each listed RF Domain member AP.
Radio	Displays each radio's administrator defined hostname and its radio designation (radio 1, radio 2 etc.).
Radio Band	Displays each client's operational radio band.
Location	Displays system assigned deployment location for the client.

- **WLANS** - Refer to this 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.
  - **Clients by Band** - This bar graph displays the total number of RF Domain member clients by their IEEE 802.11 radio type.
  - **Clients by Channel** - This pie charts displays the channels used by RF Domain member clients using 5GHz and 2.4GHz radios.
- 6 Periodically select **Refresh** to update the contents of the screen to their latest values.

## Devices

The **Devices** screen displays RF Domain member devices as links that can be selected to troubleshoot members in greater detail. Each device is listed with its factory encoded MAC address, connected client count, radio utilization and network IP address.

To display RF Domain device statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Select **Devices** from the RF Domain menu.

	Device	AP MAC Address	Type	Client Count	Radio Count	IP Address
	<a href="#">ap650-3129D8</a>	00-23-68-31-29-D8	AP650	0	1	172.168.6.25
	<a href="#">ap650-3129EC</a>	00-23-68-31-29-EC	AP650	0	1	172.168.6.26
	<a href="#">ap650-2433AC</a>	B4-C7-99-24-33-AC	AP650	0	2	172.168.6.110
	<a href="#">ap622-57F5F0</a>	B4-C7-99-57-F5-F0	AP622	0	2	172.168.6.140
Type to search in tables						
						Row Count: 4

5 Refer to the following table for information available on the **Devices** screen:

Access Point	Displays the system assigned name of each AP that is a member of the RF Domain. The name displays as a link that you can select to view configuration and network address information in greater detail.
AP MAC Address	Displays each AP's factory encoded MAC address as its hardware identifier.
Type	Displays each AP's model type.
Client Count	Displays the number of clients connected with each listed AP.
Radio Count	Displays the number of radios on each listed device. The number of radios per AP varies with the AP model type. For example, AP 6522, AP 6562, AP 7161, AP 7612 and AP 8163 models have two radios. Where as, AP 8432 and AP 8533 model have three radios.
IP Address	Displays the IP address each listed AP is using a network identifier.

6 Periodically click **Refresh** to update the contents of the screen to their latest values.

## AP Detection

The **AP Detection** screen displays information about detected APs that are not members of the selected RF Domain but have been detected within the network's device radio coverage area. They could be authorized devices or potential rogue devices requiring administration.

To view device information on detected access points:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Select **AP Detection** from the RF Domain menu.

The AP Detection screen displays.

MAC Address	Channel	SSID	First Seen	Top Reporter Hostname	Vendor	Vlan	RSSI	Is Interferer	Is Rogue	Termination Active
<a href="#">00-11-3F-DE-A</a>	11	checksum	25m 15s	ap6532-345i	Alcatel-Luce	NA	-64 dB	✓	✗	✗
<a href="#">00-11-3F-DE-A</a>	149	starttest1	25m 15s	ap6532-345i	Alcatel-Luce	NA	-59 dB	✓	✗	✗
<a href="#">00-11-3F-DE-B</a>	149	testwlanwimod	25m 15s	ap6532-345i	Alcatel-Luce	NA	-61 dB	✓	✗	✗
<a href="#">00-11-3F-DE-B</a>	149	test-rohini	25m 16s	ap6532-345i	Alcatel-Luce	NA	-73 dB	✓	✗	✗
<a href="#">00-11-3F-DE-B</a>	6	traffic_shaping	21m 56s	ap6532-345i	Alcatel-Luce	NA	-78 dB	✗	✗	✗
<a href="#">00-11-3F-DE-B</a>	149	ipsectest1	25m 15s	ap6532-345i	Alcatel-Luce	NA	-60 dB	✓	✗	✗
<a href="#">00-11-3F-E3-2i</a>	149	SR7750	25m 16s	ap6532-345i	Alcatel-Luce	NA	-70 dB	✓	✗	✗
<a href="#">00-11-3F-E3-4i</a>	100	traffic_shaping	25m 11s	ap6532-345i	Alcatel-Luce	NA	-60 dB	✓	✗	✗
<a href="#">00-14-C2-AB-f</a>	153	aaa	23m 37s	ap6532-345i	Hewlett Pacl	NA	-44 dB	✓	✗	✗
<a href="#">00-15-70-AE-3</a>	6	M-Wireless	23m 37s	ap6532-345i	Zebra Tech	NA	-61 dB	✓	✗	✗

Type to search in tables Row Count: 350

Terminate Clear All WIPS Report Refresh

5 Refer the following table for AP Detection related information:

Select AP Type	Displays detected AP information based on the option selected from the drop-down menu. The options are: <b>All</b> , <b>Rogue</b> , <b>Interferer</b> , and <b>Termination Active</b> .
MAC Address	Displays the hardware encoded MAC address of each listed AP 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 you can select to display RF Domain member device information in greater detail.
Channel	Displays the channel of operation used by the detected AP. The channel must be utilized by both the AP and its connected client and be approved for the target deployment country. This is necessary to designate the deployment as legal under FCC guidelines.
SSID	Displays the Service Set ID (SSID) of the network to which the detected AP belongs.
First Seen	Provides a timestamp when the detected AP was first seen by a RF Domain member device.
Top Reporter Hostname	Lists the administrator-assigned hostname of the top performing RF Domain member detecting the listed AP MAC address. Consider this top performer the best resource for information on the detected AP and its potential threat.
Vendor	Lists the manufacturer of the detected AP 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 AP was seen on by members of this RF Domain.
RSSI	Displays the Received Signal Strength Indicator (RSSI) of the detected AP. 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 AP is classified as an interferer.

Is Rogue	Displays whether the detected device has been classified as a rogue device whose detection threatens the interoperability of RF Domain member devices.
Termination Active	Lists whether Air Termination is active and applied to the detected AP. Air termination lets you terminate the connection between your WLAN and any AP or client associated with it. If the rogue device is an AP, all client association with the AP are removed. If the rogue device is a client, its connection with the AP is terminated. Note, Air Termination is disabled by default.

- 6 Click **Terminate** to remove the selected AP from RF Domain membership.
- 7 Click **Clear All** to reset the statistics counters to zero and begin a new data collection.
- 8 Click **WIPS Report** to launch a sub-screen to save a WIPS report (in PDF format) to a specified location.



#### Note

You are recommended to capture RF Domain member AP's client connection terminations in a format that can be archived externally.

- 9 Click **Refresh** to update the statistics counters to their latest values.

## Device Upgrade

The **Device Upgrade** screen displays information about devices, within the selected RF Domain, receiving updates and devices performing updates. 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 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Select **Device Upgrade** from the RF Domain menu.

The **Device Upgrade** screen displays.

Upgraded By	Type	Device Hostname	History Id	Last Update Status	Time Last Upgraded	Retries Count	State
ap6532-34503C	ap6532	ap6532-A6572C	5C-0E-8B-34-50-3	-	Fri Oct 4 2013 02:24:05 AM	0	done
ap6532-34503C	ap6532	ap6532-A6572C	5C-0E-8B-34-50-3	Reboot failed, re	Fri Nov 2 2012 05:39:37 AM	1	done
ap6532-34503C	ap6532	ap6532-3118E0	5C-0E-8B-34-50-3	-	Fri Nov 2 2012 05:29:31 AM	0	done
ap6532-34503C	ap6532	ap6532-A65738	5C-0E-8B-34-50-3	-	Tue Aug 28 2012 02:39:53 AM	0	done
ap6532-34503C	ap6532	ap6532-3118E0	5C-0E-8B-34-50-3	-	Tue Aug 28 2012 02:39:41 AM	0	done
ap6532-34503C	ap6532	ap6532-A65724	5C-0E-8B-34-50-3	-	Sun Aug 26 2012 04:51:35 AM	0	done
ap6532-34503C	ap6532	ap6532-3118E0	5C-0E-8B-34-50-3	-	Sun Aug 26 2012 04:50:26 AM	0	done
ap6532-34503C	ap6532	ap6532-A65724	5C-0E-8B-34-50-3	-	Fri Aug 24 2012 05:32:42 AM	0	done
ap6532-34503C	ap6532	ap6532-3118E0	5C-0E-8B-34-50-3	-	Fri Aug 24 2012 05:32:19 AM	0	done
ap6532-34503C	ap6532	ap6532-3118E0	5C-0E-8B-34-50-3	-	Fri Aug 24 2012 04:06:22 AM	0	done no-reboot
ap6532-34503C	ap6532	ap6532-A65724	5C-0E-8B-34-50-3	-	Fri Aug 24 2012 04:06:10 AM	0	done no-reboot
ap6532-34503C	ap6532	ap6532-A6572C	5C-0E-8B-34-50-3	-	Fri Aug 24 2012 03:37:29 AM	0	done

Type to search in tables Row Count: 58

5 Refer the following table for **Device Upgrade** related information:

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. With introduction of heterogeneous adoption, it is no longer necessary that the updating access point must be of the same model as the access point receiving the update. For more information on heterogeneous adoption, click <a href="#">here</a> .
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 Upgraded	Displays the date and time of the last firm ware image upgrade operation.
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.

6 Click **Clear History** to remove the upgrade records for RF Domain member devices.

7 Click **Refresh** to update the screen's statistics counters to their latest values.

## Wireless Clients

The **Wireless Clients** screen displays device information for wireless clients connected to RF Domain member APs. Review this content to determine whether a client should be removed from AP 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 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Select **Wireless Clients** from the RF Domain menu.

The **Wireless Clients** screen displays.

MAC Address	IP Address	IPv6 Address	Hostname	Role	Client Identity	Vendor	Band	AP Hostname	Radio MAC	WLAN	VLAN	Last Active	RF Domain Name
<a href="#">24-77-03-4E-AC-9C</a>	32.32.1.36	fe80::21b7::	Symbol-PC		Unknown	Intel Corp	11an	ap6532-A65	5C-0E-	11Dtest	32	Tue Mar	rf1
<a href="#">98-0C-82-46-67-E4</a>	33.33.0.14		android-adobe		Unknown	Samsung E	11bgn	ap6532-A65	5C-0E-	RF1VA	33	Tue Mar	rf1

Type to search in tables Row Count: 2

- 5 Refer the following table for **Wireless Clients** related information:

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 hostname address displays as a link that you can select to view client configuration 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 connection was defined.
Role	Lists the role assigned to each controller, service platform or AP managed client.
Client Identity	Lists the client's operating system identity (Android, Windows, etc.).
Vendor	Displays the manufacturer of each listed client as a means of assessing its support capabilities with the WiNG managed wireless infrastructure.
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 administrator-assigned hostname of the AP reporting client stats to RF Domain member devices.



Radio MAC	Displays the hardware-encoded MAC address of the AP 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 AP interoperation within the RF Domain.
VLAN	Displays the VLAN ID the client's connected AP has defined for use as a virtual interface.
Last Active	Displays the last detected transmit and receive activity for the listed client within the WiNG managed device radio coverage area.
RF Domain Name	Lists each client's RF Domain membership as defined by its connected access point and associated controller or service platform.

- 6 Click **Disconnect All Clients** to terminate each listed client's connection and RF Domain membership.
- 7 Select a specific client MAC address, and click the **Disconnect Client** to terminate this client's connection and RF Domain membership.
- 8 Periodically click **Refresh** button to update the statistics counters to their latest values.

## Wireless LANs

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 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Select **Wireless LANs** from the RF Domain menu.

The **Wireless LANs** screen displays.

	WLAN Name	SSID	Traffic Index	Radio Count	Tx Bytes	Tx User Data Rate	Rx Bytes	Rx User Data Rate
	11Dtest	11Dtest	0 (Very Low)	8	23,539,676	0 kbps	3,585,609	0 kbps
	RF1WLAN1	RF1WLAN1	0 (Very Low)	6	41,948	0 kbps	140,970	0 kbps
	RF1WLAN2	RF1WLAN2	0 (Very Low)	6	360	0 kbps	361	0 kbps
	RF1WLANEXT	RF1EXT	0 (Very Low)	6	0	0 kbps	0	0 kbps

Type to search in tables Row Count: 4

[Disconnect All Clients](#) [Refresh](#)

5 Refer the following table for **Wireless LANs** related information:

WLAN Name	Displays the name assigned to the WLAN upon its creation within the controller, service platform managed or AP network.
SSID	Displays the SSID assigned to the WLAN.
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: <ul style="list-style-type: none"> <li>• <b>0 – 20</b> - (very low utilization)</li> <li>• <b>20 – 40</b> - (low utilization)</li> <li>• <b>40 – 60</b> - (moderate utilization)</li> <li>• <b>60 and above</b> - (high utilization)</li> </ul>
Radio Count	Displays the number of radios deployed in each listed WLAN within this RF Domain. Use this information to assess each WLAN's client support capabilities in respect to the number of radio's available and their operational band.
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.

- 6 Click **Disconnect All Clients** to terminate all client's WLAN membership.
- 7 Click **Disconnect Client** to terminate a selected client's WLAN membership.
- 8 Periodically click **Refresh** to update the statistics counters to their latest values.

## Radios

The **Radio** screens displays information on RF Domain member access point radios. This information is reported as collective set of data from each radio deployed device supporting client traffic requirements within the RF Domain. Use these screens to troubleshoot radio issues negatively impacting RF Domain performance.

The **RF Domain > Radio** option has the following sub-menus:

- [Status](#)
- [RF Statistics](#)
- [Traffic Statistics](#)

### Radios Status

The **Status** screen displays network address, access point model, operational channel and client device status information for detected RF Domain member device radios serving and client support resources for the selected RF Domain.

To view the RF Domain radio statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Expand **Radios** from the RF Domain menu.

The **Radios > Status** screen displays by default.

Radio	Radio MAC	Radio Type	Access Point	AP Type	State	Channel Current(Co nfig)	Power Current(Co nfig)	Clients
<a href="#">ap6532-34503C-R1</a>	5C-0E-8B-21-	2.4 GHz WLA	<a href="#">ap6532-34503C-R1</a>	AP6532	On	6 (smt)	10 (smt)	0
<a href="#">ap6532-34503C-R2</a>	5C-0E-8B-21-	5 GHz WLAN	<a href="#">ap6532-34503C-R2</a>	AP6532	On	60w (smt)	17 (smt)	0
<a href="#">ap6532-A65724-R1</a>	5C-0E-8B-C3-	2.4 GHz WLA	<a href="#">ap6532-A65724-R1</a>	AP6532	On	1 (smt)	10 (smt)	0
<a href="#">ap6532-A65724-R2</a>	5C-0E-8B-C3-	5 GHz WLAN	<a href="#">ap6532-A65724-R2</a>	AP6532	On	44w (smt)	23 (smt)	1
<a href="#">ap6532-A65738-R1</a>	5C-0E-8B-C3-	2.4 GHz WLA	<a href="#">ap6532-A65738-R1</a>	AP6532	On	11 (smt)	10 (smt)	0
<a href="#">ap6532-A65738-R2</a>	5C-0E-8B-C3-	5 GHz WLAN	<a href="#">ap6532-A65738-R2</a>	AP6532	On	52w (smt)	17 (smt)	0

Type to search in tables Row Count: 6

[Refresh](#)

- 5 Refer the following table for **Radio Status** information:

Radio	Displays the name assigned to each listed RF Domain member access point radio. Each name displays as a link that you can be select to view radio information in greater detail.
Radio MAC	Displays the MAC address as a factory-set, numerical value hard coded for each listed RF Domain member AP 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 listed RF Domain member AP.
State	Displays the radio's current operational state.
Channel Current (Config)	Displays the current channel each listed RF Domain member AP radio is broadcasting on.
Power Current (Config)	Displays the current power level the radio is using for transmissions.
Clients	Displays the number of clients currently connected to each listed RF Domain member AP radio. Supported models can manage up to 256 clients per radio.

- Click **Refresh** to update the statistics counters to their latest values.

### *Radio RF Statistics*

The **RF Statistics** screen lists signal, noise ratio, transmit and receive, error and retry information for RF Domain member access point radios. Individual radios can be selected as needed to display (and troubleshoot) information specific to that RF Domain member radio resource.

To view the RF Domain radio statistics:

- Select the **Statistics** menu from the Web UI.
- Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- Expand **Radios** from the RF Domain menu.
- Click **RF Statistics**.

The **RF Statistics** screen displays.

Radio	Signal	Noise	SNR	Tx Physical Layer Rate	Rx Physical Layer Rate	Avg. Retry Number	Error Rate	RF Quality Index
<a href="#">ap8132-738E2C.R1</a>	N/A	-102 dbm	N/A	0 Mbps	0 Mbps	0	0 pps	(Off)
<a href="#">ap8132-738E2C.R2</a>	N/A	-98 dbm	N/A	0 Mbps	0 Mbps	0	1 pps	100 (Good)
<a href="#">ap81xx-711630.R1</a>	N/A	-94 dbm	N/A	0 Mbps	0 Mbps	0	16 pps	100 (Good)
<a href="#">ap81xx-711630.R2</a>	N/A	-96 dbm	N/A	0 Mbps	17 Mbps	0	2 pps	100 (Good)
<a href="#">ap8232-7F0DE4.R1</a>	N/A	-102 dbm	N/A	0 Mbps	0 Mbps	0	0 pps	(Off)
<a href="#">ap8232-7F0DE4.R2</a>	N/A	0 dbm	N/A	0 Mbps	0 Mbps	0	0 pps	(Off)

Type to search in tables Row Count: 6

[Refresh](#)

6 Refer the following table for the **Radio RF Statistics** information:

Radio	Displays the name assigned to each listed RF Domain member radio. Each name displays as a link that can be selected to display individual 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 AP.
SNR	Displays the <i>signal to noise ratio</i> (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: <ul style="list-style-type: none"> <li>• 0 – 50 - (Poor)</li> <li>• 50 – 75 - (Medium)</li> <li>• 75 – 100 - (Good)</li> </ul>

7 Periodically click **Refresh** to update the contents of the screen to their latest values

### Radio 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.

To view RF Domain member AP radio traffic statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Expand **Radios** from the RF Domain menu.
- 5 Click **Traffic Statistics**.

The **Radio Traffic Statistics** screen displays.

Radio	Tx Bytes	Rx Bytes	Tx Packets	Rx Packets	Tx User Data Rate	Rx User Data Rate	Tx Dropped	Traffic Index
<a href="#">ap6532-34776C.R2</a>	0	0	4,659	11,696,011	0 kbps	0 kbps	0	0 (Very Low)
<a href="#">ap6532-347800.R1</a>	0	0	14	29,780,817	0 kbps	0 kbps	0	0 (Very Low)
<a href="#">ap6532-347800.R2</a>	0	0	25,676	5,713,869	0 kbps	0 kbps	0	0 (Very Low)
<a href="#">ap6532-347830.R1</a>	0	0	0	20,684,459	0 kbps	0 kbps	0	0 (Very Low)
<a href="#">ap6532-347830.R2</a>	0	0	2,852	9,430,729	0 kbps	0 kbps	0	0 (Very Low)
<a href="#">ap6532-347854.R1</a>	0	0	0	26,455,429	0 kbps	0 kbps	0	0 (Very Low)
<a href="#">ap6532-347854.R2</a>	0	0	16,400	11,290,166	0 kbps	0 kbps	0	0 (Very Low)
<a href="#">ap6532-347B7C.R1</a>	0	0	0	28,106,250	0 kbps	0 kbps	0	0 (Very Low)
<a href="#">ap6532-347B7C.R2</a>	0	0	1,311	23,108,674	0 kbps	0 kbps	0	0 (Very Low)
<a href="#">ap7131-135BB4.R1</a>	0	0	0	0	0 kbps	0 kbps	0	(Off)
<a href="#">ap7131-135BB4.R2</a>	0	0	0	0	0 kbps	0 kbps	0	(Off)
<a href="#">ap7502-BC1340.R1</a>	0	0	15,214	12,337,344	0 kbps	0 kbps	0	0 (Very Low)
<a href="#">ap7502-BC1340.R2</a>	0	0	0	0	0 kbps	0 kbps	0	0 (Very Low)
<a href="#">ap7532-1601A8.R1</a>	0	0	15,959	22,728,619	0 kbps	0 kbps	14,917	0 (Very Low)

Type to search in tables Row Count: 36

[Refresh](#)

- 6 Refer the following table for **Radio Traffic Statistics** information:

Radio	Displays the name assigned to each listed RF Domain member access point radio. Each name displays as a link that you can select to view individual radio information in greater detail.
Tx Bytes	Displays the total number of bytes transmitted by each RF Domain member AP 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 AP 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 AP 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 AP 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 AP 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 AP radio. This rate only applies to user data and does not include any management overhead.

Tx Dropped	Displays the total number of packets dropped by each RF Domain member AP radio during transmission. This includes user data as well as management overhead packets.
Rx Errors	Displays the total number of packets containing errors, received by each RF Domain member AP radio.

- 7 Click **Refresh** to update the statistics counters to their latest values.

## Bluetooth

AP 8432 and AP 8533 model access points utilize a built-in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network. These platforms can use their Bluetooth-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 raises an alarm.

AP 8432 and AP 8533 model access points emit either iBeacon or Eddystone-URL beacons. The AP's Bluetooth radio periodically sends non-connectable, undirected LE (low-energy) advertisement packets. These advertisement packets are short, and sent on Bluetooth advertising channels that conform to established iBeacon and Eddystone-URL standards. However, portions of the advertising packet are still customizable.

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

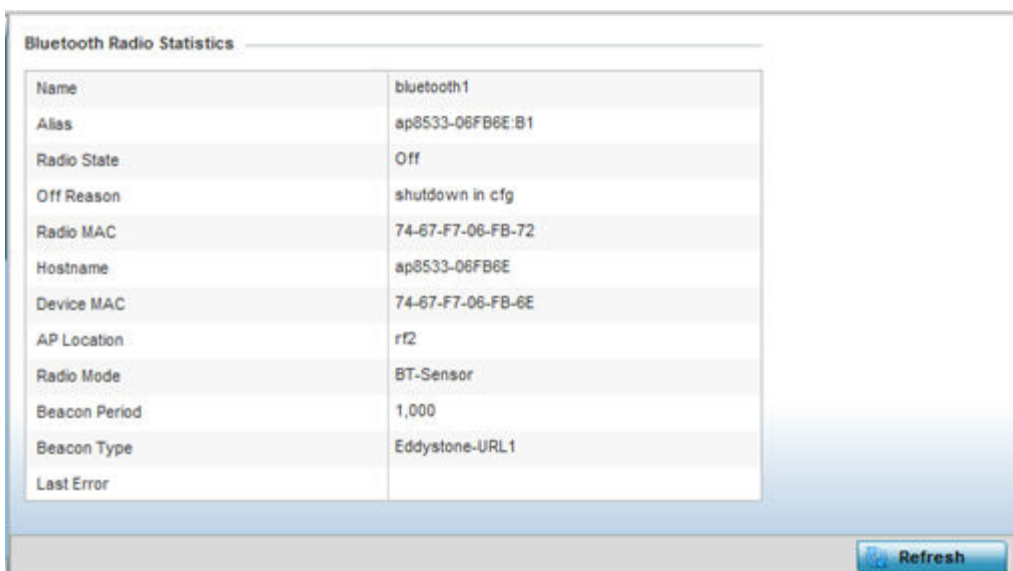
The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Click **Bluetooth**.

The **Statistics > RF Domain > Bluetooth** screen displays.



Refer the following table for **Bluetooth** related information:

Name	Lists the administrator assigned name of the access point's Bluetooth radio.
Alias	If an alias has been defined for the AP it is 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 AP, it is used in place of the AP'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 AP's hostname as its network identifier.
Device MAC	Lists the AP's factory-encoded MAC address serving as this device's hardware identifier on the network.
AP Location	Lists the AP's administrator-assigned deployment location.
Radio Mode	Lists an access point's Bluetooth radio functional mode as either <b>btsensor</b> or <b>le-beacon</b> .
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 is preventing the Bluetooth radio from operating.

- 5 Click **Refresh** to update the statistics counters to their latest values.

## Mesh

**Mesh** networking provides users wireless access to 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 mesh node connected clients:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Click **Mesh**.

The **Mesh** screen displays.



Client	Client Radio MAC	Portal	Portal Radio MAC	Connect Time

Type to search in tables Row Count: 0

**Refresh**

5 Refer the following table for Mesh statistics information:

Client	Displays the administrator-defined hostname for each mesh client connected to a RF Domain member AP radio.
Client Radio MAC	Displays the hardware-encoded MAC address for each mesh client connected to a RF Domain member AP radio.
Portal	Displays a numerical portal Index ID for the each mesh client connected to a RF Domain member AP radio.
Portal Radio MAC	Displays the hardware encoded MAC address for each radio in the RF Domain's mesh network.
Connect Time	Displays the total connection time for each listed client within the RF Domain's mesh network.

6 Click **Refresh** to update the statistics counters to their latest values.

### Mesh Point

Mesh networking provides users wireless access to 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.

*Mesh points* are APs dedicated to mesh network support. Mesh points capture and disseminate their own data and serve as a relay for other nodes.

The **RF Domain > Mesh Point** option has the following sub-menus:

- [MCX Geographical View](#) on page 970.
- [MCX Logical View](#) on page 971.
- [Device Type](#) on page 972.
- [Device Brief Info](#) on page 977.
- [Device Data Transmit](#) on page 983.



### MCX Geographical View

The **MCX Geographical View** displays a map where icons of each device in the RF Domain is overlaid. This provides a geographical overview of the location of each RF Domain member device.

To display the MCX Geographic View:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

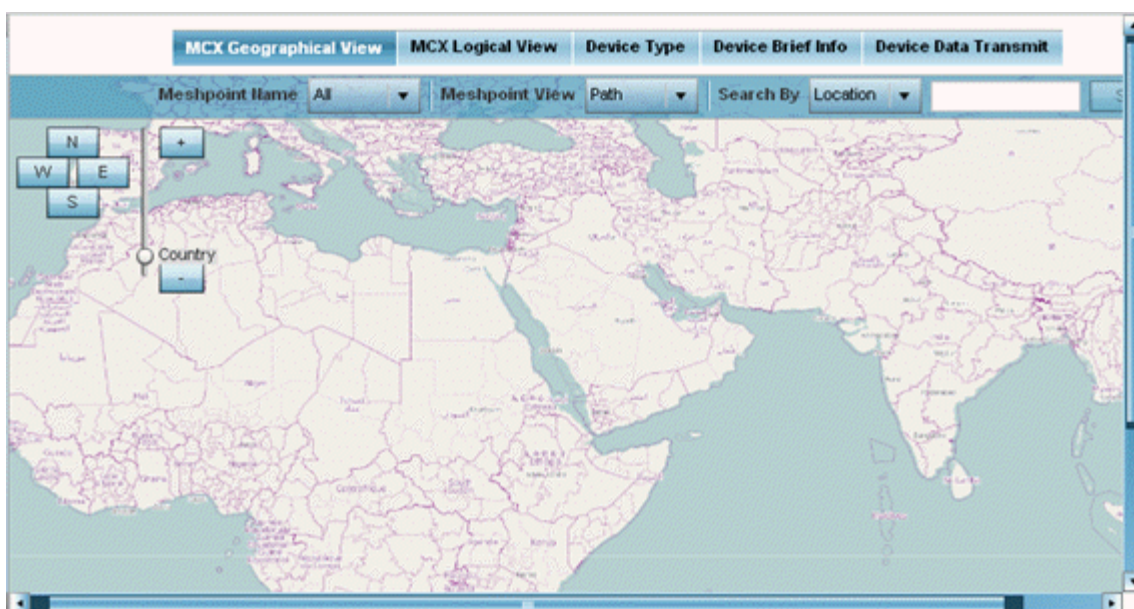
The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Select **Mesh Point** from the RF Domain menu.

The **MCX Geographical View** screen displays by default.



This screen displays a map overlaid with icons of each device deployed within the selected RF Domain. Use this screen for an overview of geographical location of RF Domain member mesh devices.

- 5 Use the **N**, **W**, **E** and **S** buttons to scroll the map up, down or side-ways in the North, East, West and South directions. Use the slider next to these buttons to zoom in and out. The available fixed zoom levels are **World**, **Country**, **State**, **Town**, **Street** and **House**.
- 6 Use the **Meshpoint Name** drop-down menu to select the mesh point name from the list displayed. Or, select **All** to view mesh statistics for all mesh points within the selected RF Domain.
- 7 Use the **Meshpoint View** drop-down menu to specify the view type as either **Path** or **Neighbor**.
- 8 Use the **Search By** drop-down menu to specify the search range as: **Location**, **Device MAC** or **Hostname**.
- 9 Based on the **Search by** option specified, enter the search criteria in the **Search** field, and click **Search**.

- 10 Click **Maximize** for full-screen view.
- 11 Periodically, click **Refresh** to update the status of the screen.

### MCX Logical View

The **MCX Logical View** screen provides a logical representation of mesh point statistics.

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an RF Domain from the list.

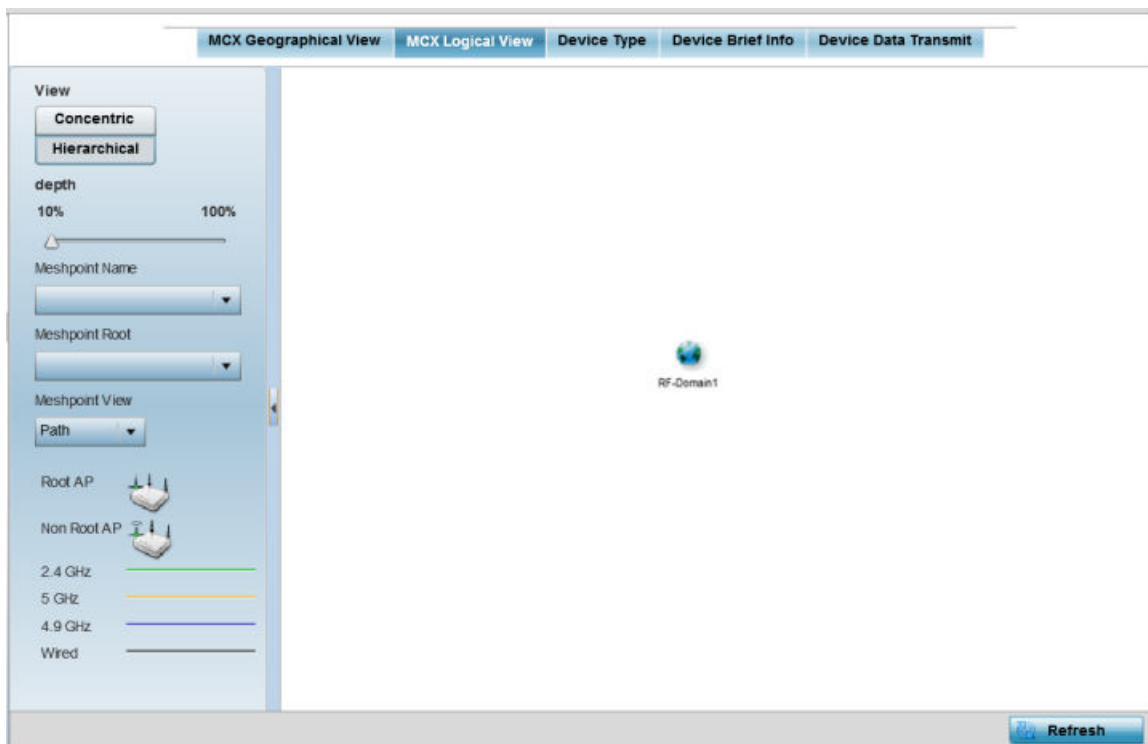
The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Select **Mesh Point** from the RF Domain menu.

The **MCX Geographical View** screen displays by default.

- 5 Click **MCX Logical View**.

The **MCX Logical View** screen displays.



This screen has two panes. The left-hand pane provides filter options to help you define the display format. The right-hand pane displays mesh statistics based on the filters specified by you in the left-hand pane.

In the left-hand pane:

- 6 Specify the **View** format as **Concentric** or **Hierarchical**.

The **Concentric** view displays the mesh as a concentric arrangement of devices, with the mesh's root node at the centre and the other mesh devices arranged in circles around it.

The **Hierarchical** view displays the mesh's root node at the top of the mesh tree, and the relationship of the mesh nodes are displayed as such.

- 7 Use the **Meshpoint Name** drop-down menu to select the mesh point. The graphical representation of the selected mesh point is displayed in the right-hand view area.
- 8 Use the **Meshpoint Root** drop-down to select the mesh root. Or, select **All Roots**.
- 9 To further refine the display, use the **Meshpoint View** drop-down menu to specify the view type as either **Path** or **Neighbor**.
- 10 Periodically click **Refresh** to update the status of the screen.

### *Device Type*

To view mesh point statistics for RF Domain member access points and their connected clients:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

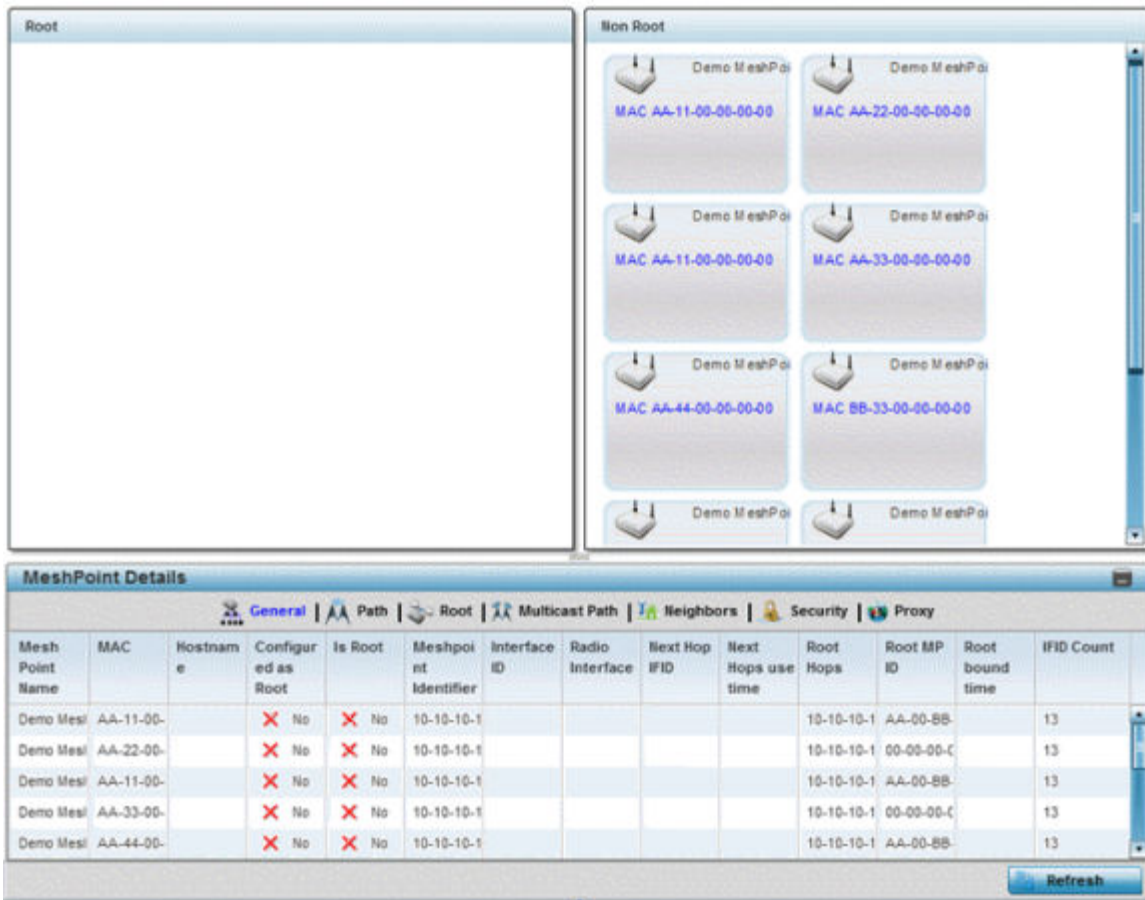
The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Select **Mesh Point** from the RF Domain menu.

The **MCX Geographical View** screen displays by default.

- 5 Click **Device Type**.

The **Device Type** screen displays by default.



This screen has the following elements:

- The **Root** field - the top, left-hand pane that displays the Mesh ID and MAC Address of the configured root mesh points in the RF Domain.
- The **Non Root** field - the top, right-hand pane that 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.
- The **MeshPoint Details** table- the bottom pane that displays the following tabs: **General, Path, Root, Multicast Path, Neighbors, Security** and **Proxy**. Refer to the following:

6 Click the **General** tab.

Refer the following table for the **General** tab information:

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. ( <b>Yes/No</b> ).
Is Root	A root mesh point is defined as a mesh point connected to the WAN and provides a wired backhaul to the network ( <b>Yes/No</b> ).

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.
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 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.

7 Click the **Path** tab.

Refer the following table for detailed information:

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.
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 ( <b>Yes/No</b> ).
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 <b>True</b> when the device is mobile and <b>False</b> 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 <b>Valid</b> of <b>Invalid</b> .
Binding	Indicates whether the path is bound or unbound.
Timeout	The timeout interval in milliseconds. 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 <i>RREQ</i> , <i>RREP</i> , or <i>RERR</i> messages that may be received related to that destination.

8 Click the **Root** tab.

Refer the following table for the **Root** tab information:

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 <b>2.4</b> and <b>5.8</b> , 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.

9 Click the **Multicast Path** tab.

Refer the following table for the **Multicast Path** tab information:

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 <b>Init</b> or <b>In Progress</b> , the timeout duration has no significance. If the state is <b>Enabled</b> , the timeout duration indicates the amount of time left before the security validity check is initiated. If the state is <b>Failed</b> , the timeout duration is the amount of time after which the system will retry.

10 Click the **Neighbors** tab.

Refer the following table for the **Neighbors** tab information:

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. <b>Yes</b> if the mesh point that is the neighbor is a root mesh point or <b>No</b> 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 <b>True</b> when the device is mobile and <b>False</b> 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 <b>2.4</b> and <b>5.8</b> , 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 <b>0</b> . If the neighbor is not a root mesh point but it has a neighbor that is a root mesh point, this value will be <b>1</b> . 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 <b>True</b> when the device is resourced and <b>False</b> 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	<p>The rank is the level of importance and is used for automatic resource management.</p> <ul style="list-style-type: none"> <li>• <b>8</b> – The current next hop to the recommended root.</li> <li>• <b>7</b> – Any secondary next hop to the recommended root to has a good potential route metric.</li> <li>• <b>6</b> – A next hop to an alternate root node.</li> <li>• <b>5</b> – A downstream node currently hopping through to get to the root.</li> <li>• <b>4</b> – 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).</li> <li>• <b>3</b> – 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.</li> <li>• <b>2</b> – Reserved for active peer to peer routes and is not currently used.</li> <li>• <b>1</b> - 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.</li> <li>• <b>0</b> – A neighbor bound to a different root node.</li> <li>• <b>-1</b> – Not a member of the mesh as it has a different mesh ID.</li> </ul> <p>All client devices hold a rank of 3 and can replace any mesh devices lower than that rank.</p>
Age	Displays the number of milliseconds since the mesh point last heard from this neighbor.

11 Click the **Security** tab.

Refer the following table for the **Security** tab information:

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.
Radio Interface	This indicates the interface that is used by the device to communicate with this neighbor. The values are <b>2.4</b> and <b>5.8</b> , 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: <ul style="list-style-type: none"> <li>• <b>Init</b> - indicates the link has not been established or has expired.</li> <li>• <b>Enabled</b> - indicates the link is available for communication.</li> <li>• <b>Failed</b> - indicates the attempt to establish the link failed and cannot be retried yet.</li> <li>• <b>In Progress</b> - indicates the link is being established but is not yet available.</li> </ul>
Timeout	Displays the maximum value in seconds that the link is allowed to stay in the <b>In Progress</b> state before timing out.
Keep Alive	<b>Yes</b> indicates that the local MP will act as a supplicant to authenticate the link and not let it expire (if possible). <b>No</b> indicates that the local MP does not need the link and will let it expire if not maintained by the remote MP.

- 12 Click the **Proxy** tab.

Refer the following table for the **Proxy** tab information:

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 (MPID) is used to distinguish the device that is the neighbor.
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 <b>4095</b> indicates that there is no VLAN ID.

- 13 Periodically click **Refresh** to update the status of the screen.

### Device Brief Info

To view mesh point statistics for RF Domain member APs and their connected clients:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Select **Mesh Point** from the RF Domain menu.

The **MCX Geographical View** screen displays by default.

- 5 Click **Device Brief Info** from the top of the screen.

The **Device Brief Info** screen displays.

All Roots and Mesh Points							
MAC	Mesh Point Name	Hostname	Configured as Root	Is Root	Meshpoint Identifier	Root Hops	IFID Count
AA-11-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
AA-22-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
AA-11-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
AA-33-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
AA-44-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
BB-33-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
AA-11-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
AA-33-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
AA-55-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13
BB-33-00-00-00-00	Demo MeshPoint		✗ No	✗ No	10-10-10-10-AA-	10-10-10-10-11-11	13

RowCount: 10

MeshPoint Details											
AA-11-00-00-00-00		Hostname									
<span>General</span>   <span>Path</span>   <span>Root</span>   <span>Multicast Path</span>   <span>Neighbors</span>   <span>Security</span>   <span>Proxy</span>											
Mesh Point Name	MAC	Hostname	Configured as Root	Is Root	Meshpoint Identifier	Next Hop IFID	Next Hops use time	Root Hops	Root MP ID	Root bound time	IFID Count
Demo MeshP	AA-11-00-00		✗ No	✗ No	10-10-10-10-			10-10-10-10-	AA-00-BB-1		13
Demo MeshP	AA-22-00-00		✗ No	✗ No	10-10-10-10-			10-10-10-10-	00-00-00-00		13
Demo MeshP	AA-11-00-00		✗ No	✗ No	10-10-10-10-			10-10-10-10-	AA-00-BB-1		13

Refresh

The **Device Brief Info** has the following sections:

- **All Roots and Mesh Points** - The top pane
- **MeshPoint Details** - The bottom pane

6 Refer the following table for the **All Roots and Mesh Points** table information:

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 that is connected to the WAN and provides a wired backhaul to the network ( <b>Yes/No</b> ).
Is Root	Indicates whether the current mesh point is a root mesh point ( <b>Yes/No</b> ).
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.

The **Mesh Point Details** field on the bottom portion of the screen displays the following tabs:

- **General**
- **Path**
- **Root**
- **Multicast Path**
- **Neighbors**
- **Security**
- **Proxy**

7 Refer the following table for the **General** tab table information:

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	A root mesh point is defined as a mesh point that is connected to the WAN and provides a wired backhaul to the network ( <b>Yes/No</b> ).
Is Root	Indicates whether the current mesh point is a root mesh point ( <b>Yes/No</b> ).
Destination Addr	The destination is the endpoint of mesh path. It may be a MAC address or a mesh point ID.
Interface ID	Uniquely identifies an interface associated with the ID. Each mesh point on a device can be associated with one or more interfaces.
Root Interface	Lists the radio interface on which the mesh point operates
Next Hop IFID	Identifies the ID of the interface on which the next hop for the mesh network can be found.
Next Hop 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 IFIDs associated with all the configured mesh points in the RF Domain.

8 Refer the following table for the **Path** tab table information:

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 ( <b>Yes/No</b> ).

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 <b>True</b> when the device is mobile and <b>False</b> 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 <b>Valid</b> of <b>Invalid</b> .
Binding	Indicates whether the path is <b>bound</b> or <b>unbound</b> .
Timeout	The timeout interval in seconds. The interpretation this value will vary depending on the value of the state. If the state is <b>Init</b> or <b>In Progress</b> , the timeout duration has no significance. If the state is <b>Enabled</b> , the timeout duration indicates the amount of time left before the security validity check is initiated. If the state is <b>Failed</b> , 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 <i>RREQ</i> , <i>RREP</i> , or <i>RERR</i> messages that may be received related to that destination.

9 Refer the following table for the **Root** tab table information:

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 <b>2.4</b> and <b>5.8</b> , 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.

10 Refer the following table for the **Multicast Path** tab table information:

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.
Timeout	The timeout interval in seconds. The interpretation this value will vary depending on the value of the state. If the state is <b>Init</b> or <b>In Progress</b> , the timeout duration has no significance. If the state is <b>Enabled</b> , the timeout duration indicates the amount of time left before the security validity check is initiated. If the state is <b>Failed</b> , the timeout duration is the amount of time after which the system will retry.

- 11 Refer the following table for the **Neighbors** tab table information:

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.
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. <b>Yes</b> if the mesh point that is the neighbor is a root mesh point or <b>No</b> if the Mesh Point that is the neighbor is not a root.
Mobility	Displays whether the mesh point is a mobile or static node. Displays <b>True</b> when the device is mobile and <b>False</b> 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 <b>2.4</b> and <b>5.8</b> , 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 <b>0</b> . If the neighbor is not a root mesh point but it has a neighbor that is a root mesh point, this value will be <b>1</b> . 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 <b>True</b> when the device is resourced and <b>False</b> 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	<p>The rank is the level of importance and is used for automatic resource management.</p> <ul style="list-style-type: none"> <li>• <b>8</b> - The current next hop to the recommended root.</li> <li>• <b>7</b> - Any secondary next hop to the recommended root to has a good potential route metric.</li> <li>• <b>6</b> - A next hop to an alternate root node.</li> <li>• <b>5</b> - A downstream node currently hopping through to get to the root.</li> <li>• <b>4</b> - 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).</li> <li>• <b>3</b> - 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.</li> <li>• <b>2</b> - Reserved for active peer to peer routes and is not currently used.</li> <li>• <b>1</b> - 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.</li> <li>• <b>0</b> - A neighbor bound to a different root node.</li> <li>• <b>-1</b> - Not a member of the mesh as it has a different mesh ID.</li> </ul> <p>All client devices hold a rank of 3 and can replace any mesh devices lower than that rank.</p>
Age	Displays the number of miliseconds since the mesh point last heard from this neighbor.

12 Refer the following table for the **Security** tab table information:

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.
Radio Interface	This indicates the interface that is used by the device to communicate with this neighbor. The values are <b>2.4</b> and <b>5.8</b> , 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	<p>Displays the Link State for each mesh point:</p> <ul style="list-style-type: none"> <li>• <b>Init</b> - indicates the link has not been established or has expired.</li> <li>• <b>Enabled</b> - indicates the link is available for communication.</li> <li>• <b>Failed</b> - indicates the attempt to establish the link failed and cannot be retried yet.</li> <li>• <b>In Progress</b> - indicates the link is being established but is not yet available.</li> </ul>
Timeout	Displays the maximum value in seconds that the link is allowed to stay in the In Progress state before timing out.
Keep Alive	<b>Yes</b> indicates that the local MP will act as a supplicant to authenticate the link and not let it expire (if possible). <b>No</b> indicates that the local MP does not need the link and will let it expire if not maintained by the remote MP.

13 Refer the following table for the **Proxy** tab table information:

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 (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.

14 Periodically click **Refresh** to update the status of the screen.

*Device Data Transmit*

To view mesh point statistics for RF Domain member APs and their connected clients:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Select **Mesh Point** from the RF Domain menu.

The **MCX Geographical View** screen displays by default.

- 5 Click **Device Data Transmit** from the top of the screen.

The **Device Data Transmit** screen displays.

The screenshot displays the 'Device Data Transmit' screen with the following sections:

- Data Bytes (Bytes)**:
 

Transmitted Bytes	
Received Bytes	
Total Bytes	
- Broadcast Packets**:
 

Tx Bcast/Mcast Pkts	
Rx Bcast/Mcast Pkts	
Total Bcast/Mcast Pkts	
- Data Packets Throughput (Kbps)**:
 

Transmitted Packets	
Received Packets	
Total Packets	
- Management Packets**:
 

Transmitted by the node	
Received by the node	
Total Through the domain	
- Data Rates (bps)**:
 

Transmit Data Rate	
Receive Data Rate	
Total Data Rate	
- Data Indicators**:
 

Traffic Index	✘ No
Max User Rate	
- Packets Rate (pps)**:
 

Transmitting packet rate	
Receiving packet rate	
Total packet rate	
- Data Distribution**:
 

Neighbor Count	
Radio Count	

A **Refresh** button is located at the bottom right of the screen.

6 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 that were transmitted through the Mesh Point node.
Management Packets: Received by the node	Displays the total number of management packets that were 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 <b>True</b> or <b>False</b> 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: Neighbor Count	Displays the total number of neighbor radios known to the Mesh Points in the RF Domain.

- 7 Select the **Refresh** button to update the screen's statistics counters to their latest values.

## SMART RF - Overview

When invoked by an administrator, Smart RF (Self-Monitoring At Run Time) 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, unmanaged 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.

The **RF Domain > SMART RF** option has the following sub-menus:

- [SMART RF - Summary](#) on page 985.
- [SMART RF - Details - Details](#) on page 988.
- [SMART RF - Details - Energy Graph](#) on page 989.
- [SMART RF - History](#) on page 990.

### *SMART RF - 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.

To view the Smart RF summary for RF Domain member access point radios:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

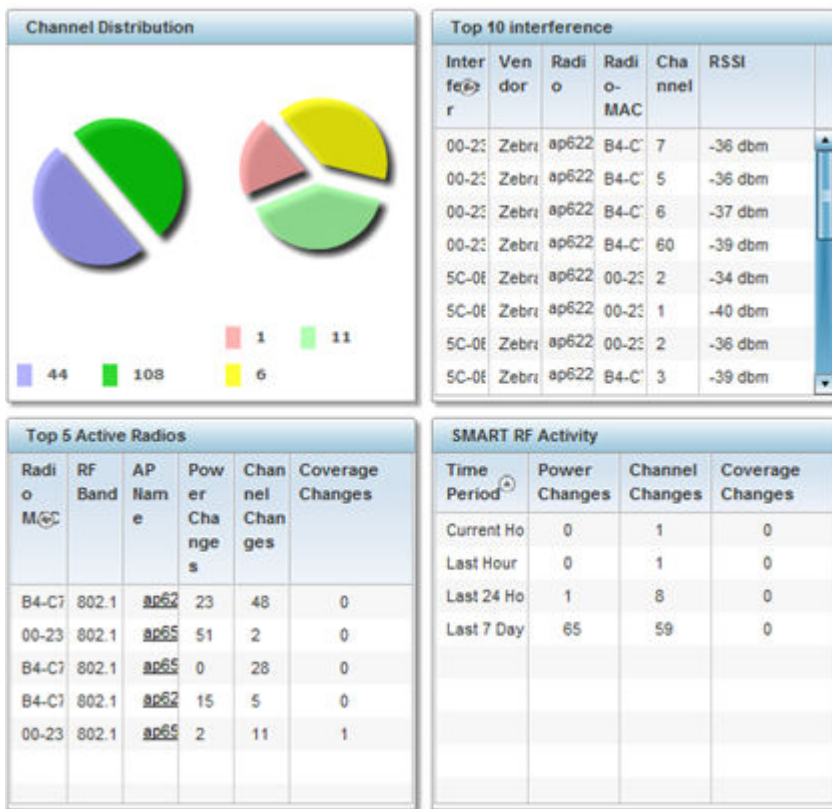
The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Select **SMART RF** from the RF Domain menu.

The **SMART RF Summary** screen displays by default.



The Summary screen displays the following SMART RF related statistics:

- 5 Use the **Channel Distribution** area to determine how RF Domain member devices are utilizing different channels to optimally support connect devices and avoid congestion and interference with neighboring devices. Use this data to 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 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 RSSI (received signal strength indication) 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 AP name used to differentiate from other RF Domain member AP radios. The name displays in the form of a link that you can select to vie 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 <b>Current Hour</b> , <b>Last 24 Hours</b> or the <b>Last Seven Days</b> . 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 Click **Refresh** to update the Summary to its latest RF Domain Smart RF information.

*SMART RF - Select Shutdown*

The **Select Shutdown** screen displays 2.4 GHz APs shutdown to maintain CCI (co-channel interference) levels within specified limits.



**Note**

This information is displayed only if select-shutdown is enabled in the smart-rf policy context. For more information, see select-shutdown.

- 1 Refer to the following table for the Smart RF Select Shutdown related statistical data:

AP Hostname	AP MAC	Radio	Radio MAC	Radio State

Type to search in tables Row Count: 0

Refresh Exit

**Figure 349: RF-Domain Smart RF Select Shutdown**

AP Hostname	Displays hostname of AP that was shutdown by Smart RF as part of the select shutdown feature. The Smart RF select-shutdown option, auto-shutdowns selected 2.4 GHz radios, in dual-band networks, to maintain CCI levels within specified limits. <b>Note:</b> For information on enabling select shutdown, see <a href="#">Configuring Smart RF Select Shutdown Settings</a> on page 408.
AP MAC	Displays the AP's MAC address
Radio	Displays the radio that was shutdown
Radio MAC	Displays the Radio's MAC address
Radio Status	Displays the Radio's current status

- 2 Click **Refresh** to update the Select Shutdown screen with the RF Domain Smart RF information.

*SMART RF - Details - Details*

To view Smart RF stats for RF Domain member AP radios:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an RF Domain from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Expand **SMART RF** from the RF Domain menu.
- 5 Click **Details**.

The **SMART RF Details** screen displays.

The screenshot shows a web interface for monitoring radio frequency (RF) statistics. On the left is a table listing various APs with columns for AP Hostname, Radio MAC Address, Radio Type, State, Channel, and Power. On the right, there are two tabs: 'Details' and 'Energy Graph'. The 'Details' tab is active, showing a 'General' section with fields for Radio MAC Address, Radio Index, Radio Type, State, AP Hostname, Channel, and Power. Below this is a 'Neighbors' table with columns for AP Hostname, Attenuation, Channel, Radio MAC Address, Power, and Radio id.

AP Hostname	Radio MAC Address	Radio Type	State	Channel	Power
ap6511-8A4	5C-0E-8B-8E-2F-E	11bgn	offline		0
ap621-E9F8	5C-0E-8B-F3-2B-7	11bgn	offline		0
ap6532-347	5C-0E-8B-22-DD-4	11an	norma	52w	4
ap81xx-711	B4-C7-99-78-61-E	11an	offline		0
ap6532-347	5C-0E-8B-21-77-7	11bgn	norma	1	10
ap6532-347	5C-0E-8B-22-DF-4	11bgn	norma	1	10
ap6532-347	5C-0E-8B-22-A2-	11bgn	norma	1	10
ap6532-347	5C-0E-8B-22-64-E	11bgn	norma	1	10
ap6532-347	5C-0E-8B-22-06-E	11an	norma	100w	17
ap650-2433	B4-C7-99-18-62-F	11an	offline		0
ap8232-7F8	FC-0A-81-8D-2E-1	11an	offline		0
ap650-2433	B4-C7-99-18-4A-1	11bgn	offline		0
ap7131-135	B4-C7-99-EC-96-C	11an	offline		0
ap7532-160	FC-0A-81-A3-10-	11an	norma	36	17
	5C-0F-8B-71-78-4	11an	norma	10Rw	4

Radio MAC Address	AP Hostname	Radio Index	Channel	Power
5C-0E-8B-21-56-00	ap6532-347854	0	1	10

AP Hostname	Attenuation	Channel	Radio MAC Address	Power	Radio id
ap7502-B	87	11	FC-0A-81-E	10	0

- 6 Refer to the **General** field to review and assess the radio's:
  - factory-encoded hardware MAC address.
  - administrator-assigned index.
  - 802.11 radio type.
  - current operational state.
  - AP's administrator-assigned hostname.
  - current operating channel and power.
- 7 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. Select individual AP hostnames to review RF Domain member radios in greater detail.

**Note**



*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.

- 8 Select **Refresh** to update the screen to its latest values.

*SMART RF - Details - Energy Graph*

The **SMART RF Energy Graph** screen displays the RF Domain member AP's radio's operating channel, noise level and neighbor count. Use this information to assess whether Smart RF neighbor recovery is needed in respect to poorly performing radios.

To access the SMART RF Energy Graph screen:

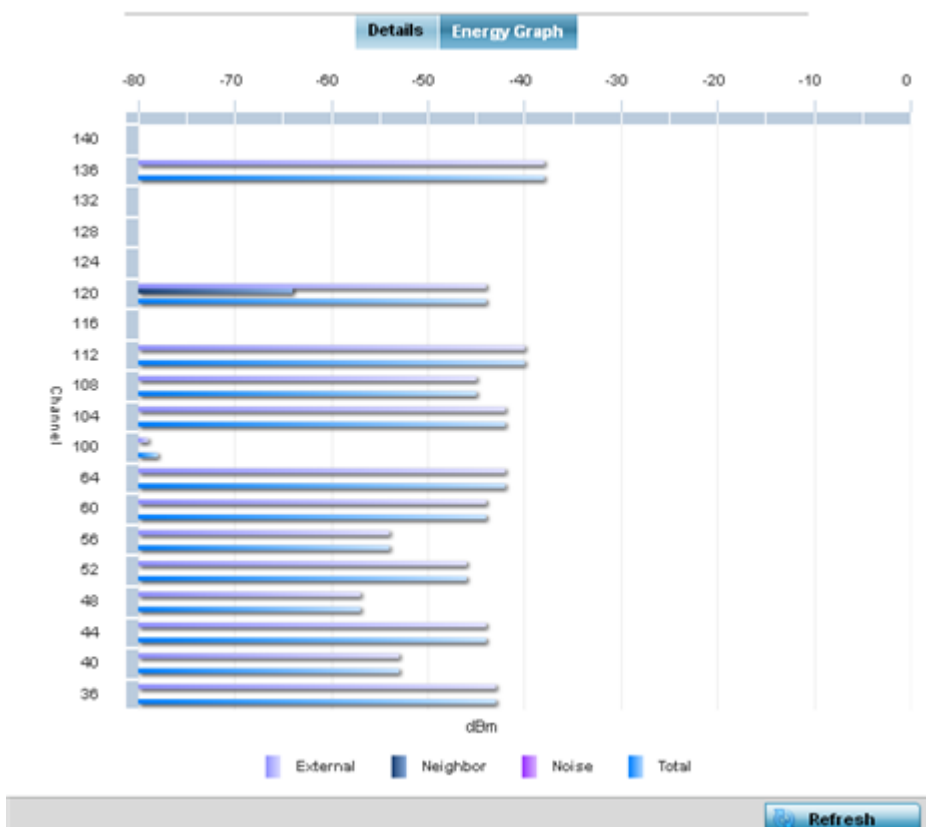
- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Expand **SMART RF** from the RF Domain menu.
- 5 Click **Details**.
- 6 Select the **Energy Graph** tab.



- 7 Select **Refresh** to update the screen to its latest values.

### SMART RF - History

Select **Smart RF History** to review Smart RF events impacting RF Domain member devices.

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- Expand **SMART RF** from the RF Domain menu.
- Click the **SMART RF History** tab.

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**

The **SMART RF History** screen displays the following RF Domain member historical data:

<b>Time</b>	Displays the time stamp when Smart RF status was updated on behalf of a Smart RF adjustment within the selected RF Domain.
<b>Type</b>	Lists a high-level description of the Smart RF activity initiated for a RF Domain member device.
<b>Description</b>	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.

- Select **Refresh** to update the screen to its latest values.

## WIPS

WIPS (Wireless Intrusion Protection System) provides continuous protection against wireless threats and acts as an additional layer of security complementing wireless VPNs and traditional encryption and authentication schemes. WIPS utilizes dedicated sensor devices designed to actively detect and locate unauthorized access points within a controller or service platform managed RF Domain.

Refer to the WIPS screens to review a client blacklist and rogue device detection events reported by RF Domain member APs.

For more information, see:

- [WIPS Client Blacklist](#)
- [WIPS Events](#)

### WIPS Client Blacklist

The **Client Blacklist** screen displays clients detected by WIPS and removed from RF Domain. Blacklisted clients are not allowed to associate to RF Domain member AP radios.

To view the WIPS client blacklist:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Expand **WIPS** from the RF Domain menu.

The **WIPS Client Blacklist** screen displays by default.

Event Name	Blacklisted Client	Time Blacklisted	Total Time	Time Left
dos-espwl-start-storm	44-55-44-55-44-55	Thu Jun 10 2012 12:26:26	2h 0m 0s	1h 0m 0s
null-probe-response	44-55-44-55-44-55	Thu Jun 10 2012 12:26:26	40m 0s	20m 0s

Row Count: 2

- 5 Review the **WIPS Client Blacklist** screen information:

Event Name	Displays the name of the blacklisting wireless intrusion event detected by a RF Domain member AP.
Blacklisted Client	Displays the MAC address (hardware identifier) 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 AP.
Total Time	Displays the duration the unauthorized (now blacklisted) device remained in the RF Domain. This is the duration for which the network was potentially vulnerable to the unauthorized device.
Time Left	Displays the time the blacklisted client remains on the list.

- 6 Select **Refresh** to update the screen to its latest values.



### WIPS Events

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 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Expand **WIPS** from the RF Domain menu.
- 5 Click **WIPS Event**.

The **WIPS Event** screen displays.

Event Name	Reporting AP	Originating Device	Detector Radio	Time Reported
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 27 2015 08:08:39 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 27 2015 10:16:36 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 6 2015 04:24:30 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 27 2015 03:14:12 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 08:03:12 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 08:01:12 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 10:47:57 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Wed May 6 2015 10:53:57 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Tue May 26 2015 03:07:07 AM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Mon May 25 2015 08:10:27 PM
ad-hoc-violation	ap7502-BC1340	00-10-18-A9-56-5D	1	Mon May 25 2015 10:59:44 AM
ad-hoc-violation	ap7502-BC1340	60-03-08-A7-93-E0	1	Fri May 15 2015 01:22:14 AM

- 6 Review the **WIPS Events** screen information:

Event Name	Displays the event name of the intrusion detected by a RF Domain member AP radio.
Reporting AP	Displays the MAC address (hardware identifier) of the RF Domain member AP reporting the event.
Originating Device	Displays the MAC address of the device generating the event.
Detector Radio	Displays the index number of the AP's radio detecting the event.
Time Reported	Displays a time stamp of when the event was reported by the RF Domain member AP radio.

- 7 Select **Clear All** to clear the statistics counters and begin a new data collection.
- 8 Select **Refresh** to update the screen to its latest values.

## Captive Portal

A captive portal is an access policy for providing 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 captive portal statistics for RF Domain member devices:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Select **Captive Portal** from the RF Domain menu.

The **Captive Portal** screen displays.

Client MAC	Hostname	Client IP	Client IPv6	Captive Portal	Port Name	Authentication	WLAN	VLAN	Remaining Time
04-E5-26-29-2B-F1		172.16.1.8		ALPHANET-C		Pending	GUEST-ACC	666	0s
24-A0-74-12-4B-2D	VNits-Phone	157.235.100	fe80::cce:a8c	ALPHANET-C		Pending	GUEST-ACC	666	0s
40-0F-95-0B-D9-49		172.16.1.9		ALPHANET-C		Pending	GUEST-ACC	666	0s
54-2E-96-54-A0-A5		172.16.1.163		ALPHANET-C		Pending	GUEST-ACC	666	0s
54-44-08-3E-00-98		172.16.1.38		ALPHANET-C		Pending	GUEST-ACC	666	0s
54-79-75-8B-A5-80	Windows-Ph	157.235.100		ALPHANET-C		Pending	GUEST-ACC	666	0s
79-3E-AC-44-D8-C6	Azil-Iphone6i	172.16.1.134	fe80::4d0:7cc	ALPHANET-C		Pending	GUEST-ACC	666	0s
90-3C-92-06-5C-F3		0.0.0.0		ALPHANET-C		Pending	GUEST-ACC	666	0s
9C-03-5B-97-03-87		172.16.1.77		ALPHANET-C		Pending	GUEST-ACC	666	0s
9C-F3-87-4C-F6-F6		0.0.0.0		ALPHANET-C		Pending	GUEST-ACC	666	0s
A4-D1-D2-55-2D-CA		172.16.1.161		ALPHANET-C		Pending	GUEST-ACC	666	0s
C0-33-5F-2B-36-B7	StephenSurti	172.16.1.139	fe80::4081:b1	ALPHANET-C		Success	GUEST-ACC	666	4h 15m 38s
C4-43-8F-F5-B2-F5		172.16.1.80		ALPHANET-C		Pending	GUEST-ACC	666	0s
D8-50-E6-7F-79-04		172.16.1.196		ALPHANET-C		Pending	GUEST-ACC	666	0s
E8-50-8B-80-CF-E0		172.16.1.111		ALPHANET-C		Pending	GUEST-ACC	666	0s

Type to search in tables Row Count: 16

[Refresh](#)

- 5 Refer the table below for **Captive Portal** related statistical data:

Client MAC	Displays the MAC address of each listed client requesting captive portal access to the controller, service platform or AP managed network. This address can be selected to display client information in greater detail.
Host Name	Displays the administrator-assigned hostname of the device requesting captive portal access to the network's RF Domain resources.
Client IP	Displays the IPv4 formatted address of each listed client using its connected RF Domain member AP for captive portal access.

Client IPv6	Displays any IPv6 formatted address of any listed client using its connected RF Domain member AP for captive portal access. IPv6 is the latest revision of the IP (Internet Protocol) 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 being 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, service platform or AP via the captive portal.
WLAN	Displays the name of the WLAN the requesting client would use for interoperation with the controller, service platform or AP.
VLAN	Displays the name of the VLAN the client would use as a virtual interface for captive portal operation with the controller, service platform or AP.
Remaining Time	Displays the time after which a connected client is disconnected from the captive portal.

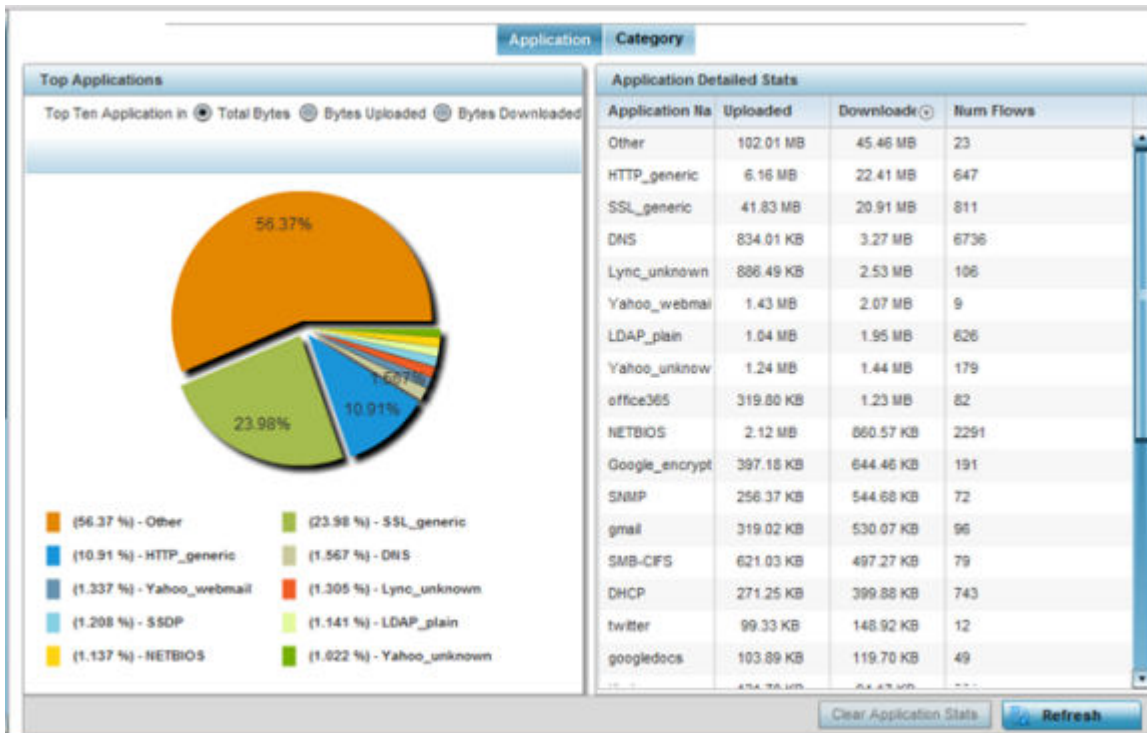
- 6 Select **Refresh** to update the screen to its latest values.

## Application Visibility

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](#) on page 495 and [Application Group](#) on page 497.

To view the application utilization statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.  
The **System** node expands to display the RF Domains created within the managed network.
- 3 Select an **RF Domain** from the list.  
The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **Application Visibility** from the RF Domain menu.  
The **Application Visibility > Application** screen displays.



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).

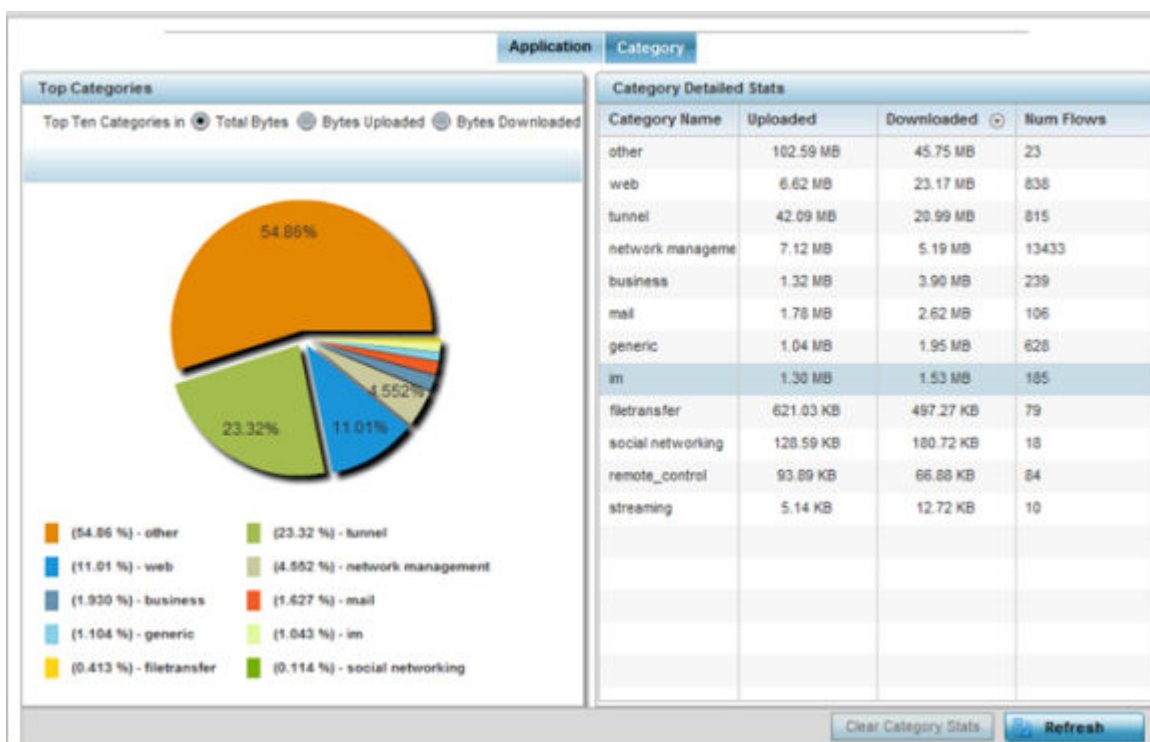
Refer to the **Application Detailed Stats** table to assess specific application data utilization:

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.

- 5 Click **Clear Application Stats** to clear the application assessment data counters and begin a new assessment.
- 6 Periodically, click **Refresh** to update the statistics counters to their latest values.
- 7 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](#) on page 495 and [Application Group](#) on page 497. The **Application Visibility > Category** screen displays.



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).
--	---

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.

- 8 Click **Clear Category Stats** to clear the application category assessment data counters and begin a new assessment.
- 9 Periodically, click **Refresh** to update the statistics counters to their latest values.

## Coverage Hole Detection

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 SNR (signal to noise 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.

### *Coverage Hole Summary*

To view a RF Domain's coverage hole summary:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.  
The **System** node expands to display the RF Domains created within the managed network.
- 3 Select an **RF Domain** from the list.  
The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.



- 3 Select an **RF Domain** from the list.

The RF Domain statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Expand **Coverage Hole Detection** from the RF Domain menu.
- 5 Select **Detail**.

The **Coverage Hole Detection > Detail** screen displays.

- 6 Use the **Filtered By** option to define whether the RF Domain’s coverage hole details are provided by a selected access point 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.
- 7 Based on the **Filtered By** option selected in the previous step, in the **Enter MAC Address** field, enter the access point’s MAC address or Hostname, or the client’s MAC address.  
This is the selected device reporting coverage hole details to the listed RF Domain member access point.
- 8 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.
MAC address	Lists the reporting access point’s MAC address.
Radio	Lists the access point radio receiving and reporting coverage hole RSSI data from the listed client MAC.



BSSID	Displays the BSSID (basic service set identifier) 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 is 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 RSSI (Received Signal Strength Indicator) 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.

- 9 Click **Clear AP Coverage Incidents** to clear the statistics counters and begin a new coverage hole summary for RF Domain member access point radios.
- 10 Click **Refresh** to update the statistics counters to their latest values.

## Controller Statistics

The **Wireless Controller** screen displays information about peer controllers (or service platforms) and their connected APs. 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 when needed.

This screen displays detailed statistics, which include network health, device inventory, connected wireless clients, adopted APs, rogue APs and WLANs. For more information, refer to the following:

- [Health](#)
- [Device](#)
- [Cluster Peers](#)
- [AP Upgrade](#)
- [Adoption](#)
- [AP Detection](#)
- [Wireless Clients](#)
- [Wireless LANs](#)
- [Policy Based Routing](#)
- [Radios](#)
- [Mesh](#)
- [Interfaces](#)
- [Power Status](#)
- [PPPoE](#)
- [OSPF](#)
- [L2TPv3](#)
- [VRRP](#)
- [Critical Resource](#)
- [Network](#)
- [DHCP Server](#)
- [Firewall](#)

- [VPN](#)
- [Viewing Certificate Statistics](#)
- [WIPS Statistics](#)
- [Advanced WIPS](#)
- [Sensor Server](#)
- [Captive Portal Statistics](#)
- [Network Time](#)

## Controller Health

The **Health** screen displays the hostname, device name, RF Domain name, radio RF quality and client RF quality of the selected RFS controller or NX series service platform.

To view health data:

- 1 Select the **Statistics** tab from the Web UI.
- 2 Select **System** from the navigation pane (on the left-hand side of the screen).
- 3 Expand the **RF Domain** node, and select one its connected **Wireless Controller/Service Platform**.
- 4 Select **Health** from the left-hand side of the UI.

The screenshot displays the 'Controller Health' page with the following sections:

- Device Details:** A table listing system information.
 

Hostname	rx9500-0C9848
Device MAC	B4-C7-99-0C-98-48
Primary IP	172.168.7.10
Type	NX9000
RF Domain Name	default
Model Number	NX-9500-100RO-WR
Version	5.5.0.0-051D
Uptime	2 days, 13 hours 44 minutes
CPU	Intel(R) Xeon(R) CPU E5645 @
RAM	16777820 kB
System Clock	2013-05-25 02:42:14 GMT
- Adopted Devices Health (w/ cluster members):** Shows 'Online' status with a green progress bar and a count of 24.
- Radio Utilization Index:** A table with columns: Utilization, Radio Id, Client Count.
 

Utilization	Radio Id	Client Count
- Radio RF Quality Index:** A table with columns: RF Quality Index, Radio Id, Radio Type.
 

RF Quality Index	Radio Id	Radio Type
- Client RF Quality Index:** A table with columns: Worst 5, Client MAC, Retry Rate.
 

Worst 5	Client MAC	Retry Rate
- Parameter Table:** A table with columns: Parameter, Transmit, Receive.
 

Parameter	Transmit	Receive
Total Bytes		
Total Packets		
Total Dropped		

A 'Refresh' button is located at the bottom right of the interface.

Review the different fields displayed on the **Controller > Health** screen.

The **Device Details** field displays the following:

Hostname	Displays the hostname of the controller or service platform.
Device MAC	Displays the MAC address of the controller or service platform.
Primary IP	Lists the network address used by this controller or service platform as a network identifier.
Type	Displays the controller type (for example, RFS 4000) or service platform type (for example, NX 9600).
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 model number of the selected controller or service platform.
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 currently utilized.
System Clock	Displays the system clock information.

The **Adopted Devices Health (w/ cluster members)** chart shows how many managed devices are online versus offline. These cluster members directly managed by the wireless controller or service platform. 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. This field displays the following:

RF Quality Index	Displays the five radios with the lowest average quality.
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** 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 five client radios with the lowest quality indices of all of those managed by the controller or service platform.
Client MAC	Displays the hardware encoded MAC address of the client.
Retry Rate	Displays the excessive retry rate of each listed controller or service platform client.

- 5 Select **Refresh** to update the statistics counters to their latest values.

## Controller Device

The **Device** screen provides detailed information about the selected device within the controller, service platform managed system.

To view system device statistics:

- 1 Select the **Statistics** tab from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen. The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, and select one its connected **Wireless Controller/Service Platform**.
- 4 Select **Device** from the left-hand side of the UI.

The screenshot displays the 'System' page for a device. It is organized into several sections:

- System:** A table with fields: Model Number (NX-9500-100R0-WR), Serial Number (B4C7990C9848), Version (5.8.0.0-029D), Boot Partition (primary), Fallback Enabled (Enabled), Fallback Image Triggered (No), and Next Boot (primary).
- System Resources:** A table with fields: Available Memory (KB) (33,157,964), Total Memory (KB) (36,960,484), Currently Free RAM (89.7%), Recommended Free RAM (10.0%), Current File Descriptors (2,544), Maximum File Descriptors (25,500), CPU Load 1 Minute (0.4%), CPU Load 5 Minutes (0.4%), and CPU Load 15 Minutes (0.4%).
- Upgrade Status:** A table with fields: Upgrade Status (Successful) and Upgrade Status Time (2015-05-04 12:53:22).
- Firmware Images:** A table with fields: Primary Build Date (04/25/2015 11:52:29), Primary Install Date (04/28/2015 17:15:54), Primary Version (5.8.0.0-029D), Secondary Build Date (05/01/2015 23:27:59), Secondary Install Date (05/04/2015 12:53:22), Secondary Version (5.8.0.0-030B), FPGA Version (Unknown), and PoE Firmware Version (Unknown).
- AP Licenses:** A table with fields: AP Licenses (48), AP Adoptions (0), and AP License (265324314234af473b77e72422e).
- AAP Licenses:** A table with fields: AAP Licenses (10,240), AAP Adoptions (27), and AAP License (265324314234af478ec59ae6d7f).
- Additional Licenses:** A table with fields: ADSEC (265324314234af47ecb4b42fb30), WPS (-), and Hotspot Analytics (265324314234af471cac33cccd3).

A **Refresh** button is located at the bottom right of the page.

The **System** field displays the following:

<b>Model Number</b>	Displays the model number for the selected controller or service platform.
<b>Serial Number</b>	Displays the serial number factory encoded on the controller or service platform at the factory.
<b>Version</b>	Displays the unique alphanumeric firmware version name for the controller or service platform firmware.
<b>Boot Partition</b>	Displays the boot partitioning type (primary or secondary).
<b>Fallback Enabled</b>	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.
<b>Fallback Image Triggered</b>	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.
<b>Next Boot</b>	Designates this version as the version used the next time the controller or service platform is booted.

The **System Resources** table displays the following:

<b>Available Memory (MB)</b>	Displays the available memory (in MB) available on the selected device (controller or service platform).
<b>Total Memory (MB)</b>	Displays the total memory resources available to the selected device.
<b>Currently Free RAM</b>	Displays the free RAM space available to the selected device. If its very low, free up some space by closing some processes.
<b>Recommended RAM</b>	Displays the recommended RAM required for routine operation.
<b>Current File Description</b>	Displays the current file description.
<b>Maximum File Description</b>	Displays the maximum file description.
<b>CPU Load 1 Minute</b>	Lists the typical device processor load over 1 minute.
<b>CPU Load 5 Minutes</b>	Lists the typical device processor load over 5 minutes.
<b>CPU Load 15 Minutes</b>	Lists the typical device processor load over 15 minutes.

The **Upgrade Status** field displays firmware upgrade statistics. The table provides the following:

<b>Upgrade Status</b>	Displays whether the image upgrade was successful.
<b>Upgrade Status Time</b>	Displays the time of the upgrade.

The **IP Domain** field displays the following:

<b>IP Domain Name</b>	Displays the name of the IP Domain service used with the selected device (controller or service platform).
<b>IP Domain Lookup state</b>	Lists the current state of the lookup operation.

The **Fan Speed** field displays the following:

<b>Number</b>	Displays the number of fans supported on the this controller or service platform.
<b>Speed (Hz)</b>	Displays the fan speed in Hz.

The **Temperature** field displays the following:

<b>Number</b>	Displays the number of temperature elements (gauges) utilized by the selected device (controller or service platform).
<b>Temperature</b>	Displays the current temperature (in Celsius) to assess a potential overheat condition.

The **Kernal Buffers** field displays the following:

<b>Buffer Size</b>	Lists the sequential buffer size.
<b>Current Buffers</b>	Displays the current buffers available to the selected device (controller or service platform).
<b>Maximum Buffers</b>	Lists the maximum buffers available to the selected device.

The **Firmware Images** field displays the following:

<b>Primary Build Rate</b>	Displays the build date when this version was created.
<b>Primary Install Date</b>	Displays the date this firmware version was installed on the controller or service platform.
<b>Primary Version</b>	Displays the primary version string.
<b>Secondary Build Date</b>	Displays the build date when this secondary version was created.
<b>Secondary Install Date</b>	Displays the date this secondary version was installed on the controller or service platform.
<b>Secondary Version</b>	Displays the secondary version string.
<b>FGPA Version</b>	Displays the FGPA version string.
<b>PoE Firmware Version</b>	Displays the version of the PoE (Power Over Ethernet) firmware if the PoE feature is available.

The **AP Licenses** field displays the following license information for access points:

<b>AP Licenses</b>	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.
<b>AP Adoptions</b>	Displays the number of APs adopted by this controller or service platform.
<b>AP License</b>	Displays the license string of the AP.

The **AAP Licenses** field displays the following license information for adaptive access points:

<b>AAP Licenses</b>	Displays the number of AAP (adaptive access point) licenses currently available. This value represents the maximum number of licenses the controller or service platform can adopt.
<b>AAP Adoptions</b>	Displays the number of AAPs adopted by this controller or service platform.
<b>AAP License</b>	Displays the license string of the AAP.

The **Additional Licenses** area displays the following information:

<b>ADSEC</b>	Displays the number of 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.
<b>WIPS</b>	Displays the number of WIPS licenses utilized by the controller or service platform.
<b>Hotspot Analytics</b>	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:

<b>Name Server</b>	Displays any custom Name Server mappings on the controller or service platform.
<b>Type</b>	Displays the type of DNS mapping, if any, on the controller or service platform.

The **IPv6 Name Servers** table displays the following:

<b>Name Server</b>	Displays any custom IPv6 formatted IP address Name Server mappings on the controller or service platform.
<b>Type</b>	Displays the type of DNS mapping, if any, on the controller or service platform.

The **IPv6 Hop Limit** table displays the following:

<b>Hop Limit</b>	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** field displays the following:

<b>IPv6 Delegated Prefix</b>	If IPv6, prefix delegation is used to assign a network address prefix, configuring the controller or service platform with the prefix.
<b>Prefix Name</b>	Lists the 32 character maximum name for the IPv6 delegated prefix used as an easy to remember alias for an entire IPv6 address.
<b>DHVPv6 Client State</b>	Displays the current DHCPv6 client state as impacted by the IPv6 delegated prefix.
<b>Interface Name</b>	Lists the interface over which IPv6 prefix delegation occurs.
<b>T1 timer (seconds)</b>	Lists the amount of time in seconds before the DHCP T1 (delay before renew) timer expires.
<b>T2 timer (seconds)</b>	Lists the amount of time in seconds before the DHCP T2 (delay before rebind) timer expires.
<b>Last Refreshed</b>	Lists the time, in seconds, since IPv6 prefix delegation has been updated.
<b>Preferred Lifetime (seconds)</b>	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.
<b>Valid Lifetime (seconds)</b>	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.

## Cluster Peers

Refer to the **Cluster Peers** screen to review device address and version information for peer devices within a cluster.

To view cluster peer statistics:

- 1 Select the **Statistics** tab from the Web UI.
- 2 Expand the **RD Domain** node.
- 3 Select the **Wireless Controller** node from the left navigation pane.
- 4 Select **Cluster Peers** from the left-hand side of the UI.

Wireless Controller	MAC Address	Type	RF Domain Name	Online	Version
<a href="#">nx8500-DFCSDC</a>	B4-C7-99-0F-C9-DC	NX9000	<a href="#">default</a>		5.5.0.0-051D

Type to search in tables Row Count: 1

[Refresh](#)

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.
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 cluster member is currently online. If online, a green check mark displays, if it is offline a red X displays.
Version	Displays the numeric firmware version currently running 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 to update the screen's statistics counters to their latest values.

## Controller Web Filtering

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

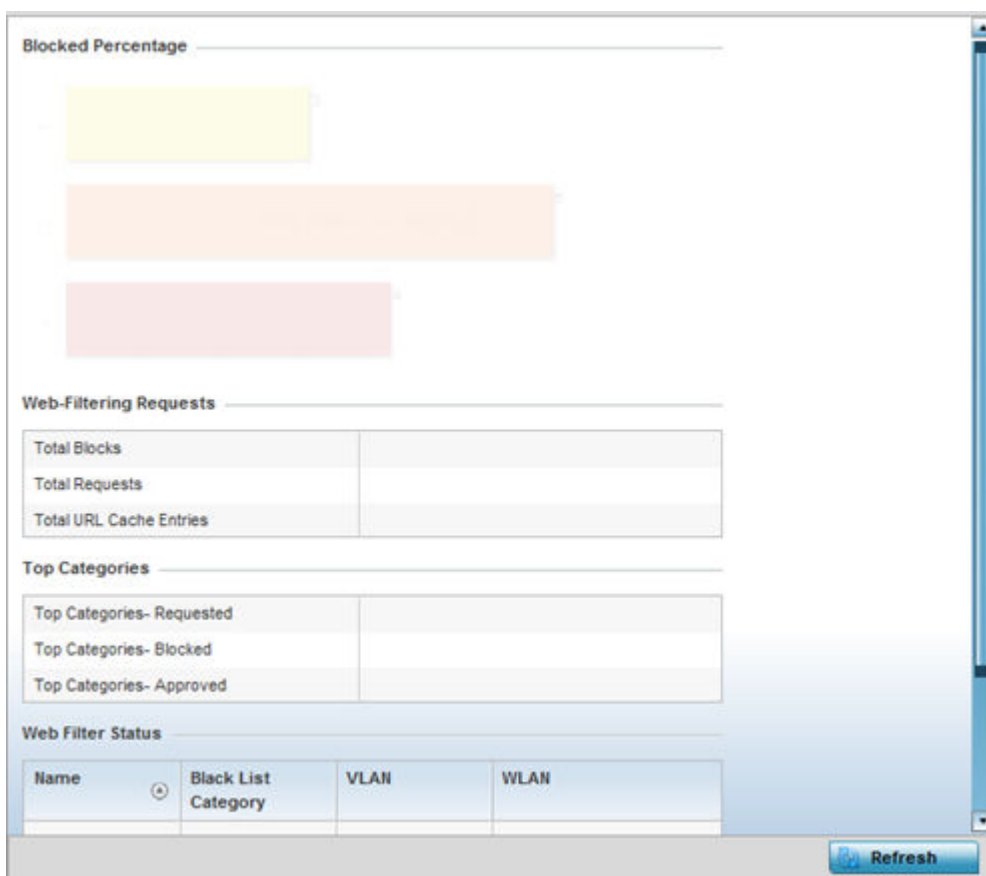


platform. A URL filter is comprised of several filter rules. A whitelist bans all sites except the categories and URL lists defined in the whitelist. The blacklist allows all sites except the categories and URL lists defined in the blacklist.

To view Web filter statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**.  
The selected device's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **Web-Filtering**.

The **Statistics > Controller/AP > Web-Filtering** screen is displayed.



- 5 Review the following Web-Filtering statistics:  
The **Web-Filtering Requests** field displays the following:

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 cached 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 adheres 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.

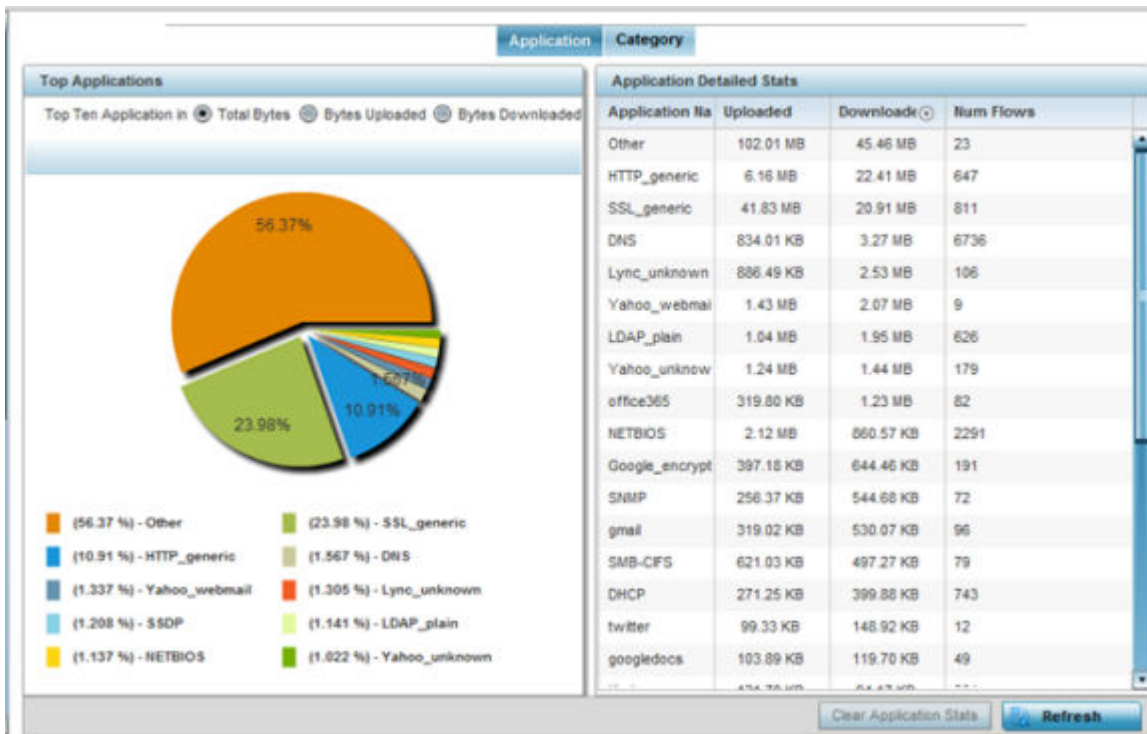
- Periodically select **Refresh** to update this screen to its latest values.

## Controller Application Visibility (AVC)

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](#) on page 495 and [Application Group](#) on page 497.



- 1 Select the **Statistics** tab from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**.  
The Controller's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **Application Visibility (AVC)** from the menu.  
The **Statistics > Controller/AP > Application Visibility (AVC) > Application** screen displays.



Refer to the **Top Applications** graph to assess the most prolific, and allowed, application data passing through the controller/access point managed network.

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).

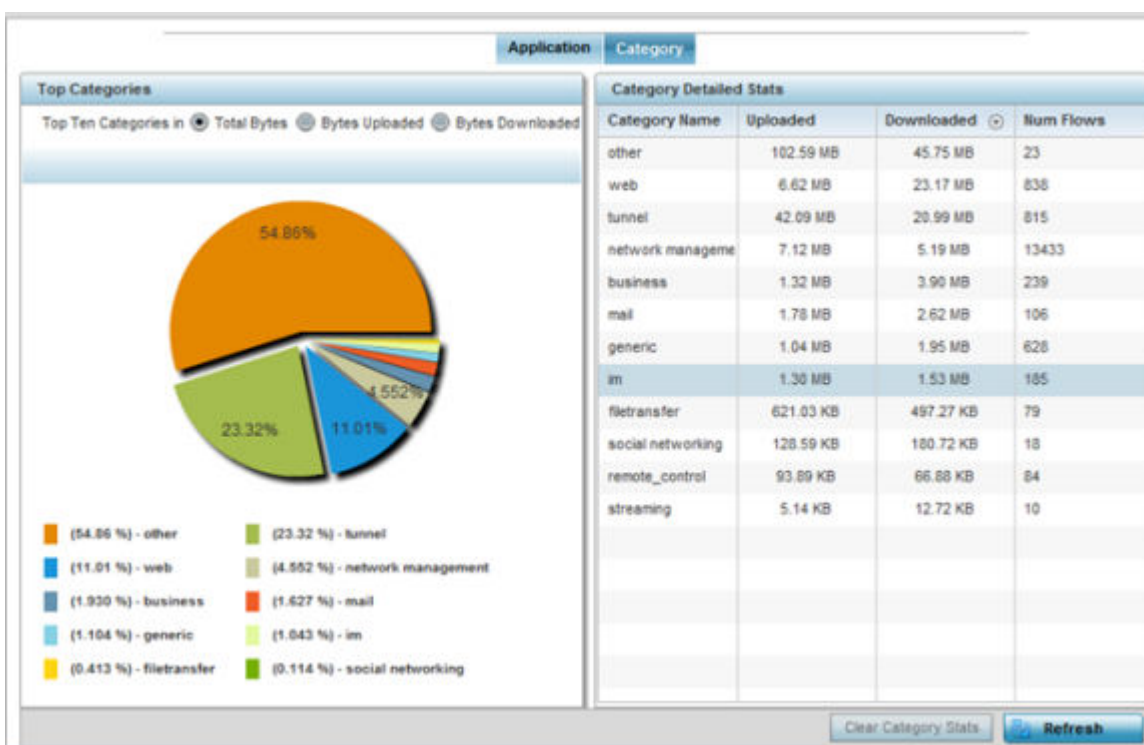
Refer to the **Application Detailed Stats** table to assess specific application data utilization:

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.

- 5 Click **Clear Application Stats** to clear the application assessment data counters and begin a new assessment. Selecting this option will not clear category stats, just application stats.
- 6 Click 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](#) on page 495 and [Application Group](#) on page 497.

The **Statistics > Controller > Application Visibility > Category** screen displays.



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).

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 managed 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.

- 7 Click **Clear Category Stats** to clear the application category assessment data counters and begin a new assessment. Selecting this option will not clear application stats, just category stats.
- 8 Click **Refresh** to update the statistics counters to their latest values.

## Controller 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 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



## Device Upgrade

The **Device Upgrade** screen displays information about 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 APs can be RF domain managers capable of receiving device firmware files from the NOC (NX 7510, NX 95XX or NX 96XX series service platforms) then provisioning other devices within their same RF domain. Controllers, service platforms and APs 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 device upgrade statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select the **Wireless Controller** node from the left navigation pane.
- 4 Select **Device Upgrade**.

Device Hostname	Type	State	Time Last Upgraded	Retries Count	Upgraded By	Last Update Status
ap621-E9F8t	ap621	done	Wed May 6 2015 01:00:04 AM	0	NX95-Pri	-
ap621-E9F8t	ap621	done	Tue May 5 2015 06:06:43 AM	0	NX95-Pri	-
ap621-E9F8t	ap621	failed	Mon May 4 2015 02:06:07 AM	3	NX95-Pri	Start Upgrade failed
ap621-E9F8t	ap621	done	Mon May 4 2015 02:06:03 AM	1	NX95-Pri	Update error: Unable to get up
ap621-E9F8t	ap621	done	Tue Apr 28 2015 06:19:36 AM	0	NX95-Pri	-
ap621-E9F8t	ap621	done	Tue Apr 21 2015 04:59:46 AM	0	NX95-Pri	-
ap621-E9F8t	ap621	done	Tue Apr 14 2015 02:18:34 AM	1	NX95-Pri	Update error: Unable to get up
ap621-E9F8t	ap621	failed	Mon Apr 13 2015 01:16:39 AM	3	NX95-Pri	download timed out
ap621-E9F8t	ap621	done	Mon Apr 13 2015 02:05:03 AM	0	NX95-Pri	-
ap621-E9F8t	ap621	done	Tue May 5 2015 02:02:28 AM	0	NX95-Pri	-
ap621-E9F8t	ap621	failed	Wed May 6 2015 01:02:09 AM	3	NX95-Pri	Start Upgrade failed
ap622-57F5f	ap622	failed	Tue May 5 2015 06:08:34 AM	3	NX95-Pri	Start Upgrade failed
ap622-57F5f	ap622	done	Tue Apr 28 2015 06:19:34 AM	0	NX95-Pri	-

Type to search in tables Row Count: 2047

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 upgrade process ( <b>done</b> , <b>failed</b> , etc.).
Time Last Upgraded	Displays the date and time of the last 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.

History ID	Displays a unique timestamp for the upgrade event.
Last Update Status	Displays the status of the last upgrade operation ( <b>Start Upgrade, Update error</b> , etc.).

- 5 Click **Clear History** to clear the screen of its current status and begin a new data collection.
- 6 Click **Refresh** to update the screen's statistics counters to their latest values.

## Adoption

The **Adoption** screens lists devices 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:

- [Adopted Devices](#)
- [AP Adoption History](#)
- [Pending Adoption](#)

### Adopted Devices

To view adopted devices statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select the **Wireless Controller** node from the left navigation pane.
- 4 Expand the **Adoption** node in the left-hand side of the UI.
- 5 Select **Adopted Devices**.

Device	Type	RF Domain Name	Model Number	Status	Errors	Adopter Hostname	Adoption Time	Startup Time
<a href="#">ap622-57F5F0</a>	AP62	simba	AP-0622-t	configured		nx9500-0C9848	Fri May 24 20	Fri May 24 2013 06
<a href="#">ap622-5864A0</a>	AP62	simba	AP-0622-t	configured		nx9500-0C9848	Wed May 22	Wed May 22 2013
<a href="#">ap650-3129D8</a>	AP65	rf 4	AP-0650-t	configured		nx9500-0C9848	Wed May 22	Wed May 22 2013
<a href="#">ap650-3129EC</a>	AP65	rf 4	AP-0650-t	configured		nx9500-0C9848	Wed May 22	Wed May 22 2013
<a href="#">ap650-312A10</a>	AP65	default	AP-0650-t	configured		nx9500-0C9848	Wed May 22	Wed May 22 2013
<a href="#">ap6511-8A4B15</a>	AP65	rf 3	AP-6511-t	configured		nx9500-0C9848	Wed May 22	Wed May 22 2013
<a href="#">ap6521-970CC6</a>	AP65	CN	AP-6521-t	configured		nx9500-0C9848	Wed May 22	Wed May 22 2013
<a href="#">ap6532-3118E0</a>	AP65	rf 2	AP-6532-t	configured		nx9500-0C9848	Wed May 22	Wed May 22 2013
<a href="#">ap6532-34503C</a>	AP65	rf 1	AP-6532-t	configured		nx9500-0C9848	Wed May 22	Wed May 22 2013
<a href="#">ap6532-347110</a>	AP65	rf 4US	AP-6532-t	configured		nx9500-0C9848	Wed May 22	Wed May 22 2013

Type to search in tables Row Count: 24

[Refresh](#)

- 6 The **Adopted Devices** screen displays the following:

Device	Displays the name assigned to the adopted device by the WiNG management software. The device 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 device managed by the selected controller.



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 the adopted device has been configured (provisioned) by its connected controller or service platform.
Errors	Lists any errors encountered the adoption.
Adopter Hostname	Lists the hostname of the adopting controller or service platform.
Adoption Time	Displays a timestamp, for each listed device, showing the date and time of adoption.
Startup Time	Lists the time the adopted device was last started up and detected on the network.

- 7 Click **Refresh** to update the screen's statistics counters to their latest values.

### *AP Adoption History*

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 AP adoption history statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller** node from the left navigation pane.
- 4 Expand the **Adoption** node in the left-hand side of the UI.
- 5 Select **AP Adoption History**.

The **Statistics > Controller > Adoption > AP Adoption History** screen displays.

Event Name	AP MAC Address	Reason	Event Time
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 12:39:38 PM
Adopted	00-15-70-38-06-49	N.A.	Sat Dec 2 2017 12:47:29 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 02:25:02 PM
Adopted	00-15-70-38-06-49	N.A.	Sat Dec 2 2017 02:29:34 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 02:55:02 PM
Adopted	00-15-70-38-06-49	N.A.	Sat Dec 2 2017 04:43:07 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 06:19:10 PM
Adopted	00-15-70-38-06-49	N.A.	Sat Dec 2 2017 08:28:09 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 11:24:08 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 11:29:16 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 11:51:02 PM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sat Dec 2 2017 11:54:34 PM
Adopted	00-15-70-38-06-49	N.A.	Sun Dec 3 2017 01:51:38 AM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sun Dec 3 2017 03:01:05 AM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Sun Dec 3 2017 03:11:22 AM
Adopted	00-15-70-38-06-49	N.A.	Sun Dec 3 2017 04:14:29 AM
Adopted	00-15-70-38-06-49	N.A.	Sun Dec 3 2017 05:47:16 AM
Adopted	00-15-70-38-06-49	N.A.	Sun Dec 3 2017 03:42:13 PM
Adopted	00-15-70-38-06-49	N.A.	Sun Dec 3 2017 06:56:20 PM
Adopted	00-15-70-38-06-49	N.A.	Mon Dec 4 2017 12:45:56 AM
Adopted	00-15-70-38-06-49	N.A.	Mon Dec 4 2017 01:47:55 AM
Adopted	B4-C7-99-6D-B5-D4	N.A.	Mon Dec 4 2017 01:51:02 AM

The AP Adoption History screen displays the following:

Event Name	Displays the current adoption status of each AP as either <b>adopted</b> or <b>un-adopted</b> .
AP MAC Address	Displays the hardware-encoded MAC (Media Access Control) address of each AP the controller or service platform has attempted to adopt.
Reason	If in case of failure to adopt, the reason for failure is displayed in this column.
Event Time	Displays <i>day, date</i> and <i>time</i> for each AP adoption attempt made by the controller or service platform.

- 6 Click **Refresh** to update the screen's statistics counters to their latest values.

### Pending Adoptions

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 pending adoption AP statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller** node from the left navigation pane.
- 4 Expand the **Adoption** node in the left-hand side of the UI.
- 5 Select **Pending Adoptions**.





- 1 Select the **Statistics** menu from the Web UI.
- 2 Select **System** from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Select **Guest User** from the left-hand side of the UI.

The **Statistics > Controller > Guest User** screen displays.

Client MAC	IP Address	IPv6 Address	Hostname	Role	Client Identity	Vendor	Band	AP Hostname	Radio MAC	WLAN	VLAN	Last Active
<a href="#">08-60-6E-9C</a>	157.235.91		android-5841	NA	Unknown	ASUSTek	11bgn	AN-17-311/	00-23-E	STOML	30	Fri Jan 10
<a href="#">24-77-03-CD</a>	157.235.91		acc125-01	NA	Unknown	Intel Corp	11an	AN-17-311/	00-23-E	STOML	30	Fri Jan 10

Type to search in tables Row Count: 2

[Disconnect Client](#) [Refresh](#)

The **Guest User** screen displays the following:

Client MAC	Displays the hard coded MAC address assigned to the guest client at the factory and can not be modified. The address displays as a link that you can select to view 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 IP (Internet Protocol) 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 Client Identity for this device. Client Identity is a set of unique fingerprints used to identify a class of devices. This information is then used to configure the permissions and access rules for the class of devices in the network.
Vendor	Displays the name of the manufacturer of the device.
Band	Displays the <b>2.4</b> or <b>5</b> 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



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: <ul style="list-style-type: none"> <li>• <b>0 – 20</b> (very low utilization)</li> <li>• <b>20 – 40</b> (low utilization)</li> <li>• <b>40 – 60</b> (moderate utilization)</li> <li>• <b>60 and above</b> (high utilization)</li> </ul>
Radio Count	Displays the number of radios currently in use by device 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 for packets transmitted by controller or service platform connected devices using this WLAN.
Rx Bytes	Displays the total number of bytes received 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.

- 5 Click **Disconnect All Clients** to terminate the all client WLAN memberships.
- 6 Click **Refresh** to update the statistics counters to their latest values.

## Policy Based Routing

The PBR (Policy Based Routing) screen displays statistics for packet path redirections. 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 managed client devices.

To review PBR statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **Policy Based Routing** from the left-hand side of the UI.

The **Statistics > Controller > Policy Based Routing** screen displays.











Radio	Displays the name assigned to each listed radio. Each radio name displays as a link that you can select to view radio configuration and network address information in greater detail.
Tx Bytes	Displays the total amount of transmitted data in bytes for each radio.
Rx Bytes	Displays the total amount of received data in bytes for each radio.
Tx Packets	Displays the total number of transmitted data in packets for each radio.
Rx Packets	Displays the total number 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: <ul style="list-style-type: none"> <li>• <b>0 – 20</b> (very low utilization)</li> <li>• <b>20 – 40</b> (low utilization)</li> <li>• <b>40 – 60</b> (moderate utilization)</li> <li>• <b>60 and above</b> (high utilization)</li> </ul>

- 6 Click **Refresh** to update the statistics counters to their latest values.

## Mesh

The **Mesh** screen provides detailed statistics on each of Mesh capable client in the selected controller or service platform radio coverage area.

A mesh network is where one where each node is able to communicate with other nodes and maintain more then one path to the other mesh nodes within the mesh network. A mesh network provides robust, reliable and redundant connectivity to all the members of the mesh network. When one member of the mesh network becomes unavailable, the other mesh nodes are still able to communicate with one another either directly or indirectly through intermediate nodes.

To view Mesh statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **Mesh** from the left-hand side of the UI.

The **Statistics > Controller > Mesh** screen displays.

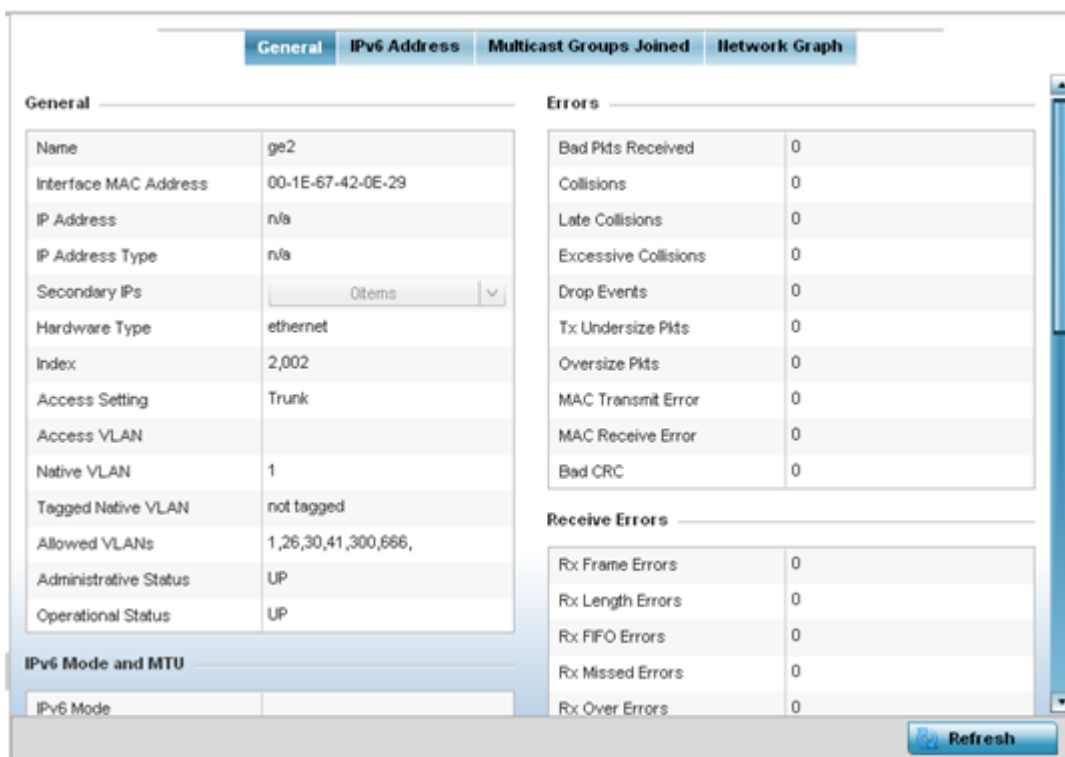


### Controller General Interface Details

To review general interface statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen. The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**
- 5 Select **Interfaces** from the left-hand side of the UI.

The **Statistics > Controller > Interfaces > General** screen displays by default in the right-hand pane.



The **General** tab provides information on a selected controller interface such as its MAC address, type and TX/RX statistics.

Name	Displays the name of the interface ge1, up 1 etc. RFS series controllers and NX series service platforms each have a unique set of interfaces.
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 IPs	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.

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.
Access Setting	Displays the VLAN mode as either <b>Access</b> or <b>Trunk</b> .
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 <b>UP</b> (operational) or <b>DOWN</b> .

The **IPv6 Mode and MTU** table displays the following information:

IPv6 Mode	Lists the current IPv6 mode utilized.
IPv6 MTU	Lists the IPv6 formatted largest packet size that can be sent over this interface.

The **Specification** table displays the following information:

Media Type	Displays the physical connection type of the interface. Medium types include: <ul style="list-style-type: none"> <li>• <b>Copper</b> - Used on RJ-45 Ethernet ports</li> <li>• <b>Optical</b> - Used on fibre optic gigabit Ethernet ports</li> </ul>
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	The mode can be either: <ul style="list-style-type: none"> <li>• <b>Access</b> - The Ethernet interface accepts packets only from native VLANs.</li> <li>• <b>Trunk</b> - The Ethernet interface allows packets from a list of VLANs you can add to the trunk.</li> </ul>
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 <b>10</b> , <b>100</b> , <b>1000</b> or <b>Auto</b> . 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 <b>half duplex</b> , <b>full duplex</b> or <b>unknown</b> .

The **Traffic** table displays the following information:

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 information:

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	Displays the number of late collisions. Late collisions occur after the first 64 octets of data has 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 information:

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 First-in First-out (FIFO) errors received at the interface. FIFO 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 information:

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. FIFO 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.

- 6 Click **Refresh** to update the statistics counters to their latest value.

### IPv6 Address

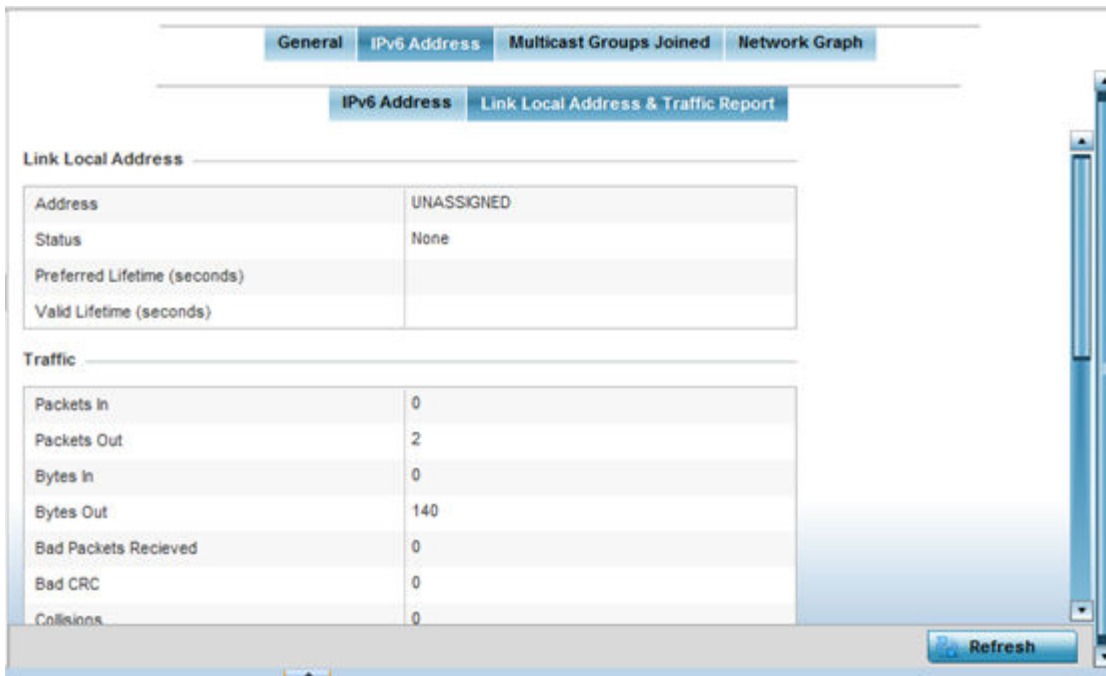
IPv6 is the latest revision of the IP (Internet Protocol) designed to replace IPv4. IPV6 provides enhanced identification and location information for computers on networks routing traffic across the Internet. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

To review IPv6 Address interface statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**
- 4 Select **Interfaces** from the left-hand side of the UI.
- 5 Select the **IPv6 Address** tab.

The **Statistics > Controller > Interfaces > IPv6 Address > IPv6 Address** screen displays by default in the right-hand pane.





This screen has the following information:

The **Link Local Address** table:

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.

The **Traffic** table displays the following information:

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.

The **Receive Errors** table displays the following information:

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.

The **Transmit Errors** table displays the following information:

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.

- 7 Click **Refresh** to update the statistics counters to their latest value.

### *Multicast Groups Joined*

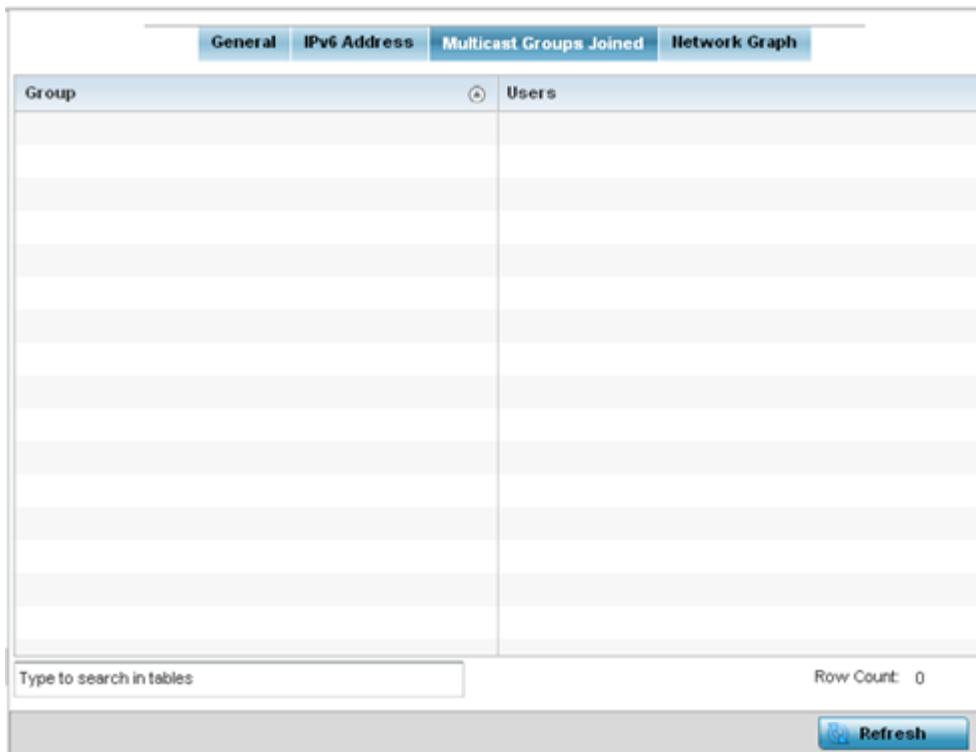
Multicast groups scale to a larger set of destinations by not requiring prior knowledge of who or how many destinations there are. Multicast devices use their infrastructure efficiently by requiring the source to send a packet only once, even if delivered to a large number of devices. Devices replicate 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 review Multicast Groups that the selected controller or service platform has joined:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **Interfaces** from the left-hand side of the UI.
- 5 Select the **Multicast Groups Joined** tab.

The **Statistics > Controller > Interfaces > Multicast Groups Joined** displays in the right-hand pane.



This table displays the following information:

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 than one group at a time.

- 6 Periodically, click **Refresh** to update the screen’s counters to their latest values.

### Network Graph

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-down menu to define the increment data is displayed on the graph.

To view the Interface Statistics graph:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.

- 4 Select a **Wireless Controller**.
- 5 Select **Interfaces** from the left-hand side of the UI.
- 6 Select the **Network Graph** tab.

The **Statistics > Controller > Interfaces > Network Graph** screen displays in the right-hand pane.



- 7 Use the **Parameters** drop-down menu to specify what is trended in the graph.

## RAID Statistics

RAID statistics are available to assist an administrator in assessing the status of the service platform 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.

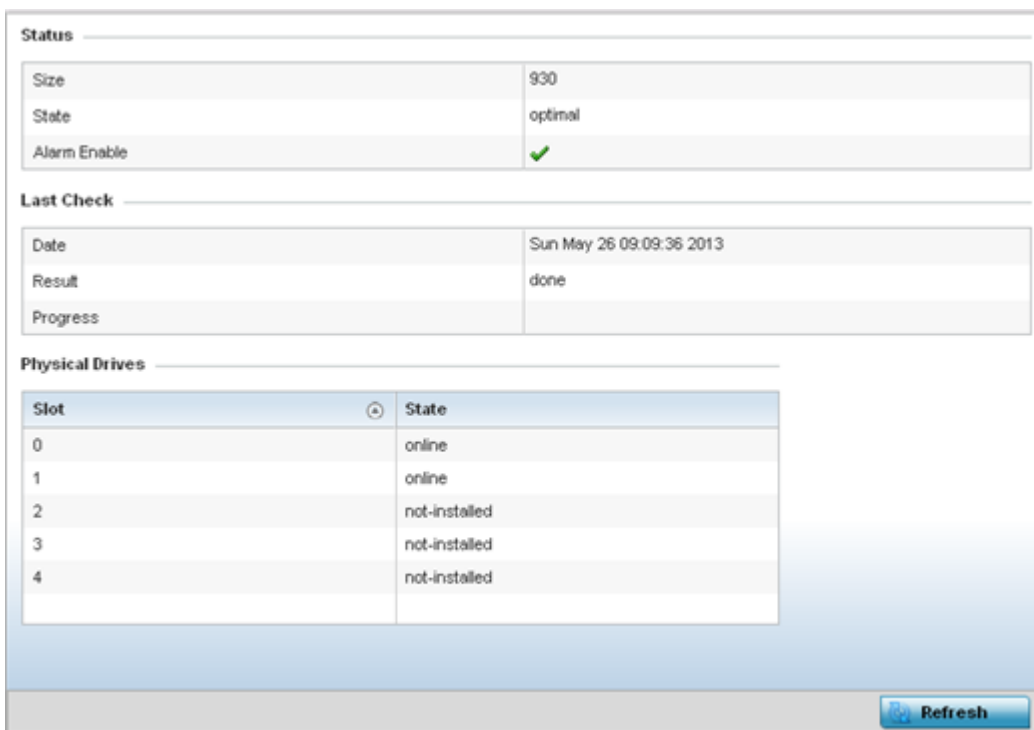
RAID controller drive arrays are available within NX 7510 and NX 95XX models only. However, they can be administrated on behalf of a profile by a different model service platform or controller.

For information on setting the service platform drive array configuration as well as the diagnostic behavior of its member drives, refer to [RAID](#) on page 916.

To view RAID statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select **Wireless Controller** .
- 4 Select **RAID** from the left-hand side of the UI.

The **Statistics > Controller > RAID** screen displays.



The **Status** field displays the following information:

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 Enabled	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.

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 completed and minutes utilized (for example, 78%/116min).

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.

- 5 Select **Refresh** at any time to update either the screen's statistic counters to their latest value.

## Power Status

Periodically review the controller or service platform power status to assess the power budget and PoE capability (if supported).

PoE is supported on WiNG model wireless controller. 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 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **Power Status** from the left-hand side of the UI.

The **Statistics > Controller > Power Status** screen displays.

Device	1				
Temperature	40C				
<b>PoE Settings</b>					
PoE Enabled	yes				
Power Limit	36.0W				
Port Name	ge3				
Priority	low				
<b>System Status</b>					
System Voltage	47.8 volts				
System Guard Band	19 watts				
Power Budget	60 watts				
Power Consumption	12 watts				
Non-Standard PoE power budget					
<b>Port Stats</b>					
Port Name	Voltage	Current	Power	Class Type	Port Status
ge1	0.0	0	0.0	0	Off, detection in progress
ge2	47.8	250	11.8	4	On, valid resistor
ge3	0.0	0	0.0	0	Off, detection in progress
ge4	0.0	0	0.0	0	Off, detection in progress
ge5	0.0	0	0.0	0	Off, detection in progress

**Refresh**

This screen provides the following information for supported controllers:

Device	Displays the administrator assigned device name for the listed controller or service platform.
Temperature	Displays the internal system temperature for the controller or service platform.
PoE Enabled	Displays whether or not PoE (Power over Ethernet) is enabled for the controller. When enabled, the controller 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. PoE is supported on RFS 4000 model controllers.
Power Limit	Displays the total watts available for Power over Ethernet support. The value should be between 0 - 40 watts.
Port Name	Displays the GE port name on the controller.
Priority	Displays the power priority for the listed port as either <b>Critical</b> , <b>High</b> or <b>Low</b> . This is the priority assigned to this port versus the power requirements of the other ports.
System Voltage	Displays the total current system voltage.
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 allocated for use in Power over Ethernet.
Power Consumption	Displays the current amount of power being consumed by PoE devices managed by 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.
Voltage	Displays the voltage in use by each PoE capable port.
Current	Displays the amount of current in milliwatts being used by each PoE capable port.
Power	Displays whether or not each PoE capable port is providing power for potential requesting devices.
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. It will display either <b>Enabled</b> or <b>Disabled</b> .

- 5 Select **Refresh** to update the statistics counters to their latest value.

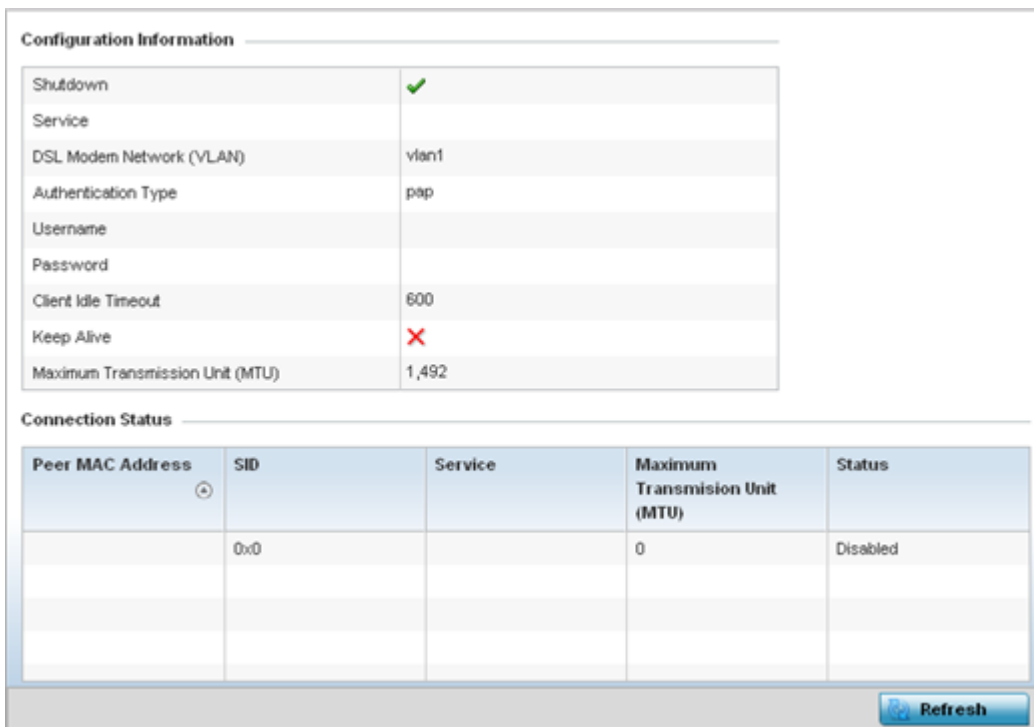
## PPPoE

The **PPPoE** statistics screen displays stats derived from 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 RFS 4000 model controllers. 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 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **PPPoE** from the left-hand side of the UI.



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 <b>None, PAP, CHAP, MSCHAP, and MSCHAP-v2.</b>
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 MTU ( <i>maximum transmission unit</i> ) 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.

- 5 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

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

## OSPF

OSPF (Open Shortest Path First) is a *link-state* IGP (interior gateway protocol). 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:

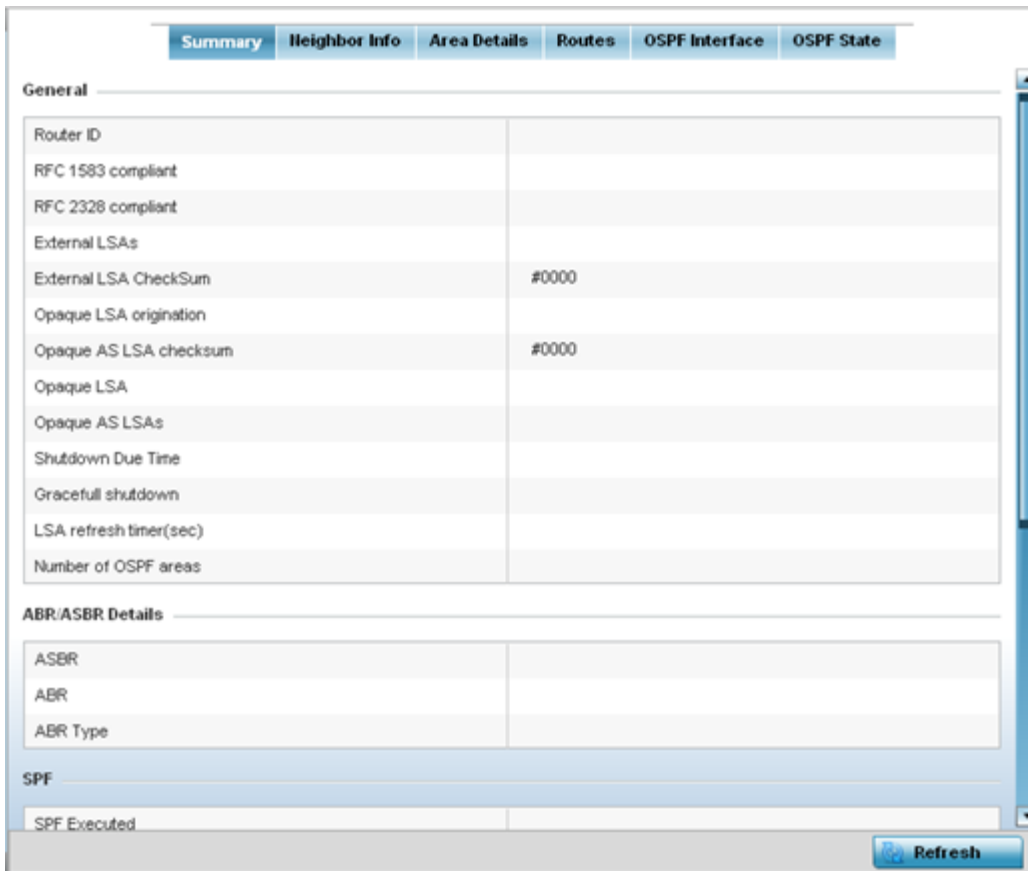
- [OSPF Summary](#) on page 1044
- [OSPF Neighbors](#) on page 1046
- [OSPF Area Details](#) on page 1047
- [AP OSPF Route Statistics](#) on page 1199
- [OSPF Interface](#) on page 1052
- [OSPF State](#) on page 1053

### OSPF Summary

To view OSPF summary statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **OSPF** from the left-hand side of the UI.

The **Statistics > Controller > OSPF > Summary** screen displays by default.



This screen describes the following data fields:

General	<p>The general field displays the router ID assigned for this OSPF connection, RFC compliance information and LSA data. OSPF version 2 was originally defined within RFC versions 1583 and 2328. The general field displays whether compliance to these RFCs have been satisfied. The OSPF LSA (Link-State Advertisement) Throttling feature provides a dynamic mechanism to slow down link-state advertisement updates in OSPF during times of network instability. It also allows faster OSPF convergence by providing LSA rate limiting in milliseconds. LSA information is provided for both external and opaque LSAs. Opaque LSAs carrying type-length-value elements. These extensions allow OSPF to run completely out of band of the data plane network. This means that it can also be used on non-IP networks, such as optical networks.</p>
ABR/ ASBR	<p>Lists ASBR (Autonomous System Boundary Router) data relevant to OSPF routing, including the <i>ASBR</i>, <i>ABR</i> and <i>ABR</i> type. An ABR (Area Border Router) 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.</p>





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 DR (designated router) 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.

- 6 Select **Refresh** to update the statistics counters to their latest values.

### OSPF Area Details

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 a 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 LSAs (Link State Advertisements) 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 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **OSPF** from the left-hand side of the UI.
- 5 Select the **Area Details** tab.

The **Statistics > Controller > OSPF > Area Details** screen displays.





Opaque Area link 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.

- 6 Select **Refresh** to update the statistics counters to their latest values.

### Controller OSPF Route Statistics

Refer to the **Routes** tab to assess the status of OSPF

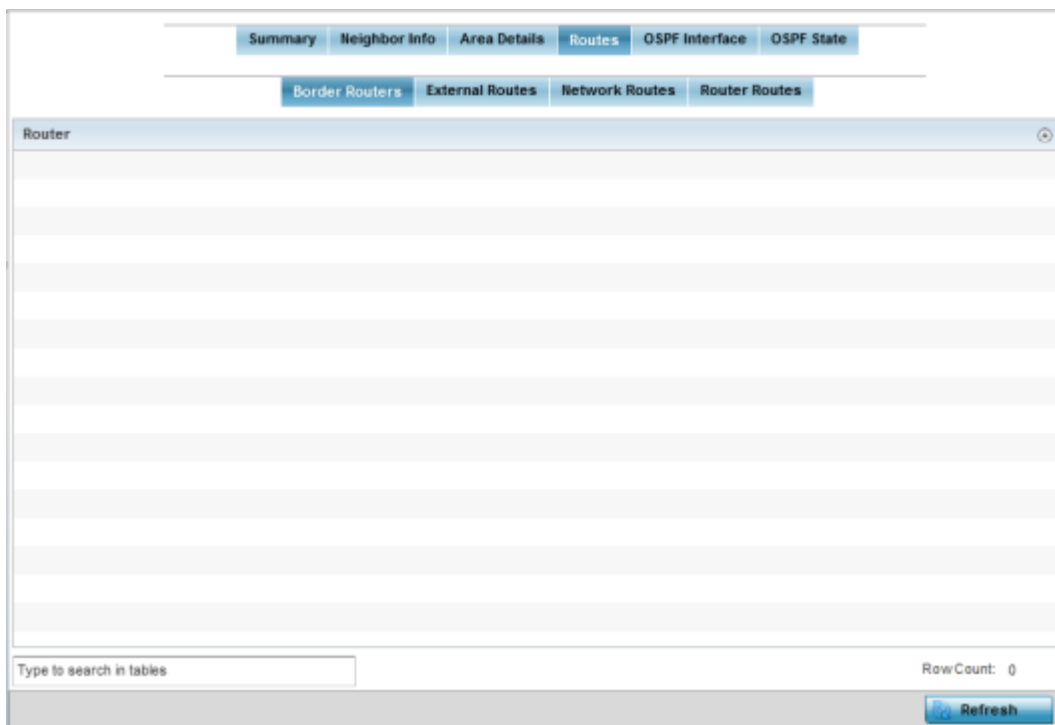
- [Border Routes](#) on page 1049.
- [AP OSPF External Routes](#) on page 1200.
- [AP OSPF Network Routes](#) on page 1201.
- [AP OSPF Router Routes](#) on page 1202.

### Border Routes

To view OSPF border route statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **OSPF** from the left-hand side of the UI.
- 5 Select the **Routes** tab.

The **Statistics > Controller > OSPF > Routes > Border Routers** screen displays by default.

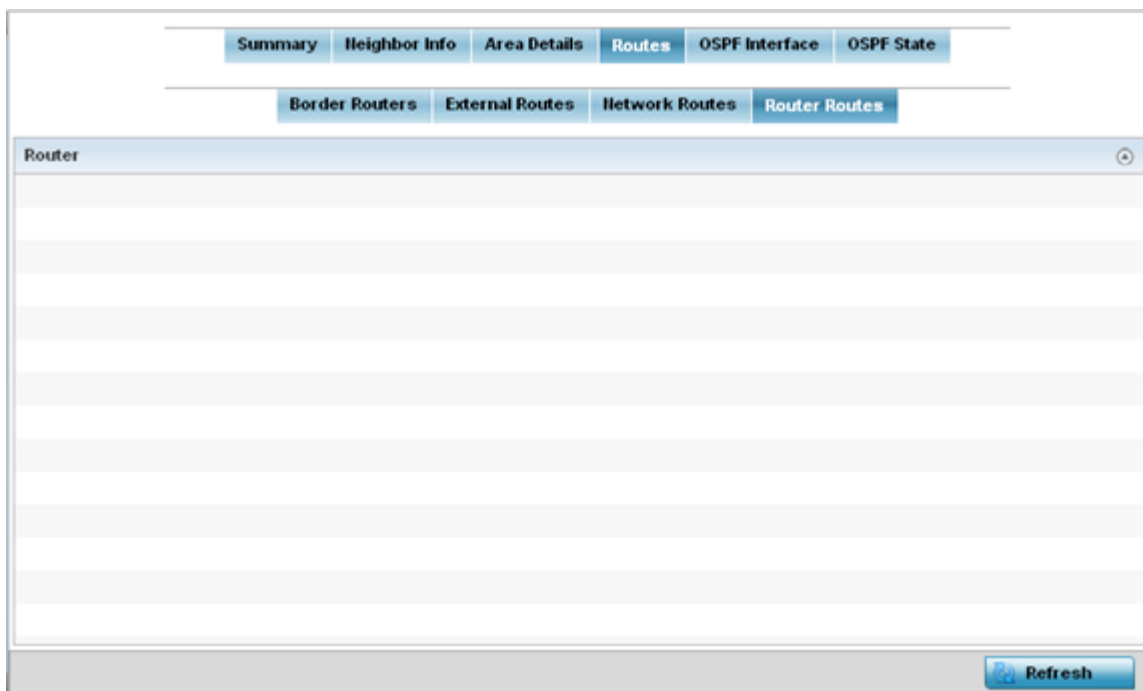






- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **OSPF** from the left-hand side of the UI.
- 5 Select the **Router Routes > Router Routes** tab.

The **Statistics > Controller > OSPF > Routes > Router Routes** screen displays.



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.

- 6 Select **Refresh** to update the statistics counters to their latest values.

### *OSPF Interface*

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:

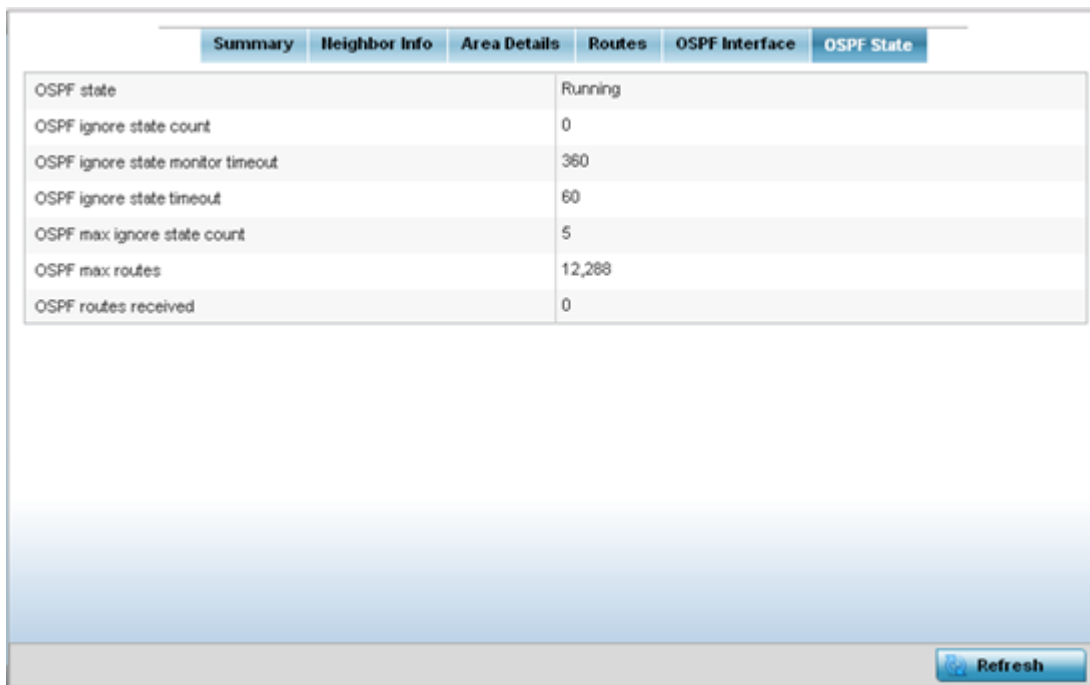
- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **OSPF** from the left-hand side of the UI.
- 5 Select the **OSPF Interface** tab.

The **Statistics > Controller > OSPF > OSPF Interface** screen displays.



- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **OSPF** from the left-hand side of the UI.
- 5 Select the **OSPF State** tab.

The **Statistics > Controller > OSPF > OSPF State** screen displays.



This screen provides the following information:

OSPF state	Displays the OSPF link state amongst neighbors within the OSPF topology. Link state information is maintained in a LSDB (link-state database) 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 and its peers within this OSPF supported broadcast domain.
OSPF ignore state monitor timeout	Displays the timeout that, when exceeded, prohibits the controller from detecting changes to the OSPF link state.
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.

- 6 Select **Refresh** to update the statistics counters to their latest values.

## BGP

BGP (Border Gateway Protocol) is an inter-ISP routing protocol which establishes routes between ISPs. ISPs use BGP to exchange routing and reachability information between AS (Autonomous Systems) 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 AS is a set of routers under the same administration that use IGP (Interior Gateway Protocol) 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).

Use BGP statistics to assess status of the controller/service platforms' BGP feature and its neighbor BGP peers. Much of the configuration information can be filtered from the Route Filters screen.



### Note

BGP is only supported on NX 95XX and NX 96XX model controllers and service platforms.

The BGP statistics page displays the following information:

- [BGP Summary](#) on page 1055
- [BGP Neighbor](#) on page 1056
- [BGP Route Filters](#) on page 1059
- [BGP State](#) on page 1063

### *BGP Summary*

To review BGP statistics summary:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **BGP** from the left-hand side of the UI.

The **Statistics > Controller > BGP > Summary** screen displays by default in the right-hand pane.

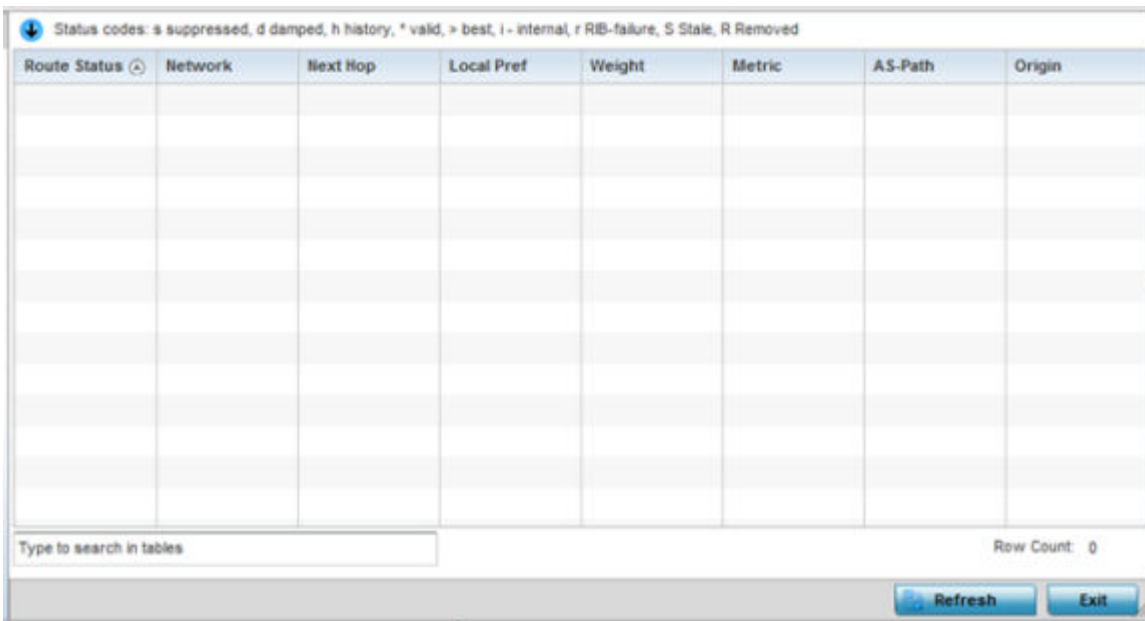






Keepalive	Displays the duration, in seconds, for the keep alive timer used to maintain the connection to each listed BGP neighbor device.
Clear Routes	Select this option (within the table) to reset and clear all routes received from this BGP neighbor.

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:



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	<p>Displays the status of this route. Route statuses include:</p> <ul style="list-style-type: none"> <li>• <b>Suppressed</b> - This route has been suppressed.</li> <li>• <b>Damped</b> - This route has been damped due to flapping.</li> <li>• <b>History</b> - This route is kept in memory to retain flap-dampening statistics. This route is not currently announced by the peer.</li> <li>• <b>Valid</b> - This route is a valid route.</li> <li>• <b>Best</b> - This route is the best route of all the routes utilized.</li> <li>• <b>RIB Failure</b> - 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.</li> <li>• <b>Removed</b> - This route has been removed from the routes list and is no longer available to BGP supported neighbor devices.</li> </ul>
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.

- Periodically, select **Refresh** to update the screen's counters to their latest value.

### BGP Route Filters

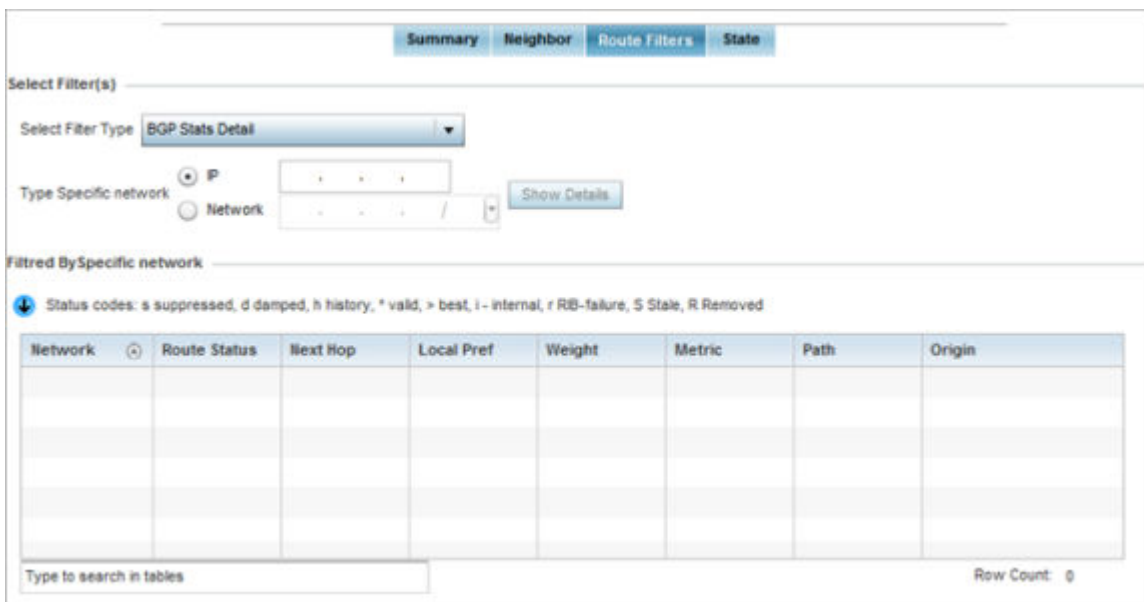
To review BGP Route statistics:

- Select the **Statistics** menu from the Web UI.
- Expand the **RF Domain** node.
- Select a **Wireless Controller**.
- Select **BGP** from the left-hand side of the UI.

The **BGP Summary** screen displays by default in the right-hand pane.

- Select the **Route Filters** tab.

The **Statistics > Controller > BGP > Route Filters** screen displays



- In the **Select Filter(s)** area, use the **Select Filter Type** drop-down menu to specify a filter. Route statistics can be filtered on the basis of the following eight (8) different parameters:
  - 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.



Select Filter(s) \_\_\_\_\_

Select Filter Type **Community List** ▼

Type Community list  **Show Details**

10 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

<b>Route Status</b>	Displays the status of this route. Route status options include: <ul style="list-style-type: none"> <li>• <b>Suppressed</b> – This route has been suppressed.</li> <li>• <b>Damped</b> – This route has been damped due to flapping.</li> <li>• <b>History</b> - This route is kept in memory to retain flap-dampening statistics. This route is not currently announced by the peer.</li> <li>• <b>Valid</b> – This route is a valid route.</li> <li>• <b>Best</b> – This route is the best route of all routes.</li> <li>• <b>RIB Failure</b> – A route with better administrative distance is already present, a memory failure exists or the number of routes in VRF exceeds the route-limit configured under the VRF instance.</li> <li>• <b>Removed</b> – This route has been removed from the routes list.</li> </ul>
<b>Network</b>	Displays network information for this route.
<b>Next Hop</b>	Displays the IP address of the next hop resource utilized in this route.
<b>Local Pref</b>	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.
<b>Weight</b>	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.
<b>Metric</b>	Lists a measure (metric) of the quality of the path. A lower value indicates a better path. This value is the MED evaluated by BGP during the best path selection process.
<b>AS-Path</b>	Displays AS path information for this route.
<b>Origin</b>	Displays the IP address of the origin for this route.

11 Select **Community** from the **Select Filter Type** list.



Select Filter(s) \_\_\_\_\_

Select Filter Type

Type Community

- 12 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.
- 13 Select **Show Details** to display the list of filtered routes.
- 14 Select **Prefix List** from the **Select Filter Type** list.

Select Filter(s) \_\_\_\_\_

Select Filter Type

Type Prefix list

- 15 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.
- 16 Select **Filter List** from the **Select Filter Type** list.

Select Filter(s) \_\_\_\_\_

Select Filter Type

Type Filter list

- 17 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.
- 18 Select **Regular Expression** from the **Select Filter Type** list.

Select Filter(s) \_\_\_\_\_

Select Filter Type

Type Regular expression

- 19 Use the **Type Regular Expression** field to filter the routes based on regular expressions. Select Show Details to display the list of filtered routes.
- 20 Select **Route Map** from the **Select Filter Type** list.

Select Filter(s) \_\_\_\_\_

Select Filter Type **Route Map** ▼

Type Route map  **Show Details**

- 21 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.
- 22 Select **Expanded Community List** from the **Select Filter Type** list.

Select Filter(s) \_\_\_\_\_

Select Filter Type **Expanded Community List** ▼

Type Expanded list  **Show Details**

- 23 Use the **Type Expanded list** to filter routes based on route-maps. Select Show Details to display a list of filtered routes.
- 24 Periodically, select **Refresh** to update the screen's counters to their latest value.

*BGP State*

To view BGP State statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **BGP** from the left-hand side of the UI.

The **BGP Summary** screen displays by default in the right-hand pane.

- 5 Select the **State** tab.

The **Statistics > Controller > BGP > State** screen displays.

Summary Neighbor Route Filters State	
Maximum routes allowed	10
Routes recieved	0
Current ignore count	0
Ignore count allowed	5
Reset time	360
Ignore time	60
Current state	Running

**Refresh**

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.

6 Periodically, select **Refresh** to update the screen’s counters to their latest value.

### L2TPv3 Tunnels

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 managed devices and other vendor 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 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **L2TPv3 Tunnels** in the left-hand side of the UI.

The **Statistics > Controller > L2TPv3 Tunnels** screen displays in the right-hand pane.

Tunnel Name	Local Addresses	Peer Addresses	Peer	Tunnel State	Tunnel Mode	Peer Host Name	Peer Control Connection ID	Control Connection ID	Up Time	Encapsulation Protocol	Critical Resource	VRRP Group	Establishment Criteria
<a href="#">L2tp-199-0-ap7632-9AEEF9-0.0.0.0</a>	2.2.2.1	2.2.2.19	1	Established	Active	ap7632-	4,292,36	1,811,44	5 days	ip		0	Always
<a href="#">L2tp-199-1-ap7612-17DE2F-0.0.0.0</a>	2.2.2.1	2.2.2.19	1	Established	Active	ap7612-	1,891,40	3,991,37	5 days	ip		0	Always
<a href="#">L2tp-199-3-ap7602-D1B28B-0.0.0.0</a>	2.2.2.1	2.2.2.19	1	Established	Active	ap7602-	2,665,68	3,796,34	5 days	ip		0	Always
<a href="#">L2tp-199-5-ap7622-D1A917-0.0.0.0</a>	2.2.2.1	2.2.2.19	1	Established	Active	ap7622-	3,490,47	658,534	4 days	ip		0	Always

Type to search in tables Row Count: 4



The following table describes the L2TPv3 statistics information:

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 pseudowire 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 the following format- <b>Days: Hours: Minutes: Seconds</b> : format. If the up time is displayed as - D:0 H:0 M: 0 S:0, it means 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 interoperated 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.

- 5 Select the **Refresh** button to update the screen's statistics counters to their latest value.
- 6 Click the **Tunnel Name** link, to view per-session statistics for a specific L2TPv3 tunnel. The sessions for the selected L2TPv3 tunnel are displayed.
- 7 Click the **VLAN ID** of the desired session to view session statistics.

- 8 Select an L2TPV3 tunnel, and click **Down** to terminate it.
- 9 Select **Down All** to terminate all configured L2TPV3 Tunnels.
- 10 Select an L2TPV3 tunnel, and click **Up** to bring it up.
- 11 Select **Up All** to bring up all configured L2TPV3 Tunnels.

## VRRP

The **VRRP** statistics screen displays VRRP (Virtual Router Redundancy Protocol) 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 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **VRRP** from the controller statistics menu.

The **Statistics > Controller > VRRP** screen displays in the right-hand pane.

The screenshot displays the VRRP statistics interface. It is divided into two main sections: 'Global Error Status' and 'Router Operations Summary'.

**Global Error Status** section contains a table with the following data:

Authentication mismatch	0
Packets with invalid checksum	0
Packets with invalid type	0
Packets with invalid VRID	0
Packets with TTL Errors	0
Last protocol error reason	None
Packets with length Error	0
Packets with invalid version	0

**Router Operations Summary** section contains a table with the following headers:

VRID	Virtual IP Address	Master IP Address	Interface Name	Version	State

At the bottom of the screen, there are three buttons: 'Clear Router Status', 'Clear Global Error Status', and 'Refresh'.

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.

Refer to the **Router Operations Summary** area 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 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.

- Optionally select a **VRID** to list the ID's VRRP information in greater detail.

The screenshot displays the VRRP configuration and status interface. It is divided into several sections:

- Configuration:**
  - VRID: 201
  - Interface Name: vlan201
  - Version: 2
  - Priority: 254
  - Delta Priority: (empty)
  - CRM Down Action: (empty)
  - No. of Virtual IP Address: 1
  - Virtual IP Addresses: 1 item (dropdown menu)
  - Advertisement Interval: 1 sec
  - Sync Group:
  - Preempt:
  - Preempt Delay: 3m 0s
- Operational State:**
  - Virtual MAC Address: 00-00-5E-00-01-C9
  - Local IP Address: 192.168.201.1
  - Critical Resource: (empty)
  - CRM Status: (empty)
  - Sync Group Failure: (empty)
  - Interface Status: up and running
- Router Status:**
  - Master Transitions: 1
  - Master Reason: master no response
  - Advertisement Pkts Received: 13
  - Advertisement Interval Errors: 0
  - Advertisement Pkts Sent: 591,320
  - Received Pkts in Init State: 0
  - Received Pkts with Priority Zero: 0
  - Sent Pkts with Priority Zero: 0
  - Address List Errors: 0
- Monitor Interface:**
  - Table with columns: Name, Interface Status
  - Table is currently empty.

At the bottom right, there are buttons for **Refresh** and **Exit**.

The **Configuration** area displays the following information:

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 <a href="http://www.ietf.org/rfc/rfc3768.txt">http://www.ietf.org/rfc/rfc3768.txt</a> (version 2) and <a href="http://www.ietf.org/rfc/rfc5798.txt">http://www.ietf.org/rfc/rfc5798.txt</a> (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 preemption. 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 preemption.

The **Operation State** area displays the following information:

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.

The **Router Status** area displays the following information:

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.

- 6 Refer to the **Monitor Interface** field to assess the names of this VRID's interface utilization and their respective statuses.
- 7 Select **Clear Router Status** to clear the **Router Operations Summary** table values to zero and begin new data collections.
- 8 Select **Clear Global Error Status** to clear the **Global Error Status** table values to zero and begin new data collections.
- 9 Select **Refresh** to update the screen's statistics counters to their latest values.

## Critical Resource

The **Critical Resources** statistics screen displays a list of device network IP addresses (gateways, routers etc.) defined as critical to the health of the controller, service platform or access point managed network. Critical resources are pinged regularly to ensure availability. If there is a connectivity issue, an event is generated stating a critical resource is unavailable.

To view Critical Resource statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **Critical Resource** from the left-hand side of the UI.

The **Statistics > Controller > Critical Resource** screen is displayed in the right-hand pane.

**General**

Monitor Interval	30s
Monitor Using Flows Interval	30s
Source IP For Port-Limited Monitoring	0.0.0.0
Monitoring Retries before Marking Resource as DO	3

**List of Critical Resources**

Critical Resource Name <span style="font-size: 0.8em;">⊕</span>	Via	Status	Mode

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).

Refer to the following **List of Critical Resources** stats:

Critical Resource Name	Displays the name of the critical resource being monitored.
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 ( <b>Up</b> or <b>Down</b> ).
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).

- 5 Select **Refresh** to update the statistics counters to their latest values.

## LDAP Agent Status

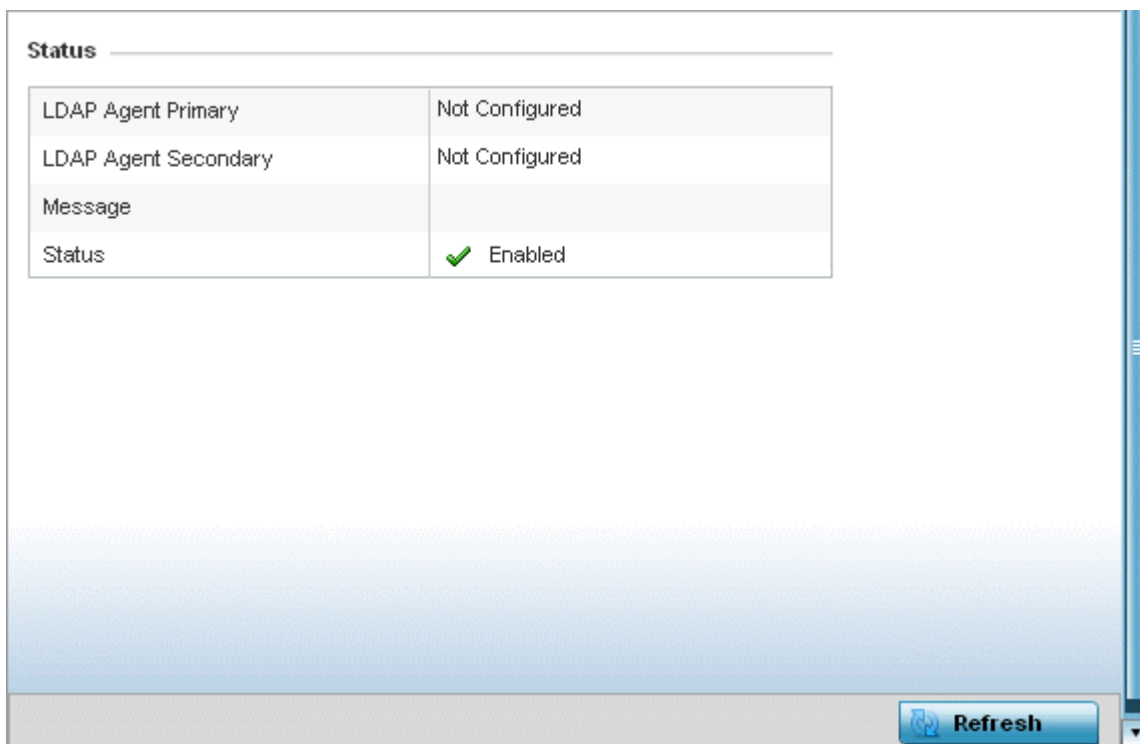
When LDAP has been specified as an external resource (as opposed to local RADIUS resources) to validate PEAP-MS-CHAP v2 authentication requests, user credentials and password information needs to be made available locally to successfully connect to the external LDAP server. Up to two LDAP Agents (primary 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](#).

To view controller or service platform LDAP agent statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **LDAP Agent Status** from the left-hand side of the UI.

The **Statistics > Controller > LDAP Agent Status** screen is displayed in the right-hand pane.



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.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## MiNT Links

Wireless controllers and APs use the MiNT protocol as the primary means of device discovery and communication for AP 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 APs during adoption using MLCP (MiNT Link Creation Protocol). They can also be manually created between a controller and AP (or) between two APs. 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 APs. Level 2 MiNT links also provide partitioning, between APs deployed at various remote sites.

To view controller or service platform Mint link statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Select **Mint Links** from the left-hand side of the UI.

The **Statistics > Controller > MiNT Links** stats is displayed in the right-hand pane.

name	listening	forced	unused	level	type	dis	devs	secure	local ip	natted	cost	hello seq num	hello interval	adj hold time	static	dyna mic	mlcp	rim	cont rol vlan	clustering
ip-172	✗	✗	✗	2	ipv4	unkno			172.16	✗	100	4	15	46	✗	✗	✓	✗	✗	✗
vlan-5	✗	✗	✗	1	vlan	68.8A				✗	10	3	4	13	✗	✗	✓	✗	✗	✗
vlan-1	✗	✗	✗	1	vlan	E.19.E				✗	10	7	4	13	✗	✗	✓	✗	✗	✗
ip-172	✗	✗	✗	2	ipv4	unkno			172.16	✗	100	4	15	46	✗	✗	✓	✗	✗	✗

Type to search in tables Row Count: 4

[Refresh](#)

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** column defines the cost for a packet to travel from its originating port to its end point destination.

The **hello seq number** and **hello interval** columns 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.

- 5 If needed, select a **Mint link** from the **name** column to display more granular information for that link.

**Mint Links**

name	vlan-10
level	1
cost	10
hello interval	4
adj hold time	13

**Adjacencies**

neighbor	state	up time	last hello
0B.19.E3.6E	up	546,679	2
12.3B.65.87	up	546,679	0
19.43.53.0D	up	546,679	3
4D.1B.B2.10	up	546,679	0
68.64.0A.8F	up	546,679	0

Refresh Exit

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 screen's data counters to their latest values.

## Guest Users

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 [Captive Portals](#).

To view the controller or service platform guest user utilization:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Select **Guest Users** from the left-hand side of the UI.

The **Statistics > Controller > Guest Users** screen displays in the right-hand pane:

Name	Configured Time (days:hrs:m ins:secs)	Remaining Time (days:hrs:m ins:secs)	Configured KiloBytes	Remaining KiloBytes	Configured Downlink Rate (kbps)	Configured Uplink Rate (kbps)	Current Downlink Rate (kbps)	Current Uplink Rate (kbps)

Row Count: 0

This 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 user'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 <a href="#">Defining User Pools</a> .
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 <a href="#">Defining User Pools</a> .
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 <a href="#">Defining User Pools</a> .
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 <a href="#">Defining User Pools</a> .

- 6 Select **Refresh** to update the screen's statistics counters to their latest value.

## GRE Tunnel

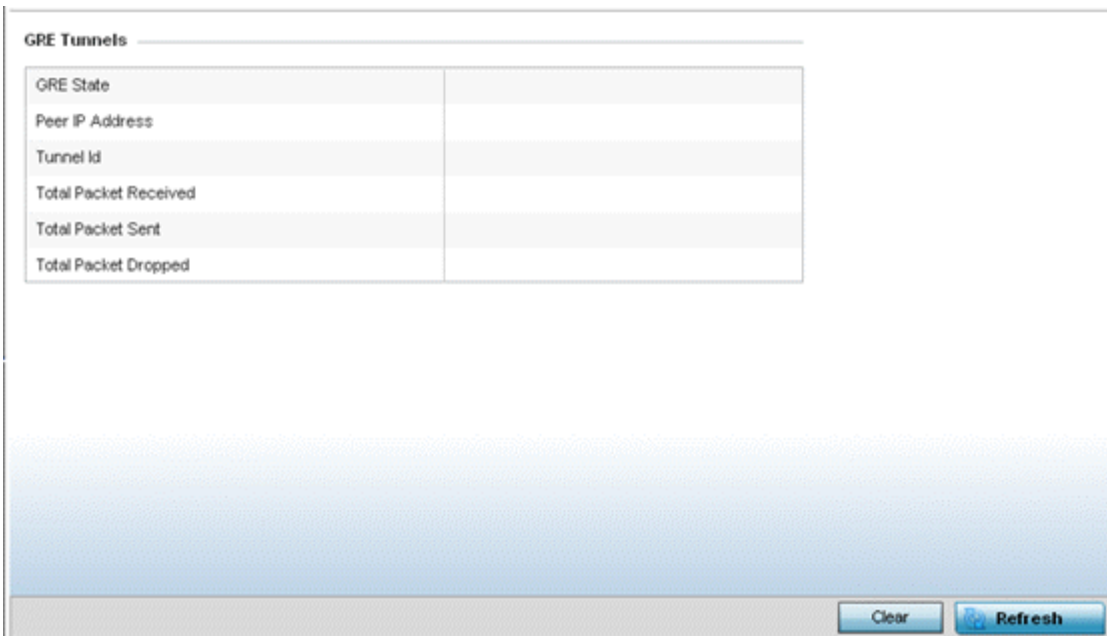
GRE (Generic Routing Encapsulation) is one of the available tunneling mechanisms, which uses IP as the transport protocol and can be used for carrying many different passenger protocols. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Select **GRE Tunnels**.

The **Statistics > Controller > GRE Tunnels** screen displays in the right-hand pane.



This 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

- 6 Select **Clear** to revert the screen counters to zero and begin a new data collection.
- 7 Select **Refresh** to update the screen’s statistics counters to their latest value.

## Dot1x

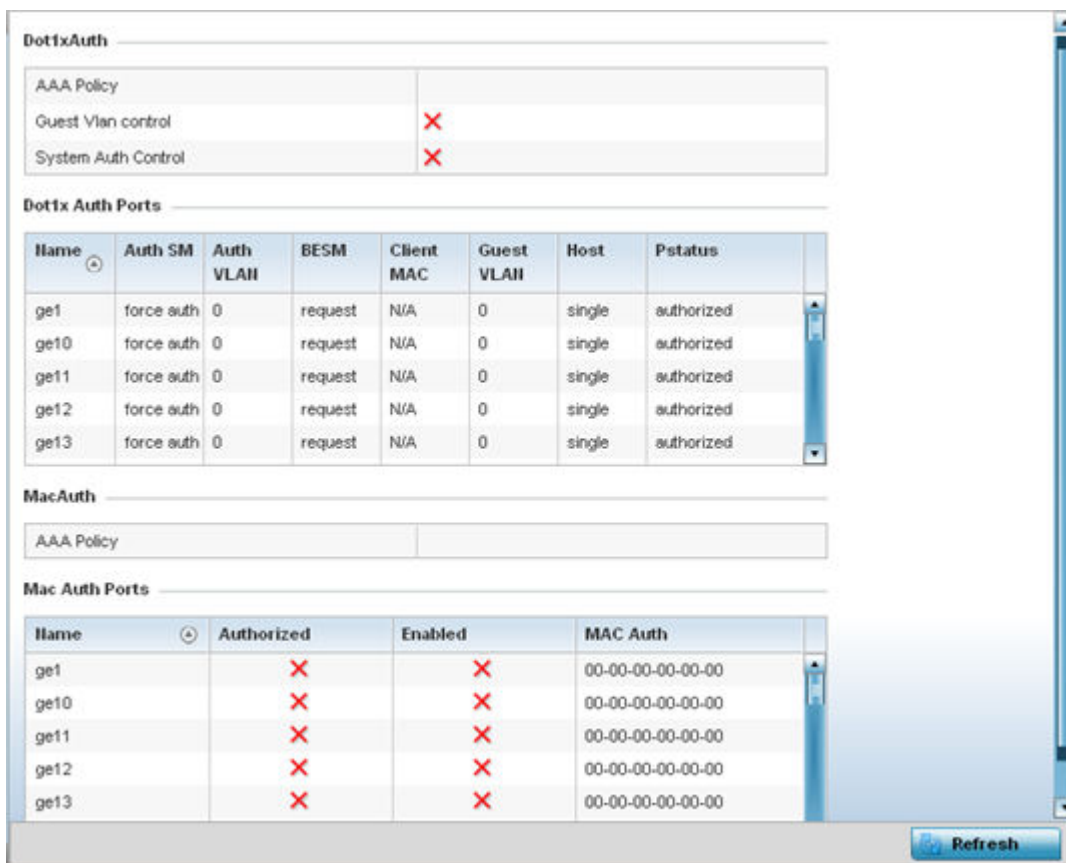
Dot1x (or 802.1x) is an IEEE standard for network authentication. Devices supporting Dot1x allow the automatic provision and connection to the wireless network without launching a Web browser at login. When within range of a Dot1x network, a device automatically connects and authenticates without needing to manually login.

To view the Dot1x statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.

- 4 Select a **Wireless Controller**.
- 5 Select **Dot1x** from the left-hand side of the UI.

The **Statistics > Controller > Dot1x** screen displays in the right-hand pane.



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.

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.

Refer to the **MacAuth** table to assess the AAA policy applied to MAC authorization requests.

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 authorized. A red X defines authorization as disabled.
Enabled	Lists whether MAC authorization using Dot1x has been or 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.

- 6 Select **Refresh** to update the screen's statistics counters to their latest value.

## Network

Use the **Network** set of management screens to view information for *ARP*, *DHCP*, *Routing* and *Bridging*. Each of these screens provides enough data to troubleshoot issues related to the following:

- [ARP Entries](#)
- [Route Entries](#)
- [Bridge](#)
- [IGMP](#)
- [DHCP Options](#)
- [Cisco Discovery Protocol](#)
- [Link Layer Discovery Protocol](#)

### *ARP Entries*

ARP (Address Resolution Protocol) 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 the ARP entries on the network statistics screen:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Networks** menu from the left-hand side of the UI.
- 6 Select **ARP Entries**.

The **Statistics > Controller > ARP Entries** stats is displayed in the right-hand pane.

ARP Entry			
IP Address	ARP MAC Address	Type	VLAN
10.233.89.253	00-0F-35-76-F4-3C	Dynamic	vlan10
10.233.89.72	00-11-25-95-F8-F8	Dynamic	vlan10
172.168.1.107	B4-C7-99-0F-C9-DC	Dynamic	vlan5
172.168.1.200	00-14-85-A0-F5-9A	Dynamic	vlan5
172.168.7.200	00-16-C7-86-A2-43	Dynamic	vlan4

Type to search in tables Row Count: 5

[Refresh](#)

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 VLAN ID where the IP address was found.

- 7 Select the **Refresh** button to update the screen’s statistics counters to their latest values.

### Route Entries

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.

To view the route entries:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Network** menu from the left-hand side of the UI.

6 Select **Route Entries**.

The **Statistics > Controller > IPv4 Route Entries** stats display by default in the right-hand pane.

Destination	Distance	Route	Flags	Gateway	Interface	Metric
10.0.0.0/8	1	10.0.0.0/8	Static	10.233.89.253	vlan10	0
10.233.89.0/24	0	10.233.89.0/24	Connected	0.0.0.0	vlan10	0
157.0.0.0/8	1	157.0.0.0/8	Static	10.233.89.253	vlan10	0
172.16.1.0/24	1	172.16.1.0/24	Static	3.0.0.1	vlan3	0
172.168.1.0/24	0	172.168.1.0/24	Connected	0.0.0.0	vlan5	0
172.168.11.0/24	0	172.168.11.0/24	Connected	0.0.0.0	vlan174	0
172.168.7.0/24	0	172.168.7.0/24	Connected	0.0.0.0	vlan4	0
192.168.1.0/24	0	192.168.1.0/24	Connected	0.0.0.0	vlan1	0
3.0.0.0/24	0	3.0.0.0/24	Connected	0.0.0.0	vlan3	0
default	1	0.0.0.0/0	Static	172.168.7.200	vlan4	0

Type to search in tables Row Count: 10

**Refresh**

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.

7 Select the **IPv6 Route Entries** tab to review route data for IPv6 formatted traffic.

The **IPv6 Route Entries** stats display in the right-hand pane.



IPv4 Route Entries		IPv6 Route Entries	
Destination	Gateway	Interface	Flag

Type to search in tables

Row Count: 0

Refresh

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.

- 8 Select **Refresh** to update the display to the latest values.

### Default Routes

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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Network** menu from the left-hand side of the UI.

6 Select **Default Routes**.

The **Statistics > Controller > IPv4 Default Routes** stats is displayed by default in the right-hand pane.

IPv4 Default Routes		IPv6 Default Routes				
DNS Server	Gateway Address	Installed	Metric	Monitor Mode	Source	Monitoring Status
	157.235.95.2	✓	100	gateway-monitoring	Static-Route	reachable

Type to search in tables Row Count: 1

**Refresh**

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	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.

7 Select the **IPv6 Default Routes** tab to review default route availabilities for IPv6 formatted traffic.

The **IPv6 Default Routes** stats is displayed by default in the right-hand pane.

IPv4 Default Routes
IPv6 Default Routes

Gateway Address <small>⊕</small>	Installed	Interface Name	Lifetime	Preference	Source	Status

Row Count: 0

Refresh

The IPv6 Default Routes stats is displayed by default in the right-hand pane.

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.

8 Select **Refresh** to update the display to the latest values.

*Bridge*

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 are very similar, since a controller is a bridge with a number of ports.

To view network bridge information:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Network** menu from the left-hand side of the UI.
- 6 Select **Bridge**.

The **Statistics > Controller > Bridge** stats is displayed in the right-hand pane.

Bridge Name	MAC Address	Interface	VLAN	Forwarding
1	00-0F-8F-19-BA-4C	ge1	1	forward
1	00-15-70-38-06-49	ge1	1	forward
1	00-15-70-81-74-2D	ge1	1	forward
1	00-23-68-88-0D-A7	ge1	1	forward
1	5C-0E-8B-18-10-91	ge1	1	forward
1	3C-CE-73-F4-47-83	ge1	1	forward
1	00-23-68-99-BB-7C	ge1	1	forward
1	00-A0-F8-68-D5-5D	ge1	1	forward
1	00-15-70-37-FD-F2	ge1	1	forward
1	00-23-68-13-9B-34	ge1	1	forward
1	00-23-68-0F-43-D8	ge1	1	forward
1	00-02-B3-28-D1-55	ge1	1	forward

Type to search in tables

Row Count: 12

Refresh

This 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 network.
Forwarding	Displays whether the bridge is forwarding packets and in a forwarding state.

- 7 Select **Refresh** to update the statistics counters to the latest values.

### IGMP

IGMP (Internet Group Management Protocol) 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 statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Network** menu from the left-hand side of the UI.
- 6 Select **IGMP**.

The **Statistics > Controller > IGMP** stats is displayed in the right-hand pane.

Group			
VLAN	Group Address	Port Members	Version

Multicast Router (MRouter)					
VLAN	Learn Mode	Port Members	Mint IDs	Query Interval	Version
10	pim-dvmrp	ge2		10	3

[Refresh](#)

The **Group** field describes the following:

<b>VLAN</b>	Displays the group VLAN where the multicast transmission is conducted.
<b>Group Address</b>	Displays the Multicast Group ID supporting the statistics displayed. This group ID is the multicast address hosts are listening to.
<b>Port Members</b>	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.
<b>Version</b>	Displays each listed group IGMP version compatibility as either version 1, 2 or 3.

The **Multicast Router (MRouter)** field describes the following:

<b>VLAN</b>	Displays the group VLAN where the multicast transmission is conducted.
<b>Learn Mode</b>	Displays the learning mode used by the router as either <b>Static</b> or <b>PIM-DVMRP</b> .
<b>Port Members</b>	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.

<b>MiNT IDs</b>	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.
<b>Query Interval</b>	Lists the IGMP query interval implemented when the querier functionality is enabled. The default value is 60 seconds.
<b>Version</b>	Lists the multicast router IGMP version compatibility as either version 1, 2 or 3. The default setting is 3.

- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

## MLD

MLD (Multicast Listener Discovery) 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 statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Network** menu from the left-hand side of the UI.
- 6 Select **MLD**.

The **Statistics > Controller > MLD** stats is displayed in the right-hand pane.

Multicast Listener Discovery (MLD) Group				
VLAN	Group Address	Port Members	Version	

IPv6 Multicast Router (MRouter)						
VLAN	MINT IDs	Learn Mode	Port Members	Query Interval	Version	

[Refresh](#)

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 <b>Static</b> or <b>PIM-DVMRP</b> .
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.

- 7 Select **Refresh** to update the screen’s statistics counters to their latest values.

LACP

LACP (Link Aggregation Control Protocol) 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 LAGs (link aggregation groups). 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 the LACP statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **LACP**.

The **Statistics > Controller > System and Aggregator Statistics** tab displays by default in the right-hand pane.

System and Aggregator Statistics		Aggregator Details					
System							
System Identifier	B4-C7-99-6C-88-09						
System Priority	2						
Aggregator Statistics							
Aggregator Name	Interface	LACPDU Sent	LACPDU Received	Marker Sent	Marker Received	Packets Error Sent	Packet Error Receive
pc1	ge2	11,877	0	0	0	0	0
Refresh							

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 LACPDU (Link Aggregation Control Protocol Data Units) sent from this device.
LACPDU Received	Displays the number of LACPDU 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.

6 Select the **Aggregator Details** tab. This field describes the following:

The screenshot shows a web interface with two tabs: "System and Aggregator Statistics" and "Aggregator Details". The "Aggregator Details" tab is active. Below the tabs is a table with the following structure:

	Aggregator Name	Interface	MAC Address	MUX machine state
➕	pc1	ge2	00-1E-67-4B-BF-BD	Attached

Below the table is a search bar labeled "Type to search in tables" and a "Row Count: 1" indicator. A "Refresh" button is located at the bottom right of the interface.

Aggregator Name	Displays the name of the 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	<p>Displays the state of the multiplexer state machine for the aggregation port. The values are:</p> <ul style="list-style-type: none"> <li>• <b>attached</b> - Displays the state as attached, when the multiplexer state machine is initiating the process of attaching the port to the selected aggregator.</li> <li>• <b>detached</b> - Displays the state as detached, when the multiplexer state machine is initiating the process of detaching the port from the aggregator.</li> <li>• <b>collecting/distributing</b> - 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.</li> </ul>

- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

### Traffic Shaping

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.

- [Traffic Shaping - Status](#) on page 1090.
- [Traffic Shaping - Statistics](#) on page 1090.

#### Traffic Shaping - Status

To view network the controller or service platform's traffic shaping status:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select the **Wireless Controller** node from the left navigation pane.
- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **Traffic Shaping**.

The **Statistics > Controller > Traffic Shaping > Status** screen displays by default.

The status screen simply lists the controller or service platform's current traffic shaping operational status.

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

#### Traffic Shaping - Statistics

To view network the controller or service platform's traffic shaping statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select the **Wireless Controller** node from the left navigation pane.
- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **Traffic Shaping**.

The **Status** screen displays by default.

- 6 Select the **Statistics** tab.

The **Statistics > Controller > Traffic Shaping > Statistics** screen displays.

Priority	Packets Sent	Packets Delayed	Packets Dropped	Current Queue Length	Current Latency (In Micro Seconds)
0	0	0	0	0	0
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0

This screen displays the following information:

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.

7 Select **Refresh** to update the screen’s statistics counters to their latest values.


*DHCP Options*

Controllers and service platforms contain an internal DHCP (Dynamic Host Configuration Protocol) server. The DHCP server can provide the dynamic assignment of IP addresses automatically to requesting clients. 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Network** menu from the left-hand side of the UI.
- 6 Select **DHCP Options**.

The **Statistics > Controller > Network > DHCP Options** screen displays.

Server Information 	Image File	Configuration	Legacy Adoption	Adoption
n/a	n/a	n/a	n/a	pool1=172.168.7.197,172.168.7.10;level=2

Type to search in tables Row Count: 1



This 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 on behalf of the access point.
Adoption	Displays pending (current) adoption information on behalf of an access point.

- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

### Cisco Discovery Protocol

CDP (Cisco Discovery Protocol) is a proprietary Data Link Layer network protocol implemented in Cisco networking equipment and used to share information about network devices.

To view a selected controller's or service platform's CDP Statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Network** menu from the left-hand side of the UI.
- 6 Select **Cisco Discovery Protocol**.

The **Statistics > Controller > Network > Cisco Discovery Protocol** screen displays in the right-hand pane.

	Capabilities	Device ID	Local Port	Platform	Port ID	TTL
▼	router	ap6522-5A842C	ge1	AP-6522-66040-WR	ge1	176
▼	router	ap6521-970CC6	ge1	AP-6521-60010-WR	ge1	173
▼	switch igmp_cap rol	Switch	ge2	cisco WS-C3560-24I	FastEthernet04	150
▼	switch router	rx9500-6C86ED	ge1	NX-9500-100R0-WR	ge1	178
▼	switch router	ap7181-8DFE4C	ge1	AP7181	ge1	168

Type to search in tables Row Count: 5

This screen displays the following:

Capabilities	Displays the capabilities code for CISCO neighbors as either <b>Router, Trans Bridge, Source Route Bridge, Switch, Host, IGMP</b> or <b>Repeater</b> .
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 TTL (time to live) for each CDP connection.

- 7 Click **Clear Neighbors** to remove all known CDP neighbors from the table.
- 8 Select **Refresh** to update the screen's statistics counters to their latest values.

*Link Layer Discovery Protocol*

The LLDP (Link Layer Discovery Protocol) 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 Link Layer Discovery Protocol statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **Link Layer Discovery Protocol**.

The **Statistics > Controller > Network > Link Layer Discovery Protocol** screen displays in the right-hand pane.

Capabilities	Device ID	Enabled Capabilities	Local Port	Platform	Port ID	TTL
bridge wlan_ap rc	ap6522-084522	bridge wlan_ap rc	up1	AP-6522-60010-L	5C-0E-8B-08-45-22	121

Type to search in tables Row Count: 1

This screen displays the following:

Capabilities	Displays a capabilities code as either <b>Router, Trans Bridge, Source RouteBridge, Switch, Host, IGMP</b> or <b>Repeater</b> .
Device ID	Displays the configured device ID or name for each device in the table.
Enabled Capabilities	Displays which capabilities are currently in utilization by the listed device.
Local Port	Displays the local port name for each LLDP capable device.
Platform	Displays the model number of the LLDP capable device.

Port ID	Displays the identifier for the local port.
TTL	Displays the TTL (time to live) for each LLDP connection.

- 6 Select **Clear Neighbors** to remove all known LLDP neighbors from the table.
- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

### *IPv6 Neighbor Discovery*

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 NA (neighbor advertisement). 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Network** menu from the left-hand side of the UI.
- 6 Select **IPv6 Neighbor Discovery**.

The **Statistics > Controller > Network > IPv6 Neighbor Discovery** screen is displayed in the right-hand pane.

IPv6 Address	MAC Address	Type	VLAN

Type to search in tables Row Count: 0

[Refresh](#)

This 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 <b>Host</b> , <b>Router</b> and <b>DHCP Server</b> .
VLAN	Lists the virtual interface (from 1 - 4094) used for the required neighbor advertisements and solicitation messages used for neighbor discovery.

- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

### Fabric Attach

Displays the current status of FA (Fabric Attach) VLAN to Individual Service Identifier (I-SID) assignments for all ports.

To view a controller or service platform's FA statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select a **Wireless Controller/Service Platform** node from the left navigation pane.
- 3 Expand the **Network** menu from the left-hand side of the UI.





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 BPDU (Bridge Protocol Data Unit) 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Network** menu from the left-hand side of the UI.
- 6 Select **MSTP**.

The **Statistics > Controller > Network > MSPT** stats is displayed in the right-hand pane.

The screenshot shows three sections of a network management interface:

- MST Config:** A table with two columns: 'CFG Name' and 'My Name'. The values are: Digest: 0xac36177f50283cd4b83821d8ab26de62, Format ID: 0, Name: 1, Revision: 0.
- MST Bridge:** A table with columns: BPDU Filter, BPDU Guard, Bridge Admin Cisco, Bridge Enabled, Bridge Oper Cisco, CIST Bridge ID, CIST Bridge Priority, and CIST Reg Root ID. The first row shows: BPDU Filter (green down arrow), BPDU Guard (red X), Bridge Admin Cisco (red X), Bridge Enabled (red X), Bridge Oper Cisco (red X), CIST Bridge ID: 1: CIST Brk, CIST Bridge Priority: 32,768, CIST Reg Root ID: 1: CIST Reg Root Id E.
- MST Bridge Port Detail:** A table with columns: Name, Role, Send MSTP, State, Type, Admin BPDU Filter, Admin BPDU Guard, Admin Edge, Admin P2P MAC, and Admin Root Guard. The first four rows show:
 

Name	Role	Send MSTP	State	Type	Admin BPDU Filter	Admin BPDU Guard	Admin Edge	Admin P2P MAC	Admin Root Guard
ge1	4	MSTP	Forwan	0	2	2	red X	red X	red X
ge10	4	STP	Forwan	0	2	2	red X	red X	red X
ge2	4	MSTP	Forwan	0	2	2	red X	red X	red X
ge3	4	MSTP	Forwan	0	2	2	red X	red X	red X

A 'Refresh' button is located at the bottom right of the interface.

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.

- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

## DHCPv6 Relay & Client

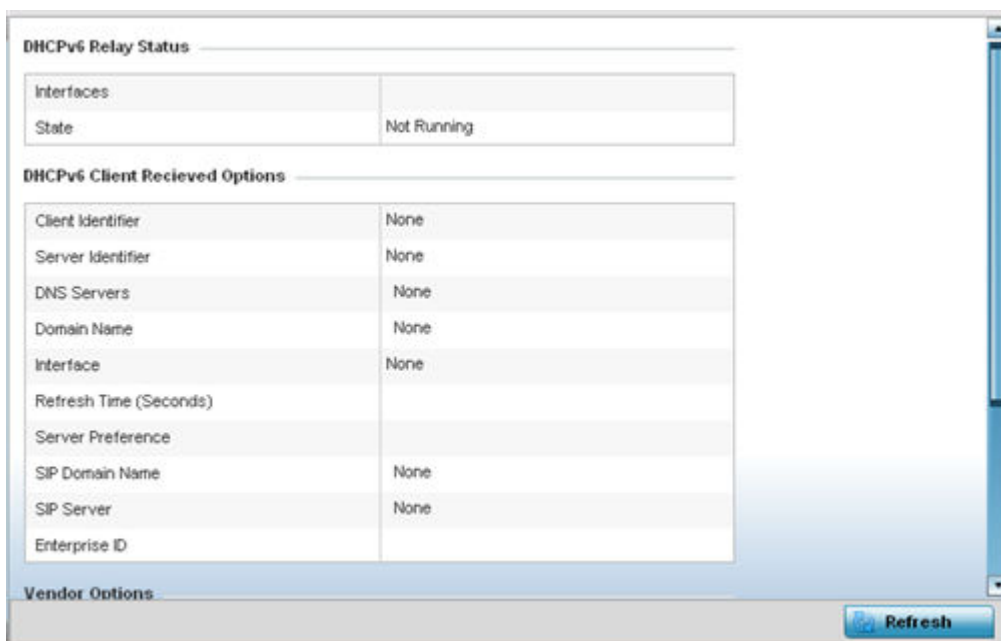
DHCPv6 is a networking protocol for configuring IPv6 hosts with IP addresses, IP prefixes or other configuration attributes required on an IPv6 network. DHCPv6 relay agents receive messages from clients and forward them a DHCPv6 server. The server sends responses back to the relay agent and the relay agent sends the responses to the client on the local link.

To view the controller or service platform's DHCPv6 relay configuration:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.

- 4 Select the **Wireless Controller** node from the left navigation pane.
- 5 Select **DHCP Relay & Client** from the left-hand side of the UI.

The **Statistics > Controller > DHCP Relay & Client** screen displays in the right-hand pane.



The **DHCP Relay Status** table 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.

The **DHCPv6 Client Received Options** table defines the following:

Client Identifier	Lists whether the reporting client is using a <i>hardware address</i> or <i>client identifier</i> 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.

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.

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

## DHCP Server

Controllers and service platforms contain an internal DHCP (Dynamic Host Configuration Protocol) server. DHCP can provide IP addresses automatically to requesting devices. 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](#)

### *Viewing General DHCP Information*

To view **General** DHCP status and binding information:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **DHCP Server** menu from the left-hand side of the UI.

The **Statistics > Controller > DHCP Server > General** screen displays by default in the right-hand pane.

DHCPv4 Status	
Interfaces	vlan1,vlan4,vlan174
State	Running

DHCPv6 Status	
Interfaces	
State	Not Running

DDNS Bindings	
IP Address	Name

[Refresh](#)

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.

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.

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.

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

### Viewing DHCP Binding Information

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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **DHCP Server** menu from the left-hand side of the UI.
- 6 Select **Bindings**.

The **Statistics > Controller > DHCP Server > Bindings** screen displays by default in the right-hand pane.

Expiry Time	IP Address	DHCP MAC Address
Wed Dec 9 17:23:10 2015	172.168.7.197	00-06-F6-69-60-C2
Thu Dec 10 00:38:37 2015	172.168.7.198	B4-C7-99-6C-86-ED

Type to search in tables Row Count: 2

This screen displays the following:

Expiry Time	Displays the expiration of the lease used by the devices requesting controller or service platform DHCP resources.
IP Address	Displays the IP address of each listed device requesting DHCP services.
DHCP MAC Address	Displays the MAC address of each device requesting DHCP services.

- 7 Select a table entry and select **Clear** to remove the client from the list of devices requesting DHCP services.
- 8 Select **Clear All** to remove all listed clients from the list of requesting clients.
- 9 Select the **Refresh** button to update the screen's statistics counters to their latest values.

#### *Viewing DHCP Server Networks Information*

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 computer an IP address, a lease (the validity of time), and other IP configuration parameters.

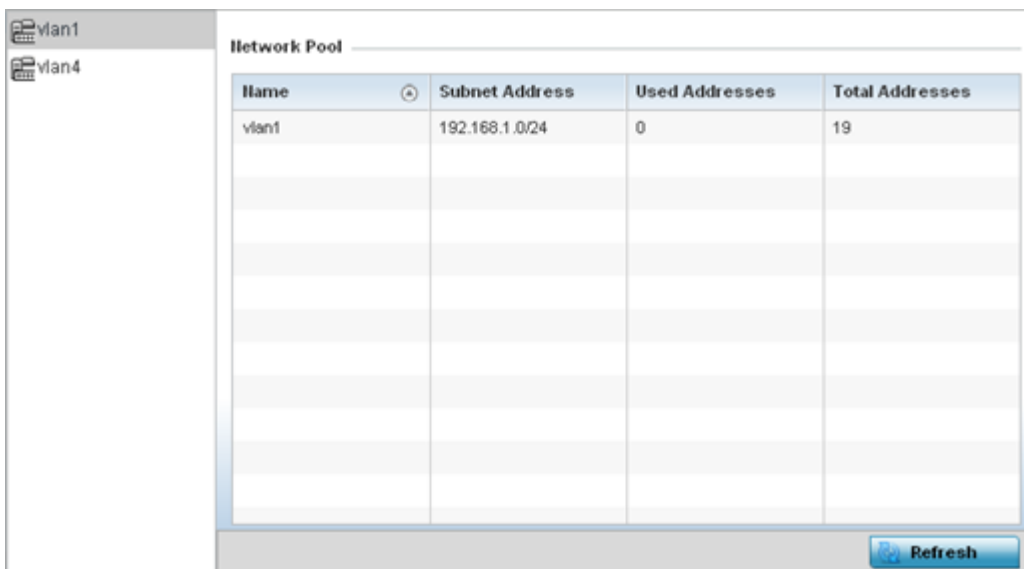
The **Networks** screen provides network pool information, such as the subnet for the addresses you want to lease from the pool, the pool name, used addresses and the total number of addresses available for lease to a requesting client.

To view the DHCP Server's Networks information:



- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **DHCP Server** menu from the left-hand side of the UI.
- 6 Select **Networks**.

The **Statistics > Controller > DHCP Server > Networks** screen displays in the right-hand pane.



This screen displays the following:

Name	Displays the name of the virtual network 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.

- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

## Firewall

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:

- [Viewing Packet Flow Statistics](#)
- [Viewing Denial of Service Statistics](#)
- [IP Firewall Rules](#)
- [MAC Firewall Rules](#)



- [NAT Translations](#)
- [Viewing DHCP Snooping Statistics](#)

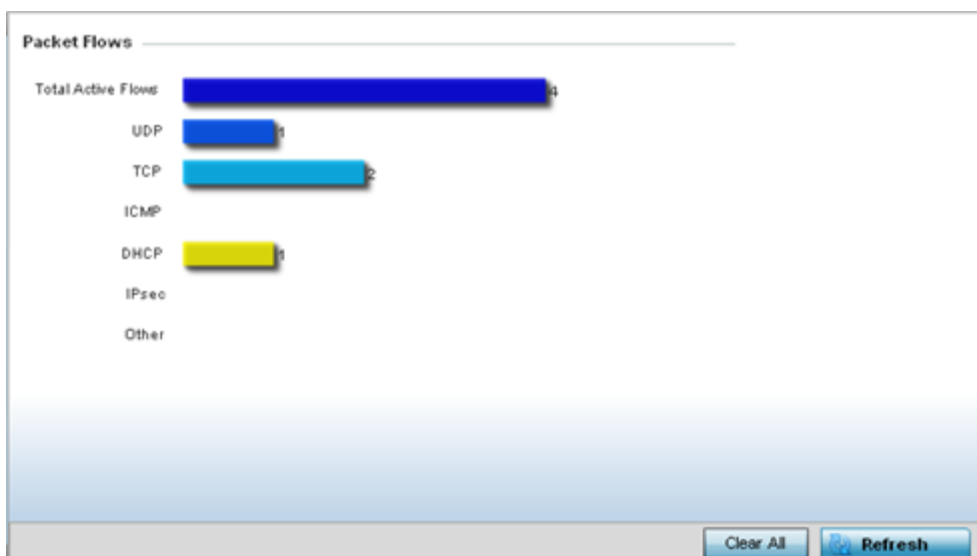
### Viewing Packet Flow Statistics

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.

To view the packet flow statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Firewall** menu from the left-hand side of the UI.
- 6 Select **Packets Flows**.

The **Statistics > Controller > Firewall > Packet Flows** screen displays in the right-Hand pane.



- 7 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.

### Viewing Denial of Service Statistics

A DoS attack (denial-of-service 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Firewall** menu from the left-hand side of the UI.
- 6 Select **Denial of Service**.

The **Statistics > Controller > Firewall > Denial of Service** screen displays in the right-hand pane.

Attack Type	Count	Last Occurrence
Ascend	5	12 days 20:36:15 ago
Broadcast/Multicast ICMP	0	Never
Chargen	0	Never
Fraggle	11	12 days 20:34:33 ago
FTP Bounce	0	Never
Router Solicit	0	Never
Invalid Protocol	0	Never
LAND	0	Never
Router Advertisement	0	Never
Smurf	0	Never
Snork	0	Never
Source Route	0	Never
IP Spoof	0	Never

Type to search in tables Row Count: 25

This screen displays the following:

Attack Type	Displays the DoS attack type. Controllers and service platforms support <b>enabling</b> or <b>disabling</b> 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 when the DoS attack was last observed by the controller or service platform's firewall.

- 7 Select **Clear All** to revert the statistics counters to zero and begin a new data collection.
- 8 Select the **Refresh** button to update the screen's statistics counters to their latest values.

### IP Firewall Rules

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:



### IPv6 Firewall Rules

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 ND (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.

Firewall rules can use one of the three following actions based on a rule criteria:

- 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 a controller or service platform's existing IPv6 firewall rules:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Firewall** menu from the left-hand side of the UI.
- 6 Select **IPv6 Firewall Rules**.

The **Statistics > Controller > Firewall > IPv6 Firewall Rule** screen displays in the right-hand pane.

Precedence	Friendly String	Hit Count

Refresh

This screen displays the following information:

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.

7 Select **Refresh** to update the screen’s statistics counters to their latest values.

### MAC Firewall Rules

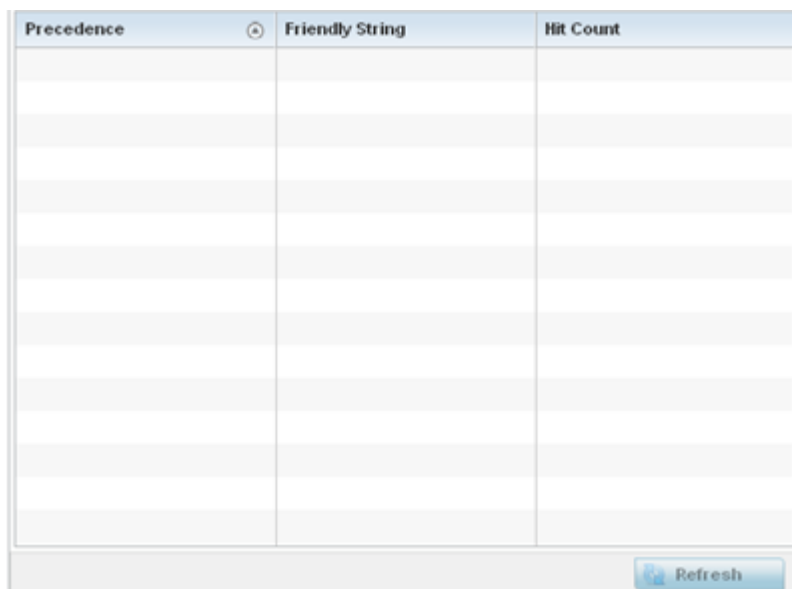
The ability to **allow** or **deny** client access by MAC address ensures malicious or unwanted users are unable to bypass security filters. Firewall rules can use one of the three following actions based on a rule criteria:

- Allow a connection.
- Allow a connection only if it is secured through the MAC firewall security.
- Block a connection.

To view a controller or service platform’s MAC firewall rules:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Firewall** menu from the left-hand side of the UI.
- 6 Select **MAC Firewall Rules**.

The **Statistics > Controller > Firewall > MAC Firewall Rules** screen displays in the right-hand pane.



This screen displays the following:



Precedence	Displays the precedence value, which are applied to packets. The rules within an ACL (Access Control Entries) 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.

- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

### *NAT Translations*

NAT (Network address translation ) 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 a controller or service platform's NAT statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Firewall** menu from the left-hand side of the UI.
- 6 Select **NAT Translations**.

The **Statistics > Controller > Firewall > NAT Translations** screen displays in the right-hand pane.

	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	128.83.2.53	53	128.83.2.53	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

Type to search in tables Row Count: 112

[Refresh](#)

This screen displays the following information:

Protocol	Displays the IP translation protocol as either <b>TCP</b> , <b>UDP</b> or <b>ICMP</b> .
Forward Source IP	Displays the internal network IP address for forward facing NAT translations.
Forward Source Port	Displays the internal network 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.

- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

### DHCP Snooping Statistics

When DHCP servers are allocating IP addresses to requesting clients, DHCP snooping can further strengthen the security on the LAN by allowing only clients with specific IP/MAC addresses.

To view the DHCP snooping statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.

- 5 Expand the **Firewall** menu from the left-hand side of the UI.
- 6 Select **DHCP Snooping**.

The **Statistics > Controller > Firewall > DHCP Snooping** screen displays in the right-hand pane.

	MAC Address	Node Type	IP Address	Netmask	VLAN	Lease Time	Time Elapsed Since Last Update
▼	00-00-00-00-00-00	Router	192.168.0.13		10		7h 36m 39s
▼	00-0C-29-84-F3-1	dhcp-client	192.168.0.217	22	10	6h 0m 0s	56m 21s
▼	00-0C-29-84-F3-1	dhcp-client	192.168.0.142	22	10	6h 0m 0s	56m 53s
▼	00-0C-29-84-F3-1	dhcp-client	192.168.0.219	22	10	6h 0m 0s	56m 18s
▼	00-0C-29-84-F3-1	dhcp-client	192.168.0.226	22	10	6h 0m 0s	56m 23s
▼	00-0C-29-84-F3-1	dhcp-client	192.168.0.209	22	10	6h 0m 0s	56m 21s
▼	00-0C-29-84-F3-1	dhcp-client	192.168.0.239	22	10	6h 0m 0s	56m 52s
▼	00-0C-29-84-F3-1	dhcp-client	192.168.0.225	22	10	6h 0m 0s	56m 22s
▼	00-0C-29-84-F3-1	dhcp-client	192.168.0.129	22	10	6h 0m 0s	56m 19s
▼	00-0C-29-84-F3-1	dhcp-client	192.168.0.213	22	10	6h 0m 0s	56m 20s
▼	00-0C-29-84-F3-1	dhcp-client	192.168.0.224	22	10	6h 0m 0s	56m 17s
▼	00-12-3F-86-99-1	dhcp-client	192.168.0.144	22	10	6h 0m 0s	32m 44s
▼	00-12-3F-86-99-1	dhcp-client	192.168.0.158	22	10	6h 0m 0s	32m 45s

Type to search in tables Row Count: 33

This screen displays the following information:

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 requesting 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.

- 7 Select **Clear All** to revert the counters to zero and begin a new data collection.
- 8 Select **Refresh** to update the screen's counters to their latest values



### IPv6 Neighbor Snooping

IPv6 snooping bundles layer 2 IPv6 hop security features, such as IPv6 ND (neighbor discovery) 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 Expand the **RF Domain** node.
- 3 Select a **Wireless Controller**.
- 4 Expand the **Firewall** menu from the left-hand side of the UI.
- 5 Select **IPv6 Neighbor Snooping**.

The **Statistics > Controller > Firewall > IPv6 Neighbor Snooping** screen displays in the right-hand pane.

MAC Address	Node Type	IPv6 Address	VLAN	Mint Id	Snoop Id	Time Elapsed Since Last Update
10-0B-A9-35-B3-C	ipv6	fe80::11c2:5073:6a...	30	4D.84.A2.70	8,896	6s
24-77-03-9D-5B-2f	tentative,ipv6	fe80::9cb9:9f20:6e...	30		6,880	3m 59s
30-F7-C5-4F-31-2f	tentative,ipv6	fe80::d5:3c9e:223...	666		5,856	1m 30s
44-6D-57-08-1A-D	ipv6	fe80::d1d0:2904:2...	30	4D.18.84.BC	9,984	11s
60-67-20-A5-B8-2	tentative,ipv6	fe80::4c41:8be:cc...	30		1,664	2m 21s
6C-71-D9-54-92-1f	ipv6	fe80::c5e9:48af:a...	100	4D.84.A2.70	10,560	14s
78-FD-94-05-8C-0	tentative,ipv6	fe80::10e4:458d:8...	666		4,736	3m 51s
84-3A-4B-AC-68-5	ipv6	fe80::6135:21a7:b...	30		6,400	32m 28s
84-3A-4B-AC-68-5	ipv6	2601:646:8d00:b1...	30		14,208	32m 28s
8C-70-5A-B5-60-D	ipv6	fe80::dd98:fb6:a...	30	4D.84.A2.70	5,857	1s
B4-B6-76-AC-EC-2	tentative,ipv6	fe80::794a:fb8f:78...	30		9,312	4m 59s
C4-D9-87-38-A6-7	ipv6	fe80::6d2a:ed2f:2c...	30		6,272	5m 23s
CC-3D-82-82-2B-C	ipv6	fe80::b01d:c01c:c...	30		544	43m 54s
E4-1F-13-6A-5C-6	ipv6	fe80::a8f3:2769:7...	6		7,968	3m 44s
F8-16-54-7B-1E-Ef	tentative,ipv6	fe80::98c0:60fa:7...	30		9,688	3m 10s

Type to search in tables Row Count: 16

This screen displays the following information:

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.

- 6 Select **Clear Neighbors** to revert the counters to zero and begin a new data collection.
- 7 Select **Refresh** to update the screen's counters to their latest values.

## VPN

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 tunneled 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 SA (security associations) between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunneled 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.

The IKE (Internet Key Exchange) 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**

### IKESA

The **IKESA** screen allows for the review of individual peer security association statistics.

To view controller or service platform's IKESA statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.

- 4 Select a **Wireless Controller**.
- 5 Expand the **VPN** menu.
- 6 Select **IKESA**.

The **Statistics > Controller > VPN > IKESA** screen displays in the right-hand pane.

Peer	Version	State	Lifetime	Local IP Address
172.168.7.197	IKEv2	ESTABLISHED	8,352	172.168.6.137

Type to search in tables Row Count: 1

Review the following VPN peer security association statistics:

Peer	Lists peer IDs for peers sharing 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 SA (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.

- 7 Select a IKE peer configuration and click **Clear** to remove the peer from the table.
- 8 Select **Clear All** to clear each peer of its current status and begin a new data collection.
- 9 Select **Refresh** to update the screen's statistics counters to their latest values.

### IPSec


IPSec 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.

Use the IPSec VPN screen to assess the tunnel status between networked peers.

To view IPSec VPN status for tunneled peers:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **VPN** menu.
- 6 Select **IPSec**.

The **Statistics > Controller > VPN > IPSec** screen displays in the right-hand pane.

Peer	Local IP Address	Protocol	State	SPI In	SPI Out	Mode
 172.168.7.197	172.168.6.137	esp	VALID	C99E4AAB	A9DC8ACE	Tunnel

Type to search in tables Row Count: 1

Review the following VPN peer security association statistics:

Peer	Lists IP addresses for peers sharing 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 <b>ESP</b> and <b>AH</b> .
State	Lists the state of each listed peer's security association.
SPI In	Lists SPI (stateful packet inspection) 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 as either <b>Main</b> or <b>Aggressive</b> . IPSec has two modes in IKEv1 for key exchanges. The Aggressive mode requires three messages be exchanged between the IPSEC peers to setup the SA. The Main mode requires six messages.

- 7 Select **Clear All** to clear each peer of its current status and begin a new data collection.
- 8 Select **Refresh** to update the screen's statistics counters to their latest values.

## Certificate Statistics

The SSL (Secure Socket Layer) protocol ensures 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:

- [Trustpoints](#) on page 1117
- [RSA Key Details](#) on page 1119

### *Trustpoints*

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 trustpoint statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Certificate** menu.
- 6 Select **Trustpoint**.

The **Statistics > Controller > Certificates > Trustpoints** screen displays in the right-hand pane.

The screenshot shows a web interface for 'default-trustpoint' with a 'Certificate Details' section. The details are as follows:

Subject Name	CN=NX9000-B4-C7-99-0C-98-48
Alternate Subject Name	
Issuer Name	CN=NX9000-B4-C7-99-0C-98-48
Serial Number	5d
RSA Key Used	default_rsa_key
IS CA	<span style="color: red;">✗</span> No
Is Self Signed	<span style="color: green;">✓</span> Yes
Server Certificate Present	<span style="color: green;">✓</span> Yes
CRL Present	<span style="color: red;">✗</span> No

Below this is the 'Validity' section:

Valid From	02:02:2013 18:31:49 UTC
Valid Until	01:31:2023 18:31:49 UTC

At the bottom is the 'Certificate Authority (CA) Details' section, which is currently empty.

This screen has the following elements:

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 ( <b>Yes/No</b> ).
Is Self Signed	Displays whether the certificate is self-signed ( <b>Yes/No</b> ).

Server Certification Present	Displays whether a server certification is present or not ( <b>Yes/No</b> ).
CRL Present	Displays whether a CRL ( <i>Certificate Revocation List</i> ) is present ( <b>Yes/No</b> ). 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.
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 <i>Subject Name</i> 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 began.
Validity Until	Displays the date when the validity of a CA expires.

Review the *Certificate Authority (CA) Details* and *Validity* information to assess the subject and certificate duration periods.

- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

### RSA Key Details

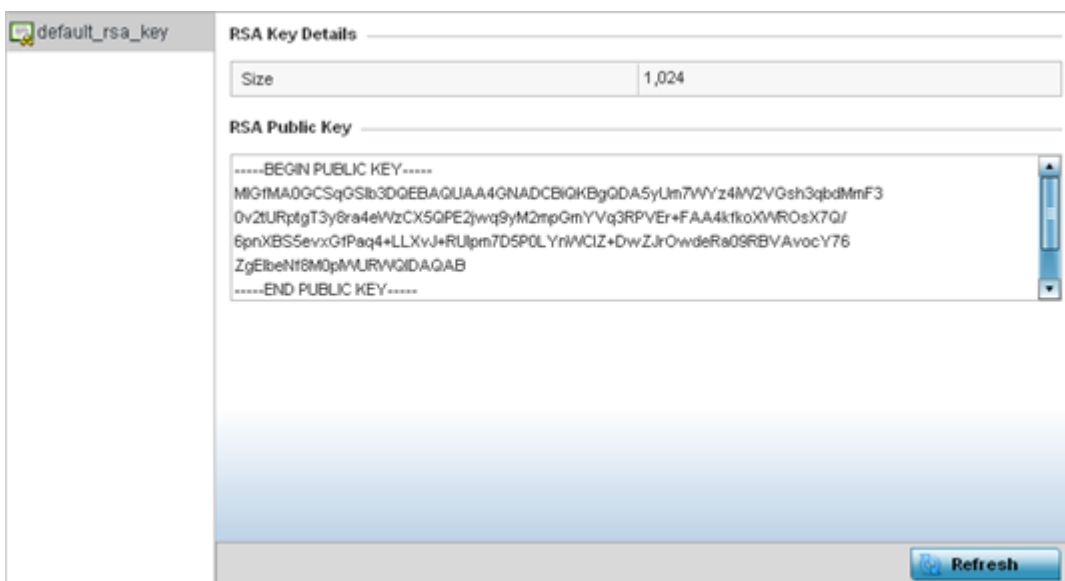
RSA (Rivest, Shamir, and Adleman) is an algorithm for public key cryptography. It's the first algorithm known to be suitable for signing as well as encryption.

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 controller or service platform's RSA Key details:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Certificate** menu.
- 6 Select **RSA Keys**.

The **Statistics > Controller > Certificates > RSA Key** screen displays.



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 used for encrypting messages. This key is known to everyone.

- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

## WIPS Statistics

A WIPS (*Wireless Intrusion Protection System*) 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:

- [Client Blacklist](#) on page 1120
- [WIPS Event Statistics](#) on page 1121

### *Client Blacklist*

The **Client Blacklist** screen 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 controller or service platform's client blacklist screen:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.



- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **WIPS** menu.
- 6 Select **Client Blacklist**.

The **Statistics > Controller > WIPS > Client Blacklist** screen displays in the right-hand pane.

Event Name	Blacklisted Client	Time Blacklisted	Total Time	Time Left
dos-espwl-start-storm	44-55-44-55-44-55	Thu Jun 10 2012 12:26:26	2h 0m 0s	1h 0m 0s
null-probe-response	44-55-44-55-44-55	Thu Jun 10 2012 12:26:26	40m 0s	20m 0s

Type to search in tables Row Count: 2

[Refresh](#)

This screen displays the following:

<b>Event Name</b>	Displays the name of the detected wireless intrusion resulting in a blacklisting of the client from controller or service platform resources.
<b>Blacklisted Client</b>	Displays the MAC address of the intruding client device pending exclusion from the controller or service platform managed network.
<b>Time Blacklisted</b>	Displays the time this client was blacklisted from interoperating with known and trusted devices within the wireless network.
<b>Total Time</b>	Displays the duration the unauthorized device remained in the WLAN before being blacklisted.
<b>Time Left</b>	Displays the time the blacklisted client remains on the list.

- 7 Select **Refresh** to update the screen’s statistics counters to their latest values.

*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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **WIPS** menu.
- 6 Select **WIPS Events**.

The **Statistics > Controller > WIPS > WIPS Events** screen displays in the right-hand pane.

Event Name	Reporting AP	Originating Device	Detector Radio	Time Reported
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Wed May 27 2015 08:08:39 PM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Wed May 27 2015 10:16:36 AM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Wed May 6 2015 04:24:30 AM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Wed May 27 2015 03:14:12 AM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Tue May 26 2015 08:03:12 PM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Tue May 26 2015 08:01:12 PM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Tue May 26 2015 10:47:57 AM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Wed May 6 2015 10:53:57 AM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Tue May 26 2015 03:07:07 AM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Mon May 25 2015 08:10:27 PM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Mon May 25 2015 10:59:44 AM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	60-03-08-A7-93-E0	1	Fri May 15 2015 01:22:14 AM

Type to search in tables Row Count: 97

This screen displays the following information:

Event Name	Displays the name of the detected intrusion event.
Originating Device	Displays the MAC address of the intruder device.
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.
Detector Radio	Displays which AP radio is making the intrusion detection.
Time Reported	Displays the time when the intrusion event was detected.

- 7 Select **Clear All** to reset the statistics counters to zero and begin a new data collection.
- 8 Select **Refresh** to update the screen's statistics counters to their latest values.

## Sensor Server

Sensor servers allow the monitor and download of device authorization data from multiple sensors and remote locations using Ethernet, TCP/IP or serial connections. Repeaters are available to extend the transmission range and combine sensors with various frequencies on the same receiver, thus extending the Advanced WIPS supported reporting range.

To view the Sensor Server statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Select **Sensor Servers** from the left-hand side of the UI.

The **Statistics > Controller > Sensor Servers** screen displays.

IP Address/Hostname	Port	Status
	0	no server defined
	0	no server defined
157.235.95.128	443	online

Type to search in tables Row Count: 3

[Refresh](#)

This screen displays the following:

IP Address	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 currently <b>connected</b> or <b>not connected</b> .

- 6 Select **Refresh** to update the screen’s statistics counters to their latest values

## Bonjour Services

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 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Select **Bonjour Services** from the left-hand side of the UI.

The **Statistics > Controller > Bonjour Services** screen displays.

Service Name	Instance Name	IP Address	Port	Vlan	Vlan Type	Expiry
_airplay_tcp.local	Apple TV (2)_airplay_tcp	32.32.32.101	7,000	32	Local	Sun Mar 9 00:59:04 2014
_ipp_tcp.local	Brother MFC-8510DN_ipp	32.32.32.103	631	32	Local	Sun Mar 9 01:41:34 2014
_ipp_tcp.local	HP MFP M425dn Service Z	32.32.32.106	631	41	Local	Sun Mar 9 01:13:46 2014
_ipp_tcp.local	HP MFP M425dn Service ;	32.32.32.106	631	32	Local	Sun Mar 9 00:56:34 2014
_rsoop_tcp.local	B8782E20922E@Apple TV	32.32.32.101	5,000	32	Local	Sun Mar 9 00:59:04 2014
_universal_sub_ipp_tcp	Brother MFC-8510DN_ipp	32.32.32.103	631	32	Local	Sun Mar 9 01:41:34 2014
_universal_sub_ipp_tcp	HP MFP M425dn Service ;	32.32.32.106	631	32	Local	Sun Mar 9 00:56:34 2014

Type to search in tables Row Count: 7

[Refresh](#)

Refer to the following Bonjour service utilization stats:

Service Name	Lists the services discoverable by the Bonjour gateway. Services can either be <i>pre-defined</i> 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 <i>local</i> bridging mode or a <i>shared tunnel</i> .
Expiry	Lists the expiration date of the listed Bonjour service, and its availability to discover resources on the LAN.

- 6 Select **Refresh** to update the screen’s statistics counters to their latest values.

## Captive Portal 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 captive portal statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **WIPS** menu.
- 6 Select **Captive Portal** from the left-hand side of the controller UI.

The **Statistics > Controller > Captive Portal** screen displays.

Client MAC	Client IP	Client IPv6	Captive Portal	Port Name	Authentication	WLAN	VLAN	Remaining Time
<a href="#">54-44-08-3E-00-98</a>	0.0.0.0		ALPHANET-GUEST-		User Redirect	GUEST-ACCESS-REGISTR	666	0s

Type to search in tables Row Count: 1

[Refresh](#)

This screen displays the following information:

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 address.
Client IPv6	Displays the requesting client's IPv6 formatted address.
Captive Portal	Displays the captive portal name that each listed client is utilizing for guest access to network 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 utilizing the access point managed captive portal.



VLAN	Displays the name of the access point VLAN the requesting client uses a virtual interface for captive portal sessions.
Remaining Time	Displays the time after which the client is disconnected from the captive portal managed Internet.

- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

## Network Time

NTP (Network Time Protocol) is central to networks that rely on their controller or service platform to supply system time to managed devices. 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 an enterprise network. The controller or service platform can optionally 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.

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](#) on page 1126.
- [NTP Association](#) on page 1127.

### *NTP Status*

The **NTP Status** screen displays performance (status) information relative to the NTP association status. Verify NTP status to assess the controller or service platform's current NTP resource.

To view the NTP status of a controller or service platform managed network:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Network Time** menu.

The **Statistics > Controller > Network Time > NTP Status** screen displays by default.

NTP Status		NTP Association							
	Clock Offset	Frequency	Leap	Precision	Reference Time	Reference	Root Delay	Root Dispersion	Stratum
<span style="color: green;">+</span>	65.322 msec	-7.2960 Hz	Clock is synchron	2^-20	d5db49b9.116	129.168.147.1	65.322 msec	0.000 msec	3
Type to search in tables						Row Count: 1			

Refer to the **NTP Status** table to review the accuracy and performance of the synchronization with a NTP server resource.

<b>Clock Offset</b>	Displays the time differential between the controller or service platform time and the NTP resource's time.
<b>Frequency</b>	An SNTP server clock's skew (difference) for the controller or service platform and the dedicated NTP resource.
<b>Leap</b>	Indicates if a second is added or subtracted to SNTP packet transmissions, or if transmissions are synchronized.
<b>Precision</b>	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.
<b>Reference Time</b>	Displays the time stamp the local clock was last set or corrected.
<b>Reference</b>	Displays the address of the time source the controller or service platform is synchronized to.
<b>Root Delay</b>	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).
<b>Root Dispersion</b>	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.
<b>Stratum</b>	Displays how many hops the controller or service platform is from its current NTP time source.

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

### *NTP Association*

The interaction between the controller or service platform and a SNTP server constitutes an *association*. SNTP associations can be either *peer* associations (a 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 controller or service platform's NTP associations:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand the **RF Domain** node.
- 4 Select a **Wireless Controller**.
- 5 Expand the **Network Time** and expand the menu to reveal its sub menu items.
- 6 Select **NTP Association**.

The **Statistics > Controller > Network Time > NTP Association** screen displays.

	Delay Time	Display	Offset	Poll	Reach	Reference IP Address	Server IP Address	State	Status	Time
	0.1	15.2	0.0	1024	255	129.188.147	129.188.147	2	Master Sync	504

Type to search in tables Row Count: 1

[Refresh](#)

This screen provides the controller or service platform's current NTP associations:

<b>Delay Time</b>	Displays the round-trip delay (in seconds) for SNTP broadcasts between the SNTP server and the controller or service platform.
<b>Display</b>	Displays the time difference between the peer NTP server and the onboard wireless controller clock.
<b>Offset</b>	Displays the calculated offset between the controller and the SNTP server. The controller adjusts its clock to match the server's time. The offset gravitates towards zero overtime, but never completely reduces its offset to zero.
<b>Poll</b>	Displays the maximum interval between successive messages (in seconds) to the nearest power of two.
<b>Reach</b>	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.
<b>Reference IP Address</b>	Displays the IP address of the time source the controller or service platform is synchronized to.
<b>Server IP Address</b>	Displays the numerical IP address of the SNTP resource (server) providing SNTP updates to the controller or service platform.



<b>State</b>	<p>Displays the NTP association status. The state can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Synced</b> - Indicates the controller or service platform is synchronized to this NTP server.</li> <li>• <b>Unsynced</b> - Indicates the controller or service platform has chosen this master for synchronization. However, the master itself is not yet synchronized to UTC.</li> <li>• <b>Selected</b> - Indicates this NTP master server will be considered the next time the controller or service platform chooses a new master to synchronize with.</li> <li>• <b>Candidate</b> - Indicates this NTP master server may be considered for selection the next time the controller or service platform chooses a NTP master server.</li> <li>• <b>Configured</b> - Indicates this NTP server is a configured server.</li> </ul>
<b>Status</b>	Displays the NTP peer's current status.
<b>Time</b>	Displays the timestamp of the last NTP packet received from the NTP peer.

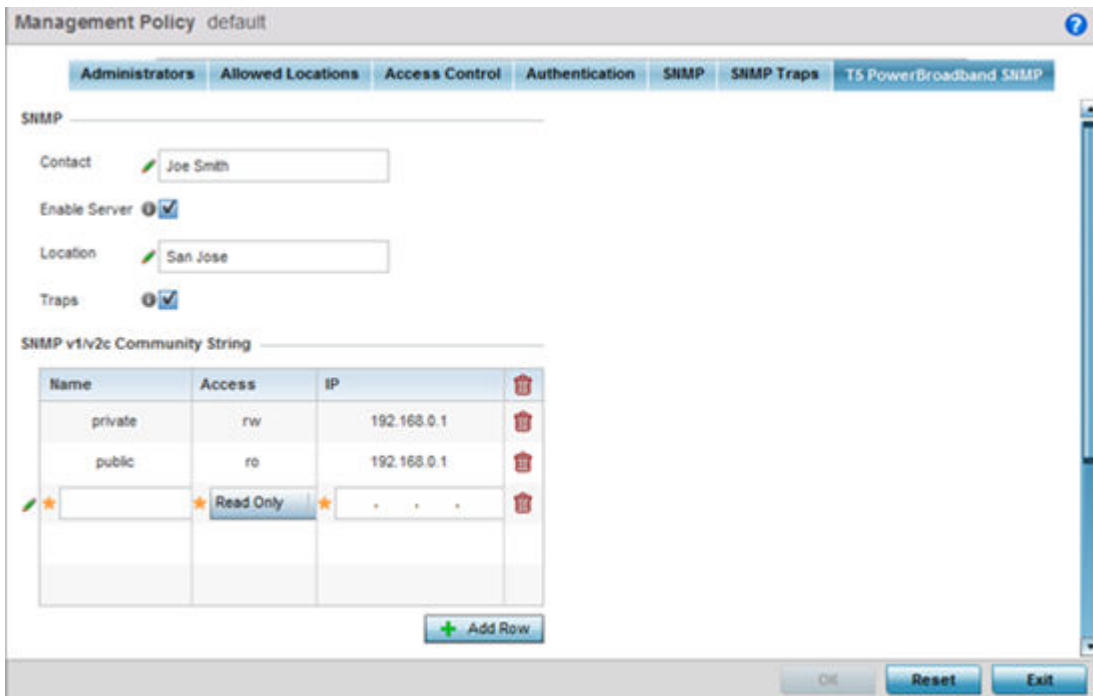
- 7 Select **Refresh** to update the screen's statistics counters to their latest values

## T5 PowerBroadband SNMP

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.



- 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.

## T5 Device

To view device statistics for a selected T5 model controller:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select **Device** from the left-hand side of the UI.

The **System** field displays the following:

Hostname	Lists the administrator assign hostname of the T5 controller applied to the device upon initial administration.
MAC	Lists the factory encoded MAC address of the T5 controller as its hardware identifier.
Type	Indicates the type of controller reporting system data.
RF Domain Name	Lists the RF Domain to which the T5 controller belongs. The RF Domain displays as a link that's selectable to display RF Domain data in greater detail.
System Clock	Displays T5 controller system time, as reported from the controller itself or its remote NTP time resource.
Uptime	Displays the duration the T5 controller has remained active since last offline or booted,
Application Version	Displays the version of the firmware running on this device.
Bootloader Version	Displays the version of the Boot Loader software available on this device.

The **Temperature** field displays the following:



Current Temperature	Displays the current T5 controller temperature in Celsius.
Fans at Variable Speed in (C)	Lists the temperature of the T5 controller as reported by the controller's fans operating at variable speed.
Fans at Full Speed in (C)	Lists the temperature of the T5 controller as reported by the controller's fans operating at full speed.

The **Firmware Images** field displays the following:

Primary Version	Displays the primary version string available for an upgrade.
Secondary Version	Displays the secondary version string available as a backup (secondary) upgrade resource.

The **Upgrade Status** field displays firmware upgrade statistics. The table provides the following:

Upgrade Status	Displays whether the image upgrade was successful.
----------------	--

- 4 Select **Refresh** to update the statistics counters to their latest values.

## T5 Wireless Client

The T5 **Wireless Clients** screen displays read only device information for wireless clients associated with the selected T5 controller and its connected CPE device radios. Use this information to assess if configuration changes are required to improve client performance.

To view wireless client's statistics

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select **Wireless Clients** from the left-hand side of the UI.

The **Wireless Clients** screen displays the following:

Device	Lists the name of the T5 controller managed CPE device radio detecting and reporting client information.
MAC Address	Displays the factory encoded hardware MAC address assigned to the client as hardware identifier.
SSID	Displays each listed client's SSID (service set id) used as a network identifier.
Last RSSI	Lists a RSSI (relative signal strength indication) in dBm for client devices connected to the selected T5 controller and its managed CPE radios.
Rx Packets	Displays the number of packets received by the listed T5 controller managed client.
Tx Packets	Displays the number of packets transmitted by the listed T5 controller managed client.
Association Status	Displays the association status of the wireless client.

Authentication Status	Displays the authentication status of the wireless client.
Retry Percentage	Displays the retry percentage for packets sent this wireless client. The retry rate helps assess the overall effectiveness of the RF environment (as displayed as a percentage) and a function of the connection rate in both directions.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 WLAN QoS

T5 controller **WLAN utilization** can be administered from one screen to assess how different data traffic is being utilized.

To administrate T5 controller WLAN QoS utilization:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select **Wireless LANs** from the left-hand side of the UI. The **Quality of Service** tab displays by default.

Refer to the following information for the listed T5 controller WLANs:

Device	Lists the WLAN(s) utilized by the selected T5 controller.
Rx Background Packets	Lists the number of background (low priority) packets received on each listed T5 controller managed WLAN since the screen was last refreshed.
Rx Best Effort Packets	Lists the number of best effort packets received on each listed T5 controller managed WLAN since the screen was last refreshed.
Tx Background Packets	Lists the number of background (low priority) packets transmitted out of each listed T5 controller managed WLAN since the screen was last refreshed.
Tx Best Effort Packets	Lists the number of best effort packets transmitted out of each listed T5 controller managed WLAN since the screen was last refreshed.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 WLAN Rates

An administrator can assess a T5 controller's WLAN utilization data rate to determine WLAN performance speed is being optimized in both the transmit and receive directions.

To assess T5 controller WLAN data rates:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select **Wireless LANs** from the left-hand side of the UI.
- 4 Select the **Rates** tab.

Refer to the following information for the listed T5 controller WLANs:

Device	Lists the WLAN member devices reporting the listed transmit and receive statistics for the T5 WLAN.
Rx Packets (1Mbps)	Lists the number of data packets received in the WLAN that have been relegated to a 1 Mbps data rate.
Rx Packets (54Mbps)	Lists the number of data packets received in the WLAN by T5 controller connected devices at 54Mbps.
Tx Packets (1Mbps)	Lists the number of data packets transmitted out of the WLAN that have been relegated to a 1 Mbps data rate.
Tx Packets (54Mbps)	Lists the number of data packets transmitted out of the WLAN at 54Mbps.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 WLAN Sizes

T5 controller managed WLANs can be administrated to assess packets sizes both received and transmitted out of the WLAN.

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **Size** tab.

Refer to the following information for the listed T5 controller WLANs:

Device	Lists the WLAN(s) utilized by the selected T5 controller.
Rx Packets (>1024 Bytes)	Lists the number of data packets received in each listed WLAN greater then 1024 bytes.
Tx Packets (>1024 Bytes)	Lists the number of data packets transmitted on each listed WLAN greater then 1024 bytes.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 MAC Table

The T5 MAC Table screen displays a dynamic list of MAC addresses learned by the T5 controller over its ethernet interfaces. Use this information to identify devices and the interfaces on which they can be found.

To view T5 MAC table:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select **MAC Table** from the left-hand side of the UI.

The **MAC Table** screen displays the following:

MAC Address	Displays the MAC address of the discovered client device.
Interface Name	Displays the interface on which the device can be found.

Device MAC	Displays the MAC address of the T5 controller that found the client device.
Vendor	Displays the Vendor (manufacturer) of the T5 discovered client device.
VLAN	Displays the T5 's VLAN (virtual interface) on which the device was discovered.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 CPE System

The T5 controller **CPE System** screen displays device hardware and SKU information for T5 controller managed CPE devices. Use this information to assess whether a controller is managing the correct CPE devices out of the total number of CPEs available.

To view CPE system information:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select and expand the **CPE** menu item to display its sub menu items.
- 4 Select **System**.

The **CPE System** screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Product Type	Displays the model (product) type of each T5 controller managed CPE.
Serial Number	Displays the hardware encoded serial number appended to each T5 controller managed CPE. The serial number is different from the MAC address and is not configurable in the user interface.
SKU	Lists each T5 managed CPE's SKU information to assess hardware product revision.
Hardware Version	Lists a hardware revision number for each listed CPE.
MAC	Lists each CPE's factory encoded MAC address used as the CPE's hardware identifier within the user interface.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 Radio Statistics

The T5 controller **Radios** screen utilizes separate tabs to display radio Summary, Statistics and WLAN Map data.

A T5 controller uses the 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 using the operating system. The tabs within the Radios section support these T5 managed CPE radio devices.

To view T5 controller managed CPE radio statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select **Radios** from the left-hand side of the UI.
- 4 Select the **Statistics** tab.

The **Statistics** tab displays the following for T5 controller managed CPE radio devices:

Name	Displays the administrator assigned name of each listed CPE radio 1 or radio 2 as its unique identifier.
Rx (Kbps)	Displays the listed CPE radio's receive data rate (in Kbps). Use this information to assess RF activity versus other T5 managed CPE radios in the same radio coverage area.
Rx Octets	Displays the number of octets (bytes) received with no errors by the listed T5 controller managed CPE radio.
Rx Packets	Lists the number of data packets received for the listed T5 managed CPE radio since this screen was last refreshed.
Tx (Kbps)	Displays the listed CPE radio's transmit data rate (in Kbps). Use this information to assess RF activity versus other T5 managed CPE radios in the same radio coverage area.
Tx Octets	Displays the number of octets (bytes) transmitted with no errors by the listed T5 controller managed CPE radio.
Tx Packets	Lists the number of data packets transmitted from the listed T5 managed CPE radio since this screen was last refreshed.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 Radio Summary

The T5 controller **Radios** screen utilizes separate tabs to display radio Summary, Statistics and WLAN Map data.

A T5 controller uses the 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 using the operating system. The tabs within the Radios section support these T5 managed CPE radio devices.

To view T5 controller managed CPE radio information:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select **Radios** from the left-hand side of the UI.

The **Summary** tab displays the following for T5 controller managed CPE radio devices: :

Name	Name Displays the administrator assigned name of each listed CPE radio 1 or radio 2 as its unique identifier.
Operational Status	Lists whether the selected radio is currently up or down in its ability be a radio coverage resource for its managing T5 controller.
MAC	MAC Displays the factory encoded Media Access Control (MAC) address of each listed CPE device radio managed by the selected T5 controller.
Transmit Power	Lists each T5 controller managed CPE radio's configured transmit power.
Channel	Lists each CPE radio's current transmit channel. Auto defines the radio as having an automatic channel assignment.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

### T5 Radio WLAN Map

The T5 controller **Radios** screen utilizes separate tabs to display radio Summary, Statistics and WLAN Map data.

A T5 controller uses the 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 using the operating system. The tabs within the Radios section support these T5 managed CPE radio devices.

To view T5 controller managed CPE radio WLAN memberships:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select **Radios** from the left-hand side of the UI.
- 4 Select the **WLAN Map** tab.

Refer to the following WLAN map membership data for T5 controller managed CPE radio devices:

Name	Displays the administrator assigned name of each listed CPE radio 1 or radio 2 as its unique identifier.
Status	Lists whether a CPE radio is currently enabled or disabled as a radio resource for the WLAN(s) the CPE radio has been mapped to.
WLAN-Radio Mapping	Displays the managed WLAN(s) each listed radio has been mapped to.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

### T5 Interface Ethernet Counter

A T5 controller can have its Ethernet ports reviewed for transmit and receive packet throughput.

T5 controllers have the following Ethernet port designations:

- T5- ge1-ge2

To view T5 controller Ethernet port counter statistics:



- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select **Interface** from the left-hand side of the UI.
- 4 Select **Ethernet Ports**. The **Counter** tab displays by default.

Review the following T5 controller Ethernet port counter data:

Name	Displays the name of the selected T5 controller's ge Ethernet port.
Rx Octets	Displays the number of octets (bytes) received by the listed T5 controller Ethernet port.
Rx Packets	Lists the number of data packets received for the listed T5 Ethernet port since this screen was last refreshed.
Rx Pause Packets	Lists the number of Ethernet flow control (Layer 2) packets received on this port since this screen was last refreshed.
Tx Octets	Displays the number of octets (bytes) transmitted by the listed T5 controller Ethernet port.
Tx Packets	Lists the number of data packets transmitted from the listed T5 Ethernet port since this screen was last refreshed.
Tx Pause Packets	Lists the number of Ethernet flow control (Layer 2) packets transmitted on this port since this screen was last refreshed.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 Interface Ethernet Description

T5 controller Ethernet ports can have numeric ID and descriptions applied for differentiation.

T5 controllers have the following Ethernet port designations:

- T5- ge1-ge2, fe1-fe2 (for up to 24 CPE devices managed by a T5 controller).

To view T5 controller Ethernet port descriptions:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select **Interface** from the left-hand side of the UI and expand it to display its sub menu items.
- 4 Select **Ethernet Ports**.
- 5 Select the **Description** tab.

Review the following T5 controller Ethernet port descriptions:

Name	Displays the name of the selected T5 controller's ge Ethernet port.
Interface Index	Lists the numeric index assignable to each T5 controller ge Ethernet port.
Description	Displays the 64 character maximum description an administrator assigns to each ge port as its unique description string.

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.



## T5 Interface Ethernet Status

T5 controller Ethernet ports can have be reviewed to assess link operational status, link speed and duplexing.

T5 controllers have the following Ethernet port designations:

- T5- ge1-ge2, fe1-fe2 (for up to 24 CPE devices managed by a T5 controller).

To view T5 controller Ethernet port link status:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select **Interface** from the left-hand side of the UI and expand it to display it sub menu items.
- 4 Select **Ethernet Ports**.
- 5 Select the **Status** tab.

Review the following T5 controller Ethernet port status:

Name	Displays the name of the selected T5 controller's ge Ethernet port.
Operational Status	Lists whether each Ethernet port link is currently up or down as a T5 controller transmit and receive resource.
Duplex	Lists either half, full or automatic as the duplex. Half duplex sends 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. Full duplex transmits data to and from the port at the same time. Using full duplex, the port can send data while receiving data as well. Automatic enables the controller to dynamically duplex as port performance needs dictate.
Speed (MB)	Speed (MB) Lists each port's current speed in MB.
Pause	Lists whether pause packet utilization is currently off or on for the port.
Admin Status	Displays

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 Interface Ethernet Utilization

T5 controller Ethernet ports can have be reviewed to assess link utilization efficiency.

T5 controllers have the following Ethernet port designations:

- T5- ge1-ge2, fe1-fe2 (for up to 24 CPE devices managed by a T5 controller).

To view T5 controller Ethernet port link status:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select **Interface** from the left-hand side of the UI and expand it to display it sub menu items.
- 4 Select the **Utilization** tab.

Review the following T5 controller Ethernet port status:

Name	Displays the name of the selected T5 controller's ge Ethernet port.
Rx (Kbps)	Displays the listed T5 controller ge Ethernet port receive data rate (in Kbps).
RX (p/s)	Lists a packet per second Ethernet port receive rate.
Rx Utilization (%)	Lists each port's receive direction utilization as a percentage of available receive bandwidth available.
Tx (Kbps)	Displays the listed T5 controller Ethernet port transmit data rate (in Kbps).
Tx (p/s)	Lists a packet per second Ethernet port transmit rate.
Tx Utilization (%)	Lists each port's transmit direction utilization as a percentage of available transmit bandwidth available.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 Radio DSL Counter

A T5 controller uses the 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 using the operating system. The tabs within the Radios section support these T5 managed CPE 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.

To view CPE DSL counter statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **DSL** menu item. The **Counter** tab displays by default.

The **DSL Counter** screen displays the following:

Name	Lists the name of the DSL utilized by each T5 controller connected CPE device.
Rx Octets	Displays the number of octets (bytes) received with no errors by the listed T5 controller managed CPE DSL.
Rx Packets	Lists the number of data packets received for the listed T5 managed CPE DSL since this screen was last refreshed.
Rx Pause Packets	Lists the number of Ethernet flow control (Layer 2) packets received for the listed T5 managed CPE DSL since this screen was last refreshed.
Tx Octets	Displays the number of octets (bytes) transmitted with no errors by the listed T5 controller managed CPE DSL.
Tx Packets	Lists the number of data packets transmitted from the listed T5 managed CPE DSL since this screen was last refreshed.
Tx Pause Packets	Lists the number of Ethernet flow control (Layer 2) packets transmitted from the listed T5 managed CPE DSL since this screen was last refreshed.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 Radio DSL Custom

A T5 controller uses the 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 using the operating system. The tabs within the Radios section support these T5 managed CPE 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.

To view **Custom** CPE DSL counter statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **DSL** menu item. Select the **Custom** tab displays by default.

The **Custom** DSL screen displays the following:

Average Response Time	List each DSL's average response time in microseconds.
Maximum (peak) Response Time	List each DSL's maximum (best to date since the screen was refreshed) response time in microseconds.
Downstream Errored Seconds	List the number of seconds downstream DSL transmissions were negatively impacted by code violations.
Downstream Severely Errored Seconds	List the number of seconds downstream DSL transmissions were severely negatively impacted by code violations.
Upstream Errored Seconds	List the number of seconds upstream DSL transmissions were negatively impacted by code violations.
Upstream Severely Errored Seconds	List the number of seconds upstream DSL transmissions were severely negatively impacted by code violations.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 Radio DSL Description

A T5 controller uses the 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 using the operating system. The tabs within the Radios section support these T5 managed CPE 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.

To view CPE DSL description data:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.

- 3 Select the **DSL** menu item. Select the **Description** tab.

The DSL Description screen displays the following:

Name	Lists the name of the DSL utilized by each T5 controller connected CPE device.
Interface Index	Lits the numeric index assigned to each CPE DSL upon its initial management and configuration.
Description	Displays the administrator assigned description for further delineation amongst T5 controller managed CPE DSLs.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 Radio DSL Status

A T5 controller uses the 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 using the operating system. The tabs within the Radios section support these T5 managed CPE 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.

To view CPE DSL status:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **DSL** menu item. Select the **Status** tab.

The DSL Description screen displays the following:

Name	Lists the name of the DSL utilized by each T5 controller connected CPE device.
Link Status	Displays whether each listed CPE DSL is currently enabled or disabled for utilization by its connected T5 controller.
Downstream Rate (Mbps)	Downstream Rate (Mbps) Lists each connected CPE DSL downstream data rate in Mbps.
Downstream Margin (dB)	Displays the DSL downstream power minus the attenuation ( in dB).
Upstream Rate (Mbps)	Lists each connected CPE DSL upstream data rate in Mbps.
Upstream Margin (dB)	Displays the DSL upstream power minus the attenuation (in dB).
Power	Lists each DSL's wattage utilization.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 Radio DSL Errors

A T5 controller uses the 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 using the operating system. The tabs within the Radios section support these T5 managed CPE 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.

To view CPE DSL error data:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **DSL** menu item. Select the **Errors** tab.

The DSL Errors screen displays the following:

Name	Lists the name of the DSL utilized by each T5 controller connected CPE device.
Line Downstream Fecs	Lists the number of Fecs detected in the downstream direction. Forward Error Correction (FEC) or channel coding is used for controlling errors over unreliable or noisy communication channels
Downstream Coding Violations	Lists the number of CPE DSL coding violations (badly coded packets) detected in the downstream direction.
Line Upstream Fecs	Lists the number of Fecs detected in the upstream direction. Forward Error Correction (FEC) or channel coding is used for controlling errors over unreliable or noisy communication channels
Upstream Coding Violations	Lists the number of CPE DSL coding violations (badly coded packets) detected in the upstream direction.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 Radio DSL Utilization

A T5 controller uses the 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 using the operating system. The tabs within the Radios section support these T5 managed CPE 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.

To view CPE DSL utilization:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **DSL** menu item. Select the **Utilization** tab.

The DSL Utilization screen displays the following:

Name	Lists the name of the DSL utilized by each T5 controller connected CPE device.
Rx (Kpbs)	Displays the listed CPE DSL's receive data rate (in Kpbs).
RX (p/s)	Lists a packet per second DSL receive rate.



Rx Utilization (%)	Lists each DSL's receive direction utilization as a percentage of available receive bandwidth available.
Tx (Kbps)	Displays the listed CPE DSL's transmit data rate (in Kbps).
Tx (p/s)	List a packet per second DSL transmit rate.
Tx Utilization (%)	Lists each DSL's transmit direction utilization as a percentage of available transmit bandwidth available.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 Fast Ethernet Counter

A T5 controller can have its Ethernet ports reviewed for transmit and receive packet throughput.

T5 controllers can have their connected CPE fe ports (1-2) analyzed for performance analysis. A single T5 controller can manage up to 24 CPE devices and 48 fe ports.

- CPE- fe1-fe2

To view T5 controller connected CPE fe port counter statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **Interface** menu item and expand it to display its sub menu items. Select **Fast Ethernet**. The **Counter** tab displays by default.

Review the following T5 controller connected CPE fe port counter data:

Name	Displays the name of each listed T5 controller controller connected CPE fe Ethernet port.
Rx Octets	Displays the number of octets (bytes) received by the listed CPE fe port.
Rx Packets	Lists the number of data packets received for the listed CPE fe port since this screen was last refreshed.
Rx Pause Packets	Lists the number of Ethernet flow control (Layer 2) packets received on this port since this screen was last refreshed.
Tx Octets	Displays the number of octets (bytes) transmitted by the listed CPE fe Ethernet port.
Tx Packets	Lists the number of data packets transmitted from the listed CPE fe port since this screen was last refreshed.
Tx Pause Packets	Lists the number of Ethernet flow control (Layer 2) packets transmitted on this port since this screen was last refreshed.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 Fast Ethernet Description

T5 controllers can have their connected CPE fe ports (1-2) analyzed for performance analysis. A single T5 controller can manage up to 24 CPE devices and 48 fe ports.

- CPE- fe1-fe2

To view T5 controller connected CPE fe port descriptions:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **Interface** menu item and expand it to display its sub menu items. Select **Fast Ethernet**. Select the **Description** tab.

Review the following CPE fe port descriptions:

Name	Displays the name of the selected CPE fe Ethernet port.
Interface Index	Lists the numeric index assignable to each CPE fe Ethernet port.
Description	Displays the 64 character maximum description an administrator assigns to each CPE fe port as its unique description string.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 Fast Ethernet Status

T5 controllers can have their connected CPE fe ports (1-2) analyzed for performance analysis. A single T5 controller can manage up to 24 CPE devices and 48 fe ports.

- CPE- fe1-fe2

To view T5 controller connected CPE fe port status:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **Interface** menu item and expand it to display its sub menu items. Select **Fast Ethernet**. Select the **Status** tab.

Review the following CPE fe port descriptions:

Name	Displays the name of the selected CPE fe Ethernet port.
Operational Status	Lists whether each Ethernet port link is currently up or down as a transmit and receive resource.
Duplex	Lists either half, full or automatic as the duplex. Half duplex sends 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. Full duplex transmits data to and from the port at the same time. Using full duplex, the port can send data while receiving data as well. Automatic enables the controller to dynamically duplex as port performance needs dictate.
Speed (MB)	Lists each port's current speed in MB.
Pause	Lists whether pause packet utilization is currently off or on for the port.
Admin Status	Admin Status Displays whether each listed port had been placed in an enabled or disabled state by the administrator.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.



## T5 Fast Ethernet Utilization

T5 controllers can have their connected CPE fe ports (1-2) analyzed for performance analysis. A single T5 controller can manage up to 24 CPE devices and 48 fe ports.

- CPE- fe1-fe2

To view T5 controller connected CPE fe port utilization:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **Interface** menu item and expand it to display its sub menu items. Select **Fast Ethernet**. Select the **Utilization** tab.

Review the following CPE fe Ethernet port utilization data:

Name	Displays the name of the selected CPE fe Ethernet port.
Rx (Kbps)	Displays the listed CPE fe Ethernet port receive data rate (in Kbps).
RX (p/s)	Lists a packet per second Ethernet port receive rate.
Rx Utilization (%)	Lists each port's receive direction utilization as a percentage of available receive bandwidth available.
Tx (Kbps)	Displays the listed CPE fe Ethernet port transmit data rate (in Kbps).
Tx (p/s)	Lists a packet per second fe Ethernet port transmit rate.
Tx Utilization (%)	Lists each fe port's transmit direction utilization as a percentage of available transmit bandwidth available.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 CPE Address

The T5 controller CPE Address screen lists the selected T5 controller's managed CPE radio devices. Use this screen to verify each CPE address credentials and whether they are currently disconnected or ready for radio coverage area support.

To view CPE address data:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **CPE** menu item and expand it to display its sub menu items. Select **Address**.

The CPE Address screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Status	Displays whether each T5 controller managed CPE is disconnected (offline) or ready to provide radio coverage area support for the T5 controller.
IP Address	Lists each CPE's current IP address used as its network identifier.
MAC Address	Displays each CPE hardware encoded MAC address used as a device hardware identifier.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

### T5 CPE Boot

The T5 controller CPE Boot screen lists the primary and secondary firmware versions available to each CPE, along with upgrade status from each device's most recent upgrade operation.

To view CPE boot configurations:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **CPE** menu item and expand it to display its sub menu items. Select **Boot**.

The CPE Boot screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Primary Version	Lists the primary version of CPE firmware currently queued for each listed T5 controller managed CPE.
Secondary Version	Lists the secondary (alternate) version of CPE firmware currently queued for each listed T5 controller managed CPE.
Next Boot	Lists whether the next boot of each listed CPE is going to utilize either the primary or secondary firmware version.
Upgrade Process	Displays a completion percentage for any pending firmware upgrade operation impacting a listed T5 controller managed CPE device.
Upgrade Status	Lists the upgrade status of T5 controller managed CPEs. If a device is not undergoing an upgrade, its status is None.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

### T5 CPE Reset

The T5 controller CPE Reset screen lists the number times a T5 controller managed CPE has been reset.

To view CPE reset status:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **CPE** menu item and expand it to display its sub menu items. Select **Reset**.

The CPE **Reset** screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Resets	Lists the number of times each T5 controller managed CPE has been reset since this screen was last refreshed. Resetting a CPE temporarily renders the CPE offline until the reset is complete.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 CPE LED

The T5 controller CPE LED screen lists whether T5 controller managed CPE devices currently have their LEDs enabled or disabled. In places like hospitals, its not uncommon for Access Points to be operational, but their LEDs off as to not disturb patients.

To view CPE LED status:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **CPE** menu item and expand it to display its sub menu items. Select **LED**.

The CPE **LED** screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
LED Status	A green checkmark defines the listed CPE as having its LEDs on and illuminated. A red X defines the listed CPE as having its LEDs off.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 CPE Reset

The T5 controller CPE Reset screen lists the number times a T5 controller managed CPE has been reset.

To view CPE reset status:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select the **CPE** menu item and expand it to display its sub menu items. Select **Reset**.

The CPE **Reset** screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Resets	Lists the number of times each T5 controller managed CPE has been reset since this screen was last refreshed. Resetting a CPE temporarily renders the CPE offline until the reset is complete.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 CPE System

The T5 controller **CPE System** screen displays device hardware and SKU information for T5 controller managed CPE devices. Use this information to assess whether a controller is managing the correct CPE devices out of the total number of CPEs available.

To view CPE system information:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.

- 3 Select and expand the **CPE** menu item to display its sub menu items.
- 4 Select **System**.

The **CPE System** screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Product Type	Displays the model (product) type of each T5 controller managed CPE.
Serial Number	Displays the hardware encoded serial number appended to each T5 controller managed CPE. The serial number is different from the MAC address and is not configurable in the user interface.
SKU	Lists each T5 managed CPE's SKU information to assess hardware product revision.
Hardware Version	Lists a hardware revision number for each listed CPE.
MAC	Lists each CPE's factory encoded MAC address used as the CPE's hardware identifier within the user interface.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 CPE Uptime

The CPE Uptime screen lists the time each T5 controller manage CPE device has been actively deployed and operational.

To view CPE device uptimes:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select and expand the **CPE** menu item to display its sub menu items.
- 4 Select **Uptime**.

The CPE **Uptime** screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Uptime	Lists the time each listed T5 controller has been deployed without interruption (reboot etc.).

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## T5 CPE Version

The CPE Version screen lists the application and boot versions utilized by T5 controller managed CPE devices.

To view CPE device version data:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.

- 3 Select and expand the **CPE** menu item to display its sub menu items.
- 4 Select **Version**.

The CPE **Version** screen displays the following:

Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
Application Verison	Lists the firmware version currently utilized and deployed with each listed T5 controller managed CPE.
Boot Loader Version	Displays the firmware version queued as the boot version for each listed T5 controller managed CPE.

- 5 Select **Refresh** to update the screen’s statistics counters to their latest values.

### T5 CPE Port Status

The T5 controller CPE Port Status screen lists the status of the ports for the T5 controller managed CPE devices.

To view CPE device version data:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Select the **Wireless Controller** node from the left navigation pane and select a T5 controller from amongst those displayed.
- 3 Select and expand the **CPE** menu item to display its sub menu items.
- 4 Select **Port Status**.

The CPE **Port Status** screen displays the following:

CPE Device	Lists the name of the T5 controller managed CPE device. Up to 24 CPEs can be managed by a single T5 controller.
CPE MAC	Lists the MAC address of the T5 controller managed CPE device.
Interface	Lists the interface on which the T5 controller managed CPE device is found.
Operation Status	Lists the operational status of the T5 controller managed CPE device.
Speed (Mbps)	Lists the interface speed of the CPE device in Mbps.
Duplex	Displays the interface as either half duplex, full duplex or unknown.

- 5 Select **Refresh** to update the screen’s statistics counters to their latest values.

### EX3500 Statistics

Use the EX3500 switch’s statistics screens to assess switch throughput and error rates in both the transmit and receive directions. Expand the topics in this section as needed to review individual Ethernet port performance utilizations.

#### EX3500 System

Refer to the **System** screen to assess EX3500 switch system data as well as switch fan utilization and device upgrade information.

Use the **System** field to assess the administrator assigned **System Name** for the switch, **System Object ID** (numeric identifier), administrative **System Contact**, **System Description**, **System Location** and **System Up Time**. The factory encoded **MAC Address** of the switch displays as the unit's hardware identifier. The **System** field also displays the switch's dedicated Web server port, whether **Web Server** functionality is enabled, the **Web Server Secure Port** and whether **Web Secure Server** is enabled for optimized Web server security. Additionally, assess whether **Telnet Server** functionality has been enabled and over which **Telnet Server Port**. Lastly, assess whether support for **Jumbo Frames** with more than 1500 bytes of payload has been enabled or disabled.

Refer to the **Fan** table to review the Fan and Unit index of each EX3500 switch fan utilized and their current Fan Status.

The **Upgrade** table lists the queued file for the upgrade operation, its Path (file location) and Status and Reload Status.

The **Temperature** table displays the current temperature (in degrees) to assess a potential overheat condition.

Periodically select **Refresh** to update the screen to its latest information.

## w

### *EX3500 Version*

The EX3500 switch **Version** screen lists hardware and switch software version information utilized for the selected EX3500 switch. Use this information when reporting any issues to Support or when assessing whether an update would improve switch performance.

To view EX3500 switch version information:

- Refer to the **Unit ID** and **Serial Number** items to assess the switch numeric identifier and serial number.
- The **Hardware Version** lists hardware version of the EX3500 switch main board.
- Refer to the **EPLD Version** to check the EPLD (erasable programmable logic device) comprising an array of PLD (programmable logic devices) that do not come pre-connected with the switch.
- The **Number of Ports** field lists built-in port utilization. The EX3524 and EX3548 are Gigabit Ethernet Layer 2 switches with either 24 or 48 10/100/1000-BASE-T ports, and four SFP (Small Form Factor Pluggable) transceiver slots for fiber connectivity.
- Refer to the **Main Power Status** item to assess the status of the internal power supply.
- Refer to the **Role** table item to review the switch's current defined network role (**master** or **slave**).
- The **Loader Version** item displays the version number of the switch loader code.
- The **Operation Code Version** lists the version number of the switch's runtime code.
- The **Adopted Version** lists the version of the management agent used by the switch to adopt to a WiNG controller.
- The **Linux Version** lists the version of the Linux operating system utilized on the switch.

Periodically select **Refresh** to update the screen to its latest information.

### EX3500 Directory Information

The **Directory Information** screen helps an administrator Opcode and Configuration files currently residing on the EX3500 switch and whether their currently designated as boot files.

Refer to the following directory information for the selected EX3500:

- Refer to the **Unit ID** item to list the ID associated with each listed configuration or opcode file.
- The **File Name** item lists the files available for utilization on the switch currently. Select **Whichboot** (from the upper left) to filter this list to just the files queued for switch boot operations.
- The **Type** item lists whether each listed file is a **OpCode** (switch runtime code) or **Config** (switch configuration) file.
- The **Startup** item lists Y/N as to whether the listed file is invoked at switch startup.
- The **Modify Time** parameter lists the last time the listed file was modified on this EX3500 switch.
- The **Size (Bytes)** item lists the byte size of the listed operation code (Opcode) or configuration file.

Periodically select **Refresh** to update the screen to its latest information.

### EX3500 Interface

Use the EX3500 switch's Ethernet and interface statistics screens to assess switch throughput and error rates in both the transmit and receive directions. Expand the topics in this section as needed to review individual Ethernet port performance utilizations.

#### EX3500 Ether

Refer to the **Ether-LIKE** screen to assess a variety of errors that may be negatively impacting the performance of each listed EX3500 switch interface.

Review the following error conditions for each listed EX3500 switch interface:

- **Interface** - Lists the impacted physical EX3500 Ethernet Port reporting the listed interface stats.
- **Alignment Errors** - Lists frames received that are not an integral number of bytes long and that fail the FCS check.
- **FCS Errors** - Lists each interface's FCS (frame check sequence) errors. refers to the extra error-detecting code added to a frame in a communications protocol.
- **Single Collision Frames** - Displays each interface's number of collisions over the selected interface.
- **Multiple Collision Frames** - Displays each interface's number of frames transmitted that met with more than one collision before the 64-bytes traversed the connection.
- **SQE Test Errors** - Lists each interface's SQE TEST ERROR message. SQEs are **Signal Quality Errors**, and are also referred as an Ethernet **heartbeat**.
- **Deferred Transmissions** - The number of frames that were ultimately sent after the system initially deferred them (the first transmission attempt was delayed because the medium was busy). This number does not include frames involved in any collisions.
- **Late Collisions** - Lists each interface's 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 each interface's number of excessive collisions. Excessive collisions occur when the traffic load increases to the point a single Ethernet network cannot handle it efficiently.

- **Internal MAC Transmit Errors** - Lists each interface's error count due to an internal MAC sublayer transmit error. This number does not include alignment, FCS, or frame-too-long errors.
- **Internal MAC Receive Errors** - Lists each interface's error count due to an internal MAC sublayer receive error. This number does not include alignment, FCS, or frame-too-long errors.
- **Frames Too Long** - Lists each interface's error count due from exceeding the standard Ethernet size limitation but had a valid CRC. Without jumbo frames enabled, these are frames over 1518 bytes or 1522 bytes for VLAN frames. With jumbo frames enabled, these are frames over 9018 bytes or 9022 bytes for VLAN frames.
- **Carrier Sense Errors** - Lists each interface's errors that occur when an interface attempts to transmit a frame, but no carrier is detected, and the frame cannot be transmitted.

Periodically select **Refresh** to update the data to the latest values.

### EX3500 Interface Extended IF

The EX3500 Interface Extended IF screen lists multicast and broadcast traffic utilization in both the transmit and receive directions.

Review the following extended interface information for the selected EX3500 switch:

- **Interface** - Lists the impacted physical EX3500 Ethernet Port reporting the listed interface stat.
- **Multicast Input** - Lists each port's number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a multicast address at this sub-layer.
- **Multicast Output** - Lists each port's number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
- **Broadcast Input** - Lists each port's number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a broadcast address at this sub-layer.
- **Broadcast Output** - Lists each port's The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

Periodically select **Refresh** to update the screen to its latest information.

### EX3500 Interface IF

Refer to the Interface Table for octet utilization and reported errors for each listed EX3500 switch port.

The table includes the following:

- **Interface** - Lists the impacted physical EX3500 Ethernet Port reporting the listed interface stat.
- **Octets Input** - Lists the total number of octets received on the listed switch port, including framing characters.
- **Octets Output** - Lists the total number of octets transmitted out of the listed switch port, including framing characters.
- **Unicast Input** - Lists the number of subnetwork-unicast packets delivered to each listed interface.
- **Unicast Output** - Lists each port's number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address.
- **Discard Input** - Number of input frames discarded because they did not conform to the general validation rules or specific usage rules defined for the listed port.



- **Discard Output** - Number of output frames discarded because they did not conform to the general validation rules or specific usage rules defined for the listed.
- **Error Input** - Lists each port's total number of erroneous input frames that could not be received.
- **Error Output** - Lists each port's total number of erroneous output frames that could not be transmitted and forwarded to their destination.
- **Unknown Protos Input** - Lists each port's number of packets received and discarded because of an unknown or unsupported protocol.

Periodically select **Refresh** to update the screen to its latest information.

### EX3500 Interface Port Utility

Refer to the **Port Utilization Statistics** screen to assess packet throughput per listed switch port.

Review the following EX3500 switch port utilizations stats:

- **Interface** - Lists the impacted physical EX3500 Ethernet Port reporting the listed stat.
- **Octet Input Per Second** - Number of octets entering the listed port in kbits/second.
- **Packet Input Per Second** - Lists each port's received packet total per second.
- **Input Utilization** - The input utilization rate for each listed port.
- **Octet Output Per Second** - Number of octets leaving each listed port in kbits/second.
- **Packet Output Per Second** - Number of packets leaving each listed port per second.
- **Output Utilization** - The output utilization rate for this listed port interface.

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

### EX3500

## EX3500 Interface Extended IF

The EX3500 Interface Extended IF screen lists multicast and broadcast traffic utilization in both the transmit and receive directions.

Review the following extended interface information for the selected EX3500 switch:

- **Interface** - Lists the impacted physical EX3500 Ethernet Port reporting the listed interface stat.
- **Multicast Input** - Lists each port's number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a multicast address at this sub-layer.
- **Multicast Output** - Lists each port's number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
- **Broadcast Input** - Lists each port's number of packets, delivered by this sub-layer to a higher sub-layer, which were addressed to a broadcast address at this sub-layer.
- **Broadcast Output** - Lists each port's The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

Periodically select **Refresh** to update the screen to its latest information.

---

## Access Point Statistics

---

**Access Point** statistics screens displays access point *performance, health, version, client support, radio, mesh, interface, DHCP, firewall, WIPS, sensor, captive portal, NTP* and *load* information.

Access point statistics are reported from AP 6511, AP 6521, AP 6532, AP 6522, AP 6562, AP 7131, AP 7161, AP 7181 or AP 8132 model access points in either Standalone or Controller AP mode or AP621 or AP650 model access points in *Dependent* mode. Dependent mode access points are reliant on their managing controller for their configuration file management and are unable to provide autonomous operation.

Access point statistics consists of the following:

- Health
- Device
- AP Upgrade
- Adoption
- AP Detection
- Wireless Clients
- Wireless LANs
- Policy Based Routing
- Radios
- Mesh
- Interfaces
- RTLS
- PPPoE
- OSPF
- L2TPv3
- VRRP
- Critical Resources
- Network
- DHCP Server
- Firewall
- VPN
- Certificates
- WIPS
- Sensor Servers
- Captive Portal
- Network Time
- Load Balancing
- Environmental Sensor

### AP Health

The **Health** screen displays a selected access point's hardware and software version. Use this information to refine the performance of an access point. The Health screen should also be the starting

point for troubleshooting an access point, since it displays a high level overview of access point performance efficiency and client support capability.

To view an access point's health:

- 1 Select the **Statistics** tab from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.

The **System** node expands to display the RF Domains created within the managed network.

- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.
- 4 Select **Health** from the left-hand side of the UI.

The screenshot displays the 'AP > Health' screen with the following sections:

- Device Details:**

Hostname	ap6532-34776C
Device MAC	5C-0E-8B-34-77-6C
Primary IP	172.168.6.23
Type	AP6532
Model Number	AP-6532-66040-OUS
RF Domain Name	<a href="#">rf4US</a>
Version	5.8.0.0-029D
Uptime	20 days, 13 hours 42 minutes
CPU	MIPS 24Kc V7.4
RAM	89844 kB
System Clock	2015-05-26 14:39:59 PDT
- Radio Utilization:**

Parameter	Transmit	Receive
Total Bytes	0	968,971
Total Packets	0	8,524
Total Dropped	24	
- Client RF Quality Index:**

Worst 5	Client MAC	Retry Rate
- Radio RF Quality Index:**

RF Quality Index	Radio Id	Radio Type
100 (Good)	<a href="#">ap6532-34776C-R1</a>	2.4 GHz WLAN
100 (Good)	<a href="#">ap6532-34776C-R2</a>	5 GHz WLAN

A 'Refresh' button is located at the bottom right of the screen.

Review the different fields displayed on the **AP > Health** screen.

The **Device Details** field displays the following:

<b>Hostname</b>	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.
<b>Device MAC</b>	Displays the MAC address of the AP. This is factory assigned and cannot be changed.
<b>Primary IP</b>	Displays the IP address of assigned to this device either through DHCP or through static IP assignment.
<b>Type</b>	Displays the access point's model type.
<b>RF Domain Name</b>	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.

<b>Model Number</b>	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.
<b>Version</b>	Displays the access point's current firmware version. Use this information to assess whether an upgrade is required for better compatibility.
<b>Uptime</b>	Displays the cumulative time since the access point was last rebooted or lost power.
<b>CPU</b>	Displays the processor core.
<b>RAM</b>	Displays the free memory available with the RAM.
<b>System Clock</b>	Displays the system clock information.

The **Radio RF Quality Index** field the following:

<b>RF Quality Index</b>	Displays access point radios and their quality indices. RF quality index indicates the overall RF performance. The RF quality indices are: <ul style="list-style-type: none"> <li>• 0 – 50 (poor)</li> <li>• 50 – 75 (medium)</li> <li>• 75 – 100 (good)</li> </ul>
<b>Radio id</b>	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.
<b>Radio Type</b>	Identifies whether the radio is a 2.4 or 5 GHz.

The **Radio Utilization** field displays the following:

<b>Total Bytes</b>	Displays the total bytes of data transmitted and received by the access point since the screen was last refreshed.
<b>Total Packets</b>	Lists the total number of data packets transmitted and received by the access point since the screen was last refreshed.
<b>Total Dropped</b>	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:

<b>Worst 5</b>	Displays clients having lowest RF quality within the network.
<b>Client MAC</b>	Displays the MAC addresses of the clients with the lowest RF indices.
<b>Retry Rate</b>	Displays the average number of retries per packet. A high number indicates possible network or hardware problems.

- 5 Select **Refresh** as needed to update the screen's statistics counters to their latest values.

## AP Device

The **Device** screen displays basic information about a selected access point. Use this screen to gather version information, boot image utilization and upgrade status. An access point's sensor server capability, power management and system resources can also be administrated from the **Device** screen.

To view the device statistics:

- 1 Select the **Statistics** tab from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **Device**.

The screenshot shows the 'System' statistics page. It contains the following data:

System	
Model Number	AP-6562-66040-OUS
Serial Number	10260522200743
Version	5.9.0.0-056R
Boot Partition	secondary
Fallback Enabled	✔ Enabled
Fallback Image Triggered	✘ No
Next Boot	secondary

Firmware Images	
Primary Build Date	11/25/2014 00:36:22
Primary Install Date	12/04/2014 10:40:16
Primary Version	5.8.0.0-00604D
Secondary Build Date	04/17/2014 18:58:06
Secondary Install Date	12/04/2014 10:49:33
Secondary Version	5.6.0.0-056R
FPGA Version	Unknown
PoE Firmware Version	Unknown

System Resources	
Available Memory (KB)	40,152
Total Memory (KB)	90,092
Currently Free RAM	44.5%
Recommended Free RAM	10.0%
Current File Descriptors	700
Maximum File Descriptors	25,500
CPU Load 1 Minute	4.2%
CPU Load 5 Minutes	4.2%
CPU Load 15 Minutes	4.1%
Smart Cache	

IPv6 Name Servers	
Name Server	Type

Sensor Lock	
Sensor Lock State	✘ No

Upgrade Status	
Upgrade Status	Successful

IPv6 Hop Limit	
Hop Limit	64

[Refresh](#)

The **System** field displays the following:

<b>Model Number</b>	Displays the model of the selected access point to help distinguish its exact SKU and country of operation.
<b>Serial Number</b>	Displays the numeric serial number set for the access point.
<b>Version</b>	Displays the software (firmware) version on the access point. Use this information to assess whether a firmware upgrade would enhance the access point's support capability.
<b>Boot Partition</b>	Displays the boot partition type.
<b>Fallback Enabled</b>	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.

<b>Fallback Image Triggered</b>	Displays whether the fallback image was triggered. The fallback image is an old version of a known and trusted operational firmware image stored in device memory. This allows a user to test a new version of firmware. If the new version fails, you can use the old version to ensure the access point's duty cycle is maintained.
<b>Next Boot</b>	Designates this version as the version used the next time the access point is booted.

The **System Resources** field displays the following:

<b>Available Memory (MB)</b>	Displays the available memory (in MB) available on the access point.
<b>Total Memory (MB)</b>	Displays the access point's total memory.
<b>Currently Free RAM</b>	Displays the access point's free RAM space. If its very low, free up some space by closing some processes.
<b>Recommended RAM</b>	Displays the recommended RAM required for routine operation.
<b>Current File Description</b>	Displays the access point's current file description.
<b>Maximum File Description</b>	Displays the access point's maximum file description.
<b>CPU Load 1 Minute</b>	Lists this access point's CPU utilization over a 1 minute span.
<b>CPU Load 5 Minutes</b>	Lists this access point's CPU utilization over a 5 minute span.
<b>CPU Load 15 Minutes</b>	Lists this access point's CPU utilization over a 15 minute span.

The **Fan Speed** field displays the following:

<b>Number</b>	Displays the number of fans supported on the listed access point. access point models each have unique fan support.
<b>Speed (Hz)</b>	Displays the fan speed in Hz.

The **Temperature** field displays the following:

<b>Number</b>	Displays the number of temperature elements (gauges) used by the access point.
<b>Temperature</b>	Displays the current temperature (in Celsius) to assess a potential access point overheat condition.

The **Kernal Buffers** field displays the following:

<b>Buffer Size</b>	Lists the sequential buffer size.
<b>Current Buffers</b>	Displays the current buffers available to the selected access point.
<b>Maximum Buffers</b>	Lists the maximum buffers available to the selected access point.

The **IP Domain** field displays the following:

<b>IP Domain Name</b>	Displays the name of the IP Domain service used with the selected access point.
<b>IP Domain Lookup state</b>	Lists the current state of an IP lookup operation.

The **IP Name Servers** field displays the following:

<b>Name Server</b>	Displays the names of the servers designated to provide DNS resources to this access point.
<b>Type</b>	Displays the type of server for each server listed.

The **Firmware Images** field displays the following:

<b>Primary Build Date</b>	Displays the build date when this access point firmware version was created.
<b>Primary Install Date</b>	Displays the date this version was installed.
<b>Primary Version</b>	Displays the primary version string.
<b>Secondary Build Date</b>	Displays the build date when this version was created.
<b>Secondary Install Date</b>	Displays the date this secondary version was installed.
<b>Secondary Version</b>	Displays the secondary version string.
<b>FPGA Version</b>	Displays whether a FPGA supported firmware load is being utilized.
<b>PoE Firmware Version</b>	Displays whether a PoE supported firmware load is being utilized.

The **Sensor Lock** field displays the following:

<b>Sensor Lock</b>	Displays whether a lock has been applied to access point sensor capabilities. Keeping an access point from performing sensor support ensures client support is continuously maintained.
--------------------	---

The **Upgrade Status** field displays the following:

<b>Upgrade Status</b>	Displays the status of the image upgrade.
<b>Upgrade Status Time</b>	Displays the time of the image upgrade.

The **Power Management** field displays the following:

<b>Power Management Mode</b>	Displays the power mode currently invoked by the selected access point.
<b>Power Management Status</b>	Lists the power status of the access point.
<b>Ethernet Power Status</b>	Displays the access point's Ethernet power status.
<b>Radio Power Status</b>	Displays the power status of the access point's radios. Each access point radio is capable of having a unique, administrator defined, transmit capability.

The **IPv6v Hop Limit** table displays the following:

<b>Hop Limit</b>	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 Name Servers** field displays the following:

<b>Name Server</b>	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.
<b>Type</b>	Lists the type of IPv6 name server mapping a human readable identifier to system identifier.





The IPv6 Delegated Prefixes table displays the following:

<b>IPv6 Delegated Prefix</b>	In IPv6, prefix delegation is used to assign a network address prefix, configuring the controller or service platform with the prefix.
<b>Prefix Name</b>	Lists the name assigned to the IPv6 delegated prefix.
<b>DHCPv6 Client State</b>	Displays the current DHCPv6 client state as impacted by the IPv6 delegated prefix.
<b>Interface Name</b>	Lists the interface over which IPv6 prefix delegation occurs.
<b>T1 timer (seconds)</b>	Lists the amount of time in seconds before the DHCP T1 (delay before renew) timer expires.
<b>T2 timer (seconds)</b>	Lists the amount of time in seconds before the DHCP T2 (delay before rebind) timer expires.
<b>Last Refreshed (seconds)</b>	Lists the time, in seconds, since IPv6 prefix delegation has been updated.
<b>Preferred Lifetime (seconds)</b>	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.
<b>Valid Lifetime (seconds)</b>	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.

- 5 Select **Refresh** to update the statistics counters to their latest values.

## AP Web Filtering

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 Web filter statistics:

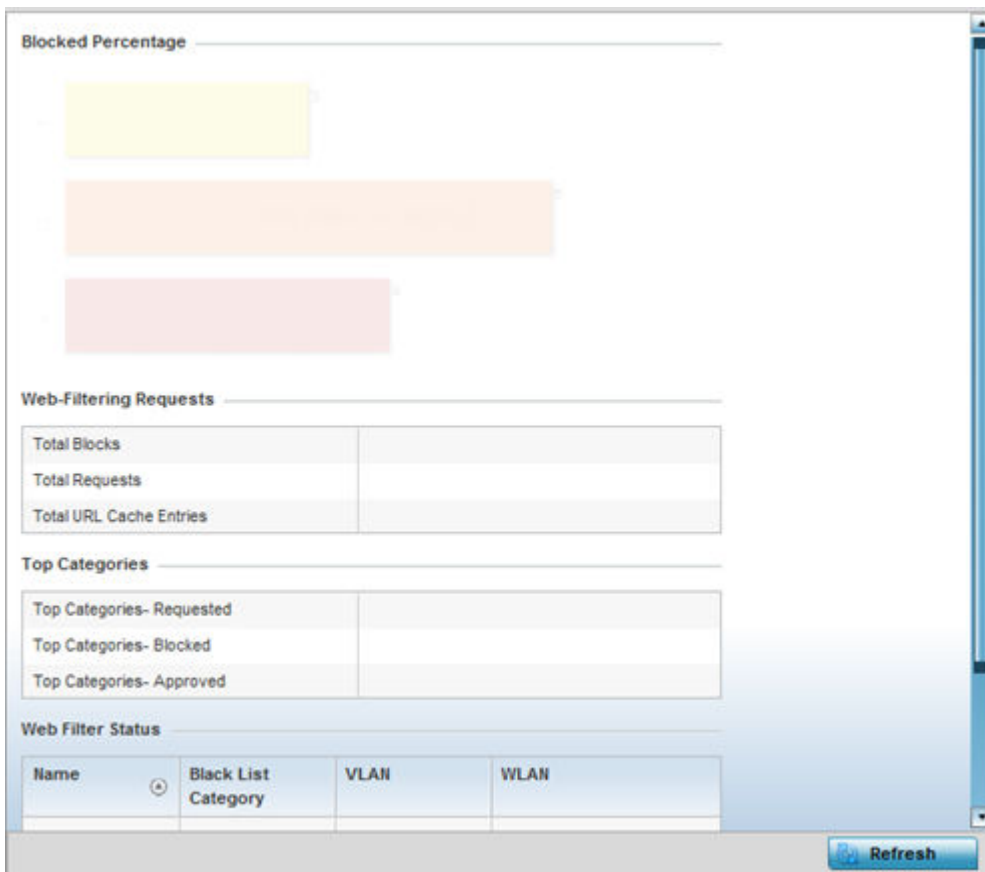
- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.

The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.



- 4 Select **Web-Filtering**.

The **Statistics > AP > Web-Filtering** screen is displayed.



- 5 Review the following Web-Filtering statistics:

The **Web-Filtering Requests** field displays the following information:

<b>Total Blocks</b>	Lists the number of Web request hits against content blocked in the URL blacklist.
<b>Total Requests</b>	Lists the total number of requests for URL content cached locally on this access point.
<b>Total URL Cache Entries</b>	Displays the number of cached 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 <i>whitelist</i> or <i>blacklist</i> .

The **Top Categories** field helps administrators assess the content most requested, blocked and approved based on the defined *whitelist* and *blacklist* permissions:

<b>Top Categories - Requested</b>	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.
<b>Top Categories - Blocked</b>	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.
<b>Top Categories - Approved</b>	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 adheres to your organization's standards for client access.

The **Web Filter Status** field displays the following information:

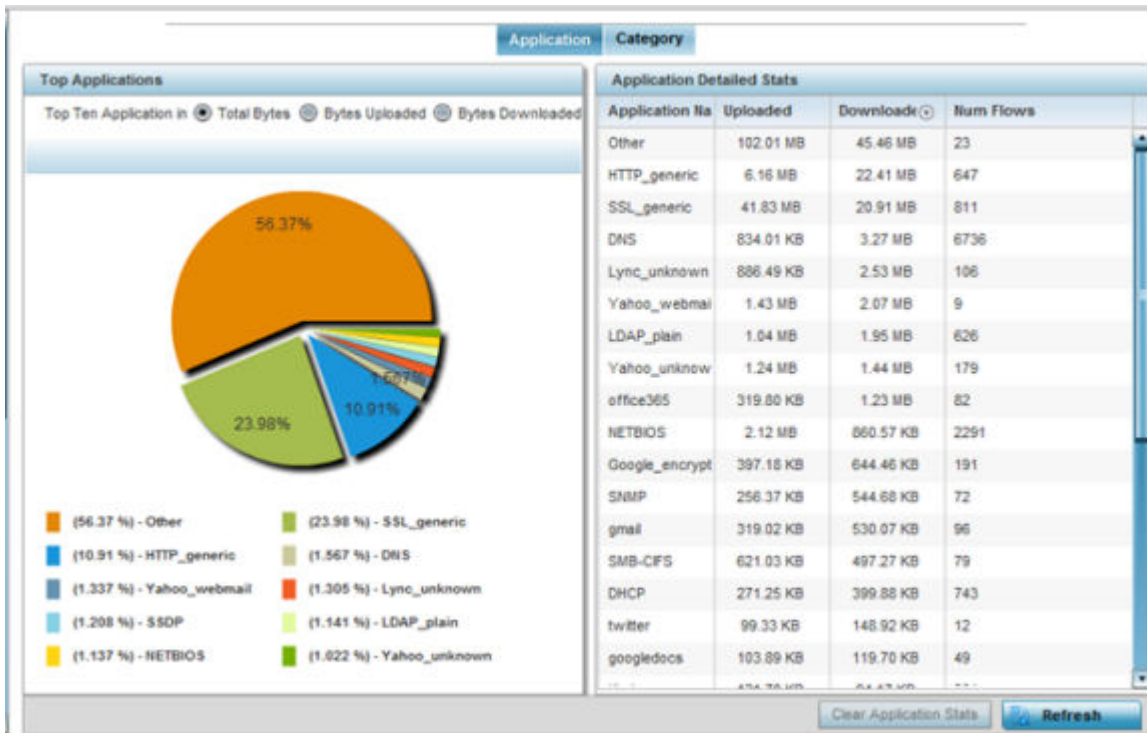
<b>Name</b>	Displays the name of the filter whose URL rule set has been invoked.
<b>Blacklist Category</b>	Lists the blacklist category whose URL filter rule set has caused data to be filtered to a requesting client. Periodically assess whether these rules are still relevant to the data requirements of requesting clients.
<b>VLAN</b>	Lists the impacted access point VLAN whose Web data traffic has been filtered based on the restrictions in the listed blacklist category.
<b>WLAN</b>	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.

- 6 Periodically, select **Refresh** to update this screen to its latest values.

## AP Application Visibility (AVC)

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 access point managed network, refer to Application Policy on page 7-54 and Application on page 7-

- 1 Select the **Statistics** tab from the Web UI.
- 2 Expand the **System** node on the top, left-hand side of the screen.  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.  
The Controller's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **Application Visibility (AVC)** from the menu.  
The **Statistics > AP > Application Visibility (AVC) > Application** screen displays.



Refer to the **Top Applications** graph to assess the most prolific, and allowed, application data passing through the controller/access point managed network.

<b>Total Bytes</b>	Displays the top ten utilized applications in respect to total data bytes passing through the access point managed network. These are only the administrator allowed applications approved for proliferation within the access point managed network.
<b>Bytes Uploaded</b>	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).
<b>Bytes Downloaded</b>	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).

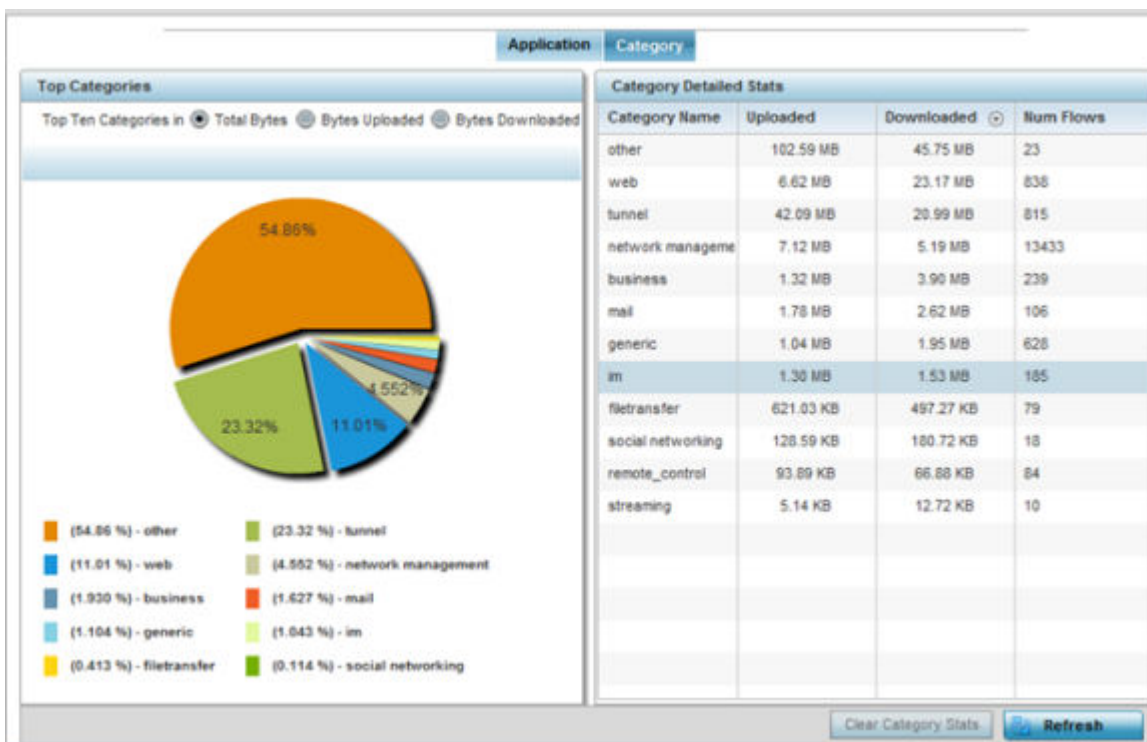
Refer to the **Application Detailed Stats** table to assess specific application data utilization:

<b>Application Name</b>	Lists the allowed application name whose data (bytes) are passing through the access point managed network.
<b>Uploaded</b>	Displays the number of uploaded application data (in bytes) passing the through the access point managed network.

<b>Downloaded</b>	Displays the number of downloaded application data (in bytes) passing through the access point managed network.
<b>Num Flows</b>	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.

- 5 Click **Clear Application Stats** to clear the application assessment data counters and begin a new assessment. Selecting this option will not clear category stats, just application stats.
- 6 Click 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- The **Statistics > Controller > Application Visibility > Category** screen displays.



Refer to the **Top Categories** graph to assess the most prolific, and allowed, application data categories utilized by the access point.

<b>Total Bytes</b>	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.
<b>Bytes Uploaded</b>	Displays the top ten application categories in respect to total data bytes uploaded through the access point managed network. If this category data is not aligned with application utilization expectations, consider allowing or denying additional categories or adjusting their precedence (priority).
<b>Bytes Downloaded</b>	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).

Refer to the **Category Detailed Stats** table to assess specific application category data utilization:

<b>Category Name</b>	Lists the allowed category whose application data (in bytes) is passing through the access point managed network.
<b>Uploaded</b>	Displays the number of uploaded application category data (in bytes) passing the through the access point managed network.
<b>Downloaded</b>	Displays the number of downloaded application category data (in bytes) passing the through the access point managed network.
<b>Num Flows</b>	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.

- 7 Click **Clear Category Stats** to clear the application category assessment data counters and begin a new assessment. Selecting this option will not clear application stats, just category stats.
- 8 Click **Refresh** to update the statistics counters to their latest values.

## AP 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 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.



## AP Device Upgrade

The **Device Upgrade** screen displays information about devices receiving updates and those devices to perform an update. 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen).
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **Device Upgrade**.

The AP Upgrade statistics screen is displayed.

Device Hostname	Type	State	Time Last Upgraded	Retries Count	Upgraded By	Last Update Status
ap6532-A65731	ap6532	failed	Mon Apr 13 2015 01:16:40 AM	3	NX95-Pri	download timed out
ap621-E9F899	ap621	failed	Mon Apr 13 2015 01:16:39 AM	3	NX95-Pri	download timed out
ap6532-34776C	ap6532	done	Tue Apr 14 2015 02:20:39 AM	2	NX95-Pri	download timed out
ap8232-7F0DE4	ap82xx	done	Tue Apr 28 2015 06:19:33 AM	1	NX95-Pri	download timed out
ap6532-347800	ap6532	failed	Mon Apr 13 2015 01:16:39 AM	3	NX95-Pri	download timed out
ap6532-A65720	ap6532	failed	Mon Apr 13 2015 01:16:40 AM	3	NX95-Pri	download timed out
ap6532-3475E4	ap6532	failed	Mon Apr 13 2015 01:16:39 AM	3	NX95-Pri	download timed out
ap8132-738E20	ap81xx	failed	Mon Apr 13 2015 01:16:40 AM	3	NX95-Pri	download timed out
ap6511-8A4B11	ap6511	failed	Mon Apr 13 2015 01:16:40 AM	3	NX95-Pri	download timed out
ap6532-A65720	ap6532	done	Wed May 6 2015 12:59:30 AM	1	NX95-Pri	Update error: Unable to get
ap6532-347800	ap6532	done	Wed May 6 2015 12:59:30 AM	1	NX95-Pri	Update error: Unable to get
ap650-2433AC	ap650	done	Wed May 6 2015 12:59:24 AM	1	NX95-Pri	Update error: Unable to get

Type to search in tables Row Count: 2047

This screen displays the following:

<b>Device Hostname</b>	Displays the administrator-assigned hostname of the access point receiving the update.
<b>Type</b>	Displays the model type of the access point receiving a firmware update.
<b>State</b>	Displays the current state of the upgrade process ( <b>done</b> , <b>failed</b> , etc.).
<b>Time Last Upgraded</b>	Displays the date and time of the last successful access point upgrade operation.
<b>Retries Count</b>	Displays the number of retries made in an access point update operation.
<b>Upgraded By</b>	Displays the MAC address of the access point that performed the upgrade.
<b>Last Update Status</b>	Displays the status of the last upgrade operation ( <b>Start Upgrade</b> , <b>Update error</b> , etc.).

- 5 Select **Clear History** to clear the screen of its current status and begin a new data collection.
- 6 Select **Refresh** to update the screen's statistics counters to their latest values.





<b>Access Point</b>	Displays the name assigned to the adopted access point as part of its device configuration.
<b>Type</b>	Displays each listed access point's model type
<b>RF Domain Name</b>	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.
<b>Model Number</b>	Displays each listed access point's model number
<b>Config Status</b>	Displays each listed access point's configuration status to help determine its service role.
<b>Config Errors</b>	Lists any configuration errors that may be hindering a clean adoption.
<b>Adopted By</b>	Lists the adopting access point.
<b>Adoption Time</b>	Displays each listed access point's time of adoption.
<b>Startup Time</b>	Displays each listed access point's in-service time since last offline.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values..

### AP Adoption History

An **AP Adoption History** screen displays a list of peer access points and their adoption event status.

To view historical statistics for adopted access points:

- 1 Select the **Statistics** tab from the Web UI.
- 2 Expand the **System** from the navigation pane (on the left-hand side of the screen). The System node expands to display RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Adoption** menu.
- 5 Select **AP Adoption History**.

The **Adoption > Adoption History** screen is displayed.

Event Name	AP MAC Address	Reason	Event Time
Adopted	00-23-68-8D-FE-4C	N.A.	Tue Aug 20 2013 04:59:52 PM
Adopted	B4-C7-99-5A-84-2C	N.A.	Tue Aug 20 2013 04:59:52 PM
Adopted	5C-0E-8B-34-7B-7C	N.A.	Tue Aug 20 2013 05:01:49 PM
Adopted	5C-0E-8B-A6-57-2C	N.A.	Tue Aug 20 2013 05:01:50 PM
Adopted	00-23-68-31-18-E0	N.A.	Tue Aug 20 2013 05:01:51 PM
Adopted	5C-0E-8B-34-77-6C	N.A.	Tue Aug 20 2013 05:01:51 PM
Adopted	5C-0E-8B-34-78-00	N.A.	Tue Aug 20 2013 05:01:51 PM
Adopted	00-23-68-31-29-D8	N.A.	Tue Aug 20 2013 05:01:51 PM
Adopted	B4-C7-99-58-64-A0	N.A.	Tue Aug 20 2013 05:01:52 PM
Adopted	B4-C7-99-71-16-30	N.A.	Tue Aug 20 2013 05:01:52 PM
Adopted	5C-0E-8B-34-76-38	N.A.	Tue Aug 20 2013 05:01:52 PM
Adopted	5C-0E-8B-34-50-3C	N.A.	Tue Aug 20 2013 05:01:52 PM
Adopted	5C-0F-8B-8A-4B-15	N.A.	Tue Aug 20 2013 05:01:52 PM

Type to search in tables Row Count: 26

**Refresh**

This screen describes the following historical data for adopted access points:

<b>Event Name</b>	Displays the adoption status of each listed access point as either <b>adopted</b> or <b>un-adopted</b> .
<b>AP MAC Address</b>	Displays the MAC address of each access point this access point has attempted to adopt.
<b>Reason</b>	Displays the reason code for each event listed in the adoption history table.
<b>Event Time</b>	Displays day, date and time for each access point adoption attempt.

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

### AP Self Adoption History

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** tab from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Adoption** menu.
- 5 Select **AP Self Adoption History**.

The **Adoption > AP Self Adoption History** screen is displayed.

Event History	Mac	Reason	Adoption Time
Adopted	B4-C7-99-0C-98-48	N.A.	Wed May 6 2015 12:49:15 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Tue May 5 2015 06:05:38 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Tue May 5 2015 05:56:35 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Wed May 6 2015 12:50:59 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Wed May 6 2015 12:56:56 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Tue May 5 2015 06:05:19 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Tue May 5 2015 05:59:58 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Wed May 6 2015 12:56:47 AM
Adopted	B4-C7-99-0C-98-48	N.A.	Wed May 6 2015 12:45:07 AM
un-adopted	B4-C7-99-0C-98-48	Adopter 19.0C.98.48 is no longer reac	Wed May 6 2015 12:42:12 AM
un-adopted	B4-C7-99-0C-98-48	Adopter 19.0C.98.48 is no longer reac	Wed May 6 2015 12:48:59 AM
un-adopted	B4-C7-99-0C-98-48	Adopter 19.0C.98.48 is no longer reac	Tue May 5 2015 05:56:11 AM

Type to search in tables Row Count: 16

**Refresh**

This screen describes the following historical data for adopted access points:

<b>Event History</b>	Displays the self adoption status of each AP as either <b>Adopted</b> or <b>un-adopted</b> .
<b>MAC</b>	Displays the MAC of the auto adopted access point.
<b>Reason</b>	Displays the adoption reason code for an access point's auto adoption.
<b>Adoption Time</b>	Displays a timestamp for the access point's auto-adoption.

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.



## AP Detection

The **AP Detection** screen displays potentially hostile access points, their SSIDs, reporting AP, and so on. Continuously re-validating 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen).
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **AP Detection**.

The **Statistics > Access Point > AP Detection** screen displays.

	Unsanctioned AP	Reporting AP	SSID	AP Mode	Radio Type	Channel	RSSI	Last Seen
📶	00-11-3F-DD-B7-20		wlan1			6	-68 dBm	2s
📶	00-11-3F-DE-AE-E0		checksum			11	-66 dBm	33s
📶	00-11-3F-DE-B9-90		traffic_shaping			6	-70 dBm	4s
📶	00-11-3F-E3-4B-90		remotevpn			6	-79 dBm	2s
📶	00-13-60-D4-A0-20		nanoDemo_1			6	-64 dBm	5s
📶	00-14-C2-AA-FF-10		asa			7	-66 dBm	3s
📶	00-15-70-AE-32-38		M-Wireless			6	-74 dBm	18s
📶	00-15-70-AE-33-E8		M-Guest			6	-68 dBm	6s
📶	00-15-70-AE-33-F8		M-Guest			6	-65 dBm	2s
📶	00-15-70-AE-37-A0		M-Wireless			1	-55 dBm	40s
📶	00-15-70-AE-38-60		M-Wireless			11	-69 dBm	33s
📶	00-15-70-C8-4F-60		test_pppoe_wlan			6	-75 dBm	17s

Type to search in tables Row Count: 190

This screen displays the following:

<b>Unsanctioned AP</b>	Displays the MAC address detected access points that are yet to be authorized for interoperability within the access point managed network.
<b>Reporting AP</b>	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.
<b>SSID</b>	Displays the WLAN SSID the unsanctioned access point was detected on.
<b>AP Mode</b>	Displays the operating mode of the unsanctioned access point.
<b>Radio Type</b>	Displays the type of the radio on the unsanctioned access point. The radio can be <i>802.11b</i> , <i>802.11bg</i> , <i>802.11gn</i> , <i>802.11a</i> or <i>802.11an</i> .
<b>Channel</b>	Displays the channel the unsanctioned access point is currently transmitting on.
<b>Last Seen</b>	Displays the time (in seconds) the unsanctioned access point was last seen on the network.
<b>RSSI</b>	Lists a RSSI (relative signal strength indication) for a detected (and perhaps unsanctioned) access point.

- 5 T
- 6 Select **Clear All** to clear the screen of its current status and begin a new data collection.
- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Wireless Clients

The **Wireless Clients** 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. Clients can be selected from amongst those displayed to display the client's configuration in greater detail.

To view wireless client statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **Wireless Clients**.

The **Statistics > Access Point > Wireless Client** screen displays.

Client MAC	IP Address	IPv6 Address	Hostname	Role	Client Identity	Vendor	Band	AP Hostname	Radio MAC	WLAN	VLAN	Last Active
<a href="#">08-60-8E-9C-</a>	157.235.91		android-5841	NA	Unknown	ASUSTel	11bgn	AN-17-311	00-23-	STCWL	30	Fri Jan 10 1
<a href="#">24-77-03-CD-</a>	157.235.91		acc125-01	NA	Unknown	Intel Corp	11an	AN-17-311	00-23-	STCWL	30	Fri Jan 10 1

Type to search in tables Row Count: 2

[Disconnect Client](#) [Refresh](#)

This screen displays the following information:

<b>Client MAC</b>	Lists the factory encoded hardware identifier for each listed client. The MAC address displays as a link that can be selected to display individual client configuration and network address information in greater detail.
<b>IP Address</b>	Displays the unique IP address of the client. Use this address as necessary throughout the applet for filtering and device intrusion recognition and approval.
<b>IPv6 Address</b>	Displays the current IPv6 formatted IP address a listed guest client is using as a network identifier. IPv6 is the latest revision of the <i>Internet Protocol (IP)</i> designed to replace IPv4. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.

<b>Hostname</b>	Displays the hostname (MAC addresses) of connected wireless clients. The hostname displays as a link that can be selected to display configuration and network address information in greater detail.
<b>Role</b>	Lists the client's defined role within the access point managed network.
<b>Client Identity</b>	Displays the unique Client Identity of this device.
<b>Vendor</b>	Lists the name of the manufacturer (hardware vendor) of each listed client to help assess its compatibility with the WiNG managed wireless infrastructure.
<b>Band</b>	Displays the 802.11 radio band on which the listed wireless client operates.
<b>AP Hostname</b>	Displays the administrator assigned name applied to the access point detecting the listed client.
<b>Radio MAC</b>	Lists the factory encoded hardware identifier assigned to the detecting access point radio.
<b>WLAN</b>	Displays the name of the WLAN the access point's using with each listed 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.
<b>VLAN</b>	Displays the VLAN ID each listed client is currently mapped to as a virtual interface for access point interoperability.
<b>Last Active</b>	Displays a time stamp when the detected client was last observed within the network.

- 5 Select a specific client MAC address and select **Disconnect Client** to terminate this client's connection and RF Domain membership.
- 6 Select **Refresh** to update the screen's statistics counters to their latest values.
- 7 The **Wireless Clients** screen displays the following:

## AP Wireless LANs

The **Wireless LANs** screen displays an access point WLAN utilization. This screen displays access point WLAN assignments, SSIDs, traffic utilization, WLAN radio utilization and transmit and receive statistics.

To review a selected access point's WLAN statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **Wireless LANs**.

The **Statistics > Access Point > Wireless WLANs** screen displays.

Client MAC	IP Address	IPv6 Address	Hostname	Role	Client Identity	Vendor	Band	AP Hostname	Radio MAC	WLAN	VLAN	Last Active
08-60-6E-9C	157.235.91		android-5841	NA	Unknown	ASUSTel	11bgn	AN-17-311	00-23-10-00-00-00	STCWL	30	Fri Jan 10 1
24-77-03-CD	157.235.91		acc125-01	NA	Unknown	Intel Corp	11an	AN-17-311	00-23-10-00-00-00	STCWL	30	Fri Jan 10 1

Type to search in tables Row Count: 2

Disconnect Client Refresh

This screen displays the following:

<b>WLAN Name</b>	Displays the name of the WLAN the access point is currently using for client support and QoS configuration segregation (voice versus data etc.).
<b>SSID</b>	Displays each listed WLAN's SSID.
<b>Traffic Index</b>	<p>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. Low indexes may require administration to assess why there's an excess of missed packets.</p> <p>Traffic indices are:</p> <ul style="list-style-type: none"> <li>• 0 - 20 (very low utilization)</li> <li>• 20 - 40 (low utilization)</li> <li>• 40 - 60 (moderate utilization)</li> <li>• 60 and above (high utilization)</li> </ul>
<b>Radio Count</b>	Displays the cumulative number of peer access point radios deployed within each listed WLAN.
<b>Tx Bytes</b>	Displays the total number of transmitted bytes on each listed WLAN.
<b>Tx User Data Rate</b>	Displays the user data rate in kbps for each listed WLAN.
<b>Rx Bytes</b>	Displays the total number of packets (in bytes) received on each listed WLAN.
<b>Rx User Data Rate</b>	Displays the received user data rate on each listed WLAN.

- 5 Select an WLAN then **Disassociate All Clients** to terminate each client connection within that WLAN.
- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

### AP Policy Based Routing

The **Policy Based Routing** screen displays statistics for selective PBR (path packet redirection). PBR can optionally mark traffic for preferential services (QoS). PBR is applied to incoming routed packets, and a





<b>Default Next Hop IP</b>	If a packet subjected to PBR does not have an explicit route to its destination, the pre-set 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.
<b>Default Next Hop State</b>	Displays whether the default hop is being applied to incoming routed packets.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Radios

The **Radio** statistics screens display information on access point radios. The actual number of radios depend on the access point model and type. The radio statistics screens display information on a per radio basis. Use this information to refine and optimize the performance of each radio and improve client throughput.

The access point's radio statistics screens detail associated radio ID, type, RF quality index etc. Use this information to assess the overall health of radio transmissions and access point deployment accuracy.

Each of these screens provide enough statistics to troubleshoot issues related to the following three areas:

- [AP Radio Status](#) on page 1177
- [AP Radio RF Statistics](#) on page 1178
- [AP Radio Traffic Statistics](#) on page 1180

Individual access point radios display as selectable links within each of the three radio screens. To review a radio's configuration in greater detail, select the link within the Radio column. Use the **Details** screen to review this radio's configuration in greater detail, as additional deployment location, configuration, Smart RF, quality index and wireless client information becomes available.

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.

### AP Radio Status

Use the **Status** screen to review access point radio stats in detail. Optionally select individual and access points and launch sub screens with granular performance data. Review radios, operational states, channel utilization and power consumption to assess whether a radio is optimally configured or physically deployed..

To view access point radio statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.









<b>Portal Radio MAC</b>	Lists the MAC addresses of those access points serving as portals within the mesh network.
<b>Connect Time</b>	Displays the elapsed connection time for each listed client in the mesh network.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Interfaces

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.

Use the following screens to review the configuration of each unique access point model interface:

- [AP Interface General Statistics](#) on page 1182
- [AP Interface IPv6 Address](#) on page 1186
- [AP Interface Multicast Groups Joined](#) on page 1189
- [AP Interface Network Graph](#) on page 1190

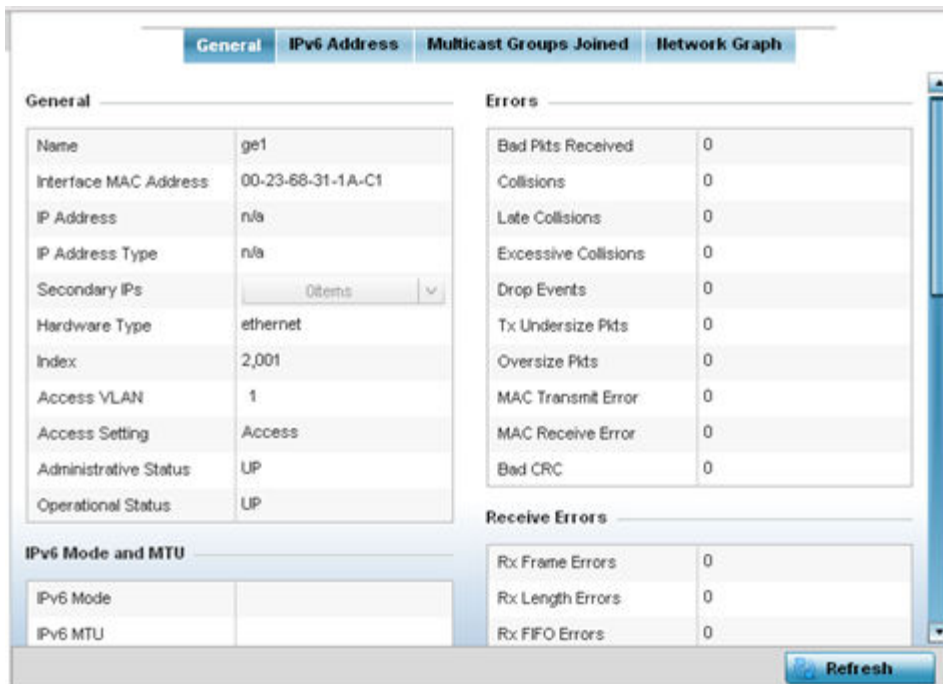
### *AP Interface General Statistics*

The **General** screen provides information on a selected access point interface such as its MAC address, type and TX/RX statistics.

To view the general interface statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Interfaces** menu.

The **Statistics > AP > Interface > General** screen displays.



- 5 Select an access point interface from those available for the selected model. The subsequent display within the **General** and **Network Graph** tabs is specific to the selected model and interface.

The **General** field describes the following:

<b>Name</b>	Displays the name of the access point interface <b>ge1</b> , <b>vlan1</b> , etc.
<b>Interface MAC Address</b>	Displays the MAC address of the access point interface.
<b>IP Address</b>	IP address of the interface.
<b>IP Address Type</b>	Displays the IP address type, either <b>IPv4</b> or <b>IPv6</b> .
<b>Secondary IP</b>	Displays a list of secondary IP resources assigned to this interface.
<b>Hardware Type</b>	Displays the hardware connected type of the interface.
<b>Index</b>	Displays the unique numerical identifier supporting the interface.
<b>Access VLAN</b>	Displays the tag assigned to the native VLAN.
<b>Access Setting</b>	Displays the mode of the VLAN as either <b>Access</b> or <b>Trunk</b> .
<b>Administrative Status</b>	Displays whether the interface is currently <b>UP</b> or <b>DOWN</b> .
<b>Operational Status</b>	Lists whether the selected interface is currently <b>UP</b> (operational) or <b>DOWN</b> .

The **IPv6 Mode and MTU** table displays the following:

<b>IPv6 Mode</b>	Lists the current IPv6 mode utilized.
<b>IPv6 MTU</b>	Lists the IPv6 formatted largest packet size that can be sent over this interface.

The **Specification** field displays the following:



<b>Media Type</b>	Displays the physical connection type of the interface. Medium types include: <b>Copper</b> - Used on RJ-45 Ethernet ports <b>Optical</b> - Used on fibre optic gigabit Ethernet ports
<b>Protocol</b>	Displays the routing protocol used by the interface.
<b>MTU</b>	Displays the MTU (maximum transmission unit) 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.
<b>Mode</b>	The mode can be either: <ul style="list-style-type: none"> <li>• <b>Access</b> - This Ethernet interface accepts packets only from the native VLANs.</li> <li>• <b>Trunk</b> - This Ethernet interface allows packets from a list of VLANs you can add to the trunk.</li> </ul>
<b>Metric</b>	Displays the metric associated with the interface's route.
<b>Maximum Speed</b>	Displays the maximum speed the interface uses to transmit or receive data.
<b>Admin. Speed</b>	Displays the speed the port can transmit or receive. This value can be either <b>10</b> , <b>100</b> , <b>1000</b> or <b>Auto</b> . This value is the maximum port speed in Mbps. Auto indicates the speed is negotiated between connected devices..
<b>Operator Speed</b>	Displays the current speed of the data transmitted and received over the interface.
<b>Admin. Duplex Setting</b>	Displays the administrator's duplex setting.
<b>Current Duplex Setting</b>	Displays the interface as either <b>half duplex</b> , <b>full duplex</b> or <b>unknown</b> .

The **Traffic** field describes the following for the selected access point interface:

<b>Good Octets Sent</b>	Displays the number of octets (bytes) with no errors sent by the interface.
<b>Good Octets Received</b>	Displays the number of octets (bytes) with no errors received by the interface.
<b>Good Pkts Sent</b>	Describes the number of good packets transmitted.
<b>Good Pkts Received</b>	Describes the number of good packets received.
<b>Mcast Pkts Sent</b>	Displays the number of multicast packets sent through the selected interface.
<b>Mcast Pkts Received</b>	Displays the number of multicast packets received through the selected interface.
<b>Ucast Pkts Sent</b>	Displays the number of unicast packets sent through the selected interface.
<b>Ucast Pkts Received</b>	Displays the number of unicast packets received through the selected interface.
<b>Bcast Pkts Sent</b>	Displays the number of broadcast packets sent through the interface.
<b>Bcast Pkts Received</b>	Displays the number of broadcast packets received through the interface.
<b>Packet Fragments</b>	Displays the number of packet fragments transmitted or received through the interface.
<b>Jabber Pkts</b>	Displays the number of packets transmitted through the interface larger than the MTU.

The **Errors** field displays the following information for the selected access point interface:

<b>Bad Pkts Received</b>	Displays the number of bad packets received through the interface.
<b>Collisions</b>	Displays the number of collisions on the interface.



<b>Late Collisions</b>	A late collision is any collision that occurs after the first 64 octets of data have been sent by the sending client. Late collisions are not normal, and are usually the result of out-of-specification cabling or a malfunctioning device.
<b>Excessive Collisions</b>	Displays the number of excessive collisions. Excessive collisions occur when the traffic load increases to the point that a single Ethernet network cannot handle it efficiently.
<b>Drop Events</b>	Displays the number of dropped packets transmitted or received through the interface.
<b>Tx Undersize Pkts</b>	Displays the number of <i>undersized</i> packets transmitted through the interface.
<b>Oversize Pkts</b>	Displays the number of <i>oversized</i> packets transmitted through the interface.
<b>MAC Transmit Error</b>	Displays the number of transmits that failed because of an internal MAC sublayer error that is not a late collision, excessive collision count, or a carrier sense error.
<b>MAC Receive Error</b>	Displays the number of received packets failed because of an internal MAC sublayer that is not a late collision, excessive collision count, or a carrier sense error.
<b>Bad CRC</b>	Displays the CRC error. The <i>Cyclical Redundancy Check</i> (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 the frame, it's considered a bad CRC.

The **Receive Errors** field displays the following information about the selected interface:

<b>Rx Frame Errors</b>	Displays the number of frame errors received at the interface. A frame error occurs when a byte of data is received, but not in the format expected.
<b>Rx Length Errors</b>	Displays the number of length errors received at the interface. Length errors are generated when the received frame length was less than (or exceeded) the Ethernet standard.
<b>Rx FIFO Errors</b>	Displays the number of FIFO errors received at the interface. <i>First-in First-Out</i> queueing is an algorithm that involves buffering and forwarding of packets in the order of arrival. FIFO entails no priority for traffic. There is only one queue, and all packets are treated equally.
<b>Rx Missed Errors</b>	Displays the number of missed packets. Packets are missed when the hardware received FIFO has insufficient space to store the incoming packet.
<b>Rx Over Errors</b>	Displays the number of overflow errors. An overflow occurs when packet size exceeds the allocated buffer size.

The **Transmit Errors** field displays the following:

<b>Tx Errors</b>	Displays the number of packets with errors transmitted on the interface.
<b>Tx Dropped</b>	Displays the number of transmitted packets dropped from the interface.
<b>Tx Aborted Errors</b>	Displays the number of packets aborted on the interface because a <i>clear-to-send</i> request was not detected.
<b>Tx Carrier Errors</b>	Displays the number of carrier errors on the interface. This generally indicates bad Ethernet hardware or cabling.
<b>Tx FIFO Errors</b>	Displays the number of FIFO errors received at the interface. <i>First-in-First-Out</i> queueing is an algorithm that involves the buffering and forwarding of packets in the order of arrival. FIFO entails no priority for traffic. There is only one queue, and all packets are treated equally.

<b>Tx Heartbeat Errors</b>	Displays the number of heartbeat errors. This generally indicates a software crash or packets stuck in an endless loop.
<b>Tx Window Errors</b>	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) in the receive window field 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 from the receiving host, it constitutes a window error.

- 6 Select **Refresh** to update the statistics counters to their latest value.

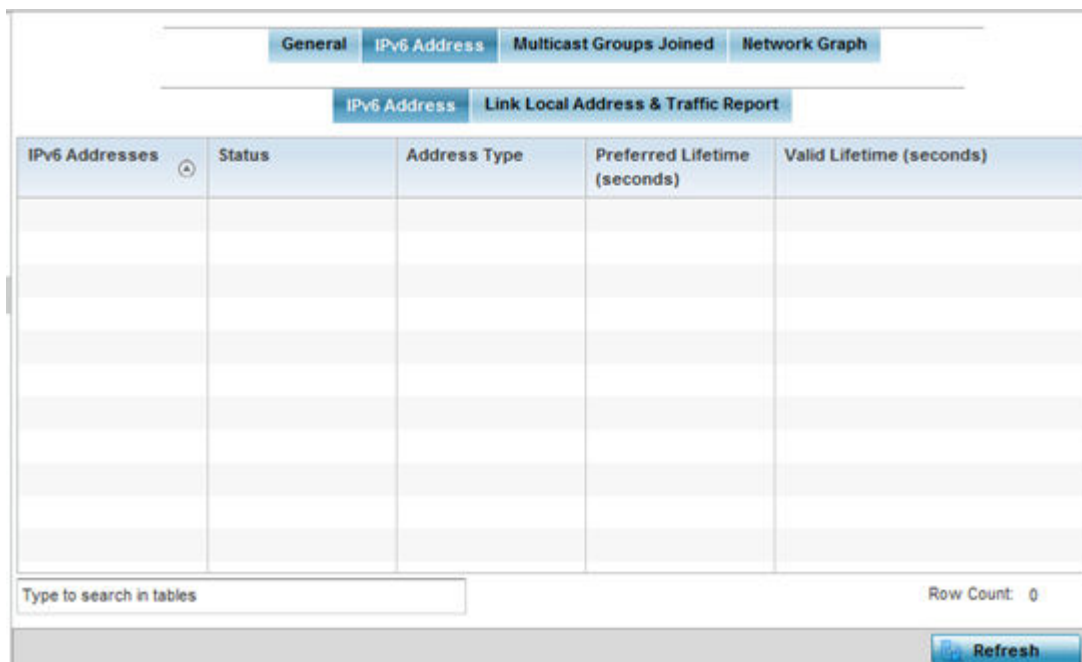
### AP Interface IPv6 Address

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 review IPv6 Address interface statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.  
The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Interfaces** menu.
- 5 Select the **IPv6 Address** tab.

The **Statistics > AP > Interfaces > IPv6 Address > IPv6 Address** screen displays by default in the right-hand pane.



The IPv6 Address table displays the following sections:

<b>IPv6 Addresses</b>	Lists the IPv6 formatted addresses currently utilized by the access point in the selected interface.
<b>Status</b>	Lists the current utilization status of each IPv6 formatted address currently in use by this access point's selected interface.
<b>Address Type</b>	Lists whether the address is <i>unicast</i> or <i>multicast</i> in its utilization over the selected access point interface.
<b>Preferred Lifetime (Seconds)</b>	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.
<b>Valid Lifetime (Seconds)</b>	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.

This screen has the following information:

The **Link Local Address** table:

<b>Address</b>	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.
<b>Status</b>	Lists the IPv6 local link address utilization status and its current availability.
<b>Preferred Lifetime (Seconds)</b>	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.
<b>Valid Lifetime (Seconds)</b>	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.

The **Traffic** table displays the following information:

<b>Packets In</b>	Lists the number of IPv6 formatted data packets received on the selected access point interface since the screen was last refreshed.
<b>Packets Out</b>	Lists the number of IPv6 formatted data packets transmitted on the selected access point interface since the screen was last refreshed.
<b>Bytes In</b>	Displays the number of octets (bytes) with no errors received by the selected interface.
<b>Bytes Out</b>	Displays the number of octets (bytes) with no errors sent by the selected interface.
<b>Bad Packets Received</b>	Displays the number of bad IPv6 formatted packets received through the interface.



<b>Bad CRC</b>	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.
<b>Collisions</b>	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.

The **Receive Errors** table displays the following information:

<b>Receive Length Errors</b>	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.
<b>Receive Over Errors</b>	Displays the number of IPv6 overflow errors received. Overflows occur when a packet size exceeds the allocated buffer size.
<b>Receive Frame Errors</b>	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.
<b>Receive FIFO Errors</b>	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.
<b>Receive Missed Errors</b>	Displays the number of missed IPv6 formatted packets. Packets are missed when the hardware received FIFO has insufficient space to store an incoming packet.

The **Transmit Errors** table displays the following information:

<b>Transmit Errors</b>	Displays the number of IPv6 formatted data packets with errors transmitted on the interface.
<b>Transmit Aborted Errors</b>	Displays the number of IPv6 formatted packets aborted on the interface because a clear-to-send request was not detected.
<b>Transmit Carrier Errors</b>	Displays the number of IPv6 formatted carrier errors on the interface. This generally indicates bad Ethernet hardware or bad cabling.
<b>Transmit FIFO Errors</b>	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.



<b>Transmit Heartbeat Errors</b>	Displays the number of IPv6 formatted heartbeat errors. This generally indicates a software crash, or packets stuck in an endless loop.
<b>Transmit Window Errors</b>	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.

- 7 Click **Refresh** to update the statistics counters to their latest value.

### *AP Interface Multicast Groups Joined*

Multicast groups scale to a larger set of destinations by not requiring prior knowledge of who or how many destinations there are. Multicast devices use 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.  
The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Interfaces** menu.
- 5 Select the **Multicast Groups Joined** tab.  
The **Statistics > AP > Interfaces > Multicast Groups Joined** displays in the right-hand pane.

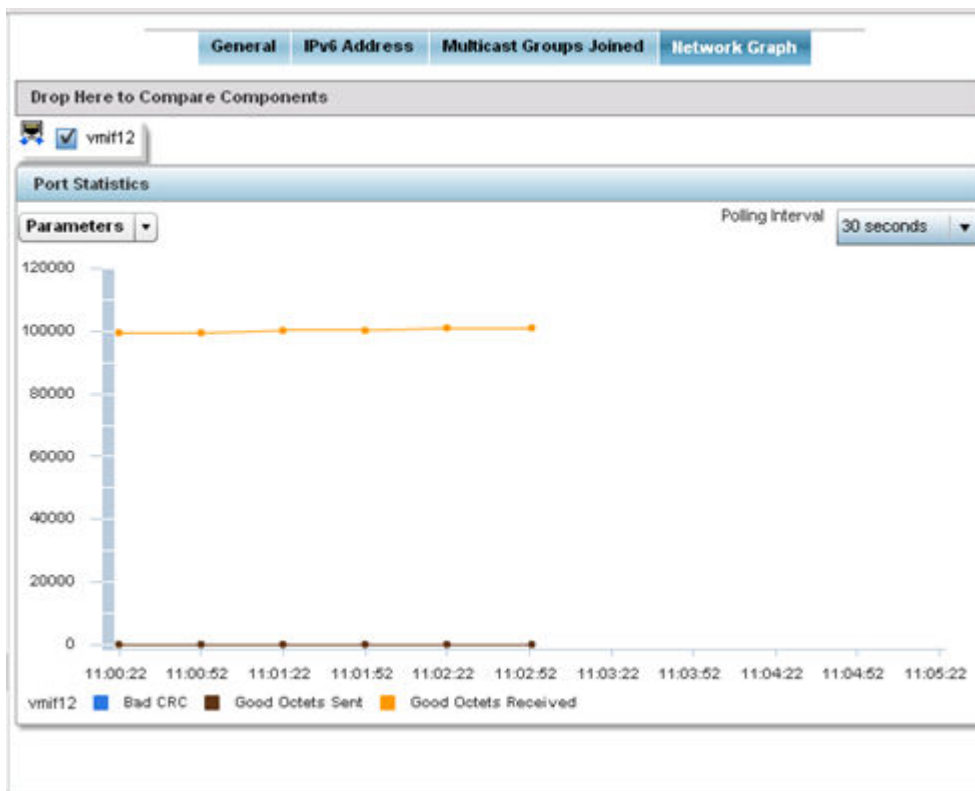


- Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.

The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- Select the **Interfaces > Network Graph** tab.

The **Statistics > AP > Interfaces > Network Graph** screen displays in the right-hand pane.



- Use the **Parameters** drop-down menu to specify what is trended in the graph.

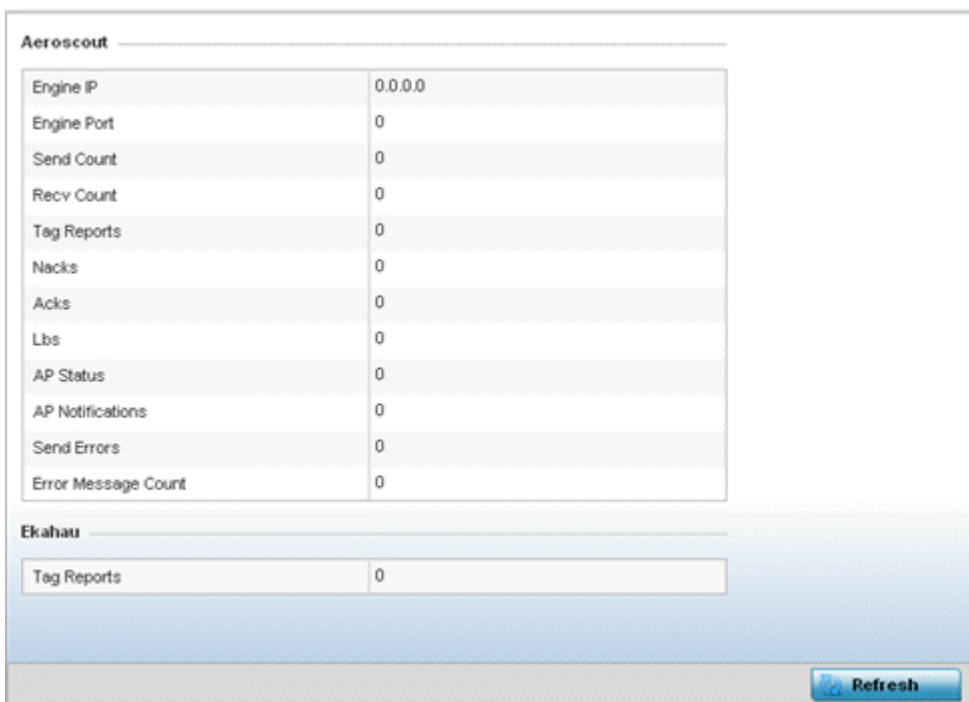
## AP RTLS

The RTLS (real time locating system) 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:

- Select the **Statistics** menu from the Web UI.
- Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- Select the **RTLS** tab.

The **Statistics > AP > RTLS** screen is displayed.



Review the following *Aeroscout tags* related statistics:

<b>Engine IP</b>	Lists the IP address of the Aeroscout locationing engine.
<b>Engine Port</b>	Displays the port number of the Aeroscout engine.
<b>Send Count</b>	Lists the number location determination packets sent by the locationing engine.
<b>Recv Count</b>	Lists the number location determination packets received by the locationing engine.
<b>Tag Reports</b>	Displays the number of tag reports received from locationing equipped radio devices supporting RTLS.
<b>Nacks</b>	Displays the number of Nack (no acknowledgement) frames received from RTLS supported radio devices providing locationing services.
<b>Acks</b>	Displays the number of Ack (acknowledgment) frames received from RTLS supported radio devices providing locationing services.
<b>Lbs</b>	Displays the number of LBS (location based service) frames received from RTLS supported radio devices providing locationing services.
<b>AP Status</b>	Provides the status of peer APs providing locationing assistance.
<b>AP Notifications</b>	Displays a count of the number of notifications sent to access points that may be available to provide RTLS support.
<b>Send Errors</b>	Lists the number of send errors received by the RTLS initiating access point.
<b>Error Message Count</b>	Displays a cumulative count of error messages received from RTLS enabled access point radios.

Review the following *Ekahau tags* related statistics:



**Tag Reports** Displays the number of tag reports received from locating equipped radio devices supporting RTLS.

- 5 Select **Refresh** to update the screen’s statistics counters to their latest values.

## AP PPPoE

The **PPPoE** statistics screen displays stats derived from an access point’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 an existing Ethernet interface.

To review a selected access point’s PPPoE statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point’s statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **PPPoE**.

The **Statistics > AP > PPPoE** screen is displayed.

The **Configuration Information** field screen displays the following:

<b>Shutdown</b>	Displays whether a high speed client mode point-to-point connection has been enabled using the PPPoE protocol.
<b>Service</b>	Lists the 128 character maximum PPPoE client service name provided by the service provider.

<b>DSL Modem Network (VLAN)</b>	Displays the PPPoE VLAN (client local network) connected to the DSL modem. This is the local network connected to DSL modem.
<b>Authentication Type</b>	Lists authentication type used by the PPPoE client whose credentials must be shared by its peer access point. Supported authentication options include <b>None</b> , <b>PAP</b> , <b>CHAP</b> , <b>MSCHAP</b> , and <b>MSCHAP-v2</b> .
<b>Username</b>	Displays the 64 character maximum username used for authentication support by the PPPoE client.
<b>Password</b>	Displays the 64 character maximum password used for authentication by the PPPoE client.
<b>Client Idle Timeout</b>	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.
<b>Keep Alive</b>	If a keep alive is utilized, the point-to-point connect to the PPPoE client is continuously maintained and not timed out.
<b>Maximum Transmission Unit (MTU)</b>	Displays the PPPoE client MTU (maximum transmission unit) 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.

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 **Refresh** to update the screen's statistics counters to their latest values.

## AP OSPF

OSPF (Open Shortest Path First) is a *link-state* IGP (interior gateway protocol). 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](#)
- [AP OSPF Interface](#) on page 1203
- [OSPF State](#)

### AP OSPF Summary

Use the **OSPF Summary** screen to review router ID, area border router, shortest path and stub router connection assignments.

To view OSPF statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **OSPF** menu.

The **Statistics > AP > OSPF > Summary** screen displays by default.

General	
Router ID	
RFC 1583 compliant	
RFC 2328 compliant	
External LSAs	
External LSA CheckSum	#0000
Opaque LSA origination	
Opaque AS LSA checksum	#0000
Opaque LSA	
Opaque AS LSAs	
Shutdown Due Time	
Gracefull shutdown	
LSA refresh timer(sec)	
Number of OSPF areas	

ABR/ASBR Details	
ASBR	
ABR	
ABR Type	

SPF

Refresh

The **Summary** screen describes the following information fields:

<b>General</b>	The general field displays the router ID assigned for this OSPF connection, RFC compliance information and LSA data. OSPF version 2 was originally defined within RFC versions 1583 and 2328. The general field displays whether compliance to these RFCs have been satisfied. The OSPF LSA (Link-State Advertisement) Throttling feature provides a dynamic mechanism to slow down link-state advertisement updates in OSPF during times of network instability. It also allows faster OSPF convergence by providing LSA rate limiting in milliseconds. LSA information is provided for both external and opaque LSAs. Opaque LSAs carrying type-length-value elements. These extensions allow OSPF to run completely out of band of the data plane network. This means that it can also be used on non-IP networks, such as optical networks.
<b>ABR/ASBR</b>	Lists ASBR (Autonomous System Boundary Router) data relevant to OSPF routing, including the ASBR, ABR and ABR type. An ABR (Area Border Router) 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.
<b>SPF</b>	Refer to the SPF field to assess the status of the SFF (shortest path forwarding) <i>execution, last SPF execution, SPF delay, SPF due in, SPF hold multiplier, SPF hold time, SPF maximum hold time and SPF timer due flag.</i>
<b>Stub Router</b>	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.

- 5 Select **Refresh** to update the statistics counters to their latest values.

### AP OSPF Neighbors

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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **OSPF** menu.
- 5 Select the **Neighbor Info** tab.

The **Statistics > AP > OSPF > Neighbor Info** screen is displayed.

<table border="1" style="float: right; margin-left: auto;"> <tr> <td>Summary</td> <td>Neighbor Info</td> <td>Area Details</td> <td>Routes</td> <td>OSPF Interface</td> <td>OSPF State</td> </tr> </table>										Summary	Neighbor Info	Area Details	Routes	OSPF Interface	OSPF State
Summary	Neighbor Info	Area Details	Routes	OSPF Interface	OSPF State										
Router ID ⚙	Neighbour Priority	IF Name	Neighbour Address	Request Count	Retransmit Count	Dead Time	Self Neighbour State	Source Address	Summary Count						

Type to search in tables Row Count: 0

**Refresh**

This screen describes the following:

<b>Router ID</b>	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.
<b>Neighbor Priority</b>	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.
<b>IF Name</b>	Lists the name assigned to the router interface used to support connections amongst OSPF enabled neighbors.
<b>Neighbor Address</b>	Lists the IP address of the neighbor sharing the router interface with each listed router ID.
<b>Request Count</b>	Lists the connection request count (hello packets) to connect to the router interface, discover neighbors and elect a designated router
<b>Retransmit Count</b>	Lists the connection retransmission count attempted in order to connect to the router interface, discover neighbors and elect a designated router. A DR (designated router) is the router interface elected among all routers on a particular multi-access network segment, generally assumed to be broadcast.
<b>Dead Time</b>	Lists the dead time between neighbors in the network topology that are currently utilizing the listed router ID.
<b>Self Neighbor State</b>	Displays the self-neighbor status assessment used to discover neighbors and elect a designated router.
<b>Source Address</b>	Displays the single source address used by all neighbor routers to obtain topology and connection status. This form of multicasting significantly reduces network load.
<b>Summary Count</b>	Routes that originate from other areas are called summary routes. Summary routes are not flooded in a totally stubby or NSSA totally stubby area.

- 6 Select **Refresh** to update the statistics counters to their latest values.



AP OSPF Area Details

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 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point’s statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **OSPF** menu.
- 5 Select the **Area Details** tab.

The **Statistics > AP > OSPF > Area Details** screen is displayed.

<a href="#">Summary</a> <a href="#">Neighbor Info</a> <a href="#">Area Details</a> <a href="#">Routes</a> <a href="#">OSPF Interface</a> <a href="#">OSPF State</a>												
OSPF Area ID	OSPF INF	Fully adj numbers	Auth Type	Total LSA	Router LSA	Network LSA	Summary LSA	ASBR Summary LSA	NSSA LSA	Opaque Area LSA CSUM	Opaque link CSUM	

Type to search in tables Row Count: 0

[Refresh](#)

The **Area Details** screen describes the following:

<b>OSPF Area ID</b>	Displays either the integer (numeric ID) or IP address assigned to the OSPF area as a unique identifier.
<b>OSPF INF</b>	Lists the interface ID (virtual interface for dynamic OSPF routes) supporting each listed OSPF area ID.
<b>Fully adj numbers</b>	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.

<b>Auth Type</b>	Lists the authentication schemes used to validate the credentials of dynamic route connections and their areas.
<b>Total LSA</b>	Lists the LSAs of all entities using the dynamic route (in any direction) in the listed area ID.
<b>Router LSA</b>	Lists the LSAs of the router supporting each listed area ID. The router LSA reports active router interfaces, IP addresses and neighbors.
<b>Network LSA</b>	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.
<b>Summary LSA</b>	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.
<b>ASBR Summary LSA</b>	Originated by ABRs when an ASBR is present to let other areas know where the ASBR is. These are supported just like summary LSAs.
<b>NSSA LSA</b>	Routers in a NSSA (Not-so-stubby-area) 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.
<b>Opaque Area link CSUM</b>	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.
<b>Opaque link CSUM</b>	Displays a Type-10 opaque link checksum with the complete contents of the LSA.

- 6 Select **Refresh** to update the statistics counters to their latest values.

### AP OSPF Route Statistics

Refer to the **Routes** tab to assess the status of OSPF

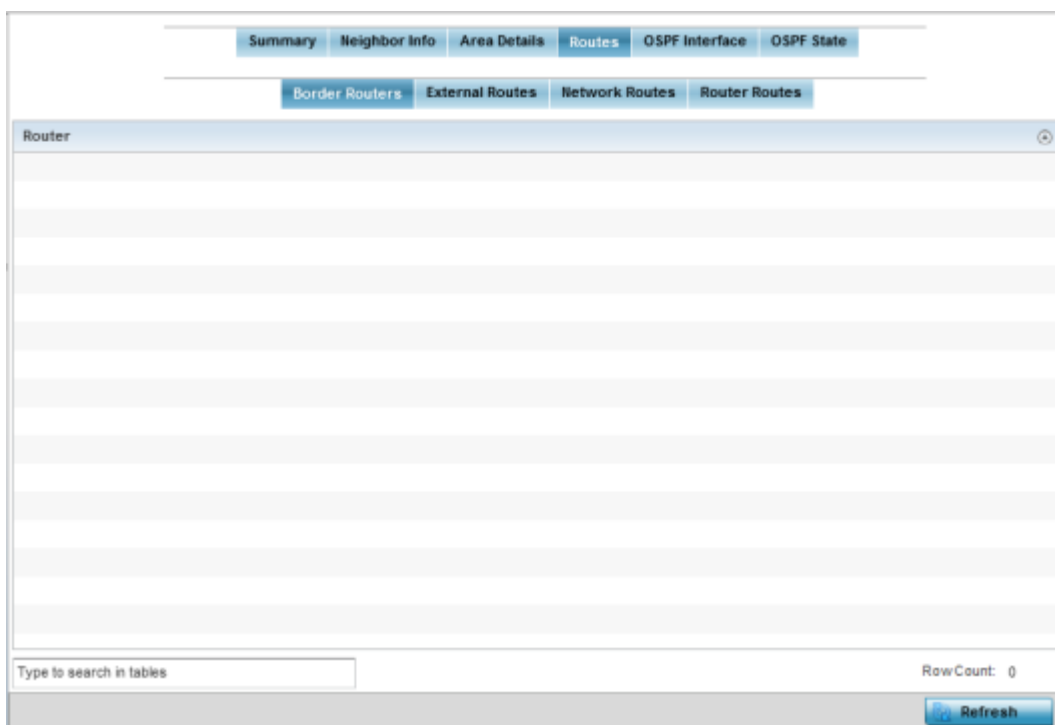
- [AP OSPF Border Routers](#) on page 1199.
- [AP OSPF External Routes](#) on page 1200.
- [AP OSPF Network Routes](#) on page 1201.
- [AP OSPF Router Routes](#) on page 1202.

### AP OSPF Border Routers

To view OSPF border routers statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **OSPF** menu.
- 5 Select the **Routes** tab.

The **Statistics > AP > Routes > Border Routers** screen displays by default.



An ABR (area border router) 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 Routers use internal OSPF routing table entries to an ABR or ASBR (Autonomous System Boundary Router). Border routers maintain an LSDB for each area supported. They also participate in the backbone.

- 6 Select **Refresh** to update the statistics counters to their latest values.

### AP OSPF External Routes

To view OSPF external route statistics:

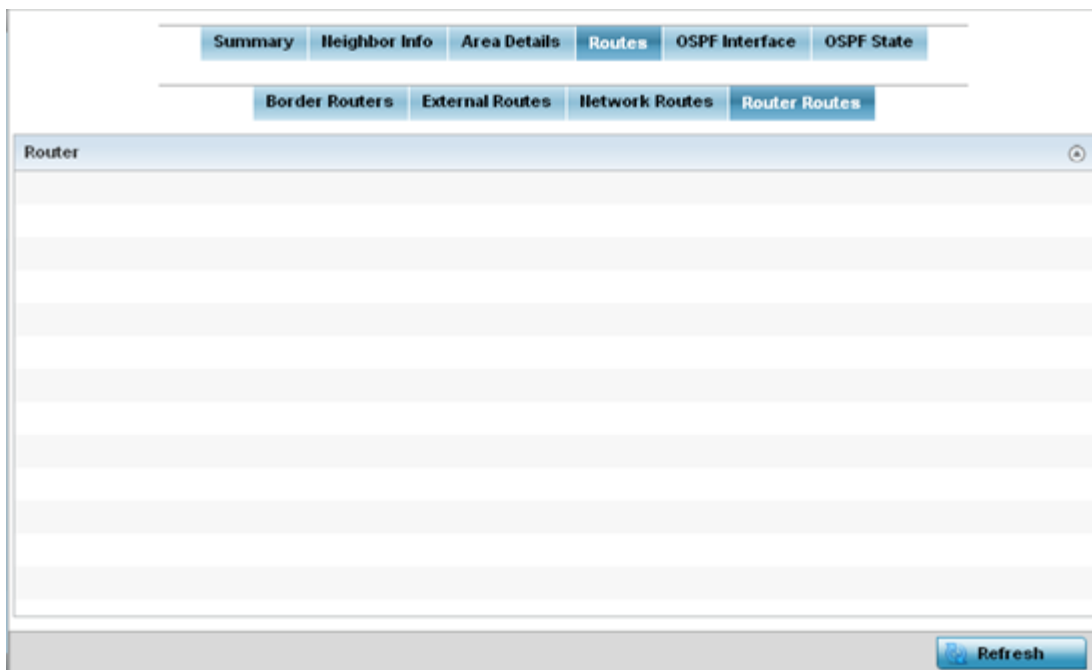
- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller** or **service platform**, and select one of its connected **access points**. The selected device's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **OSPF** from the displayed menu.
- 5 Select the **Routes > External Routes** tab.

The **Statistics > AP > Routes > External Routes** screen is displayed.









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.

- 7 Select **Refresh** to update the statistics counters to their latest values.

### AP OSPF Interface

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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **OSPF** menu.
- 5 Select the **OSPF Interface** tab.

The **Statistics > AP > OSPF > OSPF Interface** screen is displayed.



- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **OSPF** menu.
- 5 Select the **OSPF State** tab.

The **Statistics > AP > OSPF > OSPF State** screen is displayed

Summary	Neighbor Info	Area Details	Routes	OSPF Interface	OSPF State
OSPF state	Running				
OSPF ignore state count	0				
OSPF ignore state monitor timeout	360				
OSPF ignore state timeout	60				
OSPF max ignore state count	5				
OSPF max routes	256				
OSPF routes received	0				

[Refresh](#)

The **OSPF State** tab describes the following:

<b>OSPF state</b>	Displays the OSPF link state amongst neighbors within the OSPF topology. Link state information is maintained in a LSDB ( <i>link-state database</i> ) 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.
<b>OSPF ignore state count</b>	Lists the number of times state requests have been ignored between the access point and its peers within this OSPF supported broadcast domain.
<b>OSPF ignore state monitor timeout</b>	Displays the timeout that, when exceeded, prohibits an access point from detecting changes to the OSPF link state.
<b>OSPF max ignore state count</b>	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.
<b>OSPF max routes</b>	States the maximum number of routes negotiated amongst neighbors within the OSPF topology.
<b>OSPF routes received</b>	Lists the routes received and negotiated amongst neighbors within the OSPF topology.

- 6 Select **Refresh** to update the statistics counters to their latest values.

## AP Bluetooth

AP 8432 and AP 8533 model access points utilize a built-in Bluetooth chip for specific Bluetooth functional behaviors in a WiNG managed network. These platforms can use their Bluetooth-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 raises an alarm.

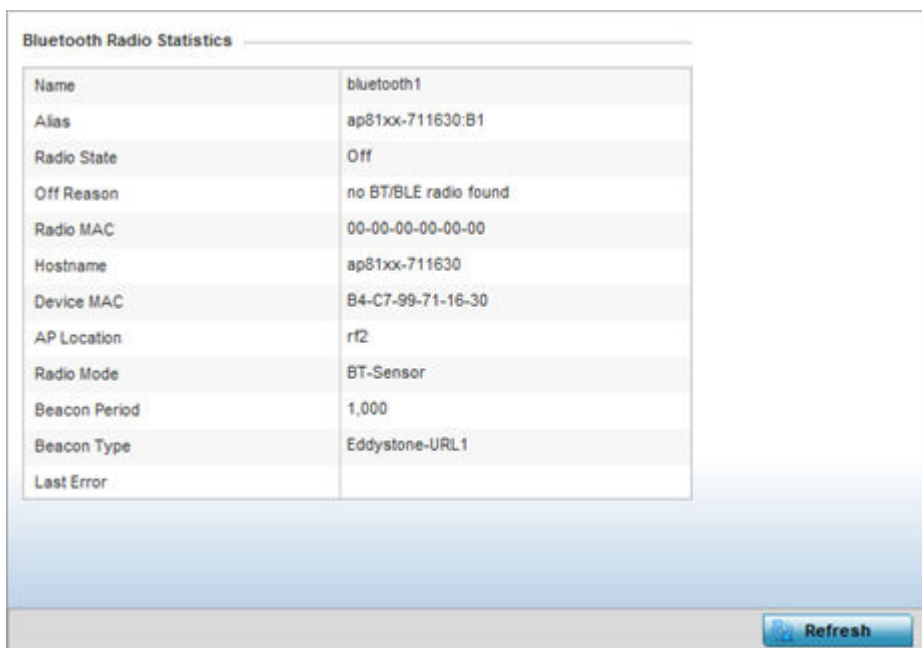
AP 8432 and AP 8533 model access points emit either iBeacon or Eddystone-URL beacons. The AP's Bluetooth radio periodically sends non-connectable, undirected LE (low-energy) advertisement packets. These advertisement packets are short, and sent on Bluetooth advertising channels that conform to established iBeacon and Eddystone-URL standards. However, portions of the advertising packet are still customizable.

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.

The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Select **Buletooth**.

The **Statistics > AP > Bluetooth** screen is displayed.



This screen displays the following access point's bluetooth information:

<b>Name</b>	Lists the administrator assigned name of the access point's Bluetooth radio.
<b>Alias</b>	If an alias has been defined for the AP it is 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 AP, it is used in place of the AP's default hostname.
<b>Radio State</b>	Displays the current operational state ( <i>On/Off</i> ) of the Bluetooth radio.
<b>Off Reason</b>	If the Bluetooth radio is <i>offline</i> , 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 AP's hostname as its network identifier.
Device MAC	Lists the AP's factory-encoded MAC address serving as this device's hardware identifier on the network.
AP Location	Lists the AP's administrator-assigned deployment location.
Radio Mode	Lists an Access Point's Bluetooth radio functional mode as either <b>bt-sensor</b> or <b>le-beacon</b> .
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 is preventing the Bluetooth radio from operating.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP L2TPv3 Tunnels

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 vendor 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **L2TPv3 Tunnels** from the menu.

The **Statistics > AP > L2TPv3 Tunnels** screen is displayed.





<b>Critical Resource</b>	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.
<b>VRRP Group</b>	Lists a VRRP group ID (if utilized). A VRRP group is only enabled when the establishment criteria is set to <i>vrrp-master</i> . 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.
<b>Establishment Criteria</b>	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.

- 5 Select **Refresh** to update the screen's statistics counters to their latest value.

## AP VRRP

The **VRRP** screen displays VRRP (Virtual Router Redundancy Protocol) 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **VRRP**.

The **Statistics > AP > L2TPv3 Tunnels** screen is displayed.

The screenshot displays the VRRP statistics interface. It is divided into two main sections: 'Global Error Status' and 'Router Operations Summary'.

**Global Error Status**

Authentication mismatch	0
Packets with invalid checksum	0
Packets with invalid type	0
Packets with invalid VRID	0
Packets with TTL Errors	0
Last protocol error reason	None
Packets with length Error	0
Packets with invalid version	0

**Router Operations Summary**

VRID	Virtual IP Address	Master IP Address	Interface Name	Version	State

At the bottom of the screen, there are three buttons: 'Clear Router Status', 'Clear Global Error Status', and 'Refresh'.

- 5 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.

- 6 Refer to the **Router Operations Summary** for the following status:

<b>VRID</b>	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.
<b>Virtual IP Address</b>	Lists the virtual interface IP address used as the redundant gateway address for the virtual route.
<b>Master IP Address</b>	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 associated with the virtual router and accepts packets addressed to the IP associated with the virtual router.
<b>Interface Name</b>	Displays the interfaces selected on the access point to supply VRRP redundancy failover support.
<b>Version</b>	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.
<b>State</b>	Displays the current state of each listed virtual router ID.

- 7 Select **Clear Router Status** to clear the Router Operations Summary table to zero and begin new data collections.
- 8 Select **Clear Global Error Status** to clear the Global Error Status table values to zero and begin new data collections.
- 9 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Critical Resources

The **Critical Resources** screen displays device IP addresses on the network (gateways, routers etc.). These IP addresses are critical to the health of the access point managed network. Critical resources are pinged regularly by the access point. If there's a connectivity issue, an event is generated stating a critical resource is unavailable. 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **Critical Resource** from the left-hand side of the UI.

The **Statistics > AP > Critical Resource** screen is displayed in the right-hand pane.

**General**

Monitor Interval	30s
Monitor Using Flows Interval	30s
Source IP For Port-Limited Monitoring	0.0.0.0
Monitoring Retries before Marking Resource as DO	3

**List of Critical Resources**

Critical Resource Name <span style="font-size: 0.8em;">⊕</span>	Via	Status	Mode

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).

Refer to the following **List of Critical Resources** stats:

<b>Critical Resource Name</b>	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.
<b>Via</b>	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.
<b>Status</b>	Defines the operational state of each listed critical resource VLAN interface ( <b>Up</b> or <b>Down</b> ).
<b>Error Reason</b>	Provides an error status as to why the critical resource is not available over its designated VLAN.
<b>Mode</b>	Defines the operational state of each listed critical resource (up or down).

- 5 Select **Refresh** to update the statistics counters to their latest values.

## AP LDAP Agent Status

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.

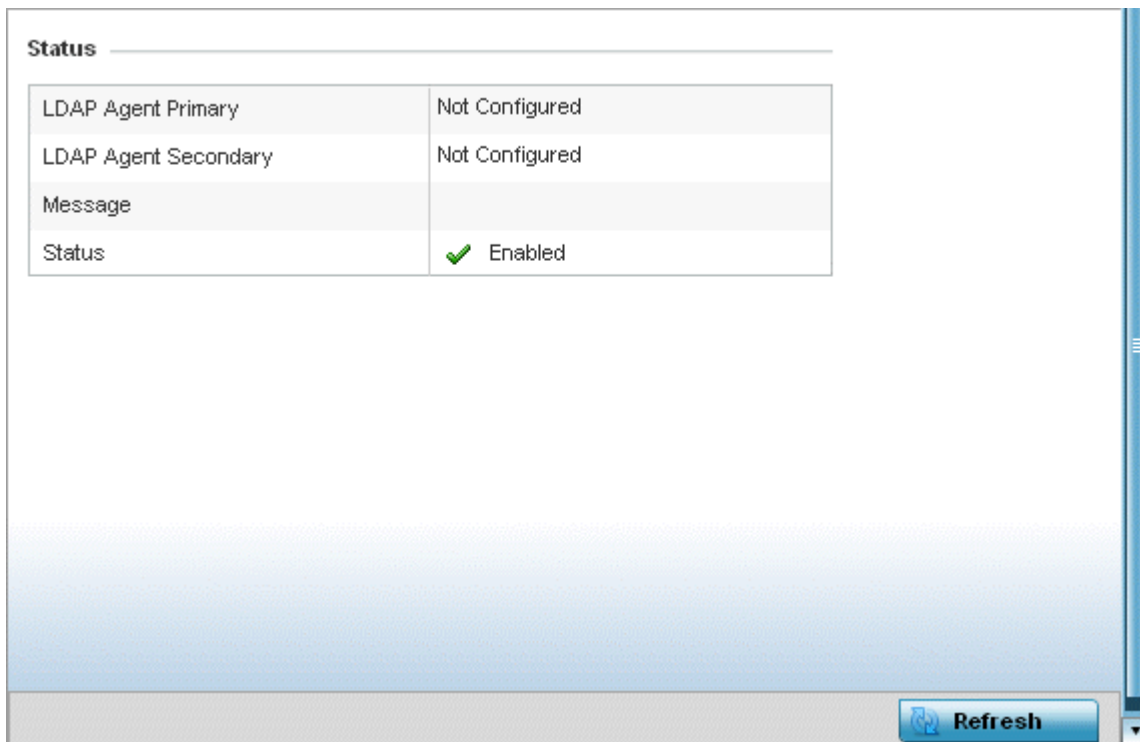
For more information on setting LDAP agents as part of the RADIUS server policy, see [Configuring RADIUS Server Policies](#).

To view access point LDAP agent statistics:



- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **LDAP Agent Status** from the left-hand side of the UI.

The **Statistics > AP > LDAP Agent Status** screen is displayed in the right-hand pane.



The LDAP Agent Status screen displays the following:

<b>LDAP Agent Primary</b>	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.
<b>LDAP Agent Secondary</b>	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.
<b>Message</b>	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.
<b>Status</b>	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.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP MiNT Links

Wireless controllers and APs use the MiNT protocol as the primary means of device discovery and communication for AP 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 Links are automatically created between controllers and APs during adoption using MLCP (MiNT Link Creation Protocol). They can also be manually created between a controller and AP (or) between two APs. 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 APs. Level 2 MiNT links also provide partitioning, between APs deployed at various remote sites.

To view access Mint link statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.

The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- Select **Mint Links** from the left-hand side of the UI.

The **Statistics > AP > Mint Links** screen is displayed in the right-hand pane.

name	listening	forced	unused	level	type	dis	devs	secure	local ip	natted	cost	hello seq num	hello interval	adj hold time	static	dyna mic	mhcp	rim	cont rol vlan	clustering
<a href="#">ip-172</a>	✗	✗	✗	2	ipv4	unkno			172.16	✗	100	4	15	46	✗	✗	✓	✗	✗	✗
<a href="#">vlan-5</a>	✗	✗	✗	1	vlan	68.8A				✗	10	3	4	13	✗	✗	✓	✗	✗	✗
<a href="#">vlan-1</a>	✗	✗	✗	1	vlan	B.19.E				✗	10	7	4	13	✗	✗	✓	✗	✗	✗
<a href="#">ip-172</a>	✗	✗	✗	2	ipv4	unkno			172.16	✗	100	4	15	46	✗	✗	✓	✗	✗	✗

Type to search in tables Row Count: 4

[Refresh](#)

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** column defines the cost for a packet to travel from its originating port to its end point destination.

The **hello seq number** and **hello interval** columns 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.

- If needed, select a **Mint link** from the **name** column to display more granular information for that link.

**Mint Links**

name	vlan-10
level	1
cost	10
hello interval	4
adj hold time	13

**Adjacencies**

neighbor	state	up time	last hello
08.19.E3.6E	up	546,679	2
12.3B.65.87	up	546,679	0
19.43.53.0D	up	546,679	3
4D.1B.B2.10	up	546,679	0
68.64.0A.8F	up	546,679	0

Refresh Exit

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.

- Periodically, select **Refresh** to update the screen's data counters to their latest values.

## AP Guest Users

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 [Captive Portals](#)

To view an access point's connected guest user client statistics:

- Select the **Statistics** menu from the Web UI.
- Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.

- Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.

The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- Select **Guest User** from the left-hand side of the UI.

The **Statistics > AP > Guest User** screen displays.

Name	Configured Time (days:hrs:m ins:secs)	Remaining Time (days:hrs:m ins:secs)	Configured KiloBytes	Remaining KiloBytes	Configured Downlink Rate (kbps)	Configured Uplink Rate (kbps)	Current Downlink Rate (kbps)	Current Uplink Rate (kbps)

Type to search in tables Row Count: 0

[Refresh](#)

This screen describes the following:

<b>Name</b>	Lists the administrator assigned name of the client utilizing the access point for guest access to the wireless network.
<b>Configured Time (days:hrs:mins:secs)</b>	Displays the restricted permissions each listed client was initially configured for their captive portal guest user session with this managing access point.
<b>Remaining Time (days:hrs:mins:secs)</b>	Displays the time each listed client has remaining in their captive portal guest user session with this managing access point.
<b>Configured KiloBytes</b>	Lists the maximum configured bandwidth consumable by the listed guest user (in kilobytes).
<b>Remaining KiloBytes</b>	Lists the remaining bandwidth available to the listed guest user (in kilobytes). This is the difference between the configured (maximum) bandwidth and the user's current utilization.
<b>Configured Downlink Rate (kbps)</b>	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 <a href="#">Defining User Pools</a> .
<b>Configured Uplink Rate (kbps)</b>	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 <a href="#">Defining User Pools</a> .





<b>Current Downlink Rate (Kbps)</b>	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 <a href="#">Defining User Pools</a> .
<b>Current Uplink Rate (Kbps)</b>	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 <a href="#">Defining User Pools</a> .

- 5 Click **Refresh** to update the statistics counters to their latest values.

## AP GRE Tunnel

*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 *Generic Routing Encapsulation (GRE)* tunnel.

To view the access point's GRE Tunnel statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **GRE Tunnel**.

The **Statistics > AP > GRE Tunnels** screen displays in the right-hand pane.

GRE Tunnels	
GRE State	
Peer IP Address	
Tunnel Id	
Total Packet Received	
Total Packet Sent	
Total Packet Dropped	

This screen describes the following:

<b>GRE State</b>	Displays the current operational state of the GRE tunnel.
<b>Peer IP Address</b>	Displays the IP address of the peer device on the remote end of the GRE tunnel.
<b>Tunnel ID</b>	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.
<b>Total Packets Received</b>	Displays the total number of packets received from a peer at the remote end of the GRE tunnel.
<b>Total Packets Sent</b>	Displays the total number of packets sent from this controller or service platform to a peer at the remote end of the GRE tunnel.
<b>Total Packets Dropped</b>	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

## AP Dot 1X

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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- Select **Dot1x** from the left-hand side of the UI.

The **Statistics > AP > Dot1X** screen is displayed.

**Dot1xAuth**

AAA Policy	
Guest Vlan control	✗
System Auth Control	✗

**Dot1x Auth Ports**

Name	Auth SM	Auth VLAN	BESM	Client MAC	Guest VLAN	Host	Pstatus
ge1	force aut	0	request	N/A	0	single	authorized
ge2	force aut	0	request	N/A	0	single	authorized

**MacAuth**

AAA Policy	
------------	--

**Mac Auth Ports**

Name	Authorized	Enabled	MAC Auth
ge1	✗	✗	00-00-00-00-00-00
ge2	✗	✗	00-00-00-00-00-00

[Refresh](#)

Refer to the following **Dot1xAuth** statistics:

<b>AAA Policy</b>	Lists the AAA policy currently being utilized for authenticating user requests.
<b>Guest Vlan Control</b>	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.
<b>System Auth Control</b>	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.

Review the following **Dot1x Auth Ports** utilization information:

<b>Name</b>	Lists the controller or service platform GE ports subject to automatic connection and authentication using Dot1x.
<b>Auth SM</b>	Lists whether Dot1x authentication is forced over the listed port.
<b>Auth VLAN</b>	Lists the numeric VLAN ID used as a virtual interface for authentication requests over the listed port.
<b>BESM</b>	Lists whether an authentication request is pending on the listed port.

<b>Client MAC</b>	Lists the MAC address of requesting clients seeking authentication over the listed port.
<b>Guest VLAN</b>	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.
<b>Host</b>	Lists whether the host is a single entity or not.
<b>Pstatus</b>	Lists whether the listed port has been authorized for Dot1x network authentication.

Refer to the **MacAuth** table to assess the AAA policy applied to MAC authorization requests.

Review the following **MAC Auth Ports** utilization information:

<b>Name</b>	Lists the controller or service platform GE ports subject to automatic connection and MAC authentication using Dot1x.
<b>Authorized</b>	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.
<b>Enabled</b>	Lists whether MAC authorization using Dot1x has been or enabled)on the listed GE port. A green checkmark designates Dot1x authorization as allowed. A red X defines authorization as disabled.
<b>MAC Auth</b>	Lists the port's factory encoded MAC address.

- 5 Select **Refresh** to update the screen's statistics counters to their latest value.

## AP Network

Use the **Network** screens to view information impacting access point ARP (hardware address determination), routing, bridging, IGMP, DHCP Cisco and link layer discovery utilization statistics.

For more information, refer to the following:

- [AP Network ARP Entries](#) on page 1220
- [AP Network Route Entries](#) on page 1221
- [AP Network Default Routes](#) on page 1223
- [AP Network Bridge](#) on page 1225
- [AP Network IGMP](#) on page 1227
- [AP Network MLD](#) on page 1228
- [AP Network Traffic Shaping](#) on page 1230
- [AP Network DHCP Options](#) on page 1231
- [AP Network Cisco Discovery Protocol](#) on page 1232
- [AP Network Link Layer Discovery Protocol](#) on page 1233
- [AP Network IPv6 Neighbor](#) on page 1235
- [AP Network MSTP](#) on page 1236

### *AP Network ARP Entries*

ARP (Address Resolution Protocol) 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 the ARP entries on the network statistics screen:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Network** menu from the left-hand side of the UI..
- 5 Select **ARP Entries**.

The **Statistics > AP > Network > ARP Entries** screen is displayed.

IP Address	ARP MAC Address	Type	VLAN
172.168.6.10	00-16-C7-86-A2-40	Dynamic	vlan1

Type to search in tables Row Count: 1

**Refresh**

The **ARP Entries** screen displays the following:

<b>IP Address</b>	Displays the IP address of the client being resolved on behalf of the controller or service platform.
<b>ARP MAC Address</b>	Displays the MAC address of the device where an IP address is being resolved.
<b>Type</b>	Defines whether the entry was added statically or created dynamically in respect to network traffic. Entries are typically static.
<b>VLAN</b>	Displays the name of the VLAN ID where the IP address was found.

- 6 Select the **Refresh** button to update the screen's statistics counters to their latest values.

### AP Network Route Entries

The **Route Entries** screen displays the destination subnet, gateway, and interface 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.

To view route entries:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **Route Entries**.

The **Statistics > AP > Network > IPv4 Route Entries** screen is displayed.

Destination	FLAGS	Gateway	Interface
172.168.6.0/24	C	direct	vlan1
default	CG	172.168.6.10	vlan1

Type to search in tables Row Count: 2

[Refresh](#)

The **IPv4 Route Entries** screen provides the following information:

<b>Destination</b>	Displays the IPv4 formatted address of the destination route address.
<b>Distance</b>	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.
<b>Route</b>	Lists the IPv4 formatted IP address used for routing packets to a defined destination.
<b>Flags</b>	The flag signifies the condition of the direct or indirect route.
<b>Gateway</b>	Displays the gateway IP address used to route packets to the destination subnet.
<b>Interface</b>	Displays the name of the controller interface or VLAN utilized by the destination subnet.
<b>Metric</b>	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.

- 6 Select the **IPv6 Route Entries** tab to review route data for IPv6 formatted traffic.

The **IPv6 Route Entries** stats display in the right-hand pane.

IPv4 Route Entries		IPv6 Route Entries	
Destination	Gateway	Interface	Flag

Type to search in tables Row Count: 0

**Refresh**

The **IPv6 Route Entries** screen provides the following information:

<b>Destination</b>	Displays the IPv6 formatted address of the destination route address. IPv6 addresses are composed of eight groups of four hexadecimal digits separated by colons.
<b>Gateway</b>	Displays the gateway IP address used to route packets to the destination subnet.
<b>Interface</b>	Displays the name of the controller interface or VLAN utilized by the destination subnet.
<b>Flag</b>	The flag signifies the condition of the direct or indirect route.

- 7 Select **Refresh** to update the display to the latest values.

### AP Network Default Routes

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's default routes:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.  
The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **Route Entries**.

The **Statistics > AP > Network > IPv4 Default Routes** screen is displayed.

IPv4 Default Routes		IPv6 Default Routes				
DNS Server	Gateway Address	Installed	Metric	Monitor Mode	Source	Monitoring Status
	157.235.95.2	✓	100	gateway-monitoring	Static-Route	reachable

Type to search in tables Row Count: 1

[Refresh](#)

The **IPv4 Default Routes** screen provides the following information:

<b>DNS Server</b>	Lists the address of the DNS server providing IPv4 formatted address assignments on behalf of the access point.
<b>Gateway</b>	Lists the IP address of the gateway resource used with the listed route.
<b>Installed</b>	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.
<b>Metric</b>	The metric (or cost) could be the distance of a router (round-trip time), link throughput or link availability.
<b>Monitor Mode</b>	Displays where in the network the route is monitored for utilization status.
<b>Source</b>	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.
<b>Monitoring Status</b>	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.

- 6 Select the **IPv6 Default Routes** tab to review default route availabilities for IPv6 formatted traffic.  
The **Statistics > AP > Network > IPv6 Default Routes** stats is displayed by default in the right-hand pane.



IPv4 Default Routes		IPv6 Default Routes				
Gateway Address	Installed	Interface Name	Lifetime	Preference	Source	Status

Type to search in tables Row Count: 0

[Refresh](#)

<b>Gateway Address</b>	Lists the IP address of the gateway resource used with the listed route.
<b>Installed</b>	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.
<b>Interface Name</b>	Displays the interface on which the IPv6 default route is being utilized.
<b>Lifetime</b>	Lists the lifetime representing the valid usability of the default IPv6 route.
<b>Preference</b>	Displays the administrator defined IPv6 preferred route for IPv6 traffic.
<b>Source</b>	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.
<b>Status</b>	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.

7 Select **Refresh** to update the display to the latest values.

*AP Network Bridge*

*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 are very similar, since a controller is a bridge with a number of ports.

The **Bridge** screen provides details about the IGS (Integrate Gateway Server ), 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*

This screen also provides information about the MRouter (Multicast Router), 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **Bridge**.

The **Statistics > AP > Bridge** stats is displayed in the right-hand pane.

Bridge Name	MAC Address	Interface	VLAN	Forwarding
1	B4-C7-99-71-16-30	ge1	38	forward
1	B4-C7-99-71-16-30	ge1	37	forward
1	B4-C7-99-57-F5-F0	ge1	39	forward
1	00-23-68-31-29-EC	ge1	1	forward
1	00-16-C7-86-A2-07	ge1	38	forward
1	5C-0E-8B-34-71-10	ge1	1	forward
1	5C-0E-8B-34-78-54	ge1	36	forward
1	B4-C7-99-58-64-A0	ge1	1	forward
1	B4-C7-99-58-64-A0	ge1	36	forward
1	5C-0E-8B-0E-3C-40	ge1	40	forward
1	00-A0-F8-66-E9-0F	ge1	1	forward
1	5C-0E-8B-0E-3C-40	ge1	37	forward

Type to search in tables Row Count: 55

[Refresh](#)

This screen displays the following:

<b>Bridge Name</b>	Displays the numeric ID of the network bridge.
<b>MAC Address</b>	Displays the MAC address (factory encoded hardware identifier) of the bridge.
<b>Interface</b>	Displays the interface (access point physical port name) where the bridge transferred packets. Supported access points models have different port configurations.
<b>VLAN</b>	Displays the VLAN the bridge is using as a virtual interface within the network.
<b>Forwarding</b>	Displays whether the bridge is forwarding packets and is in a forwarding state. A bridge can only forward packets.

- 6 Select **Refresh** to update the counters to their latest values.

## AP Network IGMP

IGMP is a protocol used for managing members of IP multicast groups. An access point listens to IGMP network traffic and forwards IGMP multicast packets to radios on which interested hosts are connected. On the wired side of the network, the access point floods all the wired interfaces. IGMP reduces unnecessary multicast traffic floods within the network and help reduce administrative overhead.

To view a AP-managed network's IGMP configuration:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **IGMP**.

Group			
VLAN	Group Address	Port Members	Version

Multicast Router (MRouter)						
VLAN	Learn Mode	Port Members	Mint IDs	Query Interval	Version	
10	pim-dvmrp	ge2		10	3	

[Refresh](#)

The **Group** field describes the following:

<b>VLAN</b>	Displays the group VLAN where the multicast transmission is conducted.
<b>Group Address</b>	Displays the Multicast Group ID supporting the statistics displayed. This group ID is the multicast address hosts are listening to.
<b>Port Members</b>	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.
<b>Version</b>	Displays each listed group IGMP version compatibility as either version 1, 2 or 3.

The **Multicast Router (MRouter)** field describes the following:

<b>VLAN</b>	Displays the group VLAN where the multicast transmission is conducted.
<b>Learn Mode</b>	Displays the learning mode used by the router as either <b>Static</b> or <b>PIM-DVMRP</b> .

<b>Port Members</b>	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.
<b>MiNT IDs</b>	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.
<b>Query Interval</b>	Lists the IGMP query interval implemented when the querier functionality is enabled. The default value is 60 seconds.
<b>Version</b>	Lists the multicast router IGMP version compatibility as either version 1, 2 or 3. The default setting is 3.

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

### AP Network MLD

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 statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.  
The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **MLD**.  
The **Statistics > AP > MLD** stats is displayed in the right-hand pane.

Multicast Listener Discovery (MLD) Group				
VLAN	Group Address	Port Members	Version	

IPv6 Multicast Router (MRouter)						
VLAN	MINT IDs	Learn Mode	Port Members	Query Interval	Version	

[Refresh](#)

The Multicast Listener Discovery (MLD) Group field describes the following:

<b>VLAN</b>	Displays the group VLAN where the MLD groups multicast transmission is conducted.
<b>Group Address</b>	Displays the Multicast Group ID supporting the statistics displayed. This group ID is the multicast address hosts are listening to.
<b>Port Members</b>	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.
<b>Version</b>	Displays each listed group’s version compatibility as either version 1, 2 or 3.

The IPv6 Multicast Router (MRouter) field describes the following:

<b>VLAN</b>	Displays the group VLAN where the multicast transmission is conducted.
<b>MINT IDs</b>	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.
<b>Learn Mode</b>	Displays the learning mode used by the router as either <b>Static</b> or <b>PIM-DVMRP</b> .
<b>Port Members</b>	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.
<b>Query Interval</b>	Lists the query interval implemented when the querier functionality is enabled. The default value is 60 seconds.
<b>Version</b>	Lists the multicast router version compatibility as either version 1, 2 or 3. The default setting is 3.

- 6 Select **Refresh** to update the screen’s statistics counters to their latest values.

## AP Network Traffic Shaping

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.

- [Traffic Shaping - Status](#) on page 1230
- [Traffic Shaping - Statistics](#) on page 1230

### Traffic Shaping - Status

To view network Access Point traffic shaping status:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.  
The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **Traffic Shaping**.  
The **Statistics > AP > Traffic Shaping > Status** screen displays by default.  
The status screen simply lists the AP's current traffic shaping operational status.
- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

### Traffic Shaping - Statistics

To view network Access Point traffic shaping statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.  
The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **Traffic Shaping**.  
The **Statistics > AP > Traffic Shaping > Statistics** screen is displayed.

Rate		0 Kbps			
Traffic Shaping Priority Stats					
Priority	Packets Sent	Packets Delayed	Packets Dropped	Current Queue Length	Current Latency (In Micro Seconds)
0	0	0	0	0	0
1	0	0	0	0	0
2	0	0	0	0	0
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0
6	0	0	0	0	0
7	0	0	0	0	0
				Clear	Refresh

This screen displays the following information:

<b>Rate</b>	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.
<b>Priority</b>	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.
<b>Packets Sent</b>	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.
<b>Packets Delayed</b>	Lists the packets defined as less important than prioritized traffic streams and delayed as a result of traffic shaping filter rules applied.
<b>Packets Dropped</b>	Lists the packets defined as less important than prioritized traffic streams, delayed and eventually dropped as a result of traffic shaping filter rules applied.
<b>Current Length</b>	Lists the packet length of the data traffic shaped to meet downstream requirements.
<b>Current Latency</b>	Traffic shaping latency is the time limit after which packets start dropping as a result of the traffic prioritization filter rules applied.

- 6 Select **Refresh** to update the screen’s statistics counters to their latest values.

### AP Network DHCP Options

Supported access points can use internal or external DHCP server resources to provide the dynamic assignment of IP addresses to requesting clients. DHCP 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **DHCP Options**.

The **Statistics > AP > Network > DHCP Options** screen displays.

Server Information	Image File	Configuration	Legacy Adoption	Adoption
server_information_1	image_1	configuration_1	n/a	n/a
server_information_2	image_2	configuration_2		

Type to search in tables Row Count: 2

This screen describes the following:

<b>Server Information</b>	Displays the DHCP server hostname used on behalf of the access point.
<b>Image File</b>	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.
<b>Configuration</b>	Displays the name of the configuration file on the DHCP server.
<b>Legacy Adoption</b>	Displays legacy (historical) device adoption information on behalf of the access point.
<b>Adoption</b>	Displays pending (current) adoption information on behalf of an access point.

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

*AP Network 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **Cisco Discovery Protocol**.

The **Statistics > AP > Network > Cisco Discovery Protocol** screen displays in the right-hand pane.

Capabilities	Device ID	Local Port	Platform	Port ID	TTL
switch igmp_cap rc	Switch	ge1	cisco WS-C3560-2	FastEthernet0/5	121

Type to search in tables Row Count: 1

This screen displays the following:

<b>Capabilities</b>	Displays the capabilities code for CISCO neighbors as either <b>Router, Trans Bridge, Source Route Bridge, Switch, Host, IGMP</b> or <b>Repeater</b> .
<b>Device ID</b>	Displays the configured device ID or name for each device in the table.
<b>Local Port</b>	Displays the local port name (access point physical port) for each CDP capable device. Supported access point models have unique port configurations.
<b>Platform</b>	Displays the model number of the CDP capable device interoperating with the access point.
<b>Port ID</b>	Displays the access point's numeric identifier for the local port.
<b>TTL</b>	Displays the TTL for each CDP connection.

- 6 Click **Clear Neighbors** to remove all known CDP neighbors from the table.
- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

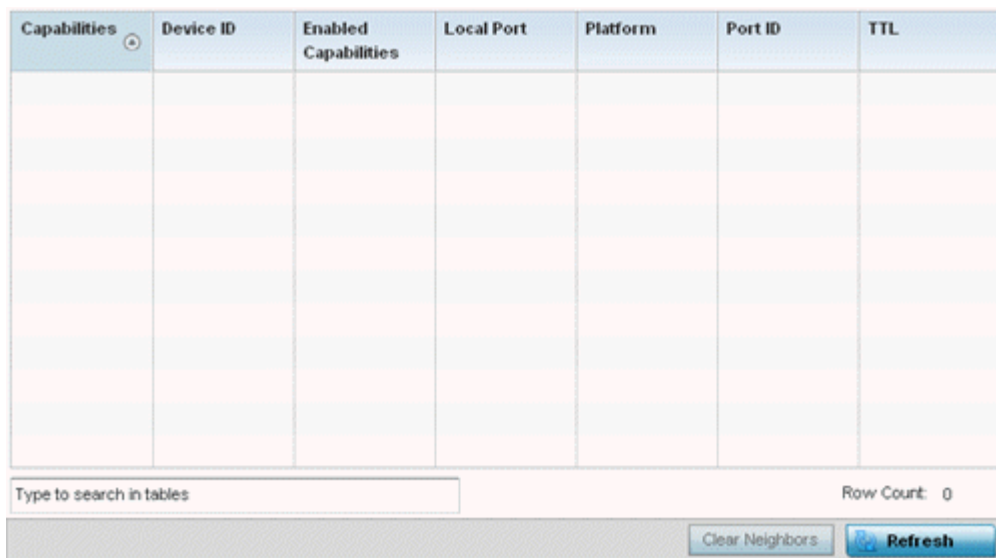
### AP Network Link Layer Discovery Protocol

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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **Link Layer Discovery**.

The **Statistics > AP > Network > Link Layer Discovery Protocol** screen displays in the right-hand pane.



This screen displays the following:

<b>Capabilities</b>	Displays a capabilities code as either <b>Router, Trans Bridge, Source RouteBridge, Switch, Host, IGMP</b> or <b>Repeater</b> .
<b>Device ID</b>	Displays the configured device ID or name for each device in the table.
<b>Enabled Capabilities</b>	Displays which device capabilities are currently enabled.
<b>Local Port</b>	Displays the local port name (access point physical port) for each LLDP capable device. Supported access point models have unique port configurations.
<b>Platform</b>	Displays the model number of the LLDP capable device interoperating with the access point.
<b>Port ID</b>	Displays the identifier for the local port.
<b>TTL</b>	Displays the TTL for each LLDP connection.

- 6 Select **Clear Neighbors** to remove all known LLDP neighbors from the table.
- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

### *AP Network IPv6 Neighbor*

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.

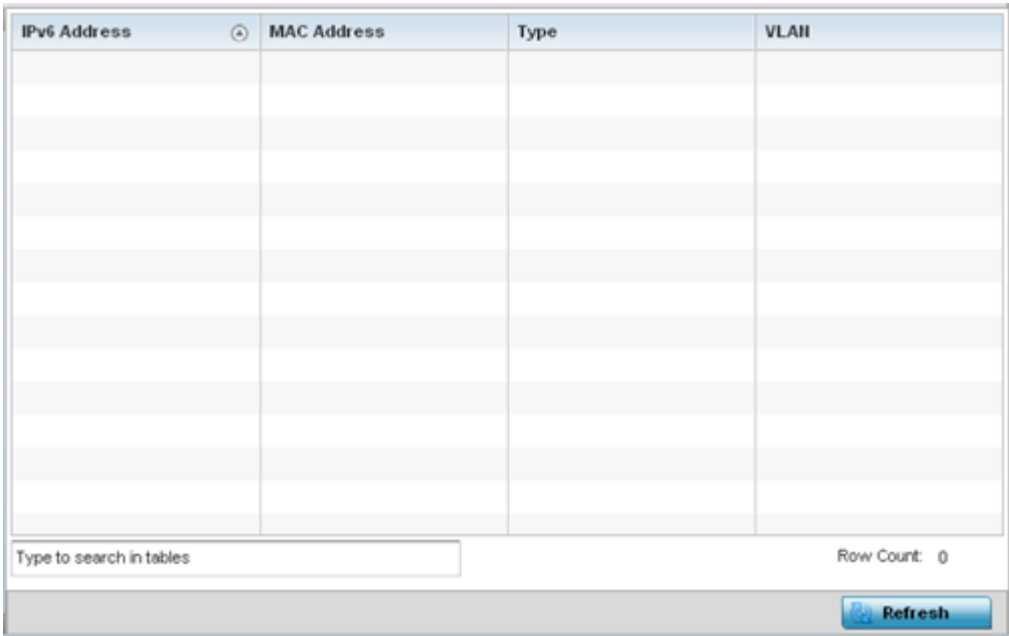
Upon receiving a neighbor solicitation message, the destination replies with NA (neighbor advertisement). The source address in the advertisement is the IPv6 address of the device sending the message. The destination address in the advertisement message is the IPv6 address of the device sending the neighbor 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.  
The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Network** menu from the left-hand side of the UI.
- 5 Select **IPv6 Neighbor**.  
The **Statistics > AP > Network > IPv6 Neighbor Discovery** screen is displayed in the right-hand pane.



This screen displays the following:

<b>IPv6 Address</b>	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.
<b>MAC Address</b>	Lists the factory encoded hardware MAC address of the neighbor device using an IPv6 formatted IP address as its network identifier.
<b>Type</b>	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 <b>Host, Router</b> and <b>DHCP Server</b> .
<b>VLAN</b>	Lists the virtual interface (from 1 - 4094) used for the required neighbor advertisements and solicitation messages used for neighbor discovery.

- 6 Select **Refresh** to update the screen’s statistics counters to their latest values.

*AP Network MSTP*

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 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 an access point's MSTP statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.  
The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Network** menu from the left-hand side of the UI.

- 5 Select **MSTP**.

The **Statistics > AP > Network > MSTP** screen is displayed in the right-hand pane.

The screenshot shows the MSTP configuration and bridge details. It includes three main sections: MST Config, MST Bridge, and MST Bridge Port Detail.

**MST Config**

CFG Name	My Name
Digest	0xac36177f50283cd4b83821d8ab26de62
Format ID	0
Name	1
Revision	0

**MST Bridge**

	BPDU Filter	BPDU Guard	Bridge Admin Cisco	Bridge Enabled	Bridge Oper Cisco	CIST Bridge ID	CIST Bridge Priority	CIST Reg Root ID
	✗	✗	✗	✗	✗	1: CIST Brk	32,768	1: CIST Reg Root Id E

**MST Bridge Port Detail**

Name	Role	Send MSTP	State	Type	Admin BPDU Filter	Admin BPDU Guard	Admin Edge	Admin P2P MAC	Admin Root Guard
ge1	4	MSTP	Forwan	0	2	2	✗	✗	✗
ge10	4	STP	Forwan	0	2	2	✗	✗	✗
ge2	4	MSTP	Forwan	0	2	2	✗	✗	✗
ge3	4	MSTP	Forwan	0	2	2	✗	✗	✗

A **Refresh** button is located at the bottom right of the interface.

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.

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP DHCPv6 Relay & Client

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 view the access point's DHCPv6 relay configuration:

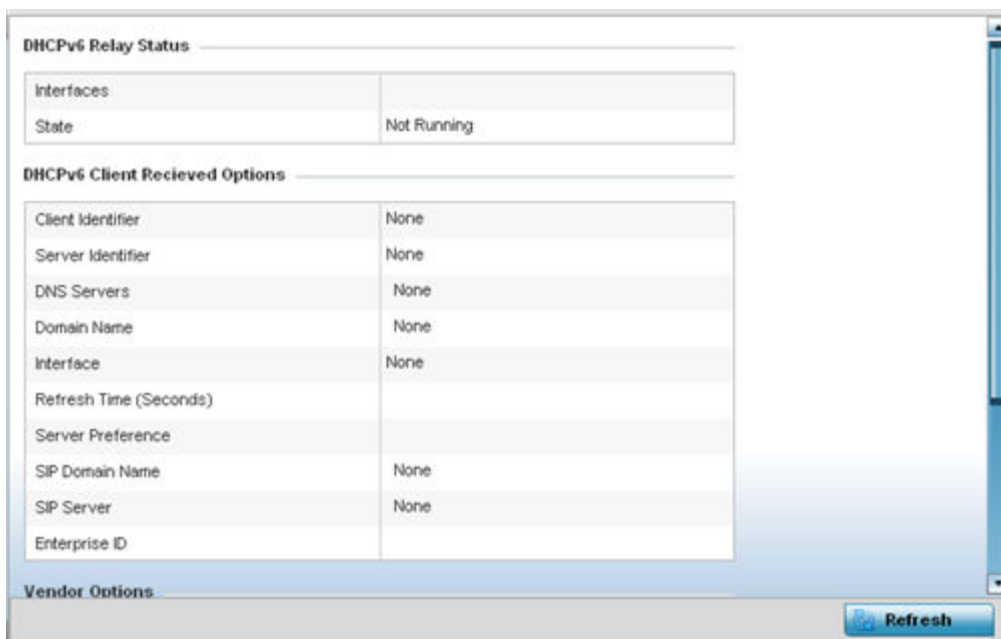
- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.

- Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.

The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- Select **DHCPv6 Relay & Client**.

The **Statistics > Controller > DHCP Relay & Client** screen displays in the right-hand pane.



The DHCP Relay Status table defines the following:

<b>Interfaces</b>	Displays the access point interface used for DHCPv6 relay.
<b>State</b>	Displays the current operational state of the DHCPv6 server to assess its availability as a viable IPv6 provisioning resource.

The DHCPv6 Client Received Options table defines the following:

<b>Client Identifier</b>	Lists whether the reporting client is using a <i>hardware address</i> or <i>client identifier</i> as its identifier type within requests to the DHCPv6 server.
<b>Server Identifier</b>	Displays the server identifier supporting client DHCPv6 relay message reception.
<b>DNS Servers</b>	Lists the DNS server resources supporting relay messages received from clients.
<b>Domain Name</b>	Lists the domain to which the remote server resource belongs.
<b>Interface</b>	Displays the interfaces dedicated to client DHCPv6 relay message reception.
<b>Refresh Time (Seconds)</b>	Lists the time (in seconds) since the data populating the DHCPv6 client received options table has been refreshed.
<b>Server Preference</b>	Lists the preferred DHCPv6 server resource supporting relay messages received from clients.
<b>SIP Domain Name</b>	Lists the SIP domain name supporting DHCPv6 client telephone extensions or voice over IP systems.



<b>SIP Server</b>	Displays the SIP server name supporting DHCPv6 telephone extensions or voice over IP systems.
<b>Enterprise ID</b>	Lists the enterprise ID associated with DHCPv6 received client options.

Refer to the **Vendor Options** table for the following:

<b>Code</b>	Lists the relevant numeric DHCP vendor code.
<b>Data</b>	Lists the supporting data relevant to the listed DHCP vendor code.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP DHCP Server

Access points' utilize an internal DHCP server. DHCP can provide IP addresses automatically to requesting wireless clients. 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 client.

To review DHCP server statistics, refer to the following:

- [AP DHCP - General](#) on page 1240
- [AP DHCP - Bindings](#) on page 1241
- [AP DHCP - Networks](#) on page 1242

### *AP DHCP - General*

To view **General** DHCP status and binding information:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **DHCP Server** menu.

The **Statistics > AP > DHCP Server > General** screen displays by default in the right-hand pane.



The screenshot shows a web-based interface with three main sections:

- DHCPv4 Status:** A table with two rows: 'Interfaces' containing 'vlan1,vlan4,vlan174' and 'State' containing 'Running'.
- DHCPv6 Status:** A table with two rows: 'Interfaces' (empty) and 'State' containing 'Not Running'.
- DDNS Bindings:** A table with two columns: 'IP Address' and 'Name'. The table is currently empty.

A 'Refresh' button is located at the bottom right of the interface.

The **DHCPv4 Status** and **DHCPv6 Status** tables defines the following:

<b>Interfaces</b>	Displays the access point interface used with the DHCPv4 or DHCPv6 resource for IP address provisioning.
<b>State</b>	Displays the current operational state of the DHCPv4 or DHCPv6 server to assess its availability as a viable IP provisioning resource.

The **DDNS Bindings** table displays the following:

<b>IP Address</b>	Displays the IP address assigned to the requesting client.
<b>Name</b>	Displays the domain name mapping corresponding to the listed IP address.

The **DHCP Manual Bindings** table displays the following:

<b>IP Address</b>	Displays the IP address for clients requesting DHCP provisioning resources.
<b>Client Id</b>	Displays the client's ID used to differentiate requesting clients.

### *AP DHCP - Bindings*

The **DHCP Binding** 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 a network's DHCP Bindings:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **DHCP Server** menu.
- 5 Select **Bindings**.

The **Statistics > AP > DHCP Server > Bindings** screen displays by default in the right-hand pane.

Expiry Time	IP Address	DHCP MAC Address
Wed Dec 9 17:23:10 2015	172.168.7.197	00-06-F6-69-60-C2
Thu Dec 10 00:38:37 2015	172.168.7.198	B4-C7-99-6C-86-ED

Type to search in tables Row Count: 2

This screen displays the following:

<b>Expiry Time</b>	Displays the expiration of the lease used by the devices requesting controller or service platform DHCP resources.
<b>IP Address</b>	Displays the IP address of each listed device requesting DHCP services.
<b>DHCP MAC Address</b>	Displays the MAC address of each device requesting DHCP services.

- 6 Select a table entry and select **Clear** to remove the client from the list of devices requesting DHCP services.
- 7 Select **Clear All** to remove all listed clients from the list of requesting clients.
- 8 Select the **Refresh** button to update the screen's statistics counters to their latest values.

### AP DHCP - Networks

A controller, service platform or access point's 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 DHCP server assigns an IP address, a lease (the validity of time), and other IP configuration parameters to a client on an administrator assigned lease basis.

The **Networks** screen provides network pool information, such as the subnet for the addresses you want to lease from the pool, the pool name, used addresses and the total number of addresses available for lease to a requesting client.

To view the DHCP Server's Networks information:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **DHCP Server** menu.
- 5 Select **Networks**.

The **Statistics > AP > DHCP Server > Networks** screen displays in the right-hand pane.

Name	Subnet Address	Used Addresses	Total Addresses
vlan1	192.168.1.0/24	0	19

This screen displays the following:

<b>Name</b>	Displays the name of the virtual network from which IP addresses can be issued to DHCP client requests on the listed controller or service platform interface.
<b>Subnet Address</b>	Displays the subnet for the IP addresses used from the network pool.
<b>Used Addresses</b>	Displays the number of host IP addresses allocated by the DHCP server.
<b>Total Addresses</b>	Displays the total number of IP addresses available in the network pool for requesting clients.

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Firewall

A *firewall* is a wireless network security mechanism designed to block unauthorized access while permitting authorized device communications. Firewalls use a set of *permit* or *deny* filters to manage access point resource requests based on a set of administrator defined rules.

The access point's firewall statistics are partitioned into the following:

- Packet Flows
- Denial of Service
- IP Firewall Rules
- MAC Firewall Rules
- NAT Translations
- DHCP Snooping

### AP Firewall Packet Flows

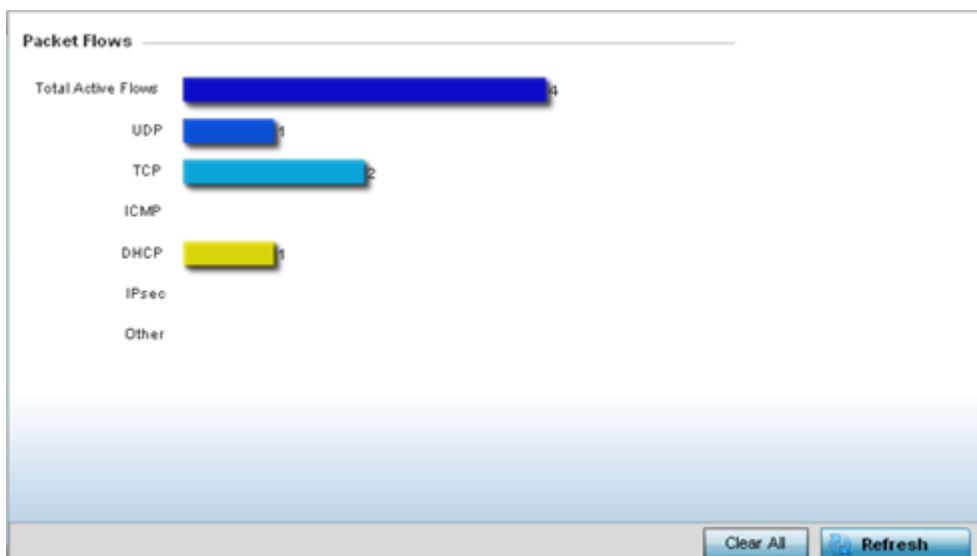
The **Packet Flows** screen displays data traffic packet flow utilization. The chart represents the different protocol flows supported, and displays a proportional view of the flows in respect to their percentage of data traffic utilized.

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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Firewall** menu.

The **Statistics > AP > Firewall > Packet Flows** screen displays by default in the right-Hand pane.



- 5 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.

### AP Denial of Service

A 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 an access point’s DoS attack configuration:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point’s statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Firewall** menu.
- 5 Select **Denial of Service**.

The **Statistics > AP > Firewall > Denial of Service** screen displays in the right-hand pane.

Attack Type	Count	Last Occurrence
Ascend	0	Never
BroadcastMulticast ICMP	0	Never
Chargen	0	Never
Fraggle	0	Never
FTP Bounce	0	Never
Router Solicit	0	Never
Invalid Protocol	0	Never
LAND	0	Never
Router Advertisement	0	Never
Smurf	0	Never
Snork	0	Never
Source Route	0	Never
IP Spoof	0	Never
TCP Bad Sequence	0	Never

Type to search in tables Row Count: 25

This screen displays the following:

<b>Attack Type</b>	Displays the DoS attack type.
<b>Count</b>	Displays the number of times the access point's firewall has detected each listed DoS attack.
<b>Last Occurrence</b>	Displays when the attack event was last detected by the access point firewall.

- 6 Select **Clear All** to revert the statistics counters to zero and begin a new data collection.
- 7 Select the **Refresh** button to update the screen's statistics counters to their latest values.

### AP IPv4 Firewall Rules

Create firewall IP address rules to let any computer send or receive traffic from, programs, system services, computers or users. IP firewall rules can be created to provide one of the three actions listed below:

- 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 an access point's IP firewall rules:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Firewall** menu.
- 5 Select **IP Firewall Rules**.

The **Statistics > AP > Firewall > IP Firewall Rule** screen displays in the right-hand pane.

Precedence	Friendly String	Hit Count
10	permit tcp any any rule-precedence	0
11	permit udp any eq 67 any eq dhcp	0
20	deny udp any range 137 138 any r	0
21	deny ip any 224.0.0.0/4 rule-prece	0
22	deny ip any host 255.255.255.255	0
100	permit ip any any rule-precedence	0

Type to search in tables Row Count: 6

[Refresh](#)

This screen displays the following:

<b>Precedence</b>	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.
<b>Friendly String</b>	This is a string that provides more information as to the contents of the rule.
<b>Hit Count</b>	Displays the number of times each WLAN ACL has been triggered.

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

### AP IPv6 Firewall Rules

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 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.

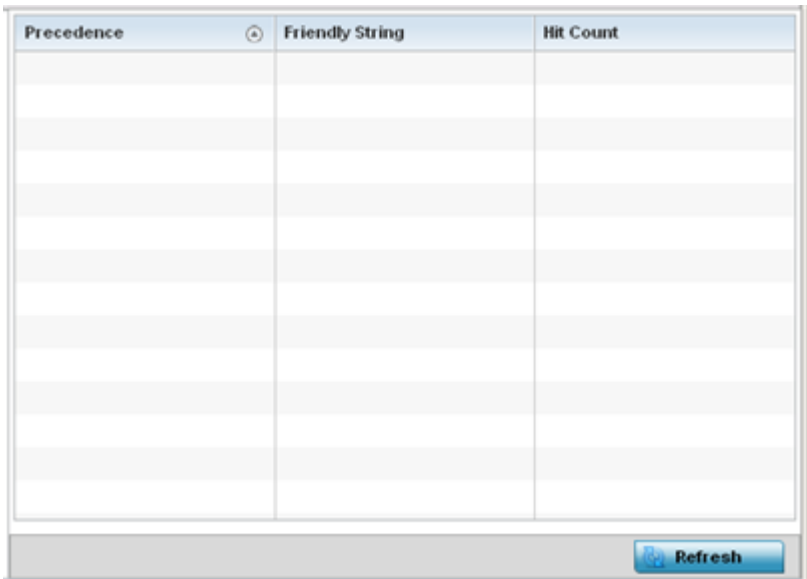
Firewall rules can use one of the three following actions based on a rule criteria:

- *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 an access point's existing IPv6 firewall rules:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.  
The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Firewall** menu.
- 5 Select **IPv6 Firewall Rules**.

The **Statistics > AP > Firewall > IPv6 Firewall Rules** screen displays in the right-hand pane.



This screen displays the following information:

<b>Precedence</b>	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.
<b>Friendly String</b>	This is a string that provides more information as to the contents of the IPV6 specific IP rule. This is for information purposes only.
<b>Hit Count</b>	Displays the number of times each IPV6 ACL has been triggered.

- 6 Select **Refresh** to update the screen’s statistics counters to their latest values.

*AP MAC Firewall Rules*

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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point’s statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.



- Expand the **Firewall** menu.
- Select **MAC Firewall Rules**.

The **Statistics > AP > Firewall > MAC Firewall Rules** screen displays in the right-hand pane.

The screenshot shows a web interface for a device named 'macad5'. It displays a table with three columns: 'Precedence', 'Friendly String', and 'Hit Count'. The table contains one row with the value '10' in the 'Hit Count' column. Below the table is a search input field labeled 'Type to search in tables' and a 'Refresh' button. The 'Row Count' is shown as '1'.

Precedence	Friendly String	Hit Count
	firewall	10

This screen displays the following:

<b>Precedence</b>	Displays the precedence value, which are applied to packets. The rules within an 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.
<b>Friendly String</b>	This string provides more information as to the contents of the rule. This is for information purposes only.
<b>Hit Count</b>	Displays the number of times each WLAN ACL has been triggered.

- Select **Refresh** to update the screen's statistics counters to their latest values.

### AP NAT Translations

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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Firewall** menu.
- 5 Select **NAT Translations**.

The **Statistics > AP > Firewall > NAT Translations** screen displays in the right-hand pane.

	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	157.235.91.9	4,441	10.233.89.68	22	172.168.1.11	22	157.235.91.9	4,441
	tcp	157.235.91.9	4,250	10.233.89.68	22	172.168.1.11	22	157.235.91.9	4,250
	tcp	10.233.89.67	2,625	10.233.89.68	22	172.168.1.11	22	10.233.89.67	2,625
Type to search in tables		Row Count: 3							
Refresh									

This screen displays the following information:

<b>Protocol</b>	Displays the IP translation protocol as either <b>TCP</b> , <b>UDP</b> or <b>ICMP</b> .
<b>Forward Source IP</b>	Displays the internal network IP address for forward facing NAT translations.
<b>Forward Source Port</b>	Displays the internal network port for forward facing NAT translations.
<b>Forward Dest IP</b>	Displays the external network destination IP address for forward facing NAT translations.
<b>Forward Dest Port</b>	Displays the external network destination port for forward facing NAT translations.
<b>Reverse Source IP</b>	Displays the internal network IP address for reverse facing NAT translations.
<b>Reverse Source Port</b>	Displays the internal network port for reverse facing NAT translations.
<b>Reverse Dest IP</b>	Displays the external network destination IP address for reverse facing NAT translations.
<b>Reverse Dest Port</b>	Displays the external network destination port for reverse facing NAT translations.

- 6 Select **Refresh** to update the screen's statistics counters to their latest values.

### AP DHCP Snooping

When DHCP servers are allocating IP addresses to requesting clients on the LAN, DHCP snooping can be configured to better enforce LAN security by allowing only clients with specific IP/MAC addresses.

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Firewall** menu.
- 5 Select **DHCP Snooping**.

The **Statistics > AP > Firewall > DHCP Snooping** screen displays in the right-hand pane.

	MAC Address	Node Type	IP Address	Netmask	VLAN	Lease Time	Time Elapsed Since Last Update
	00-16-C7-86-A	router,dhcp-sei	172.168.6.10		1		7h 58m 44s
	00-16-C7-86-A	router,dhcp-sei	38.38.38.1		38		9h 33m 43s
	00-40-96-A8-4f	dhcp-client,wir	38.38.0.245	16	38	1d 0h 0m 0s	9h 33m 43s
	B4-C7-99-73-B	switch-SVI	172.168.6.137		1		7h 58m 44s

Type to search in tables Row Count: 4

[Clear All](#) [Refresh](#)

This screen displays the following information:

<b>MAC Address</b>	Displays the MAC address of the client requesting DHCP resources from the access point.
<b>Node Type</b>	Displays the NetBios node with an IP pool from which IP addresses can be issued to client requests on this interface.
<b>IP Address</b>	Displays the IP address used for DHCP discovery, and requests between the DHCP server and DHCP clients.
<b>Netmask</b>	Displays the subnet mask used for DHCP discovery, and requests between the DHCP server and DHCP clients.
<b>VLAN</b>	Displays the virtual interface used for a new DHCP configuration.
<b>Lease Time</b>	When a DHCP server allocates an address for a requesting 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.
<b>Time Elapsed since Last Update</b>	Displays the amount of time elapsed since the DHCP server was last updated.

- 6 Select **Clear All** to revert the counters to zero and begin a new data collection.
- 7 Select **Refresh** to update the screen's counters to their latest values

### AP IPv6 Neighbor Snooping

IPv6 snooping bundles layer 2 IPv6 hop security features, such as IPv6 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.

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 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.  
The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Firewall** menu.
- 5 Select **IPv6 Neighbor Snooping**.

The **Statistics > AP > Firewall > IPv6 Neighbor Snooping** screen displays in the right-hand pane.

MAC Address	Node Type	IPv6 Address	VLAN	Mint Id	Snoop Id	Time Elapsed Since Last Update
10-0B-A9-35-B3-C	ipv6	fe80::11c2:5073:6	30	4D.84.A2.70	8,896	6s
24-77-03-9D-5B-2	tentative,ipv6	fe80::9cb9:9f20:6	30		6,880	3m 59s
30-F7-C5-4F-31-2	tentative,ipv6	fe80::d5:3c9e:223	666		5,856	1m 30s
44-6D-57-08-1A-D	ipv6	fe80::d1d0:2904:2	30	4D.18.84.BC	9,984	11s
60-67-20-A5-B8-2	tentative,ipv6	fe80::4c41:8be:cc	30		1,664	2m 21s
6C-71-D9-54-92-1	ipv6	fe80::c5e9:48af:a	100	4D.84.A2.70	10,560	14s
78-FD-94-05-8C-0	tentative,ipv6	fe80::10e4:458d:8	666		4,736	3m 51s
84-3A-4B-AC-68-5	ipv6	fe80::6135:21a7:b	30		6,400	32m 28s
84-3A-4B-AC-68-5	ipv6	2601:646:8d00:b1	30		14,208	32m 28s
8C-70-5A-B5-60-D	ipv6	fe80::dd98:fb6:a	30	4D.84.A2.70	5,857	1s
B4-B6-76-AC-EC-2	tentative,ipv6	fe80::794a:fb8f:78	30		9,312	4m 59s
C4-D9-87-38-A6-7	ipv6	fe80::6d2a:ed2f:2c	30		6,272	5m 23s
CC-3D-82-82-2B-C	ipv6	fe80::b01d:c01c:c	30		544	43m 54s
E4-1F-13-6A-5C-6	ipv6	fe80::a8f3:2769:7	6		7,968	3m 44s
F8-16-54-7B-1E-E	tentative,ipv6	fe80::98c0:60fa:7	30		9,888	3m 10s

Type to search in tables Row Count: 16

This screen displays the following information:

<b>MAC Address</b>	Displays the hardware encoded MAC address of an IPv6 client reporting to the controller or service platform.
<b>Node Type</b>	Displays the NetBios node type from an IPv6 address pool from which IP addresses can be issued to requesting clients.
<b>IPv6 Address</b>	Displays the IPv6 address used for DHCPv6 discovery and requests between the DHCPv6 server and DHCP clients.
<b>VLAN</b>	Displays the controller or service platform virtual interface ID used for a new DHCPv6 configuration.
<b>Mint Id</b>	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.
<b>Snoop Id</b>	Lists the numeric snooping session ID generated when Access Points listen to IPv6 formatted network traffic and forward IPv6 packets to radios.
<b>Time Elapsed Since Last Update</b>	Displays the amount of time elapsed since the DHCPv6 server was last updated.

- 6 Select **Clear Neighbors** to revert the counters to zero and begin a new data collection.
- 7 Select **Refresh** to update the screen's counters to their latest values.

## AP VPN

IPsec VPN provides a secure tunnel between two networked peer access points. Administrators can define which packets are sent within the tunnel, and how they are protected. When a tunneled 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 SA between two peers. SAs define the protocols and algorithms applied to sensitive packets and specify the keying mechanisms used by tunneled 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.

The 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**

### AP VPN IKESA

The **IKESA** screen allows for the review of individual peer security association statistics.

To view an access point's IKESA statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **VPN** menu.
- 5 Select **IKESA**.

The **Statistics > AP > VPN > IKESA** screen displays in the right-hand pane.

	Peer	Version	State	Lifetime	Local IP Address
	172.168.7.197	IKEv2	ESTABLISHED	8,352	172.168.6.137

Type to search in tables Row Count: 1

Review the following VPN peer security association statistics:

<b>Peer</b>	Lists peer IDs for peers sharing 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.
<b>Version</b>	Displays each peer's IKE version used for auto IPSec secure authentication with the IPSec gateway and other controllers or service platforms.
<b>State</b>	Lists the state of each listed peer's SA (whether established or not).
<b>Lifetime</b>	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.
<b>Local IP Address</b>	Displays each listed peer's local tunnel end point IP address. This address represents an alternative to an interface IP address.

- 6 Select a IKE peer configuration and click **Clear** to remove the peer from the table.
- 7 Select **Clear All** to clear each peer of its current status and begin a new data collection.
- 8 Select **Refresh** to update the screen's statistics counters to their latest values.

#### AP VPN IPSec

To view an access point's IPSec VPN statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **VPN** menu.
- 5 Select **IPSec**.

The **Statistics > AP > VPN > IPSec** screen displays in the right-hand pane.

Peer	Local IP Address	Protocol	State	SPI In	SPI Out	Mode
172.168.7.197	172.168.6.137	esp	VALID	C99E4AAB	A9DC8ACE	Tunnel

Type to search in tables Row Count: 1

[Clear All](#) [Refresh](#)

Review the following VPN peer security association statistics:

<b>Peer</b>	Lists IP addresses for peer IDs for peers sharing 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.
<b>Local IP Address</b>	Displays each listed peer’s local tunnel end point IP address. This address represents an alternative to an interface IP address.
<b>Protocol</b>	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 <b>ESP</b> and <b>AH</b> .
<b>State</b>	Lists the state of each listed peer’s security association.
<b>SPI In</b>	Lists SPI status for incoming IPSec tunnel packets. SPI tracks each connection traversing the IPSec VPN tunnel and ensures they are valid.
<b>SPI Out</b>	Lists SPI status for outgoing IPSec tunnel packets. SPI tracks each connection traversing the IPSec VPN tunnel and ensures they are valid.
<b>Mode</b>	Displays the IKE mode as either <b>Main</b> or <b>Aggressive</b> . IPSec has two modes in IKEv1 for key exchanges. The Aggressive mode requires three messages be exchanged between the IPSEC peers to setup the SA. The Main mode requires six messages.

- 6 Select **Clear All** to clear each peer of its current status and begin a new data collection.
- 7 Select **Refresh** to update the screen's statistics counters to their latest values.



## AP Certificates

The SSL protocol ensures secure transactions between Web servers and browsers. SSL uses a third-party CA 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:

- [AP Certificates Trustpoints](#) on page 1256
- [AP Certificates RSA Keys](#) on page 1258

### *AP Certificates Trustpoints*

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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Certificates** menu.

The **Statistics > AP > Certificates > Trustpoints** screen displays by default right-hand pane.



**Certificate Details**

Subject Name	CN=AP8132-B4-C7-99-73-BE-2C
Alternate Subject Name	
Issuer Name	CN=AP8132-B4-C7-99-73-BE-2C

Serial Number	6a
RSA Key Used	default_rsa_key
IS CA	<span style="color: red;">✗</span> No
Is Self Signed	<span style="color: green;">✔</span> Yes
Server Certificate Present	<span style="color: green;">✔</span> Yes
CRL Present	<span style="color: red;">✗</span> No

**Validity**

Valid From	08:23:2012 06:30:35 UTC
Valid Until	08:23:2013 06:30:35 UTC

**Certificate Authority (CA) Details**

Subject Name	
Alternate Subject Name	
Issuer Name	

The **Certificate Details** field displays the following:

<b>Subject Name</b>	Describes the entity to which the certificate is issued.
<b>Alternate Subject Name</b>	Lists alternate subject information about the certificate as provided to the certificate authority.
<b>Issuer Name</b>	Displays the name of the organization issuing the certificate.
<b>Serial Number</b>	Lists the unique serial number of the certificate.
<b>RSA Key Used</b>	Displays the name of the key pair generated separated, or automatically when selecting a certificate.
<b>IS CA</b>	Indicates whether this certificate is an authority certificate ( <b>Yes/No</b> ).
<b>Is Self Signed</b>	Displays whether the certificate is self-signed ( <b>Yes/No</b> ).
<b>Server Certification Present</b>	Displays whether a server certification is present or not ( <b>Yes/No</b> ).
<b>CRL Present</b>	Displays whether a CRL is present ( <b>Yes/No</b> ). 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:



<b>Valid From</b>	Displays the certificate's issue date.
<b>Valid Until</b>	Displays the certificate's expiration date.

The **Certificate Authority (CA) Details** field displays the following:

<b>Subject Name</b>	Displays information about the entity to which the certificate is issued.
<b>Alternate Subject Name</b>	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 <i>Subject Name</i> field.
<b>Issuer Name</b>	Displays the organization issuing the certificate.
<b>Serial Number</b>	Lists the unique serial number of each certificate issued.

The **Certificate Authority Validity** field displays the following:

<b>Validity From</b>	Displays the date when the validity of a CA began.
<b>Validity Until</b>	Displays the date when the validity of a CA expires.

Review the *Certificate Authority (CA) Details* and *Validity* information to assess the subject and certificate duration periods.

- Periodically select the **Refresh** button to update the screen's statistics counters to their latest values.

### AP Certificates RSA Keys

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 access point's RSA Key details:

- Select the **Statistics** menu from the Web UI.
- Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- Expand the **Certificates** menu.
- Select **RSA Keys**.

The **Statistics > AP > Certificates > RSA Keys** screen displays by default right-hand pane.

**RSA Key Details**

Size: 1,024

**RSA Public Key**

```
-----BEGIN PUBLIC KEY-----
MIG1MA0GCsqGSib3DQEBAQUAA4GNADCBgQD3HABCZl2G2FVn9Wwabgk76VUO
ksECRPLdq8YDhdKv7+3UR8MXHO5cJz1IRIT6kAeJHvEa3c2B6zVwoNal9K2DaS
9CbJco+KHvZ+i2puwO1f4zkLfk6mYT+6qguJPPJcnw2ehCTaiVCJO3+qggFlicu7
M4Jz+xiGid19yMhtwIDAQAB
-----END PUBLIC KEY-----
```

Refresh

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 used for encrypting messages. This key is known to everyone.

- Periodically select **Refresh** to update the screen's statistics counters to their latest values.

## AP WIPS

A WIPS monitors the wireless network's radio spectrum for the presence of unauthorized access points, and take measures to prevent an intrusion. Unauthorized attempts to access an access point 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 blacklisted devices (unauthorized access points) intruding 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:

- [AP WIPS Client Blacklist](#) on page 1259
- [AP WIPS Events](#) on page 1260

### *AP WIPS Client Blacklist*

The access point's **Client Blacklist** displays blacklisted clients detected by this access point using WIPS. Blacklisted clients are not allowed to associate to this access point.

To view the WIPS client blacklist for this access point:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **WIPS** menu.

The **Statistics > AP > WIPS > Client Blacklist** screen displays by default right-hand pane

Event Name	Blacklisted Client	Time Blacklisted	Total Time	Time Left
dos-eapol-start-storm	44-55-44-55-44-55	Thu Jun 10 2010 12:26:28 PM	2h 0m 0s	1h 0m 0s
null-probe-response	44-55-44-55-44-55	Thu Jun 10 2010 12:26:28 PM	40m 0s	20m 0s

Type to search in tables

Row Count: 2

Refresh

This screen displays the following:

<b>Event Name</b>	Displays the name of the detected wireless intrusion resulting in a blacklisting of the client.
<b>Blacklisted Client</b>	Displays the MAC address of the unauthorized and blacklisted device intruding this access point's radio coverage area.
<b>Time Blacklisted</b>	Displays the time when the client was blacklisted by this access point.
<b>Total Time</b>	Displays the time the unauthorized (now blacklisted) device remained in this access point's WLAN.
<b>Time Left</b>	Displays the time the blacklisted client remains on the list.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

### AP WIPS Events

Periodically review the **WIPS Events** screen to assess whether any new or existing events require additional administration to protect the security of authorized devices. Events are listed by name, detecting AP, originating device, detector radio and time. The reporting AP can be selected to review that AP's configuration in greater detail.

To view an access point's WIPS Events statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **WIPS** menu.
- 5 Select **WIPS Events**.

The **Statistics > AP > WIPS > WIPS Events** screen displays by default right-hand pane.

Event Name	Reporting AP	Originating Device	Detector Radio	Time Reported
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Wed May 27 2015 08:08:39 PM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Wed May 27 2015 10:16:36 AM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Wed May 6 2015 04:24:30 AM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Wed May 27 2015 03:14:12 AM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Tue May 26 2015 08:03:12 PM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Tue May 26 2015 08:01:12 PM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Tue May 26 2015 10:47:57 AM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Wed May 6 2015 10:53:57 AM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Tue May 26 2015 03:07:07 AM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Mon May 25 2015 08:10:27 PM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	00-10-18-A9-56-5D	1	Mon May 25 2015 10:59:44 AM
ad-hoc-violation	<a href="#">ap7502-BC1340</a>	60-03-08-A7-93-E0	1	Fri May 15 2015 01:22:14 AM

Type to search in tables Row Count: 97

This screen displays the following information:

<b>Event Name</b>	Displays the name of the detected wireless intrusion event.
<b>Originating Device</b>	Displays the MAC address of the intruder device.
<b>Reporting AP</b>	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.
<b>Detector Radio</b>	Displays the number of the detecting access point radio.
<b>Time Reported</b>	Displays the time when the intrusion event was detected.

- 6 Select **Clear All** to reset the statistics counters to zero and begin a new data collection.
- 7 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Sensor Servers

Sensor Servers allow the monitor and download of data from multiple access points in sensor mode 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.

- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **Sensor Servers**.

The **Statistics > AP > Sensor Servers** screen displays.

IP Address/Hostname	Port	Status
	0	no server defined
	0	no server defined
157.235.95.128	443	online

Type to search in tables Row Count: 3

**Refresh**

This screen displays the following:

<b>IP Address</b>	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.
<b>Port</b>	Displays the numerical port where the sensor server is listening. Unconnected server resources are not able to provide sensor reporting.
<b>Status</b>	Displays whether the server is currently <b>connected</b> or <b>not connected</b> .

- 5 Select **Refresh** to update the screen's statistics counters to their latest values

## AP Bonjour Services

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 Expand the **System** node from the navigation pane (on the left-hand side of the screen).  
The System node expands to display the RF Domains created within the managed network.

- Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**.

The Access Point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.

- Select **Bonjour Services** from the left-hand side of the UI.

The **Statistics > AP > Bonjour Services** screen displays.

Service Name	Instance Name	IP Address	Port	Vlan	Vlan Type	Expiry
_airplay_tcp.local	Apple TV (2)_airplay_tcp	32.32.32.101	7,000	32	Local	Sun Mar 9 00:59:04 2014
_ipp_tcp.local	Brother MFC-8510DN_ipp	32.32.32.103	631	32	Local	Sun Mar 9 01:41:34 2014
_ipp_tcp.local	HP MFP M425dn Service Z	32.32.32.106	631	41	Local	Sun Mar 9 01:13:46 2014
_ipp_tcp.local	HP MFP M425dn Service :	32.32.32.106	631	32	Local	Sun Mar 9 00:56:34 2014
_rsop_tcp.local	B8782E20922E@Apple TV	32.32.32.101	5,000	32	Local	Sun Mar 9 00:59:04 2014
_universal_sub_ipp_tcp	Brother MFC-8510DN_ipp	32.32.32.103	631	32	Local	Sun Mar 9 01:41:34 2014
_universal_sub_ipp_tcp	HP MFP M425dn Service :	32.32.32.106	631	32	Local	Sun Mar 9 00:56:34 2014

Type to search in tables Row Count: 7

[Refresh](#)

Refer to the following Bonjour service utilization stats:

<b>Service Name</b>	Lists the services discoverable by the Bonjour gateway. Services can either be <i>pre-defined</i> Apple services (scanner, printer, etc.) or an alias not available on the predefined list.
<b>Instance Name</b>	Lists the name of each Bonjour service instance (session) utilized by the controller or service platform.
<b>IP Address</b>	Lists the network IP address utilized by the listed Bonjour service providing resources to the controller or service platform.
<b>Port</b>	Displays the port used to secure a connection with the listed Bonjour service.
<b>Vlan</b>	Lists the VLAN(s) on which a listed Bonjour service is routable.
<b>Vlan Type</b>	Lists the VLAN type as either a <i>local</i> bridging mode or a <i>shared tunnel</i> .
<b>Expiry</b>	Lists the expiration date of the listed Bonjour service, and its availability to discover resources on the LAN.

- Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Captive Portal

A *captive portal* forces HTTP clients, requesting network access, to use a special Web page for authentication before using the access point provisioned 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 an access point's captive portal statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **Captive Portal**.

The **Statistics > AP > Captive Portal** screen displays.

Client MAC	Client IP	Client IPv6	Captive Portal	Port Name	Authentication	WLAN	VLAN	Remaining Time
<a href="#">54-44-08-3E-00-98</a>	0.0.0.0		ALPHANET-GUEST		User Redirect	GUEST-ACCESS-REGISTR	666	0s

Type to search in tables Row Count: 1

[Refresh](#)

This screen displays the following information:

<b>Client MAC</b>	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.
<b>Client IP</b>	Displays the requesting client's IPv4 address.
<b>Client IPv6</b>	Displays the requesting client's IPv6 formatted IP address.
<b>Captive Portal</b>	Displays the captive portal name that each listed client is utilizing for guest access to access point resources.
<b>Port Name</b>	Lists the access point port name supporting the captive portal connection with the listed client MAC address.
<b>Authentication</b>	Displays the authentication status of the requesting client.
<b>WLAN</b>	Displays the name of the WLAN utilizing the access point managed captive portal.



<b>VLAN</b>	Displays the name of the access point VLAN the requesting client uses as virtual interface for captive portal sessions.
<b>Remaining Time</b>	Displays the time after which the client is disconnected from the captive portal managed Internet.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Network Time

NTP (Network Time Protocol) is central to networks that rely on their controller or service platform to supply system time to managed devices. 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 an enterprise network. The controller or service platform can optionally 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.

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:

- [AP NTP Status](#) on page 1265
- [AP NTP Association](#) on page 1266

### *AP NTP Status*

To view an access point's NTP Status:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Network Time** menu

The **Statistics > AP > Network Time > NTP Status** screen displays by default.

	Clock Offset	Frequency	Leap	Precision	Reference Time	Reference	Root Delay	Root Dispersion	Stratum
	65.322 msec	-7.2960 Hz	Clock is synchron	2^-20	d5db49b9.116	129.188.147.1	65.322 msec	0.000 msec	3

Use this screen to review the accuracy and performance of the synchronization with a NTP server resource.

<b>Clock Offset</b>	Displays the time differential between the access point’s time and its NTP resource’s time.
<b>Frequency</b>	Indicates the SNTP server clock’s skew (difference) for the access point.
<b>Leap</b>	Indicates if a second is added or subtracted to SNTP packet transmissions, or if transmissions are synchronized.
<b>Precision</b>	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.
<b>Reference Time</b>	Displays the time stamp the access point’s clock was last synchronized or corrected.
<b>Reference</b>	Displays the address of the time source the access point is synchronized to.
<b>Root Delay</b>	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).
<b>Root Dispersion</b>	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.
<b>Stratum</b>	Displays how many hops the access point is from its current NTP time resource.

- 5 Select **Refresh** to update the screen’s statistics counters to their latest values.

*AP NTP Association*

The interaction between an access point and its dedicated external NTP server resource constitutes an *NTP Association*. NTP associations can be either *peer* associations (the access point synchronizes to another system or allows another system to synchronize to it), or *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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select the **Network Time** menu.
- 5 Select the **NTP Association** tab.

The **Statistics > AP > Network Time > NTP Association** screen displays.

		NTP Status			NTP Association					
Delay Time	Display	Offset	Poll	Reach	Reference IP Address	Server IP Address	State	Status	Time	
0.1	15.2	0.0	1024	255	129.168.147.	129.168.147.	2	Master Sync	504	
Type to search in tables									Row Count: 1	
									Refresh	

This screen displays the following:

<b>Delay Time</b>	Displays the round-trip delay (in seconds) for broadcasts between the NTP server and the access point.
<b>Display</b>	Displays the time difference between the peer NTP server and the access point's clock.
<b>Offset</b>	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.
<b>Poll</b>	Displays the maximum interval between successive messages in seconds to the nearest power of two.
<b>Reach</b>	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.
<b>Reference IP Address</b>	Displays the address of the time source the access point is synchronized to.
<b>Server IP Address</b>	Displays the numerical IP address of the SNTP resource (server) providing SNTP updates to the access point.

<b>State</b>	Displays the NTP association status. This can be one of the following: <ul style="list-style-type: none"> <li>• <b>Synced</b> - Indicates the controller or service platform is synchronized to this NTP server.</li> <li>• <b>Unsynced</b> - Indicates the controller or service platform has chosen this master for synchronization. However, the master itself is not yet synchronized to UTC.</li> <li>• <b>Selected</b> - Indicates this NTP master server will be considered the next time the controller or service platform chooses a new master to synchronize with.</li> <li>• <b>Candidate</b> - Indicates this NTP master server may be considered for selection the next time the controller or service platform chooses a NTP master server.</li> <li>• <b>Configured</b> - Indicates this NTP server is a configured server.</li> </ul>
<b>Status</b>	Displays how many hops the access point is from its current NTP time source.
<b>Time</b>	Displays the time of the last statistics update.

- 6 Select **Refresh** to update the screen's statistics counters to their latest values

## AP Load Balancing

An access point's traffic load can be viewed graphically 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. Operating channels can also be filtered. 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 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **Load Balancing**.

The **Statistics > AP > Load Balancing** screen is displayed.



The **Load Balancing** screen displays the following:

<b>Load Balancing</b>	Select any of the options to display any or all of the following information in the graph below: <b>AP Load</b> , <b>2.4GHz Load</b> , <b>5GHz Load</b> , and <b>Channel</b> . 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.
<b>Client Requests Events</b>	The Client Request Events displays the <i>Time</i> , <i>Client</i> , <i>Capability</i> , <i>State</i> , <i>WLAN</i> and <i>Requested Channels</i> for all client request events on the access point. All supported access point models support up to 256 clients per access point.

- 5 Select **Refresh** to update the screen's statistics counters to their latest values.

## AP Environment Statistics

An AP 8132 sensor module is a USB environmental sensor extension to an AP 8132 model access point. It provides a variety of sensing mechanisms, allowing the monitoring and reporting of the AP 8132's radio coverage area. The output of the sensor's detection mechanisms are viewable using either the Environmental Sensor screen.

For more information, refer to the following:

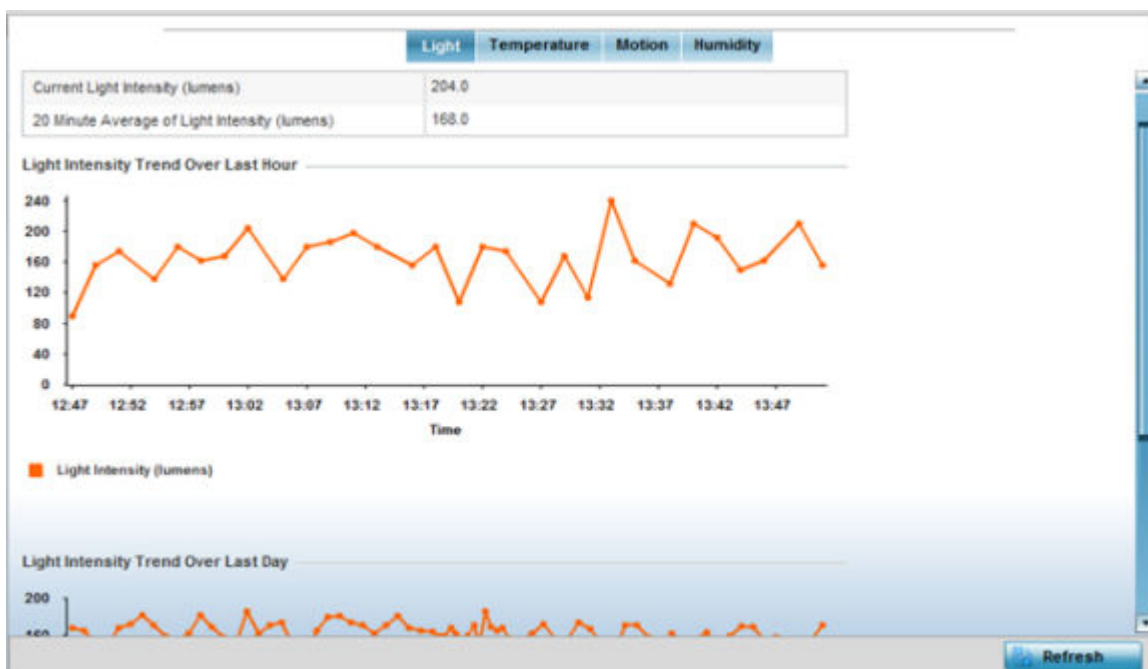
- [AP Light Sensor](#) on page 1270.
- [AP Temperature Sensor](#) on page 1271.
- [AP Motion Sensor](#) on page 1272.
- [AP Humidity Sensor](#) on page 1273,

### AP Light Sensor

To view an AP 8132 model access point's environmental light statistics:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Select **Environment**. The **Statistics > AP 8132 > Environment > Light** tab displays by default.

Additional **Temperature**, **Motion** and **Humidity** tabs available for unique sensor reporting. Each of these sensor measurements helps the administrator determine whether the AP 8132's immediate deployment area is occupied by changes in the access point's environment.



- 5 Refer to the **Light** table to assess the sensor's detected light intensity within the AP 8132 immediate deployment area.

Light intensity is measured by the sensor in lumens. The table displays the **Current Light Intensity (lumens)** and the **20 Minute Average of Light Intensity (lumens)**. Compare these two items to determine whether the AP 8132's 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.

- 6 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.
- 7 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 AP 8132 can be upgraded or powered off during specific hours of the day.
- 8 Select **Refresh** at any time to update the screen's statistics counters to their latest values.

### AP Temperature Sensor

To view an AP 8132 model access point's environmental temperature:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Environment** menu.
- 5 Select the **Temperature** tab.

The **Statistics > AP 8132 > Environment > Temperature** tab displays.



- 6 Refer to the **Temperature** table to assess the sensor's detected temperature within the AP 8132's immediate deployment area.

Temperature is measured in centigrade. The table displays the **Current Temperature (centigrade)** and the **20 Minute Average Temperature (centigrade)**. Compare these two items to determine whether the AP 8132's deployment location remains consistently heated.

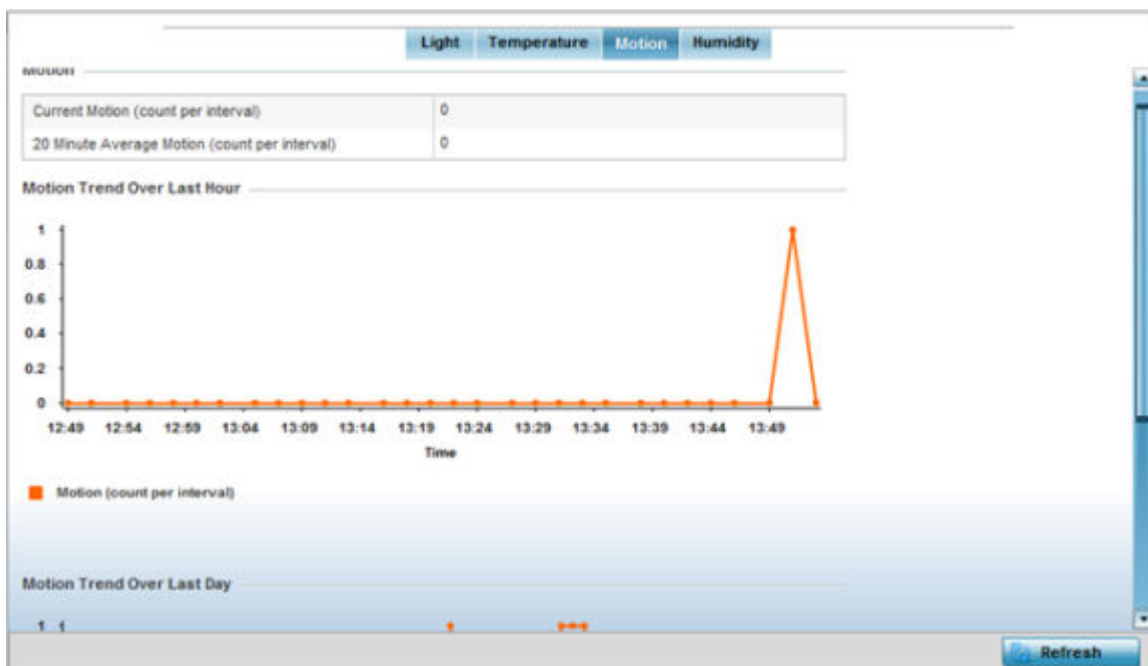
- 7 Refer to the **Temperature Trend Over Last Hour** graph to assess the fluctuation in ambient temperature over the last hour. Use this graph in combination with the Light and Motions graphs (in particular) to assess the deployment area's activity level.
- 8 Refer to the **Temperature Trend Over Last Day** graph to assess whether deployment area temperature is consistent across specific hours of the day. Use this information to help determine whether the AP 8132 can be upgraded or powered off during specific hours of the day.
- 9 Select **Refresh** at any time to update the screen's statistics counters to their latest values.

### AP Motion Sensor

To view an AP 8132 model access point's deployment area motion activity:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Environment** menu.
- 5 Select the **Motion** tab.

The **Statistics > AP 8132 > Environment > Motion** tab displays.



- 6 Refer to the **Motion** table to assess the sensor's detected movement within the AP 8132's immediate deployment area.

Motion is measured in intervals. The table displays the **Current Motion (count per interval)** and the **20 Minute Average Motion (count per interval)**. Compare these two items to determine whether the AP 8132's deployment location remains consistently occupied by client users.



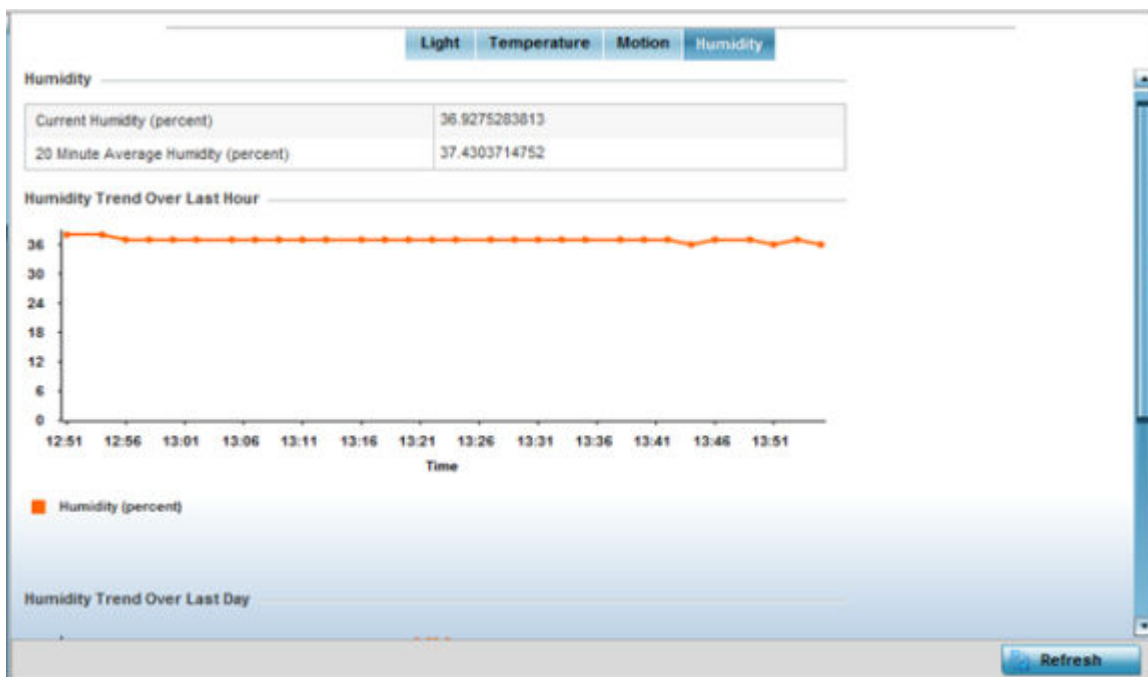
- 7 Refer to the **Motion Trend Over Last Hour** graph to assess the fluctuation in user movement over the last hour. Use this graph in combination with the Light and Temperature graphs (in particular) to assess the deployment area's activity level.
- 8 Refer to the **Motion Trend Over Last Day** graph to assess whether deployment area user movement is consistent across specific hours of the day. Use this information to help determine whether the AP 8132 can be upgraded or powered off during specific hours of the day.
- 9 Select **Refresh** at any time to update the screen's statistics counters to their latest values.

### AP Humidity Sensor

To view an AP 8132 model access point's deployment area humidity:

- 1 Select the **Statistics** menu from the Web UI.
- 2 Expand the **System** node from the navigation pane (on the left-hand side of the screen). The System node expands to display the RF Domains created within the managed network.
- 3 Expand an **RF Domain** node, select a **controller or service platform**, and select one of its connected **access points**. The access point's statistics menu displays in the right-hand side of the screen, with the **Health** tab selected by default.
- 4 Expand the **Environment** menu.
- 5 Select the **Humidity** tab.

The **Statistics > AP 8132 > Environment > Humidity** tab displays.



- 6 Refer to the **Humidity** table to assess the sensor's detected humidity fluctuations within the AP 8132's immediate deployment area.

Humidity is measured in percentage. The table displays the **Current Humidity (percent)** and the **20 Minute Average Humidity (percent)**. Compare these two items to determine whether the AP 8132's deployment location remains consistently humid (often a by-product of temperature).

- 7 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.
- 8 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 AP 8132 can be upgraded or powered off during specific hours of the day.
- 9 Select **Refresh** at any time to update the screen's statistics counters to their latest values.

## AP IOT Imagotag

WiNG AP 8432 model access points support SES-imagotag's ESL tags. An Imagotag-enabled AP recognizes the ESL communicator and facilitates communication between communicator and tags. To enable an AP 8432 as an infrastructure device facilitating communication between the ESL communicator and tags, an Imagotag policy is applied either to the AP's self (standalone AP) or to the AP's profile (adopted AP). Use this option to view the configuration of the ESL communicator.



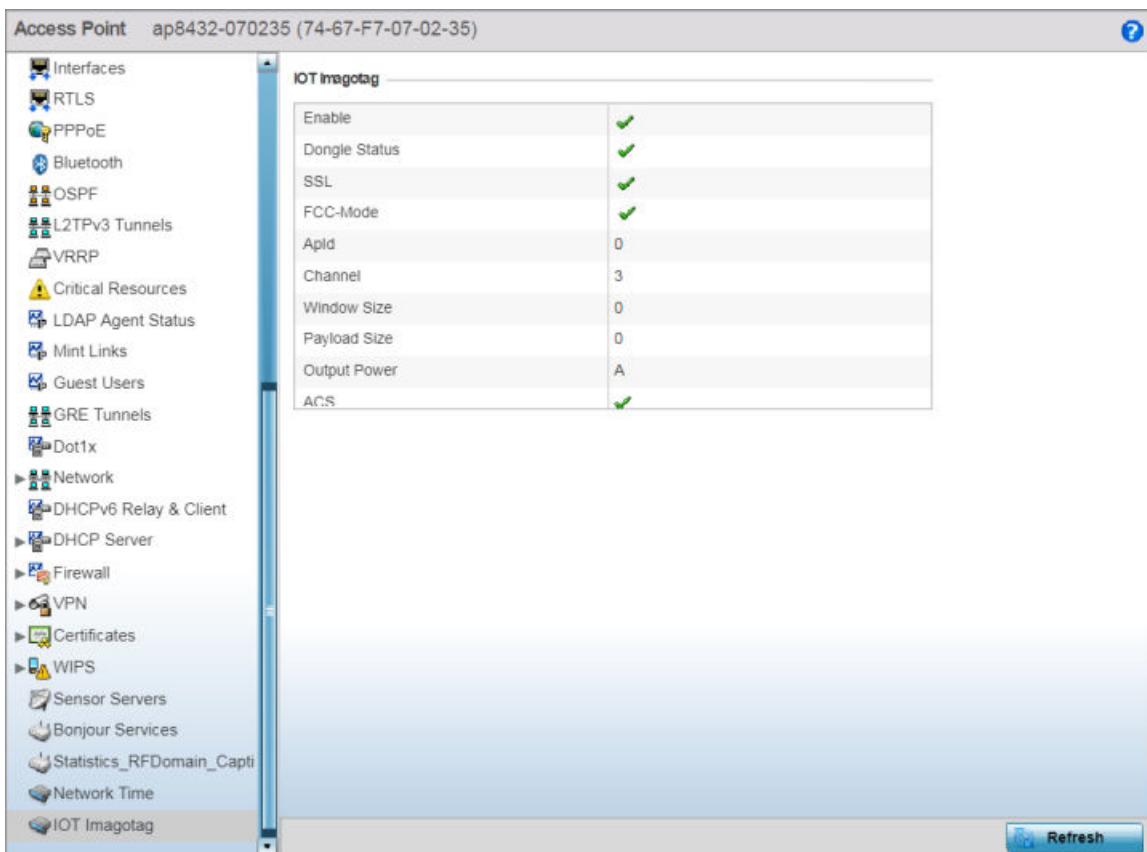
### Note

For information on enabling IOT Imagotag on an AP 8432, see [Setting the Imagotag Policy](#) on page 850

To view an AP 8432 model access point's ESL communicator 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 an RF Domain, select a controller or service platform, and select one of its connected AP 8432 access point.

- 3 Select **IOT Imagotag** from the AP's statistics menu.



**Figure 351: Statistics Access Point IOT Imagotag screen**

The IOT Imagotag screen displays the following:

Enable	Displays the status of the policy: Enabled/Disabled. A green check mark indicates that the policy is enabled. A red cross mark indicates that the policy is disabled.
Dongle Status	Displays the ESL communicator (USB Dongle) status - Connected/Disconnected.
SSL	Displays if SSL (Secure Socket Layer) encryption mode of communication is enabled or not. A green check mark indicates that this option is enabled. A red cross mark indicates that this option is disabled.
FCC-Mode	Displays if FCC compatibility mode is enabled or not on the ESL communicator. A green check mark indicates that this option is enabled. A red cross mark indicates that this option is disabled.
Apld	Displays the Imagotag enabled AP's ID.
Channel	Displays the channel assigned for ESL communicator to tag communication in the 2.4 GHz band.
Window Size	Displays the transmission window size set for messages exchanged between ESL communicator and tags.
Payload Size	Displays the maximum payload size in packets exchanged between ESL communicator and tags.

Output Power	Displays the maximum output power set for the ESL communicator.
ACS	Displays if ACS (Auto-Channel Selection) status - Enabled/Disabled.

## Wireless Client Statistics

**Wireless Client** statistics display read-only stats for a client selected from its connected access point, controller or service platform topology. Client stats help administrate client performance within an access point, controller or service platform managed network. Use this information to assess if configuration changes are required to improve client throughput.

Wireless client stats can be administrated using the following:

- [Client Health](#) on page 1276.
- [Client Details](#) on page 1279.
- [Client Traffic](#) on page 1282.
- [Client WMM TSPEC](#) on page 1285.
- [Client Association History](#) on page 1286.
- [Client Graph](#) on page 1287.

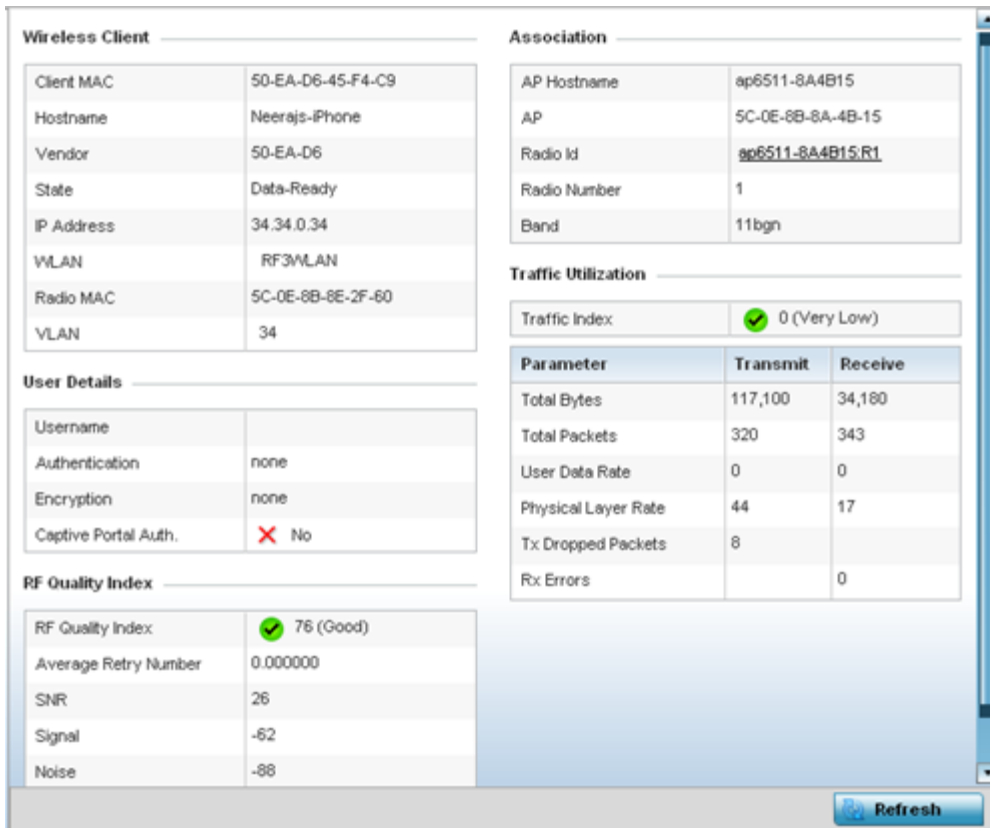
### Client Health

The **Health** screen displays performance information of a selected wireless client, in respect to the client's connected access point radio and managing controller, service platform or access point.

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 an RF Domain, select a controller, an access point, then a connected client.
- 3 Select **Health**.

The **Statistics > Wireless Client > Health** screen displays by default.



**Figure 352: Wireless Client - Statistics - Health Screen**

Refer the tables below for wireless client related data.

The **Wireless Client** field displays the following:

<b>Client MAC</b>	Displays the factory encoded MAC address of the selected wireless client.
<b>Hostname</b>	Lists the hostname assigned to the client when initially managed by the controller, service platform or access point.
<b>Vendor</b>	Displays the vendor name (manufacturer) of the wireless client.
<b>State</b>	Displays the current operational state of the wireless client. The client's state can be <b>idle</b> , <b>authenticated</b> , <b>roaming</b> , <b>associated</b> or <b>blacklisted</b> .
<b>IP Address</b>	Displays the IP address the selected wireless client is currently utilizing as a network identifier.
<b>WLAN</b>	Displays the client's connected access point WLAN membership. This is the WLAN whose QoS settings should account for the client's radio traffic objective.
<b>Radio MAC</b>	Displays the access point radio MAC address the wireless client is connected to on the network.
<b>VLAN</b>	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:

<b>Username</b>	Displays the unique name of the administrator or operator supporting the client's managing controller, service platform or access point.
<b>Authentication</b>	Lists the authentication scheme applied to the client for interoperation with the access point.
<b>Encryption</b>	Lists the encryption scheme applied to the client for interoperation with the access point.
<b>Captive Portal Authentication</b>	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:

<b>RF Quality Index</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• 0 - 20 (Very poor quality)</li> <li>• 20 - 40 (Poor quality)</li> <li>• 40 - 60 (Average quality)</li> <li>• 60 - 100 (Good quality)</li> </ul>
<b>Retry Rate</b>	Displays the average number of retries per packet. A high number indicates possible network or hardware problems.
<b>SNR</b>	Displays the SNR ratio of the connected wireless client.
<b>Signal</b>	Displays the power of the radio signals in - dBm.
<b>Noise</b>	Displays the disturbing influences on the signal by interference of signals in - dBm.
<b>Error Rate</b>	Displays the number of received bit rates altered due to noise, interference and distortion. It is a unit-less performance measure.

The **Association** field displays the following:

<b>AP Hostname</b>	Lists the administrator assigned device name of the client's connected access point.
<b>AP</b>	Displays the MAC address of the client's connected access point.
<b>Radio</b>	Lists the target access point that houses the radio. Select the access point to view performance information in greater detail.
<b>Radio ID</b>	Lists the hardware encoded MAC address the radio uses as a hardware identifier that further distinguishes the radio from others within the same device.
<b>Radio Number</b>	Displays the access point's radio number (either 1, 2 or 3) to which the selected client is associated.
<b>Radio Type</b>	Displays the radio type. The radio can be <i>802.11b</i> , <i>802.11bg</i> , <i>802.11bgn</i> , <i>802.11a</i> or <i>802.11an</i> .

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)

This table displays the following:

<b>Total Bytes</b>	Displays the total bytes processed by the access point's connected wireless client.
<b>Total Packets</b>	Displays the total number of packets processed by the wireless client.
<b>User Data Rate</b>	Displays the average user data rate in both directions.
<b>Physical Layer Rate</b>	Displays the average packet rate at the physical layer in both directions.
<b>Tx Dropped Packets</b>	Displays the number of packets dropped during transmission.
<b>Rx Errors</b>	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.

- 4 Select **Refresh** to update the screen's statistics counters to their latest values.

## Client Details

The **Details** screen provides granular performance, network address, connection and association 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 an RF Domain, select a controller, an access point, then a connected client.
- 3 Select **Details**.

The **Statistics > Wireless Client > Details** screen is displayed.



**Figure 353: Wireless Client Detailed Statistics Screen**

The **Wireless Client** field displays the following:

SSID	Displays the client's 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 RF Domain member, 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.



<b>Client Identity</b>	Displays the unique vendor identity (Android, Windows, etc.) of the listed device as it appears to its adopting controller or service platform.
<b>Client Identity Precedence</b>	Lists the numeric precedence this client uses in establishing its identity amongst its peers.
<b>Protected Management Frames</b>	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.
<b>Transmit Power Management</b>	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:

<b>Username</b>	Displays the unique name of the administrator or operator managing the client's connected access point, controller or service platform.
<b>Authentication</b>	Lists the authentication scheme applied to the client for interoperation with its connected access point radio.
<b>Encryption</b>	Lists the encryption scheme applied to the client for interoperation with its connected access point radio.
<b>Captive Portal Auth.</b>	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:

<b>Idle Time</b>	Displays the time for which the wireless client remained idle.
<b>Last Active</b>	Displays the time in seconds the wireless client was last interoperating with its connected access point.
<b>Last Association</b>	Displays the duration the wireless client was in association with its connected access point.
<b>Session Time</b>	Displays the duration for which a session can be maintained by the wireless client without it being dis-associated from its connected access point radio.
<b>SM Power Save Mode</b>	Displays whether this feature is enabled on the wireless client. The SM (spatial multiplexing) 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: <b>static operation</b> and <b>dynamic operation</b> .
<b>Power Save Mode</b>	Displays whether this feature is enabled or not. To prolong battery life, the 802.11 standard defines an optional <i>Power Save Mode</i> , which is available on most 802.11 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.
<b>WMM Support</b>	Displays whether WMM is enabled or not in order to provide data packet type prioritization between the access point and connected client.
<b>40 MHz Capable</b>	Displays whether the wireless client has 802.11n channels operating at 40 MHz.
<b>Max Physical Rate</b>	Displays the client's maximum data rate at the physical layer.
<b>Max User Rate</b>	Displays the maximum client's permitted user data rate.
<b>MC2UC Streams</b>	Lists the number of multicast to unicast data streams detected.

The **Association** field displays the following:

<b>AP</b>	Displays the MAC address of the wireless client's connected access point.
<b>BSS</b>	Displays the BSS (Basic Service Set) the access point belongs to. A BSS is a set of stations that can communicate with one another.
<b>Radio Number</b>	Displays the access point radio number the wireless client is connected to.
<b>Radio Type</b>	Displays the radio type. The radio can be <b>802.11b</b> , <b>802.11bg</b> , <b>802.11bgn</b> , <b>802.11a</b> or <b>802.11an</b> .
<b>Rate</b>	Displays the permitted data rate for controller managed access point and client interoperation.

The **802.11 Protocol** field displays the following:

<b>High-Throughput</b>	Displays whether high throughput is supported. High throughput is a measure of successful packet delivery over a communication channel.
<b>RIFS</b>	Displays whether RIFS is supported. RIFS is a required 802.11n feature that improves performance by reducing the amount of dead time between OFDM transmissions.
<b>Negotiated Fast BSS Transition</b>	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.
<b>Unscheduled APSD</b>	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.
<b>AID</b>	Displays the AID (Association ID) 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.
<b>Max AMSDU Size</b>	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.
<b>Max AMPDU Size</b>	Displays the maximum size of AMPDU. AMPDU is a set of Ethernet frames to the same destination wrapped in an 802.11n MAC header. AMPDUs are used in noisy environments to provide reliable packet transmission. This value is the maximum AMPDU size in bytes.
<b>Interframe Spacing</b>	Displays the time interval between two consecutive Ethernet frames.
<b>Short Guard Interval</b>	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 ISI (inter-symbol interference). 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 **Refresh** to update the screen's statistics counters to their latest values.

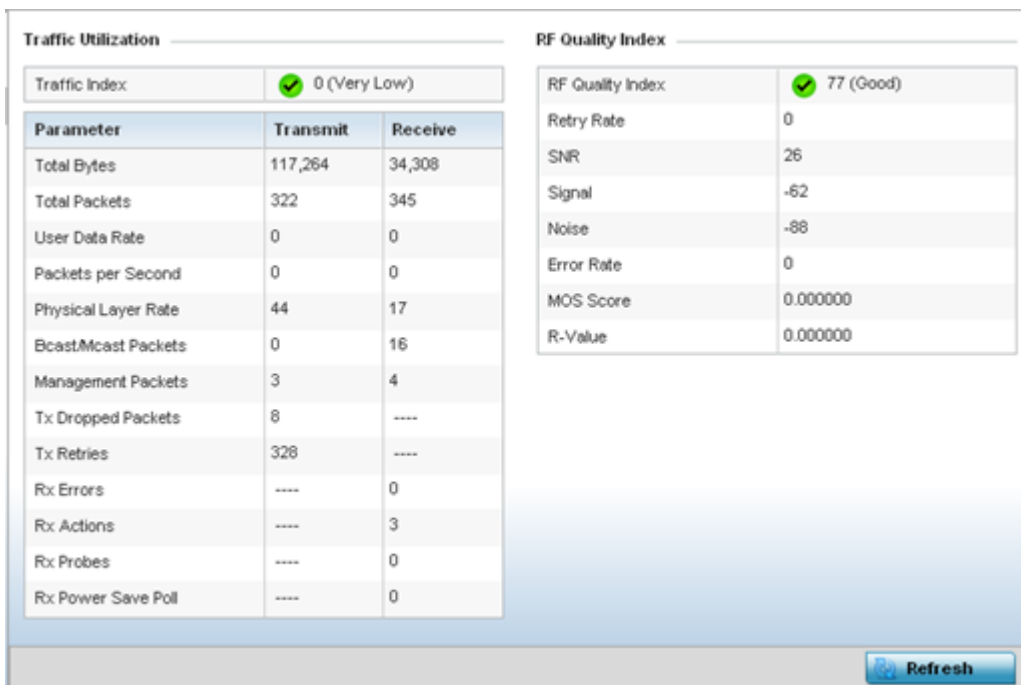
## Client Traffic

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 an RF Domain, select a controller, an access point, then a connected client.
- 3 Select **Traffic**.

The **Statistics > Wireless Client > Traffic** screen is displayed.



The **Traffic Utilization** statistics employs 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. The 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:

<b>Total Bytes</b>	Displays the total bytes processed (in both directions) by the access point's connected client.
<b>Total Packets</b>	Displays the total number of data packets processed (in both directions) by the access point's connected wireless client.
<b>User Data Rate</b>	Displays the average user data rate.
<b>Packets per Second</b>	Displays the packets processed per second.
<b>Physical Layer Rate</b>	Displays the data rate at the physical layer level.
<b>Bcast/Mcast Packets</b>	Displays the total number of broadcast/management packets processed by the client.
<b>Management Packets</b>	Displays the number of management (overhead) packets processed by the client.

<b>Tx Dropped Packets</b>	Displays the client's number of dropped packets while transmitting to its connected access point.
<b>Tx Retries</b>	Displays the total number of client transmit retries with its connected access point.
<b>Rx Errors</b>	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.
<b>Rx Actions</b>	Displays the number of receive actions during data transmission with the client's connected access point.
<b>Rx Probes</b>	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.
<b>Rx Power Save Poll</b>	Displays the power save using the PSP (Power Save Poll ) 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:

<b>RF Quality Index</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• 0 - 20 (Very low utilization)</li> <li>• 20 - 40 (Low utilization)</li> <li>• 40 - 60 (Moderate utilization)</li> <li>• 60 and above (High utilization)</li> </ul>
<b>Retry Rate</b>	Displays the average number of retries per packet. A high number indicates possible network or hardware problems.
<b>SNR (dBm)</b>	Displays the connected client's SNR. A high SNR could warrant a different access point connection to improve performance.
<b>Signal (dBm)</b>	Displays the power of the radio signals in - dBm.
<b>Noise (dBm)</b>	Displays the disturbing influences on the signal in - dBm.
<b>Error Rate (ppm)</b>	Displays the number of received bit rates altered due to noise, interference and distortion. It is a unit-less performance measure.
<b>MOS Score</b>	Displays average voice call quality using the MOS (Mean Opinion Score ) 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.
<b>R-Value</b>	<i>R-value</i> is a number or score used to quantitatively express the quality of speech in communications systems. This is used in digital networks that carry VoIP (Voice over IP ) traffic. The R-value can range from 1 ( <i>worst</i> ) to 100 ( <i>best</i> ) 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 **Refresh** to update the screen's statistics counters to their latest values.



## Client WMM TSPEC

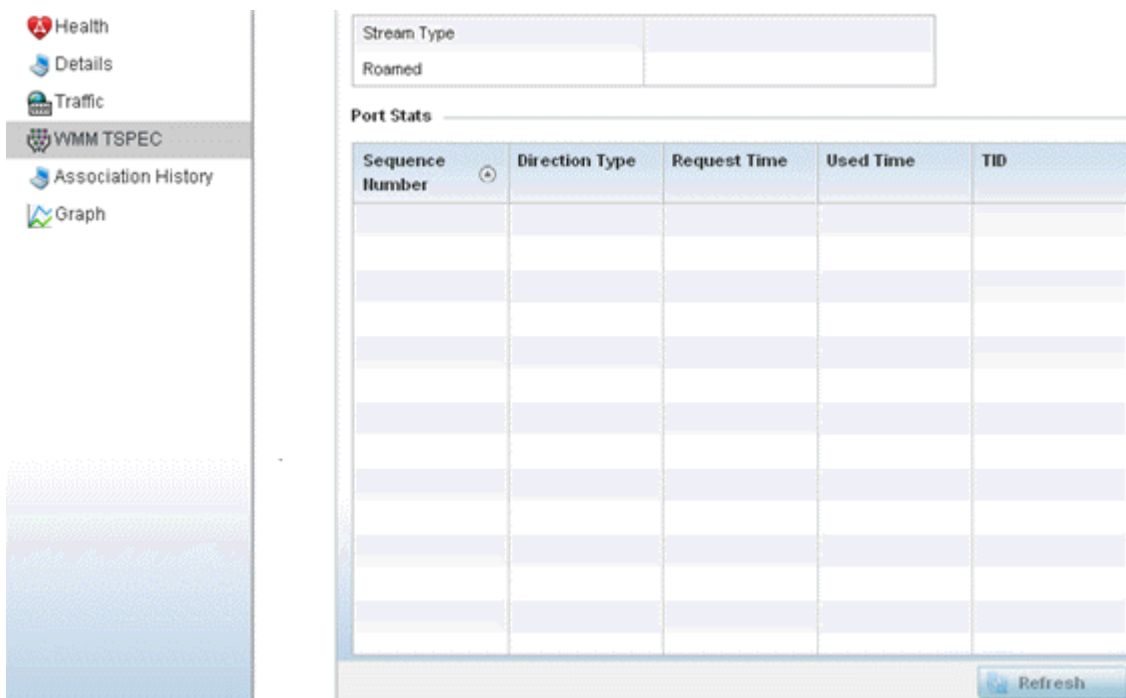
The 802.11e TSPEC (Traffic Specification) provides a set of parameters that define the characteristics of the traffic stream, (operating requirement and scheduling etc.). The sender's TSPEC specifies parameters available within packet flows. Both sender and the receiver use TSPEC.

The TSPEC screen provides the 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 an RF Domain, select a controller, an access point, then a connected client.
- 3 Select **WMM TPSEC**.

The **Statistics > Wireless Client > WMM TPSEC** screen is displayed.



The top portion of the screen displays the TSPEC stream type and whether the client has roamed.

The **Ports Stats** field displays the following:

<b>Sequence Number</b>	Lists the system assigned sequence number that's unique to this WMM TPSEC <b>uplink</b> or <b>downlink</b> data stream.
<b>Direction Type</b>	Displays whether the WMM TPSEC data stream is in the <b>uplink</b> or <b>downlink</b> direction.
<b>Request Time</b>	Lists each sequence number's request time for WMM TPSEC traffic in the specified direction. This is time allotted for a request before packets are actually sent.

<b>Used Time</b>	Displays the time the client used TSPEC. The client sends a DELTS (delete traffic stream) message when it has finished communicating.
<b>TID</b>	Displays the parameter for defining the traffic stream. TID identifies data packets as belonging to a unique traffic stream.

- Periodically, select **Refresh** to update the screen to its latest values.

### Client Association History

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 managed network.

To view a selected client's association history:

- Select the **Statistics** menu from the Web UI.
- Select **System** from the navigation pane (on the left-hand side of the screen). Expand an RF Domain, select a controller, an access point, then a connected client.
- Select **Association History**.

The **Statistics > Wireless Client > Association History** screen is displayed.

Access Point	BSSID	Channel	Band	Time
5C-0E-8B-8A-4B-15	5C-0E-8B-8E-2F-60	1	2.4Ghz	Mon Jun 10 2:38:49 2013
5C-0E-8B-8A-4B-15	5C-0E-8B-8E-2F-60	1	2.4Ghz	Mon Jun 10 2:35:43 2013
5C-0E-8B-8A-4B-15	5C-0E-8B-8E-2F-60	1	2.4Ghz	Mon Jun 10 0:32:55 2013

Row Count: 3

- Refer to the following to determine this client's access point association history:

<b>access point</b>	Lists the access point MAC address this client has connected to, and is being managed by
<b>BSSID</b>	Displays the BSSID of each previously connected access point.
<b>Channel</b>	Lists the channel shared by both the access point and client for interoperation, and to avoid congestion with adjacent channel traffic.

<b>Band</b>	Lists the 2.4 or 5GHz radio band this clients and its connect access point are using for transmit and receive operations.
<b>Time</b>	Lists the historical connection time between each listed access point and this client.

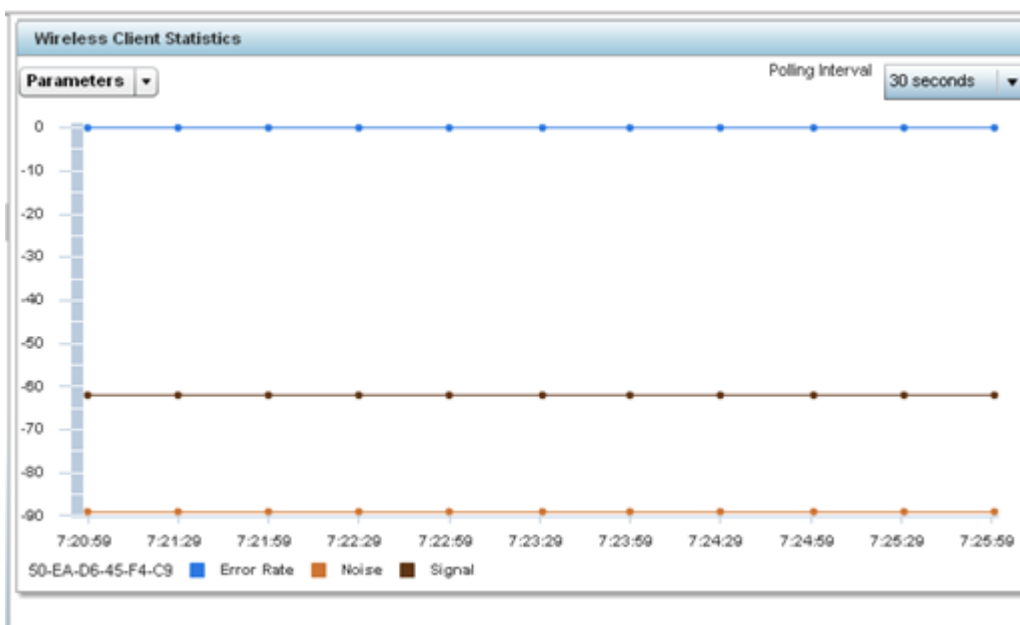
- 5 Select **Refresh** to update the screen to it's latest values.

## Client Graph

Use the **Graph** to assess a connected client's radio performance and diagnose performance issues that may be negatively impacting 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 an RF Domain, select a controller, an access point, then a connected client.
- 3 Select **Graph**.
- 4 Use the **Parameters** drop-down menu to define from 1- 3 variables assessing 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**. The default value is *30 seconds*.



- 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.

---

## Guest Access 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 Cumulative Statistics](#) on page 1288
- [Guest Access Social Media Statistics](#) on page 1290
- [Guest Access Reports](#) on page 1292
- [Guest Access Notifications](#) on page 1293
- [Guest Access Database](#) on page 1295

### Guest Access Cumulative 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.

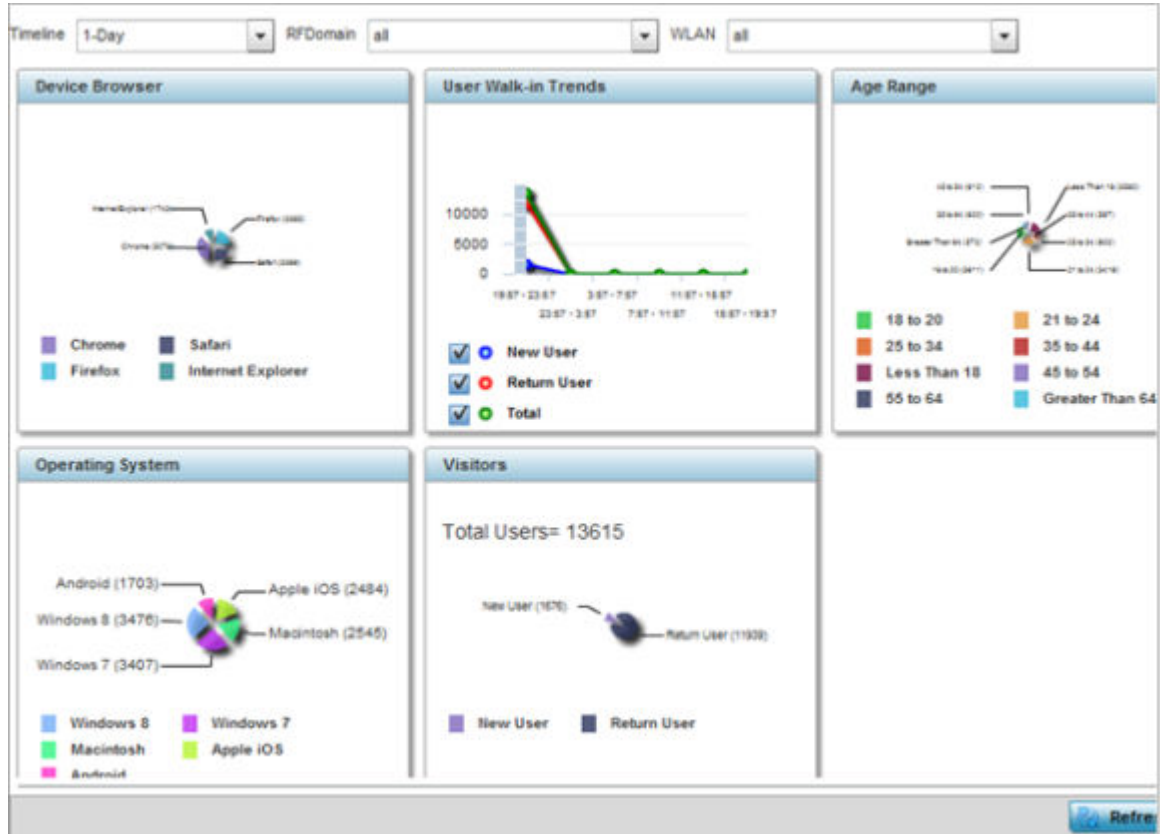
To view a cumulative set of client guest access statistics:

- 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).

The **Guest Access > Statistics** page displays in the right-hand pane, with the **Statistics** screen selected by default.



**Figure 354: Guest Access - Statistics Screen**

- 3 Use the following filters, available at the top of the screen, to filter guest access statistical data.

<b>Timeline</b>	Use the drop-down menu to specify whether statistics are gathered for <b>1-Day, 1-Month, 1-Week, 2-Hours, 30-Mins</b> or <b>5-Hours</b> . Timelines support the latest time period from present. For example, specifying 30-Mins displays statistics for the most recent 30 minutes trended.
<b>RFDomain</b>	Use the drop-down menu to select a single RF Domain from which to filter guest access statistics. Optionally select <b>All</b> to include data from each RF Domain supported.
<b>WLAN</b>	Use the drop down menu to filter guest access statistics to a specific WLAN. Optionally select <b>All</b> to include data from all WLANs within the selected RF Domain.  <b>Note:</b> A WLAN can belong to more than one RF Domain.

- 4 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:

<b>Device Browser</b>	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.
<b>User Walk-in Trends</b>	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.
<b>Age Range</b>	Displays guest user age differentiation in pie-chart format. Age ranges are uniquely color coded as: <b>Less Than 18, 18 to 20, 21 to 24, 25 to 34, 35 to 44, 45 to 54, 55 to 64</b> and <b>Greater Than 64</b> . 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.
<b>Operating System</b>	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.
<b>Visitors</b>	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.
<b>Customer Loyalty App</b>	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.
<b>Devices</b>	Displays guest client device type utilization in pie-chart format. Each client device type (Windows PC, Macintosh, Apple iPad, and Android Mobile) 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.
<b>Gender</b>	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.

## Guest Access Social Media 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.

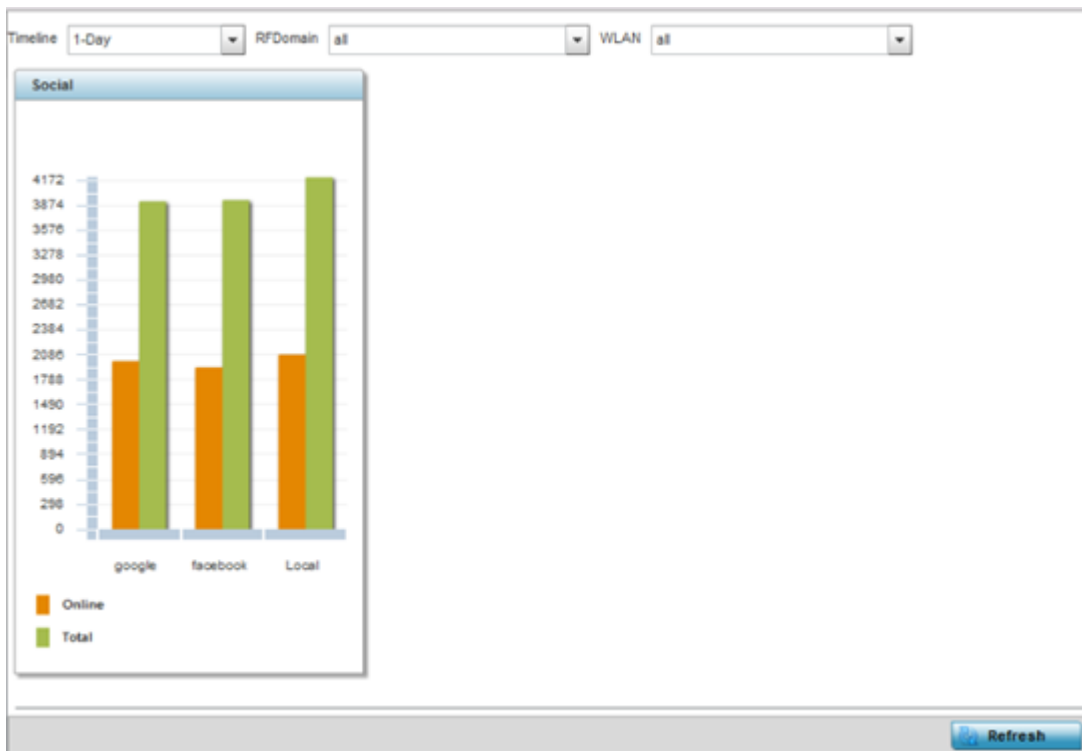
To view guest access social media utilization for guest clients:

- 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**).

The Guest Access statistics menu is displayed in the right-hand pane, with the **Statistics** screen selected by default.

- 3 Select **Social** from the statistics menu.

The **Guest Access > Social** page displays.



**Figure 355: Guest Access - Social Media - 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 social media trending:

<b>Timeline</b>	Use the drop-down menu to specify whether statistics are gathered for <b>1-Day</b> , <b>1-Month</b> , <b>1-Week</b> , <b>2-Hours</b> , <b>30-Mins</b> or <b>5-Hours</b> . Timelines support the latest time period from present. For example, specifying 30-Mins displays statistics for the most recent 30 minutes trended.
<b>RFDomain</b>	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.
<b>WLAN</b>	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.

## Guest Access Reports

Report queries can be filtered and run to obtain information on targeted guest clients within the WiNG guest network.

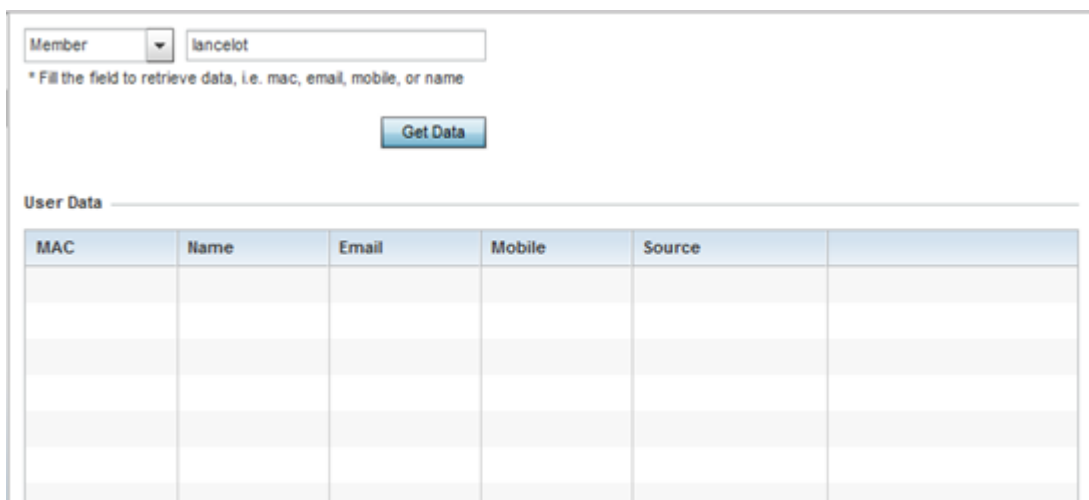
To generate customized guest client reports:

- 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**).

The Guest Access statistics menu is displayed in the right-hand pane, with the **Statistics** screen selected by default.

- 3 Select **Reports** from the statistics menu.

The **Guest Access > Reports** page displays.



**Figure 356: Guest Access - Reports Screen**

- 4 Use 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 the client’s **MAC** address, **Name**, **Mobile**, **Email**, **Member** or **Time** (login duration). Once provided, enter an appropriate search string to generate a report for the target guest client.
- 5 After specifying the data filter criteria, select **Get Data**.
- 6 Refer to the **User Data** table to review the following report output:

<b>MAC</b>	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.
<b>Name</b>	Lists the name used for guest access authentication and pass code generation.

<b>Email</b>	Lists the E-Mail address used for guest access authentication and the receipt of the required passcode.
<b>Mobile</b>	Lists the guest client's registered mobile number used for guest access authentication requests and the receipt of the required passcode.
<b>Source</b>	Lists the source (Facebook, Google) whose username and password were used as the client's social media authenticator.

## Guest Access Notifications

For each registered guest user, a passcode is sent by E-mail, SMS (short message service) 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.

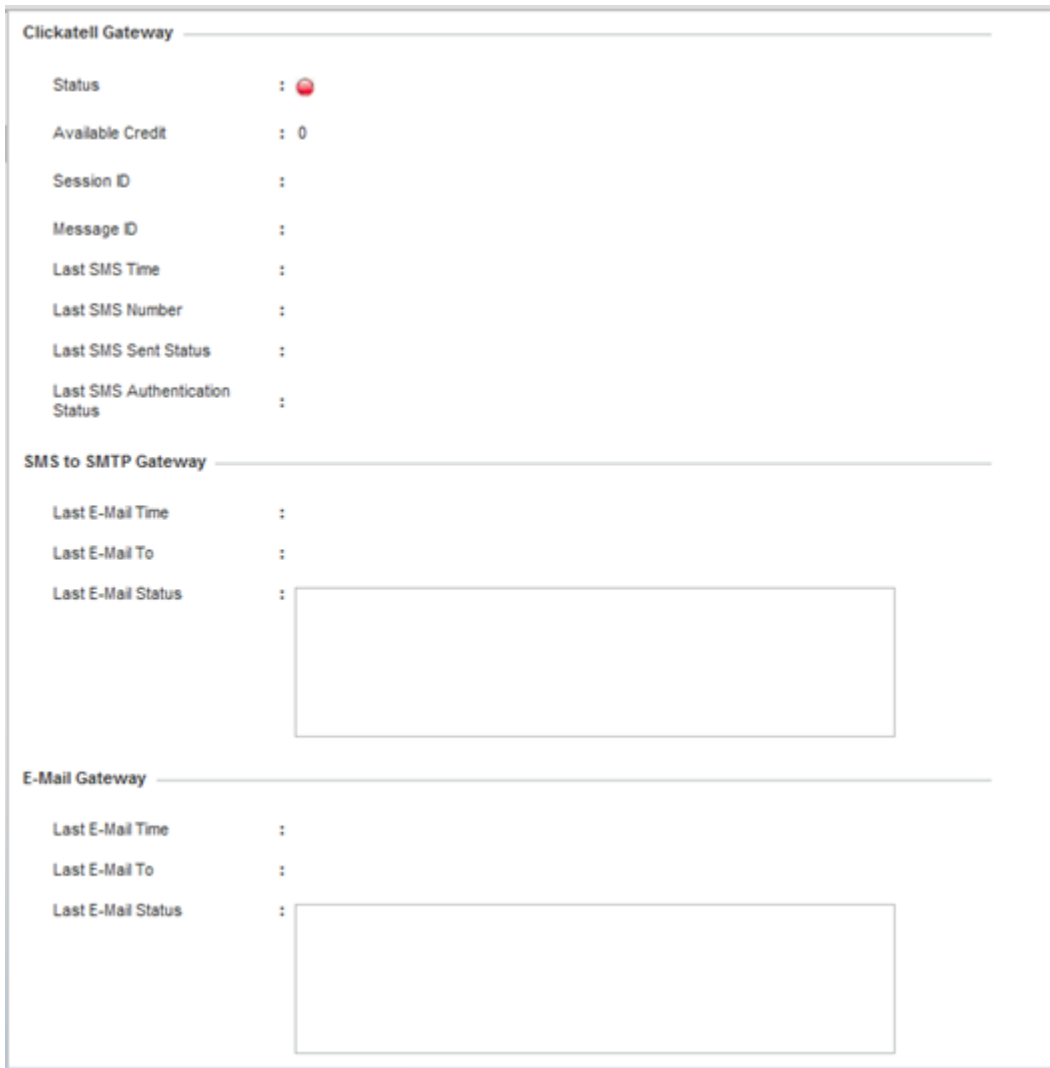
The SMS is the text messaging service component of phone, E-Mail and mobile systems. SMS uses standardized communications protocols to allow fixed or mobile phone devices to exchange text messages.

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**).

The Guest Access statistics menu is displayed in the right-hand pane of the UI. The cumulative statistics screen is displayed by default.

- 3 Select **Notification** from the statistics menu.  
The **Guest Access > Notification** page displays.



**Figure 357: Guest Access - Notification Screen**

- 4 Review the following **Clickatell Gateway** information. By default, clickatell is the host SMS gateway server resource for guest access.

<b>Status</b>	Displays an icon as a visual indicator of the gateway status. <i>Green</i> defines the gateway as available. <i>Red</i> indicates the gateway is down and unavailable.
<b>Available Credit</b>	PENDING
<b>Session ID</b>	Lists an event ID for the clickatell gateway session credential and passcode exchange.
<b>Message ID</b>	Lists the unique SMS message ID created for the successful message exchange with the clickatell host SMS gateway server.
<b>Last SMS Time</b>	Lists the timestamp appended to the sent time of the clickatell SMS gateway message.

<b>Last SMS Number</b>	Lists the numeric status code returned in response to a SMS gateway server guest access request.
<b>Last SMS Sent Status</b>	Lists the associated status strings returned in response to a SMS gateway server guest access request.
<b>Last SMS Authentication Status</b>	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.

<b>Last E-Mail Time</b>	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.
<b>Last E-Mail To</b>	Lists the recipient of the most recent SMS to SMTP server credential E-mail exchange containing the required passcode for the registered guest.
<b>Last E-Mail Status</b>	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.

<b>Last E-Mail Time</b>	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.
<b>Last E-Mail To</b>	Lists the recipient of this session's server E-Mail credential exchange containing the required passcode for the authenticating guest client.
<b>Last E-Mail Status</b>	Lists the completion status of the most recent server E-Mail credential exchange containing the required passcode for the authenticating guest client.

## Guest Access Database

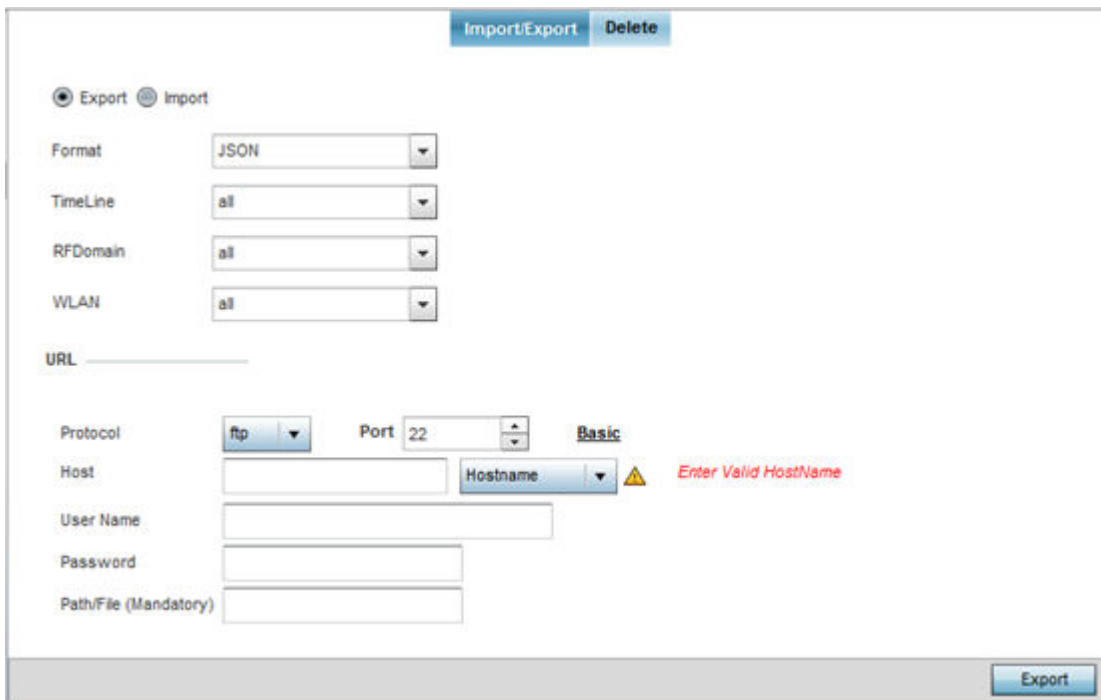
Guest client statistics are uniquely available for wireless clients requesting the required pass code, authentication and access into the WiNG managed guest client network.

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**).

The Guest Access statistics menu is displayed in the right-hand pane, with the **Statistics** screen selected by default.

- 3 Select **Database** from the statistics menu.  
The **Guest Access > Database** page displays.



**Figure 358: 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:

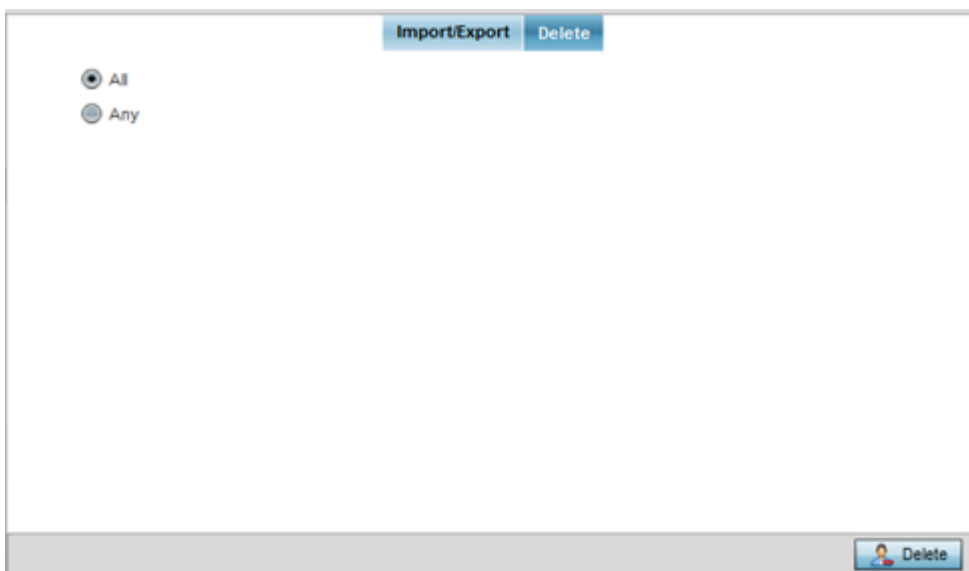
<b>Format</b>	Define whether the guest access data is exported in <b>JSON</b> or <b>CSV</b> format. JSON (JavaScript Object Notation ) is an open standard format using text to export data objects consisting of attribute value pairs. A CSV (comma-separated values ) file stores tabular data in plain text. 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.
<b>Timeline</b>	Use the drop-down menu to specify whether guest access statistics are exported for the previous <b>1-Day, 1-Month, 1-Week, 2-Hours, 30-Mins</b> or <b>5-Hours</b> . Timelines support the latest time period from present. For example, specifying 30-Mins exports statistics trended over the most recent 30 minutes.
<b>RFDomain</b>	Use the drop-down menu to select a single RF Domain from which to filter social media guest access statistics. Optionally select <b>All</b> to include data from each RF Domain supported.
<b>WLAN</b>	Use the drop down menu to filter guest access social media statistics to a specific WLAN. Optionally select <b>All</b> to include data from all WLANs within the selected RF Domain.  <b>Note:</b> A WLAN can belong to more then one RF Domain.



- 6 When exporting or importing guest access data (regardless of format), provide the following URL data to accurately configure the remote host.

<b>Protocol</b>	Select the data transfer protocol used for exporting or importing guest access data. Available options include: <ul style="list-style-type: none"> <li>• tftp</li> <li>• ftp</li> <li>• sftp</li> </ul>
<b>Port</b>	Use the spinner control to set the virtual port for the for the export or import operation.
<b>Host</b>	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 <b>IPv4 Address</b> to use an IPv4 formatted address as the host. Select <b>IPv6 Address</b> 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.
<b>User Name</b>	If using FTP or SFTP as the data transfer protocol, enter the <i>username</i> required by the remote FTP or SFTP server resource.
<b>Password</b>	If using FTP or SFTP as the data transfer protocol, enter the <i>password</i> required by the remote FTP or SFTP server resource.
<b>Path/File (Mandatory)</b>	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 CLI (command line interface).

- 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.  
The **Guest Access > Database > Delete** Screen displays.



**Figure 359: Guest Access - Database - Delete Screen**

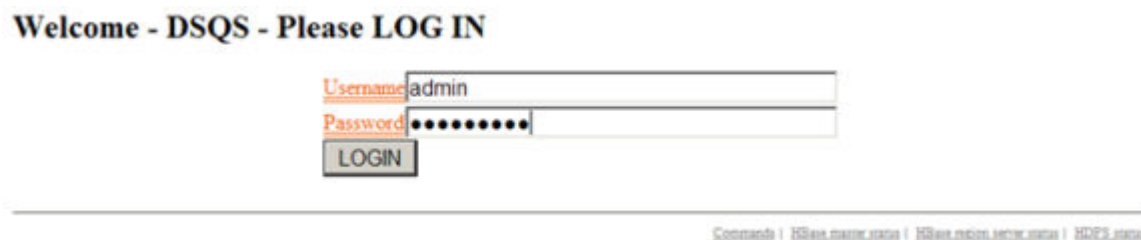
- 9 Select **All** to remove the contents of the entire database. Select **Any** to invoke a drop-down menu where **MAC, Name, Mobile, Email** or a **WLAN** can be selected to refine the database removal to just a selected entity. Enter the name of the MAC address, user, mobile number or WLAN you wish to remove from the database, then select **Delete**.

## Analytics Developer Interface

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 NX 95XX, NX 96XX and NX 7510 models.

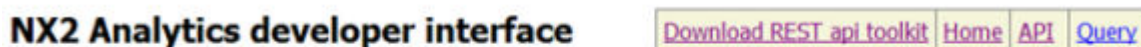
To access the developer interface:

- 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 360: Statistics - Analytics Developer Interface - Login Screen**

- 2 Provide the same **Username** and **Password** credentials you're currently utilizing for a typical controller login. On login, the following screen displays:



**Figure 361: Statistics - Analytics Developer Interface - Home Screen**

Refer to the following for more detailed descriptions of the functionality available to administrators using the analytics developer interface:

- [Download REST API Toolkit](#) on page 1298.
- [REST API Assessment](#) on page 1300.

3

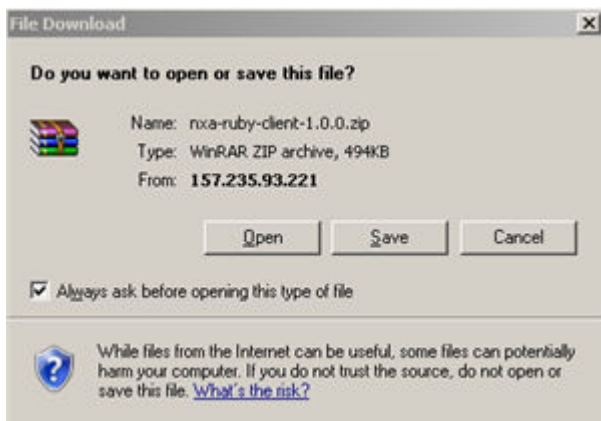
## Download REST API Toolkit

Sample REST (Representational State Transfer) 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 362: Download Rest API Toolkit - 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%20http://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 NXStatsClient <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 NXStatsClient 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

## REST API Assessment

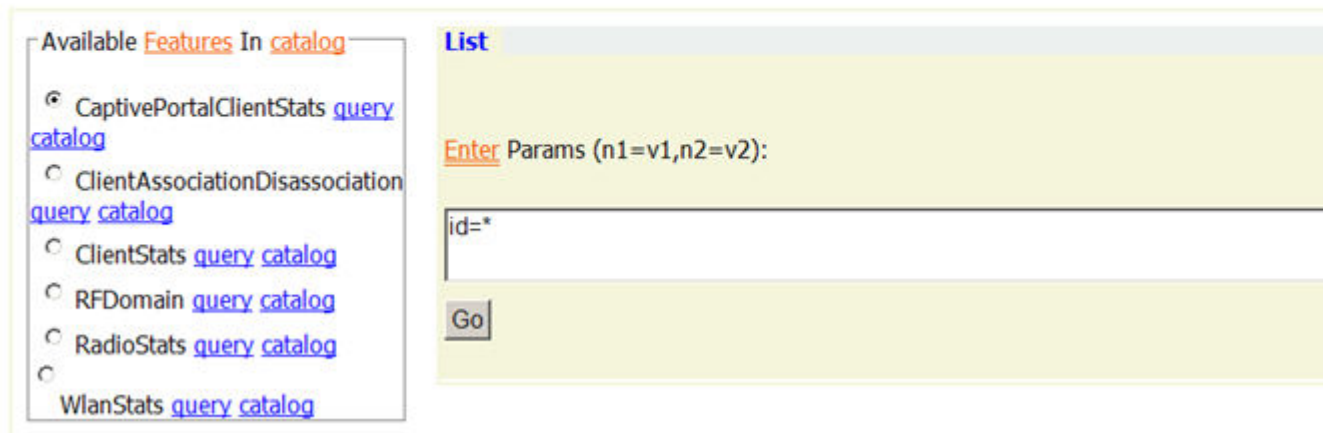
Refer to the toolkit's API functionality to review a collection of APIs for specific feature groups, including captive portals, client associations and disassociations, client stats, RF Domains.

To review the toolkit's built-in set of APIs:

- 1 Select API from the Web UI.  
The REST API Toolkit's Built-in API Set displays.

## NX2 Features Interface

Current Feature is catalog features



The screenshot shows a web interface for the REST API Toolkit. On the left, there is a list titled "Available Features In catalog". The list contains several radio buttons, each followed by a feature name and a link to a query page. The first feature, "CaptivePortalClientStats", is selected. To the right of the list is a section titled "List" with a yellow background. Below this title is a text input field with the placeholder text "Enter Params (n1=v1,n2=v2):". The input field contains the text "id=\*". Below the input field is a "Go" button.

**Figure 363: Developer Interface - REST API ToolKit - Built-in API Set**

- 2 Select an available feature from the catalog of features.



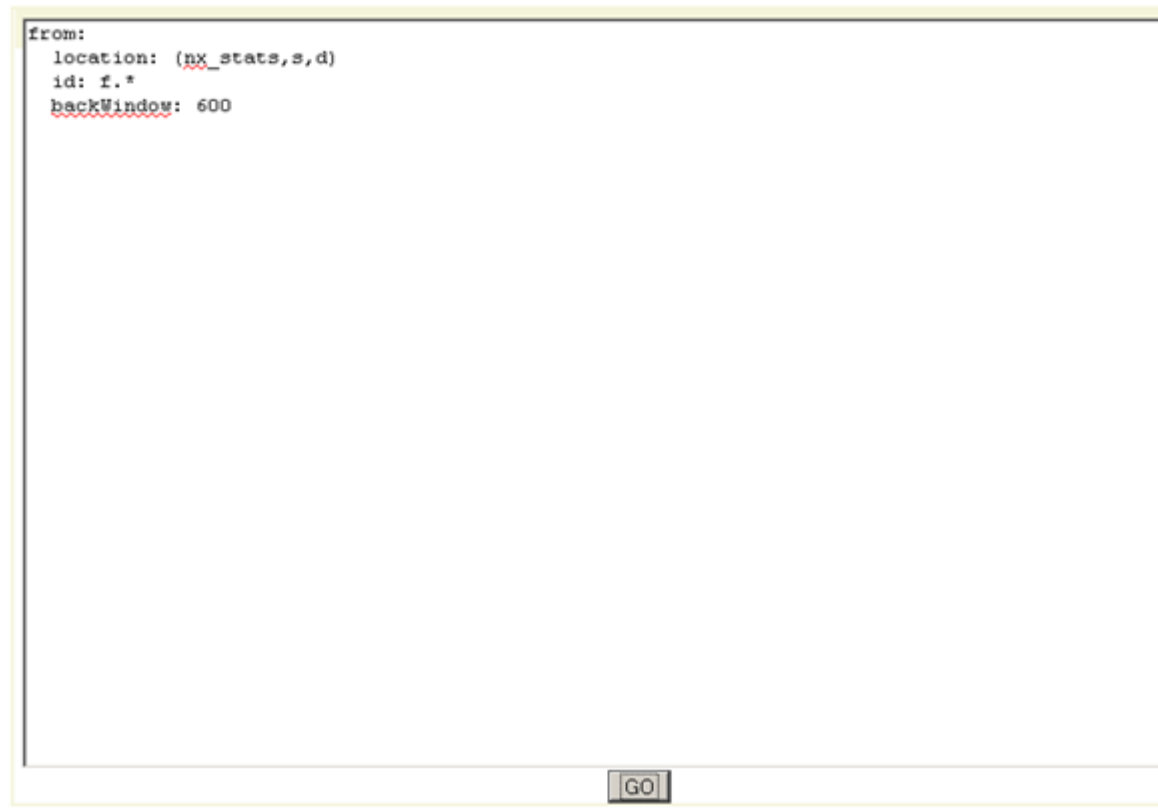
### Note

You 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.

The NX2 Query Interface displays.

## NX2 Raw Query Interface



**Figure 364: Developer Interface - NX2 Raw Query Interface**

- 4 Select **Go** to initiate the query for the selected item.

```

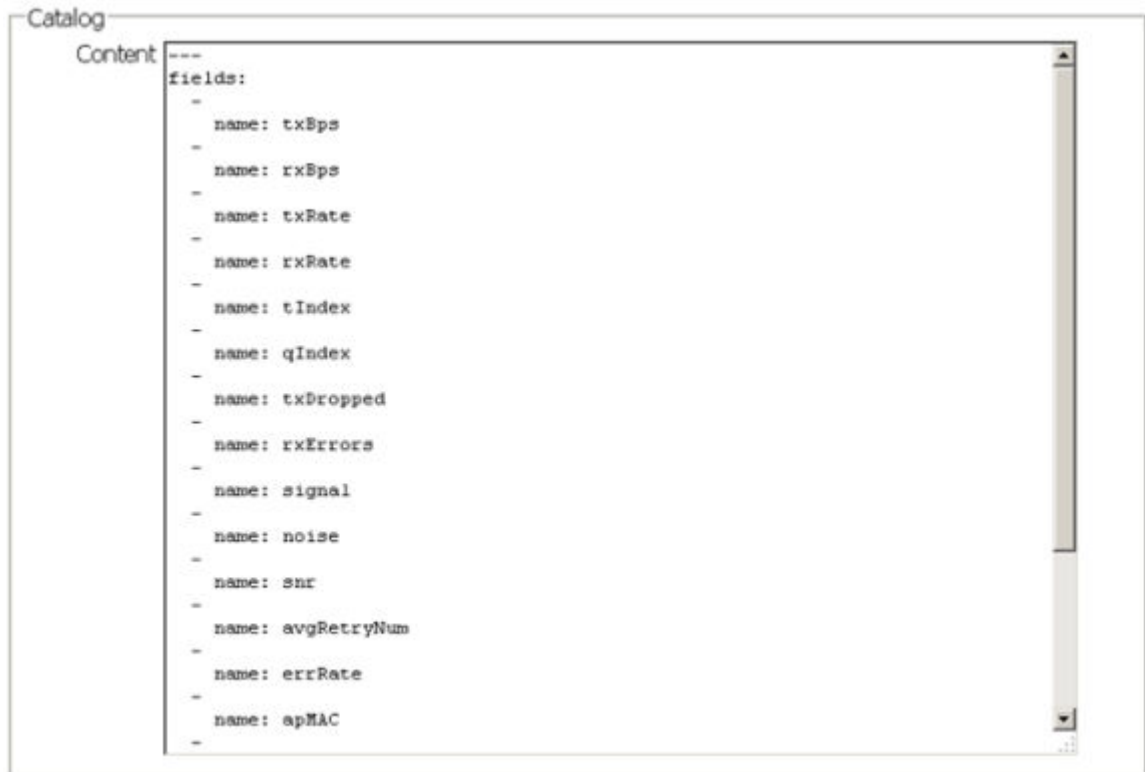
- <data>
  - <RFDomainStats>
    <smu>92</smu>
    <txPps>0</txPps>
    <rxBps>0</rxBps>
    <signal>0</signal>
    <numANRadios>1</numANRadios>
    <numSensors>1</numSensors>
    <tIndex>0</tIndex>
    <numAClients>0</numAClients>
    <numRadios>3</numRadios>
    <rfDomain>default</rfDomain>
    <threatLevel>0</threatLevel>
    <totalPps>0</totalPps>
    <rxErrors>0</rxErrors>
    <totalMgmtPkts>0</totalMgmtPkts>
    <rxPps>0</rxPps>
    <totalBps>0</totalBps>
    <txPkts>41</txPkts>
    <numBGNClients>0</numBGNClient:
    <numANClients>0</numANClients>
    <txBytes>13170</txBytes>
    <rxBCMCPkts>0</rxBCMCPkts>
    <numBGNRadios>1</numBGNRadio:
    <numAClients>0</numAClients>
    <rxBytes>6042</rxBytes>
    <noise>-92</noise>
    <numBGClients>0</numBGClients>
    <txDropped>0</txDropped>
    <rxPkts>46</rxPkts>
    <numBClients>0</numBClients>
    <maxUserRate>0</maxUserRate>
    <txMgmtPkts>0</txMgmtPkts>
    <qIndex>100</qIndex>
    <txBCMCPkts>0</txBCMCPkts>
    <txBps>0</txBps>
    <totalBytes>19212</totalBytes>

```

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.

**Figure 365: Developer Interface - REST API - Raw Query Result**

- 5 From the NX2 Features Interface, select a feature from those available and select 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.

**Figure 366: Developer Interface - REST API - Catalog**



# 16 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 is 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 889.