Using the Avaya OS for Avaya WLAN AP 9100 Series

Release 8.1
NN47252-102
Issue 05.01
July 2016

Notices

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of

printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY

INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE

(“AVAYA”). Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order

documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products”, or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Table of Contents

List of Figures

Introduction

This chapter introduces the Avaya WLAN 9100 Series Solution, with an overview of its key features and benefits.

The Avaya WLAN 9100 Series Solution

Figure 1. WAP

The Avaya family of products includes the following:

- **Avaya Wireless Access Points**

  Avaya APs are designed to provide distributed intelligence, integrated switching capacity, application-level intelligence, increased bandwidth, and smaller size. The radios support IEEE802.11 ac, a, b, g, and n clients, and feature the capacity and performance needed to replace switched Ethernet to the desktop.

- **Wireless LAN Orchestration System (WOS)**

  WOS is used for managing large wireless deployments from a centralized Web-based interface. WOS is capable of managing large numbers of

WAPs, including automated software and firmware upgrades for the network.

WOS is hosted on your own server. It manages all aspects of your Avaya wireless network. For detailed information, refer to *Using the Avaya Wireless Orchestration System (NN47252-103).*

Nomenclature

In some instances the terms **product** and **unit** may be used to refer to Access Points. When discussing specific products from the Avaya family, the product name is used (for example, WAP9122). The WAP's operating system is referred to as the Avaya OS (AOS). The Web Management Interface for browser-based management of the WAP is referred to as WMI.

WAPs have very flexible radio capabilities—each of the radios may be independently configured to support IEEE802.11a, 11b, 11g, or 11n clients or a combination of client types. On WAPs featuring 802.11ac, this option is also included. One radio may be assigned as the RF **monitor** radio, supporting intrusion detection and prevention, self-monitoring, and other services. Radios support both 2.4GHz and 5 GHz, and are named **radio1, radio2, ... radio*n***.

The Wireless LAN Orchestration System is referred to as WOS. The Power over Ethernet system may be referred to as PoE.

Why Choose the Avaya Access Point?

The deployment of wireless is a necessity as businesses strive for greater flexibility in the workplace and the need for employee mobility rises. The user community is placing spiraling and often unanticipated demands on the wireless network, with the rapid proliferation of devices such as iPads and wireless enabled phones. Avaya High Density APs have the capability to support the large number of user devices present in today's environments, with superior range and coverage.

Wireless has come a long way in the past few years and now offers the performance, reliability and security that Enterprise customers have come to expect from their networks. The technology is being driven by these major IEEE standards:

- **802.11ac**
  Operates in the 5 GHz range, using a number of advanced techniques to achieve a maximum speed of 1.733 Gbps. These techniques include improvements on the methods used for 802.11n, below.
- **802.11n**
  Uses multiple antennas per radio to boost transmission speed as high as 450Mbps, increasing throughput, range, and maximum number of users. 802.11n is backwards compatible with 802.11a/b/g.
- **802.11a**
  Operates in the 5 GHz range with a maximum speed of 54 Mbps.
- **802.11b**
  Operates in the 2.4 GHz range with a maximum speed of 11 Mbps.
- **802.11g**
  Supports a higher transmission speed of 54 Mbps in the 2.4 GHz range and is backwards compatible with 802.11b.

Whether you have just a few users or many users, the Avaya AP has the scalability and flexibility to serve your needs.

See Also

Key Features and Benefits
Wireless Access Point Product Overview
The Avaya WLAN 9100 Series Solution

Wireless Access Point Product Overview

The WAP is a high capacity, multi-mode device. Its distributed intelligence eliminates the use of separate controllers and their accompanying bottlenecks. Each radio can achieve up to 1.733 Gbps throughput, depending on the model.

Figure 2. Sample WAP

The Wireless AP (regardless of the product model) is Wi-Fi® compliant and simultaneously supports 802.11ac (on .11ac models), 802.11a, 802.11b, 802.11g, and 802.11n clients. The multi-state design allows you to assign radios to 2.4 GHz and 5 GHz bands (or both) in any desired arrangement. Integrated switching and active enterprise class features such as VLAN support and multiple SSID capability enable robust network compatibility and a high level of scalability and system control. The Wireless LAN Orchestration System (WOS) allows global management of hundreds of WAPs from a central location.

Multiple versions of the WAP with different numbers of radios support a variety of deployment applications.

Avaya WLAN 9100 Product Family

WAP9112 Wall Mounted 2-Radio Access Points

The WAP9112 is a Gigabit Wi-Fi wall AP with integrated wired 4-port Gigabit switch designed for in-room connectivity. This AP supports 802.11ac standards with two 2x2 Wave 1 radios, and is designed for multi-device wired and wireless connectivity in hotel rooms, dormitories, hospital rooms, offices, and similar locations. Using existing in-wall cabling, the WAP9112 delivers Wi-Fi access, connectivity to multiple wired devices and pass-through access for legacy devices like POTS. These models have omni-directional antennas.

Feature	WAP9112
No. radios: 802.11 a/b/g/n/ac/Monitor	2
Radio type	2x2
Integrated antennas	4
Integrated wireless switch ports	1
Gigabit Uplink Port	1
Wireless bandwidth	1.1 Gbps
Users supported	256

The WAP9112 runs a different operating system than Avaya OS, and the WMI and CLI described in this book **do not apply to the WAP9112.** This model should be managed using WOS.

WAP9114 Ceiling Mount 2-Radio Access Points

The WAP9114 is a low cost Gigabit Wi-Fi AP with two 2x2 802.11ac Wave 1 radios, optimized for high performance/low complexity networks such as those in classrooms, hotel rooms, hotspots, and SME offices. These models have omni-directional antennas.

Feature	WAP9112
No. radios: 802.11 a/b/g/n/ac/Monitor	2
Radio type	2x2
Integrated antennas	4
Integrated wireless switch ports	1
Gigabit Uplink Port	1
Wireless bandwidth	1.1 Gbps
Users supported	254

The WAP9114 runs a different operating system than Avaya OS, and the WMI and CLI described in this book **do not apply to the WAP9114.** This model should be managed using WOS.

WAO9122 Outdoor 2-Radio Access Points

These outdoor Access Points have one Gigabit Ethernet port and two multi-state radios (2.4GHz or 5GHz). They support 600Mbps total, connecting up to 240 users at one time.

The Access Point provides flexibility for delivering wireless service in low-to-medium user density scenarios, in challenging deployments in areas with high RF attenuation, and in isolated or physically separated locations.

These models have an integrated controller, firewall, threat sensor, and spectrum analyzer. Outdoor units have external antennas.

Feature	WAO9122
No. radios: 802.11 a/b/g/n/monitor	2
Radio type	2x2
Integrated wireless switch ports	2
Integrated RF spectrum analyzer, threat sensors	Yes
Gigabit Uplink Port	1
Wireless bandwidth	600 Mbps
Users supported	240

WAP9122/9123, WAP9132/9133 2-Radio Access Points

The WAP9122/9123 Access Points are 802.11a/b/g/n capable with a unique ability to be upgraded to 802.11ac via optional licenses. These Access Points provide investment protection to customers who do not require or do not want to invest in 802.11ac capability today. When 802.11ac requirements arise, the customers can simply purchase and apply licenses to some or all of the access points driven by business needs. Other than the license cost, there are no other operational expenses involved in the 802.11n to 802.11ac upgrade for these APs.

The WAP9132/9133 Access Points are high performance 802.11ac compliant out of the box. They offer customers flexibility to deploy 802.11ac fresh installations or migrate from existing 802.11n to 802.11ac capable networks.

These Access Points provide robust wireless service in low-to-medium user density scenarios. They have two Gigabit Ethernet ports and two multi-state radios (2.4GHz or 5GHz), so that as more of your clients migrate to 802.11ac, you can increase the number of radios operating at 5 GHz. Each of the two 3x3 802.11ac radios supports 1.3Gbps, connecting up to 240 users at one time with 2.6Gbps total Wi-Fi bandwidth.

WAP9122/9123 models initially support 802.11n, but may be upgraded to support 802.11ac.

These models have an integrated controller, firewall, threat sensor spectrum analyzer, and application-level intelligence. They have omni-directional antennas.

WAP9132/9133 models support 802.11ac operation and a unique feature that optimizes wireless performance by automatically segmenting faster 802.11ac clients from slower Wi-Fi clients. Since Wi-Fi is a shared medium, this separation ensures slower 802.11a/b/g/n clients do not slow down 802.11ac clients and prevent them from achieving high performance.

Note that the outdoor WAO9132 AP and the plenum-rated indoor WAE9132 AP are similar to the WAP9132 (which has 2x2 802.11ac radios), except that 9132 APs use customer-provided external antennas rather than having integrated antennas. See the Avaya *Installing the Avaya WLAN Access Point WAE9132-WAO9132* guide for more information.

Feature	WAP9122	WAP9123	WAP9132	WAP9133
No. of radios	2	2	2	2
Radios that support 802.11 a/b/g/n/monitor	2	2	2	2
Radios that also support 802.11ac	2*	2*	2	2
Radio type	2x2	3x3	2x2	3x3
Integrated omni-directional antennas	4	6	4	6
Integrated wireless switch ports	2	2	2	2
Integrated RF spectrum analyzer, threat sensors	Yes	Yes	Yes	Yes
Gigabit Uplink Ports	2	2	2	2
Wireless bandwidth	300Mbps/ 1.7Gbps+	450Mbps/ 2.6Gbps+	1.7Gbps	2.6Gbps
Users supported	240	240	240	240

* = optional license required.

+ = if optional 802.11ac license is installed.

WAP9144 2-Radio Access Points

These APs have two Gigabit Ethernet ports and two multi-state radios (2.4GHz or 5GHz) supporting 802.11ac Wave 2 and 802.11a/b/g/n. Each of the two 4x4 802.11ac radios supports 1.733 Gbps, connecting up to 390 users at one time with up to 3.47 Gbps total Wi-Fi bandwidth.

The Avaya WAP9144 AP is designed for offices, classrooms, meeting spaces and any location where the speed of data delivery is critical. It integrates multi-state radios with high gain directional antennas, an onboard multi-gigabit switch, controller, firewall, threat sensor and spectrum analyzer.

Feature	WAP9144
No. radios: 802.11 ac/a/b/g/n/monitor	2
Radio type	4x4
Integrated antennas	8
Integrated wireless switch ports	2
Integrated RF spectrum analyzer, threat sensors	Yes
Gigabit Uplink Ports	2
Wireless bandwidth	3.47 Gbps
Users supported	390

A unique feature optimizes wireless performance by automatically segmenting faster 802.11ac clients from slower Wi-Fi clients. Since Wi-Fi is a shared medium, this separation ensures slower 802.11a/b/g/n clients do not slow down 802.11ac clients and prevent them from achieving high performance.

WAP9172/9173 Access Points

These WAPs have two Gigabit Ethernet ports and four multi-state radios (2.4GHz or 5GHz) supporting 802.11ac and 802.11a/b/g/n. Each of the WAP9173's four 3x3 802.11ac radios supports 1.3Gbps, connecting up to 512 users at one time with up to 5.2 Gbps total Wi-Fi bandwidth.

These models support high performance for medium to high density needs. They integrate multi-state radios with high gain directional antennas, an onboard multi-gigabit switch, controller, firewall, threat sensor and spectrum analyzer on a modular chassis designed for extensibility.

Feature	WAP9172	WAP9173
No. radios: 802.11 ac/a/b/g/n/monitor	4	4
Radio type	2x2	3x3
Integrated antennas	8	12
Integrated wireless switch ports	4	4
Integrated RF spectrum analyzer, threat sensors	Yes	Yes
Gigabit Uplink Ports	2	2
Wireless bandwidth	3.4 Gbps	5.2 Gbps
Users supported	512	512

A unique feature optimizes wireless performance by automatically segmenting faster 802.11ac clients from slower Wi-Fi clients. Since Wi-Fi is a shared medium, this separation ensures slower 802.11a/b/g/n clients do not slow down 802.11ac clients and prevent them from achieving high performance.

9170 Series WAPs must run AvayaOS Release 7.2 or above.

See Also

Key Features and Benefits

Wireless Access Point Product Overview

Enterprise Class Security

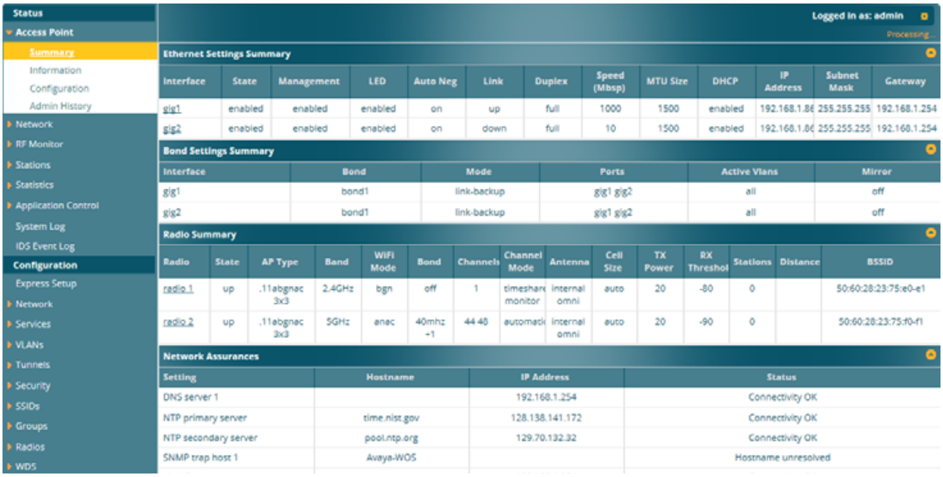
The latest and most effective wireless encryption security standards, including Wireless Protected Access (WPA) and WPA2 with 802.11i Advanced Encryption Standard (AES) are available on the WAP. In addition, the use of an embedded RADIUS server (or 802.1x with an external RADIUS server) ensures user authentication—multiple WAPs can authenticate to the WOS, ensuring only authorized WAPs become part of the wireless network. With the Avaya Advanced Feature Sets, intrusion detection and prevention, site monitoring, and RF spectrum analysis are performed in the background by the WAP automatically.

Power over Ethernet (PoE)

WAPs are powered over a cable that carries data as well—Power over Ethernet (PoE). See the Installation Guide for the AP for compatible injectors or powered switches.

Enterprise Class Management

The WAP can be used with its default settings, or it can be initially configured using WOS. Settings may also be customized using the WAP's embedded WMI. The WMI enables easy configuration and control from a graphical console, plus a full complement of troubleshooting tools and statistics.



Ethernet Settings Summary

Interface	State	Management	LED	Auto Neg	Link	Duplex	Speed (Mbsp)	MTU Size	DHCP	IP Address	Subnet Mask	Gateway
gig1	enabled	enabled	enabled	on	up	full	1000	1500	enabled	192.168.1.8(	255.255.255	192.168.1.254
gig2	enabled	enabled	enabled	on	down	full	10	1500	enabled	192.168.1.8(	255.255.255	192.168.1.254

Bond Settings Summary

Interface	Bond	Mode	Ports	Active Vlans	Mirror
gig1	bond1	link-backup	gig1 gig2	all	off
gig2	bond1	link-backup	gig1 gig2	all	off

Radio Summary

Radio	State	AP Type	Band	WiFi Mode	Bond	Channels	Channel Mode	Antenna	Cell Size	TX Power	RX Threshol	Stations	Distance	BSSID
radio 1	up	.11abgnac 3x3	2.4GHz	bgn	off	1	timeshare monitor	internal omni	auto	20	-80	0		50:60:28:23:75:e0-e1
radio 2	up	.11abgnac 3x3	5GHz	anac	40mhz +1	44 48	automati	internal omni	auto	20	-90	0		50:60:28:23:75:f0-f1

Network Assurances

Setting	Hostname	IP Address	Status
DNS server 1		192.168.1.254	Connectivity OK
NTP primary server	time.nist.gov	128.138.141.172	Connectivity OK
NTP secondary server	pool.ntp.org	129.70.132.32	Connectivity OK
SNMP trap host 1	Avaya-WOS		Hostname unresolved

Figure 3. WMI: WAP Status

In addition, a fully featured Command Line Interface (CLI) offers IT professionals a familiar management and control environment. Simple Network Management Protocol (SNMP) is also supported to allow management from an SNMP compliant management tool, such as the optional WOS.

For deployments of more than five WAPs, we recommend that you use the WOS. WOS offers a rich set of features for fine control over large deployments.

Key Features and Benefits

This section describes some of the key product features and the benefits you can expect when deploying the WAP.

Fast Roaming

Fast roaming utilizes the Avaya Roaming Protocol ensuring fast and seamless roaming capabilities between WAPs at both Layer 2 and Layer 3.

Powerful Management

The WOS offers real time monitoring and management capabilities for the wireless network.

Secure Wireless Access

Multiple layers of authentication and encryption ensure secure data transmissions. The WAP is 802.11i compliant with line-rate encryption support for 40 and 128 bit WEP, WPA and WPA2 with TKIP and AES encryption. Authentication is provided via 802.1x, including PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, EAP-GTC, EAP-AKA, EAP-AKA-Prime, and Lightweight Extensible Authentication Protocol (LEAP) passthrough. Intrusion detection and prevention provide proactive monitoring of the environment for threats.

Applications Enablement

The WAP’s Quality of Service (QoS) functionality combined with true switch capabilities enable high density video and Voice over Wireless LAN deployments. Compliant with 802.1p and 802.1Q standards.

See Also

Wireless Access Point Product Overview

Power over Ethernet (PoE)

Why Choose the Avaya Access Point?

Advanced Feature Sets

The WAP offers a family of powerful functionality packages, including the RF Performance Manager (RPM), RF Security Manager (RSM), RF Analysis Manager (RAM), and Application Control. These four packages are separately licensed for operation on your WAP. RPM, RSM, and RAM are automatically included as part of all WAPs. Application Control is an optional feature.

Avaya Advanced RF Performance Manager (RPM)

The Avaya RPM optimizes the bandwidth usage and station performance of wireless networks. Leveraging the multiple integrated access point (multi-radio) design of the WAP, RPM manages the allocation of wireless bandwidth to wireless stations across multiple RF channels. The result maximizes overall network performance with superior flexibility and capacity.

Today's wireless infrastructure is faced with ever increasing numbers and variations of wireless enabled clients, whether in the form of notebooks, tablets, smart phones, IP phones, printers, projectors, cameras, RFID tags, etc. The advent of higher speed wireless and its increased use of the 5GHz spectrum adds to the number of variables today's wireless networks must accommodate. Backwards compatibility with older clients is crucial, however their operation in a wireless network can significantly hinder the performance of faster clients. As an example, 802.11b wireless stations communicate more than 10 times slower than 802.11n stations.

With each of the WAP’s multiple radios operating on a different channel, RPM selects the ideal radio for each station. High-speed stations are grouped together on radios with other high speed stations, while lower speed stations are combined with other lower speed stations. This ensures optimal performance for high-speed 802.11ac stations without compromise.

The complete feature set of the RPM package includes:

- Wireless Distribution System (WDS) for point-to-point communication
- Wireless Mode per radio
- Sharp Cell technology
- Wireless Data Rate Optimization
- Wireless Traffic Shaping
- Wireless Voice Call Admission Control
- Fast Layer 2 and 3 Roaming
- Standby Mode

Avaya Advanced RF Security Manager (RSM)

The Avaya RSM improves security and minimizes the risk in deploying 802.11 wireless networks. Leveraging an integrated 24/7 threat sensor and hardware-based encryption/decryption in each WAP, RSM secures the wireless network from multiple types of threats. The result delivers uncompromised overall network security with superior flexibility and performance.

Wireless networks face a number of potential security threats in the form of rogue access points, ad-hoc clients, unauthorized clients, wireless-based attacks, eavesdropping, etc. As “bring your own device” (BYOD) becomes ubiquitous in enterprise networks, defending against these threats becomes more critical. With the WAP’s threat sensor radio scanning all channels in the 2.4GHz and 5GHz spectrums, RSM searches for security threats and automatically mitigates them.

High performance encryption/decryption in the enterprise wireless network is a must. The wireless network needs to support each client using the highest level of encryption (WPA2 Enterprise/128 bit AES) and without degrading the overall performance of the network. Avaya incorporates hardware-based encryption/decryption into each WAP, delivering line-rate encryption at the edge of the network instead of at a choke point within a centralized controller.

The complete feature set of the RSM package includes:

- Wireless IDS/IPS (Intrusion Detection/Prevention System)
- Wireless stateful firewall

- User group policies
- Authenticated guest access gateway
- NAC integration

Avaya Advanced RF Analysis Manager (RAM)

The RF Advanced Analysis Manager (RAM) tests and troubleshoots wireless networks. The deployment of 802.11ac presents a set of unique challenges based on technology differences with legacy 802.11a/b/g/n networks, both on the wireless infrastructure and client side. Avaya RAM equips each WAP with a powerful set of tools and features to optimally tune and verify an 802.11ac installation, as well as give IT administrators the ability to troubleshoot issues that may occur within the wireless environment.

802.11ac deployment will continue to evolve over the next several years with additional performance and optional functions, along with an ongoing stream of IEEE 802.11 amendments. This changing wireless landscape mandates that appropriate tools are available to the user to analyze, optimize, and troubleshoot their changing environments.

The distributed architecture of the WAP enables the execution of powerful wireless and networking analysis at the edge of the network where packets traverse the wireless-to-wired boundary. The WAP includes an embedded wireless controller with the necessary computing and memory resources to provide these functions securely at the network's edge.

The key elements of the RAM package include:

- RF Analysis – An embedded Spectrum Analyzer leverages the dedicated threat sensor radio in each WAP to provide a continual view of utilization, interference, and errors across all available wireless channels.
- Packet Analysis – Integrated packet capture provides filterable views of all traffic traversing on the wired and wireless interfaces of the WAP.
- Performance Analysis – Embedded traffic generation enables the throughput of the WAP’s wireless or wired interfaces to be analyzed.
- Failure Recovery – Radio Assurance provides an automatic self-test and self healing mechanism that ensures continuous system operation.

- Netflow Support
- Network Tools: ping, RADIUS ping, traceroute

Avaya Application Control

The Application Control feature is available on WAPs to provide real-time visibility of application usage by users across the wireless network. Network usage has changed enormously in the last few years, with the increase in smart phone and tablet usage stressing networks.

The WAP uses Deep Packet Inspection (DPI) to determine what applications are being used and by whom, and how much bandwidth they are consuming. These applications are rated by their degree of risk and productiveness. The results are presented to you both graphically and in tables. Filters can be used to implement per-application policies that keep network usage focused on productive uses, eliminating risky and non-business-oriented applications such as BitTorrent. You can increase the priority of mission-critical applications like VoIP and Scopia. See “Application Control Windows” on page 130 for more information.

About this User’s Guide

This User’s Guide provides detailed information and procedures that will enable wireless network administrators to install, configure and manage the Wireless WAP so that end users can take full advantage of the product’s features and functionality without technical assistance.

Organization

Topics and procedures are organized by function under the following chapter headings:

- **Introduction**

  Provides a brief introduction to wireless technology, an overview of the product, including its key features and benefits, and presents the product specifications.

- **Installing the WAP**

  Defines prerequisites for deploying and installing the WAP and provides instructions to help you plan and complete a successful installation.

- **The Web Management Interface**

  Offers an overview of the product's embedded Web Management Interface, including its content and structure. It emphasizes what you need to do to ensure that any configuration changes you make are applied, and provides a list of restricted characters. It also includes instructions for logging in to the WAP with your Web browser.

- **Viewing Status on the WAP**

  Describes the status and statistics displays available on the WAP using its embedded Web Management Interface.

- **Configuring the WAP**

  Contains procedures for configuring the WAP using its embedded Web Management Interface.

- **Using Tools on the WAP**

  Contains procedures for using utility tools provided in the Web Management Interface. It includes procedures for upgrading the system firmware, uploading and downloading configurations and other files, using diagnostic tools, and resetting the WAP to its factory defaults.

- **The Command Line Interface**

  Includes the commands and the command structure used by the WAP's Command Line Interface (CLI), and provides a procedure for establishing a Telnet connection to the WAP. This chapter also includes some sample key configuration tasks using the CLI.

- **Appendix A: Quick Reference Guide**

  Contains the product's factory default settings.

- **Appendix B: FAQ and Special Topics**

  Offers guidance to resolve technical issues, including general hints and tips to enhance your product experience, and a procedure for isolating problems within a WAP-enabled wireless network. Also includes Frequently Asked Questions (FAQs) and Avaya contact information.

- **Appendix C: Auditing PCI DSS**

  Discusses using WAP features to assist in meeting security standards for PCI DSS audits.

- **Glossary of Terms**

  Provides an explanation of terms directly related to Avaya product technology, organized alphabetically.

- **Index**

  The index is a valuable information search tool. Use the index to locate specific topics discussed in this User’s Guide. Simply click on any page number in the index to jump to the referenced topic.

Notes and Cautions

The following symbols are used throughout this User’s Guide:

✎ *This symbol is used for general notes that provide useful supplemental information.*

! *This symbol is used for cautions. Cautions provide critical information that may adversely affect the performance of the product.*

Screen Images

Some screen images of the Web Management Interface have been modified for clarity. For example, an image may have been cropped to highlight a specific area of the screen, and / or sample data may be included in some fields.

Installing the WAP

The instructions for planning and completing a successful installation include the following topics:

Installation Prerequisites

WAP deployment requires the presence of hardware and services in the host wired / wireless network, including:

- **Power Source**

  WAPs are powered via Power over Ethernet. PoE supplies power over the same Cat 5e or Cat 6 cable used for data, thus reducing cabling and installation effort. PoE power injector modules are typically placed near your Gigabit Ethernet switch. An AC outlet is required for each injector module.

  See the Installation Guide for the WAP for compatible injectors or powered switches.

- **Ethernet ports**

  You need at least one 100 / 1000 BaseT port to establish wired Gigabit Ethernet connectivity.

! *The WAP's Ethernet ports should be connected to an Ethernet switch, not an Ethernet hub—if a hub is used, we recommend that you do not bond-pair Ethernet ports.*

- **Secure Shell (SSH) utility**

  To establish secure remote command line access to the WAP, you need a Secure Shell (SSH) utility, such as PuTTY. The utility **must** be configured to use SSH-2, since the WAP will only allow SSH-2 connections.

- **Secure Web browser**

  Avaya supports the latest version of the following Browsers: Internet Explorer, Mozilla Firefox, Chrome, or Safari. A secure Web browser is required for Web-based management of the WAP. The browser must be on the same subnet as the WAP, or you must set a static route for management as described in the warning above.

Optional Network Components

The following network components are optional.

- **Wireless LAN Orchestration System (WOS)**

  The optional WOS offers powerful management features for small or large WAP deployments.

Client Requirements

The WAP should only be used with Wi-Fi certified client devices.

See Also

Coverage and Capacity Planning

Planning Your Installation

Planning Your Installation

This section provides guidelines and examples to help you plan your WAP deployment to achieve the best overall coverage and performance. We recommend you conduct a site survey to determine the best location and settings for each WAP you install.

General Deployment Considerations

For optimal placement of WAPs, we recommend that a site survey be performed by a qualified Avaya partner.

The 9170 Series WAP's unique multi-radio architecture generates 360 degrees of sectored high-gain 802.11a/b/g/n/ac coverage that provides extended range. (Note that 9120/9130 Series radios are omni-directional rather than sectored.) The number, thickness and location of walls, ceilings or other objects that the wireless signals must pass through may affect the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise at your location. To maximize wireless range, follow these basic guidelines:

1. Keep the number of walls and ceilings between the WAP and your receiving devices to a minimum—each wall or ceiling can reduce the wireless range from between 3 and 90 feet (1 to 30 meters). Position your devices so that the number of walls or ceilings is minimized.

2. Be aware of the direct line between each device. For example, a wall that is 1.5 feet thick (half a meter) at 90° is actually almost 3 feet thick (or 1 meter) when viewed at a 45° angle. At an acute 2° degree angle the same wall is over 42 feet (or 14 meters) thick. For best reception, try to ensure that your wireless devices are positioned so that signals will travel straight through a wall or ceiling.

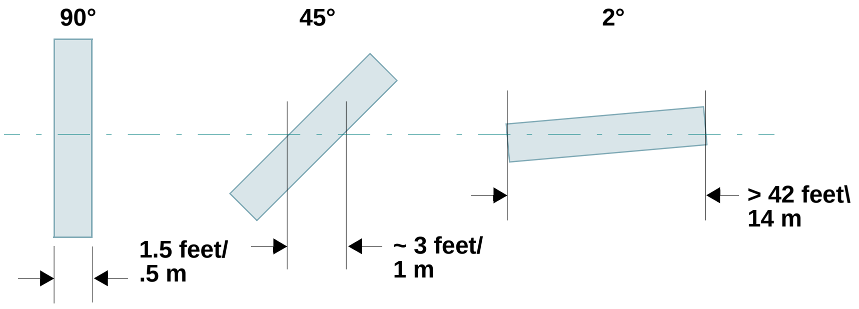


Figure 4. Wall Thickness Considerations

3. Try to position wireless client devices so that the signal passes through drywall (between studs) or open doorways and not other materials that can adversely affect the wireless signal.

See Also

Coverage and Capacity Planning

Common Deployment Options

Installation Prerequisites

Coverage and Capacity Planning

This section considers coverage and capacity for your deployment(s), including placement options, RF patterns and cell sizes, area calculations, roaming considerations, and channel allocations.

Placement

Use the following guidelines when considering placement options:

1. The best placement option for the WAP is ceiling-mounted within an open plan environment (cubicles rather than fixed walls).
2. Keep the WAP away from electrical devices or appliances that generate RF noise. Because the WAP is generally mounted on ceilings, be aware of its position relative to lighting (especially fluorescent lighting)—we recommend maintaining a distance of at least 3 to 6 feet (1 to 2 meters).

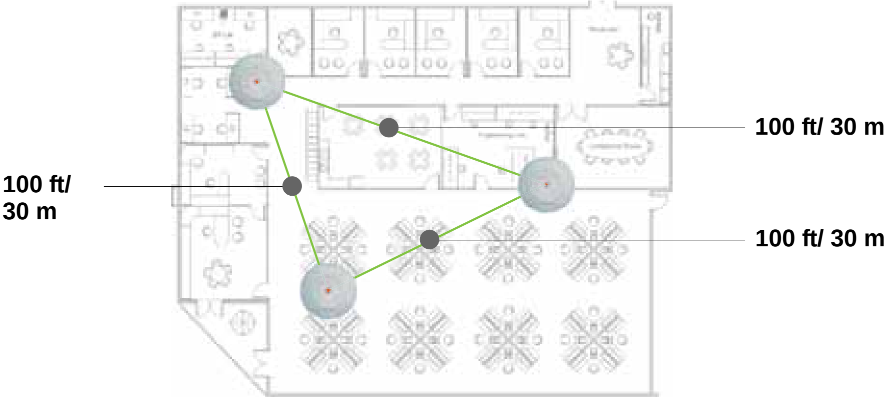


Figure 5. Unit Placement

3. If using multiple WAPs in the same area, maintain a distance of at least 100ft / 30m between WAPs if there is direct line-of-sight between units, or at least 50ft / 15m if a wall or other barrier exists between units.

RF Patterns

The WAP allows you to control—automatically or manually—the pattern of wireless coverage that best suits your deployment needs. You can choose to operate with full coverage, half coverage, or custom coverage (by enabling or disabling individual sectors).

Capacity and Cell Sizes

Cell sizes should be estimated based on the number of users, the applications being used (for example, data / video / voice), and the number of WAPs available at the location. The capacity of a cell is defined as the minimum data rate desired for each sector multiplied by the total number of sectors being used.

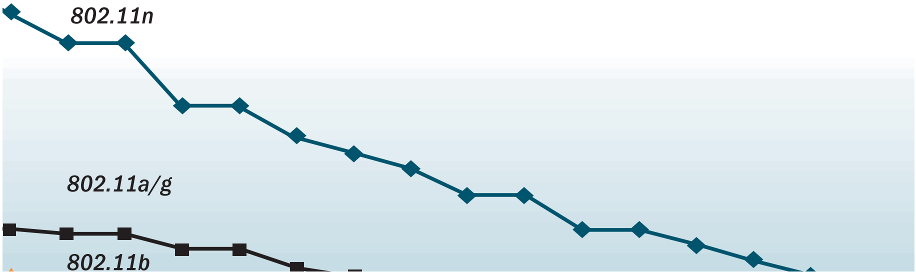


Figure 6. Connection Rate vs. Distance

Figure 6 shows relative connection rates for 802.11n vs. 802.11a / g and 802.11b, and the effect of distance on the connection rates. 802.11ac rates behave like 802.11n over distance—see Figure 15 for 802.11ac data rates). Wireless environments can vary greatly so the actual rates may be different depending on the specific network deployment.

Fine Tuning Cell Sizes

Adjusting the transmit power allows you to fine tune cell sizes. There are four standard sizes—Small, Medium, Large, or Max (the default is **Max**). There is also an Auto setting that automatically determines the best cell size, and a Manual setting that allows you to choose your power settings directly.

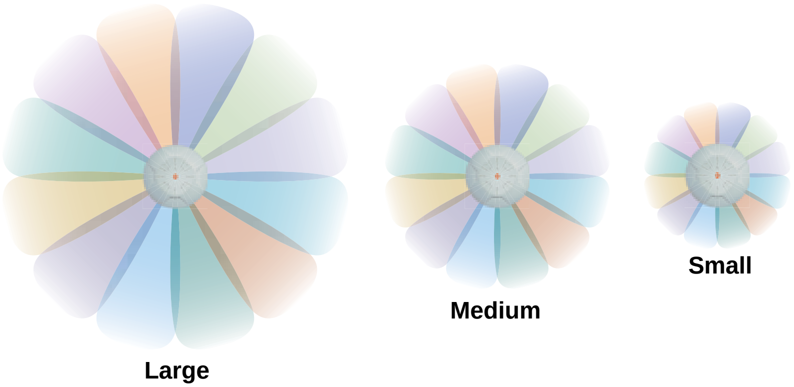


Figure 7. Transmit Power

Auto Cell Size is an automatic, self-tuning mechanism that balances cell size between WAPs to guarantee coverage while limiting the RF energy that could extend beyond the organizational boundary. Auto Cell uses communication between WAPs to dynamically set radio power so that complete coverage is provided to all areas, yet at the minimum power level required. This helps to minimize potential interference with neighboring networks. Additionally, WAPs running Auto Cell automatically detect and compensate for coverage gaps caused by system interruptions. To enable the Auto Cell Size feature, go to “RF Power and Sensitivity” on page 332.

There are two ways of performing Auto Cell Size—by band (Multichannel Auto Cell) or by channel (this is the default version). Auto Cell by channel adjusts the size of two or more neighboring AP radios that are on the same channel (Figure 8 A and B). Multichannel Auto Cell adjusts cell sizes of neighboring radios on the same band (2.4GHz or 5GHz) even if they are on different channels. A potential application of Autocell by Band is depicted in Figure 8 B and C. In this example, cell sizes are to be adjusted so that they are contained in each room. The goal is for stations to associate to the AP located in the same room with them.

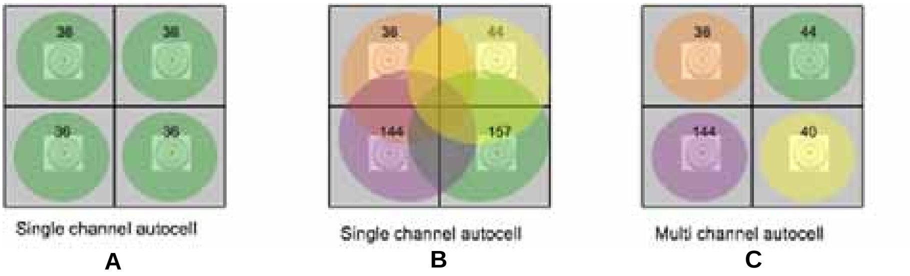


Figure 8. Auto Cell Size Options

Multichannel Auto Cell is configured by turning off **Auto Cell by Channel** in “Procedure for Configuring Global 802.11an Radio Settings” on page 306 for the 5GHz band, and in “Procedure for Configuring Global 802.11b/g Radio Settings” on page 312 for the 2.4GHz band. Note that Multichannel Auto Cell is run separately for each band. Thus, to optimize cell size of both 2.4G and 5G, the Auto Cell function should be run once for each of these pages. APs **must** be at least 15 feet apart for Auto Cell to work properly.

If you are installing many units in proximity to each other, we recommend that you use Auto Cell Size; otherwise, reduce the transmit power using manual settings to avoid excessive interference with other WAPs or installed APs. See also, “Coverage and Capacity Planning” on page 25.

Roaming Considerations

Cells should overlap approximately 10 - 15% to accommodate client roaming.

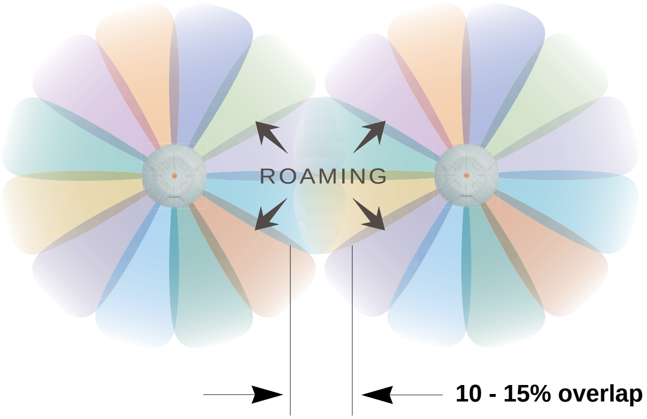


Figure 9. Overlapping Cells

Allocating Channels

Because the WAP is a multi-channel device, allocating the best channels to radios is important if peak performance is to be maintained.

*Note that Auto Channel normally assigns individual channels. However, if you select **Auto bond 5GHz channels** on the **Global Settings .11n** page, and have 40MHz channels set up prior to running Auto Channel, those bonds will be preserved. 80MHz bonds will not be preserved.*

Automatic Channel Selection

In the automatic mode, channels are allocated dynamically, driven by changes in the environment. Auto Channel assignment is performed by scanning the surrounding area for RF activity on all channels, then automatically selecting and setting channels on the WAP to the best channels available. This function is typically executed when initially installing WAPs in a new location and may optionally be configured to execute periodically to account for changes in the RF environment over time. Auto Channel selection has significant advantages, including:

- Allows the WAP to come up for the first time and not interfere with existing equipment that may be already running, thereby limiting co-channel interference.
- More accurately tunes the RF characteristics of a wireless installation than manual configuration since the radios themselves are scanning the environment from their physical location.
- May be configured to run periodically.

To set up the automatic channel selection feature, go to “Advanced RF Settings” on page 329.

Other Factors Affecting Throughput

Throughput of the WAP can be affected by many factors such as distance, number of stations, obstacles, construction materials used at the site, etc. In addition, features applied to traffic may have an effect. Performance may decrease as you add increasing numbers of SSIDs, VLANs, and features such as Application Control, encryption, etc. WAO 9122 models are more prone to performance degradation since they have less memory than other models.

See Also

Installation Prerequisites

About IEEE 802.11ac

802.11ac is a continuation of the IEEE 802.11 standard. It multiplies the maximum data rate—eventually, up to ten times the 802.11n maximum. Along with increased data rates, it offers simultaneous transmission to multiple clients.

802.11ac is being rolled out in two phases. Wave 1 products currently available support 80MHz channels and up to 3 data streams for a maximum data rate of 1.3 Gbps. Wave 2 and future products will add 160MHz channels and up to 8 streams, for a maximum data rate of 6.93Gbps.

Avaya currently supports up to three streams (in units with 3x3 radios) and 80 MHz bonded channels. Avaya models that offer 802.11ac support this technology on all radios, not just on one. Radios are individually configurable to different modes or groups of modes (such as 802.11a, 11b, 11g, and 11n). Avaya optimizes 802.11ac performance with an innovation that intelligently separates fast and slow devices on separate radios to maximize system performance.

The major advantages of 802.11ac are:

- Faster speeds than 802.11n over the same coverage area, operating at up to 1.3 Gbps in Wave 1 and up to 1.733 Gbps in Wave 2. While the maximum distance that a Wi-Fi signal can reach is unchanged with 802.11ac, multiple antennas increase the data rate at every distance.
- Operates only in the less congested 5 GHz spectrum, which offers “cleaner” air and supports much greater capacity than the 2.4 GHz spectrum still used by 802.11n.
- Supports simultaneous communications to multiple clients on a single channel with multi-user MIMO in Wave 2.
- Extends the techniques pioneered in 802.11n: more antennas, more spatial streams and wider channels to improve throughput.

The techniques that 802.11ac uses to realize these performance improvements and the expected results are discussed in:

- **“Up to Eight Simultaneous Data Streams—Spatial Multiplexing” on page 33**
- **“MIMO (Multiple-In Multiple-Out)” on page 33**

- **“MU-MIMO (Multi-User Multiple-In Multiple-Out)” on page 34**
- **“Higher Precision in the Physical Layer” on page 36**
- **“80 MHz and 160 MHz Channel Widths (Bonding)” on page 37**
- **“802.11ac Data Rates” on page 38**
- **“Client Separation” on page 39**

It is important to consider 80 MHz and 160 MHz Channel Widths (Bonding) when planning your deployment, since it contributes greatly to 802.11ac’s speed improvements and because it is configured separately for each radio. Your selection of channel width in Radio Settings—40 MHz, 80 MHz, or 20 MHz (if bonding is turned off)—has a major effect on your channel planning. A global setting is provided to enable or disable 802.11ac mode. See “Global Settings .11ac” on page 321 to configure operation.

There are other factors to keep in mind when planning a roll-out of 802.11ac. Please see “802.11ac Deployment Considerations” on page 39.

Up to Eight Simultaneous Data Streams—Spatial Multiplexing

Spatial Multiplexing transmits completely separate data streams on different antennas (in the same channel) that are recombined to produce new 802.11ac data rates. Previously used for 802.11n, the maximum number of streams for 802.11ac has been increased to eight. Higher data rates are achieved by splitting the original data stream into separate data streams. Each separate stream is transmitted on a different antenna (using its own RF chain). MIMO signal processing at the receiver can detect and recover each stream. Streams are then recombined, yielding higher data rates.

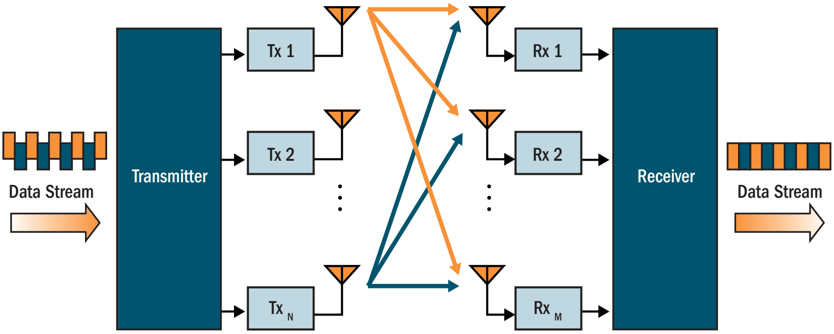


Figure 10. Spatial Multiplexing

The date rate increases directly with the number of transmit antennas used. Note that mobile devices in the near future will support up to three or four streams at most, with many supporting less.

MIMO (Multiple-In Multiple-Out)

MIMO (Multiple-In Multiple-Out) signal processing is one of the core technologies of 802.11n and 802.11ac. It mitigates interference and maintains broadband performance even with weak signals.

Prior to 802.11n, a data stream was transmitted via one antenna. At the receiving end, the antenna with the best signal was selected to receive data. MIMO signal processing uses multiple antennas to send and receive data. It takes advantage of multipath reflections to improve signal coherence and greatly increase receiver sensitivity (Figure 11). Multipath signals were considered to be interference by

802.11a/b/g radios, and degraded performance. In 802.11n and 802.11ac, these signals are used to enhance performance.

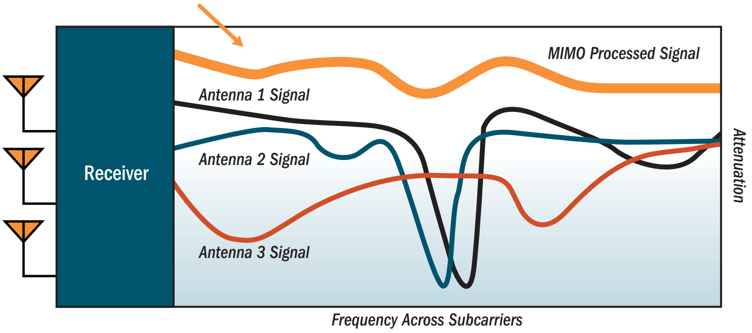


Figure 11. MIMO Signal Processing

802.11ac increases the number of antennas and spatial streams from a maximum of four in 802.11n to a maximum of eight, contributing to much higher maximum data rates (up to 6.93Gbit/s). The spatial streams can be concurrently allocated to more than one receiving device when the AP operates in multi-user MIMO mode (MU-MIMO, see the next section).

MU-MIMO (Multi-User Multiple-In Multiple-Out)

MU-MIMO (multi-user multiple-in/multiple-out) signal processing uses multiple antennas on the transmitter and receiver operating on the same channel. With spatial multiplexing in 802.11ac, up to 8 data streams may be concurrently transmitted. MU-MIMO's innovation allows the streams to be split between multiple devices at once.

With 802.11n, whenever the radio transmitted data, all of the traffic at any instant of time was directed to a single client. As a consequence, if a set of devices included a mix of fast and slow client clients, the fast traffic was often substantially delayed by the transmission to slower clients. 802.11ac MU-MIMO works by directing some of the spatial streams to one client and other spatial streams to other clients, up to four at a time

For example, in the figure below, the transmitter has four antennas. Three are transmitting to an 802.11ac laptop that has three antennas, while the remaining one is directed to a mobile phone. When a transmission is complete, the antennas are reallocated.

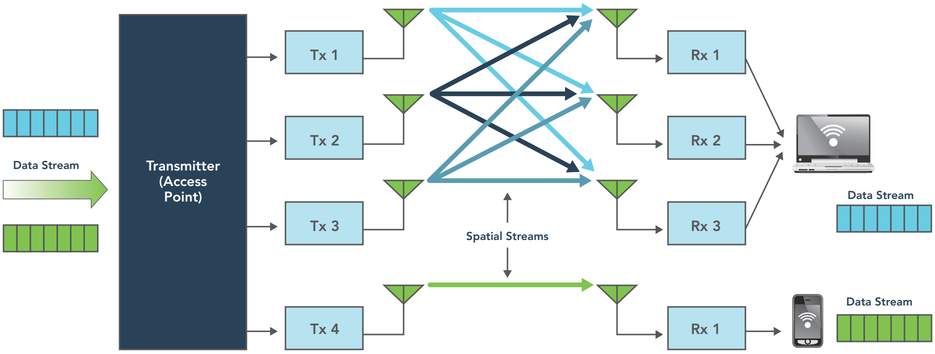


Figure 12. MU-MIMO with Four Antennas

The table below illustrates how data streams might be allocated to multiple users on an 802.11ac transmitter with multiple antennas.

# of AP Antennas	Possible Combinations of Receiver Antennas
2	1 station w/ 2 antennas -or- 2 stations w/ 1 antenna
3	1 station w/ 3 antennas -or- 1 station w/ 2 antennas + 1 station w/ 1 antenna -or- 3 stations w/ 1 antenna
4	1 station w/4 antennas -or- 2 stations w/2 antennas -or- 1 station w/2 antennas + 2 stations w/1 antenna -or- 4 stations w/ 1 antenna
8	1 station w/ 8 antennas -or- 2 stations w/ 4 antennas -or- 1 station w/ 4 antennas + 2 stations w/ 2 antennas -or- 2 stations w/ 2 antennas + 4 stations w/1 antenna -or- … many other combinations …

Higher Precision in the Physical Layer

Wi-Fi utilizes several digital modulation techniques and automatically switches between them to optimize for throughput or range. The basic unit of data transmitted is called a symbol. The number of points in the modulation constellation determines the number of bits of data conveyed with each symbol.

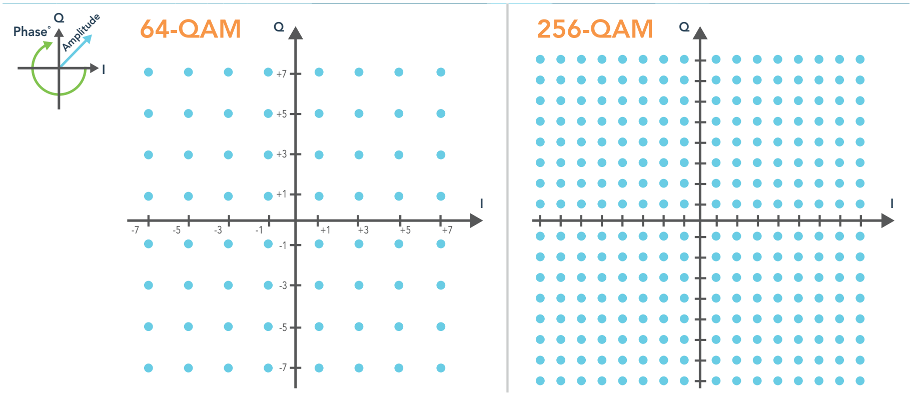


Figure 13. Physical Layer Data Encoding

802.11n uses 16 Quadrature Amplitude Modulation (QAM), which conveys log2(16) = 4 bits per symbol and 64 QAM, which conveys 6 bits per symbol. 802.11ac adds 256 QAM which conveys 8 bits per symbol for a 33% increase in throughput vs. the highest 802.11n data rate.

You may select the highest Modulation and Coding Scheme (MCS) level allowed with **1**, **2**, or **3 Spatial Streams** (see the **Max MCS** setting in "Procedure for Configuring Global 802.11ac Radio Settings" on page 322). You may limit the highest level of modulation to 64-QAM, or allow 256-QAM. It also determines the coding scheme used for error correction. Higher MCS levels allocate fewer bits to error correction, and thus more bits are used for data. The default value is **MCS9**, the highest level.

The higher the MCS value, the higher the data rate, as shown in the table below. WAPs support MCS7 -MCS9. Higher MCS levels require higher signal-to-noise ratios (i.e., a less noisy environment) and shorter transmission distances.

MCS index value	Modulation	Code rate (R)
0	BPSK	1/2
1	QPSK	1/2
2	QPSK	3/4
3	16-QAM	1/2
4	16-QAM	3/4
5	64-QAM	2/3
6	64-QAM	3/4
7	64-QAM	5/6
8	256-QAM	3/4
9	256-QAM	5/6

80 MHz and 160 MHz Channel Widths (Bonding)

Channel bonding increases data rates by combining two, four, or eight adjacent 20 MHz channels into one channel. This increases the data rate proportional to the width of the bond.

Bonding is specified on the Radio Settings page for each radio in terms of the primary channel and the width of the bond. Be aware that Channel Bonding impacts channel planning, since you are using multiple channels per radio.

802.11ac allows creation of 20, 40, 80, or 160 MHz wide channels. The 160MHz channel can also be a combination of two non-contiguous 80MHz channels (80+80). Although channel bonding increases bandwidth, wider channels are more susceptible to signal interference which may lead to reduced range and poorer signal quality. Figure 14 is an example showing how Channels 36-64 may be used: as eight 20 MHz channels; four 40 MHz channels; two 80 MHz channels; or one 160 MHz channel. Avaya currently supports channels up to 80 MHz wide.

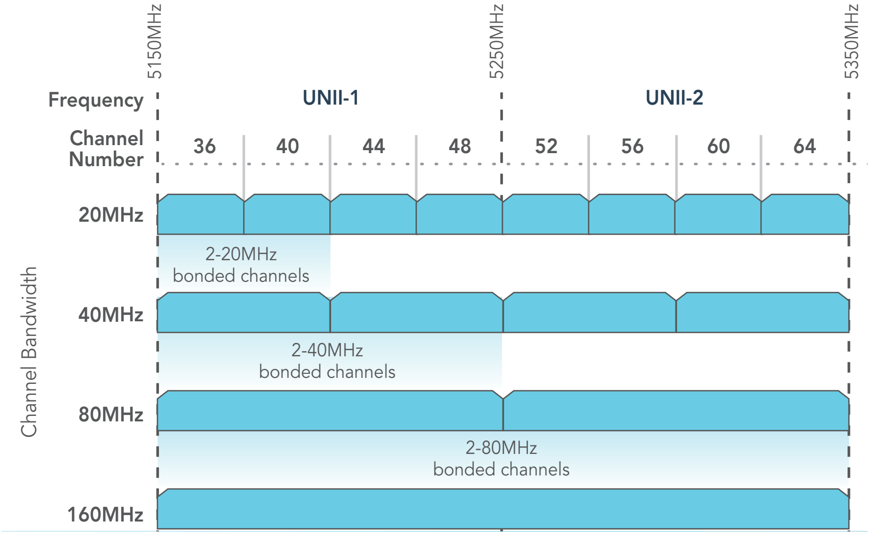
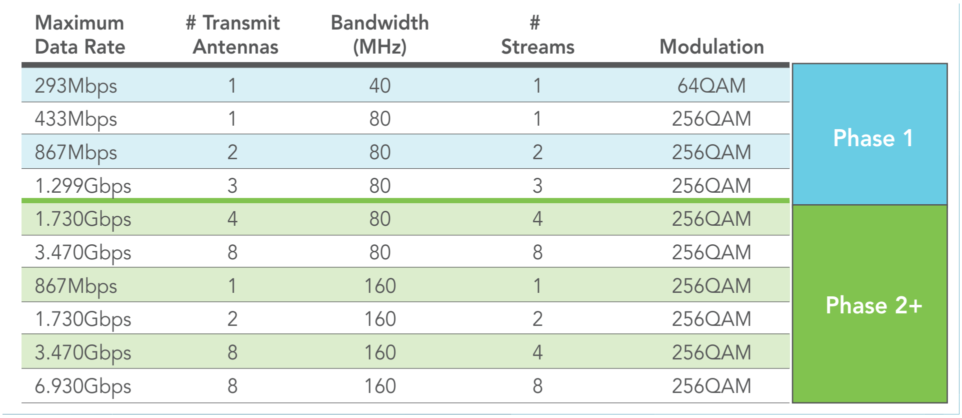


Figure 14. Channel Bonding (Channels 36-64 shown)

802.11ac Data Rates



Maximum Data Rate	# Transmit Antennas	Bandwidth (MHz)	# Streams	Modulation	
293Mbps	1	40	1	64QAM	Phase 1
433Mbps	1	80	1	256QAM	
867Mbps	2	80	2	256QAM	
1.299Gbps	3	80	3	256QAM	
1.730Gbps	4	80	4	256QAM	Phase 2+
3.470Gbps	8	80	8	256QAM	
867Mbps	1	160	1	256QAM	
1.730Gbps	2	160	2	256QAM	
3.470Gbps	8	160	4	256QAM	
6.930Gbps	8	160	8	256QAM	

Figure 15. Maximum 802.11ac Data Rates

IEEE 802.11ac data rates are dependent on the number of spatial streams obtained through the use of MU-MIMO, 80 vs. 160MHz channel widths, the number of transmit antennas, and the type of modulation. Figure 15 shows the maximum data rate achievable at each level, with many additional lower rates occurring at each level dependent on signal level, signal to noise ratio in the environment, etc.

Phase 1 802.11ac, first available in consumer products in 2012 and enterprise products in 2013, supports up to 80MHz channels and up to 3 spatial streams for a maximum data rate of 1.3Gbps.

Phase 2 and beyond products, expected starting in 2014, will add 160MHz channels and up to 8 spatial streams for a maximum data rate of 6.9Gbps.

Client Separation

Avaya 802.11ac radios use an innovative technique to optimize wireless performance by automatically separating faster 802.11ac clients from slower Wi-Fi clients. Since Wi-Fi is a shared medium, this separation ensures that slower 802.11a/b/g/n clients do not starve the performance of 802.11ac clients. For example, the data rate of an 802.11n client is less than 25% of the rate of an 802.11ac client, and thus will take four times as much air time for a given amount of data. This takes available bandwidth away from faster clients, reducing their performance significantly. The technique intelligently separates clients by type onto different radios, grouping fast clients separately from slow clients, thereby maximizing performance for all. The technique is supported on all Avaya 802.11ac products, and may be enabled or disabled as part of the Load Balancing feature. See Step 27 on page 302.

802.11ac Deployment Considerations

The theoretical data rates shown are just that, theoretical. For 802.11ac deployments, numerous factors affect real-world performance. These are some important considerations in the deployment of networks that include 802.11ac:

- **Wireless networks are not wired networks.** Wired network users who share a Gigabit network can expect to see bursts of up to 900Mbps, depending on their hardware. Maximum Wi-Fi data rates are reduced by signaling overhead and media contention. Most 802.11ac users will see data rates less than 100Mbps as the effective bandwidth is shared among all devices connecting to a given radio.

- **Migration to 802.11ac will take time.** Older Wi-Fi technologies will continue to be with us for years. In order for 802.11ac to provide maximum data rates, it is important to keep interference from earlier Wi-Fi standards at a minimum. For example, 802.11n devices operating in the 5GHz band can slow down 802.11ac devices to 300Mbps or 450Mbps depending on the 2x2 or 3x3 MIMO technology used.
- **Infrastructures must be upgraded as well.** The bandwidth required out of 802.11ac APs will certainly exceed 1Gbps and may reach 10Gbps. The links from the APs to the core network must keep pace with this need. Centralized firewalls, LAN controllers, and authentication servers may also reach their limits. Migration to a decentralized architecture, with intelligence at the edge of the network may be a more scalable solution, avoiding single points of failure.
- **More power.** Multi-antenna APs handling 802.11ac speeds will likely require more power. Power planning for your access switches should be carefully considered.
- **A new site survey may be needed.** Wireless networks established as recently as a few years ago were probably designed for coverage and not capacity. APs were placed so that there were no dead zones, without considering future capacity needs. With the increasing use of mobile devices, new site surveys that ensure enough bandwidth for anticipated usage should precede deployment of 802.11ac APs.
- **Manage application usage.** With 802.11ac, a range of applications are now practical on mobile devices that were previously only used over wired networks or on laptops. Uncontrolled use of Wi-Fi bandwidth can cause wireless networks to quickly degrade. Network control elements must control use of applications and prioritize critical applications.

Power Planning

All WAP models support Power over Ethernet (PoE) with an integrated splitter.

Power over Ethernet

To deliver power to the WAP, you must use Power over Ethernet (PoE) modules or powered switches that are compatible with your WAP. They provide power over Cat 5e or Cat 6 cables to the WAP without running power cables.

When using Cat 5e or Cat 6 cable, power can be provided up to a distance of 100m.

See Also

Coverage and Capacity Planning

Network Management Planning

Security Planning

Security Planning

This section offers some useful guidelines for defining your preferred encryption and authentication method. For additional information, see "Understanding Security" on page 205 and the Security section of "Frequently Asked Questions" on page 490.

Wireless Encryption

Encryption ensures that no user can decipher another user's data transmitted over the airwaves. There are three encryption options available to you, including:

- **WEP-40bit or WEP-128bit**
  Because WEP is vulnerable to cracks, we recommend that you only use this for legacy devices that cannot support a stronger encryption type.
- **Wi-Fi Protected Access (WPA)**
  This is much more secure than WEP and uses TKIP for encryption.
- **Wi-Fi Protected Access (WPA2) with AES**
  This is government-grade encryption—available on most new client adapters—and uses the AES–CCM encryption mode (Advanced Encryption Standard–Counter Mode).

Authentication

Authentication ensures users are who they say they are. Users are authenticated when they attempt to connect to the wireless network and periodically thereafter. The following authentication methods are available with the WAP:

- **RADIUS 802.1x**
  802.1x uses a remote RADIUS server to authenticate large numbers of clients, and can handle different authentication methods (EAP-TLS, EAP-TTLS, EAP-PEAP, and EAP-LEAP Passthrough). Administrators may also be authenticated via RADIUS when preferred, or to meet particular security standards.
- **Avaya Internal RADIUS server**
  Recommended for smaller numbers of users (about 100 or less). Supports EAP-PEAP only

- **Pre-Shared Key**
  Uses a pass-phrase or key that is manually distributed to all authorized users. The same passphrase is given to client devices and entered into each WAP.

- **MAC Access Control Lists (ACLs)**
  MAC access control lists provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network, and can be used in addition to any of the above authentication methods. ACLs are good for embedded devices, like printers and bar-code scanners (though MAC addresses can be spoofed). The WAP supports 1,000 global ACL entries. You may also define per-SSID access control lists, with up to 1000 entries each.

Meeting PCI DSS Standards

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by major credit card companies. It lays out a set of requirements that must be met in order to provide adequate security for sensitive data. The WAP may be configured to assist in satisfying PCI DSS standards. For details, please see “Auditing PCI DSS” on page 509. Note that the license installed on the WAP must include the Advanced RF Security Manager (RSM) to support the PCI audit command.

See Also

Network Management Planning
Power Planning

Port Requirements

A number of ports are used by various WAP features and by the Wireless LAN Orchestration System (WOS). The Port Requirements table on page 45 lists ports and the features that require them (WOS port requirements are included in the table for your convenience). If you are using a feature, please make sure that the ports that it requires are not blocked by firewalls or other policies, and that they do not conflict with any other port assignments.

As an example, WOS port requirements are illustrated in Figure 16. WOS requires ports 161, 162, and 443 to be passed between WAPs and the WOS server. Similarly, port 9443 is required for communication between the WOS server and WOS clients, and port 25 is typically used by the WOS server to access an SMTP server to send email notifications.

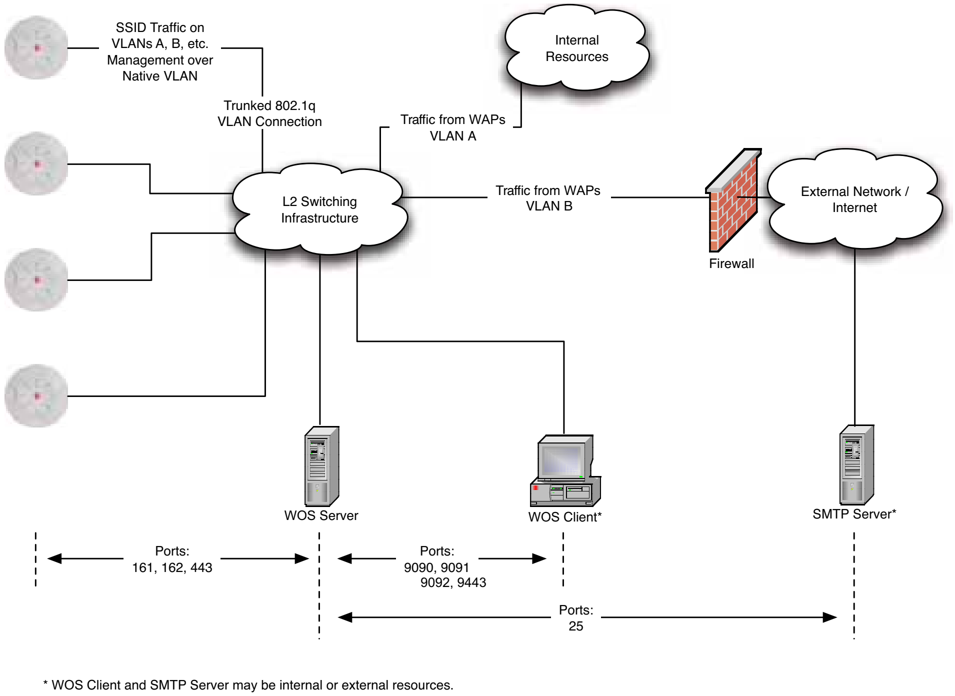


Figure 16. Port Requirements for WOS

The following table lists port requirements for the WAP and for WOS, how the ports are used, and whether they may be changed.

Port	Application	Peer	Configurable
	WAP		
icmp	Ping	WOS Server	No
20 tcp 21 tcp	FTP	Client	Yes
22 tcp	SSH	Client	Yes
23 tcp	Telnet	Client	Yes
25 tcp	SMTP	Mail Server	No
69 udp	TFTP	TFTP Server	No
123 udp	NTP	NTP Server	No
161 udp	SNMP	WOS Server	No
162 udp	SNMP Traphost Note - Up to four Traphosts may be configured.	WOS Server	Yes - but required by WOS
443 tcp	HTTPS (WMI,WPR)	Client	Yes
514 udp	Syslog	Syslog Server	No
1812, 1645 udp	RADIUS (some servers use 1645)	RADIUS Server	Yes
1813, 1646 udp	RADIUS Accounting (some servers still use 1646)	RADIUS Accounting Server	Yes
2055 udp	Netflow	Client	Yes
5000 tcp	Virtual Tunnel	VTUN Server	Yes
22610 udp	Avaya Roaming	WAPs	Yes
22612 udp	Avaya Console (Console Utility)	Admin Workstation	Yes

Port	Application	Peer	Configurable
WOS			
icmp	Ping	WAPs	No
22 tcp	SSH	WAPs	Yes
25 tcp	SMTP	Mail Server	Yes
123 udp	NTP	NTP Server	No
161 udp	SNMP	WAPs	No
162 udp	SNMP Traphost 1	WAPs	Via WOS config file
443 tcp	HTTPS	WAPs	No
514 udp	Resident Syslog server	Internal*	Via WOS config file
1099 tcp	RMI Registry	Internal*	No
2000 tcp	WOS Back-end Server	Internal*	No
3306 tcp	MySQL Database	Internal*	No
8001 tcp	Status Viewer	Internal*	No
8007 tcp	Tomcat Shutdown	Internal*	During installation
8009 tcp	Web Container	Internal*	During installation
9090 tcp	WOS Webserver	WOS client	During installation
9091 tcp	WOS Client Server	WOS client	Via WOS config file
9092 tcp	WOS Client Server	WOS client	Via WOS config file
9443 tcp	WOS WMI SSL	WOS web client	Yes
* Internal to WOS Server, no ports need to be unblocked on other network devices			

See Also

Management Control

External Radius

Services

VLAN Management

Network Management Planning

Network management can be performed using any of the following methods:

- WOS is hosted on your own server. WOS manages large WAP deployments from a centralized Web-based interface and offers the following features:
    - Globally manage large numbers of WAPs
    - Seamless view of the entire wireless network
    - Easily configure large numbers of WAPs
    - Rogue AP monitoring
    - Easily manage system-wide firmware updates
    - Monitor performance and trends
    - Aggregation of alerts and alarms
- The WAP's Command Line Interface, using an SSH (Secure Shell) utility, like PuTTY. The utility **must** be set up to use SSH-2, since the WAP will only allow SSH-2 connections.
- Web-based management, using the WAP's embedded Web Management Interface (WMI). This method provides configuration and basic monitoring tools, and is good for small deployments (one or two units).

See Also

Power Planning

Security Planning

WDS Planning

WDS (Wireless Distribution System) creates wireless backhaul connections between WAPs, allowing your wireless network to be expanded using multiple WAPs without the need for a wired backbone to link them. WDS features include:

- Automatic radio load balancing
- If desired, you may allow clients to associate to a BSS on the same radio interface used for a WDS Host Link. This will take bandwidth from the WDS link.
- Multiple WDS links can provide link redundancy (failover capability). A network protocol (Spanning Tree Protocol—STP) prevents WAPs from forming network loops.

WDS links have a Host/Client relationship similar to the usual radio/station pattern for WAPs:

- A *WDS Client Link* associates/authenticates to a host (target) WAP in the same way that stations associate to radios. The client side of the link must be configured with the root MAC address of the target (host) WAP.
- A *WDS Host Link* acts like a radio by allowing one WDS Client Link to associate to it. A WAP may have both client and host links.

WDS configuration is performed only on the client-side WAP. See “WDS” on page 356. Note that both WAPs must be configured with the same SSID name.

Common Deployment Options

The following table lists some typical and recommended deployment options for a number of the features that have been discussed in this chapter.

Function	Number of Wireless WAPs	
	One or Two	Three or More
Power	Power over Ethernet	Power over Ethernet UPS backup (recommended)
Failover	Recommended	Highly recommended
VLANs	Optional	Optional use, Can be used to put all APs on one VLAN or map to existing VLAN scheme
Encryption	WPA2 with AES (recommended) PSK or 802.1x	WPA2 with AES (recommended) 802.1x keying
Authentication	Internal RADIUS server EAP-PEAP Pre-Shared Key	External RADIUS server
Management	WOSor Internal WMI Internal CLI (via SSHv2)	WOS

See Also

Coverage and Capacity Planning

Network Management Planning

Planning Your Installation

Power Planning

Security Planning

Installation Workflow

This workflow illustrates the steps that are required to install and configure the WAP successfully. Review this flowchart before attempting to install the unit on a customer’s network.

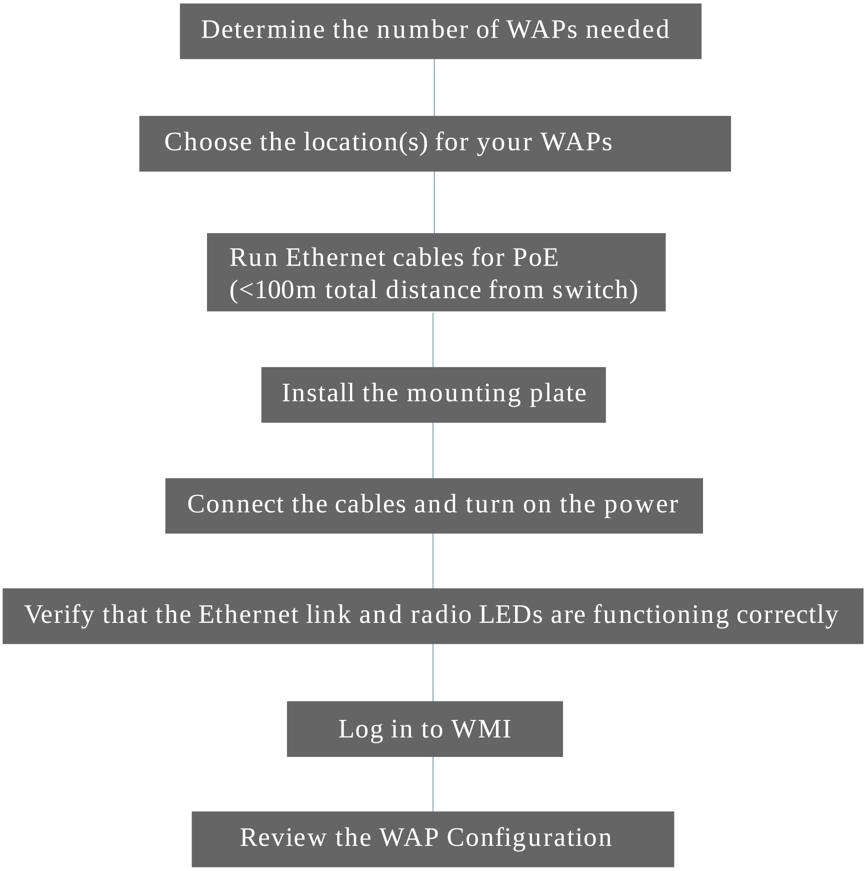

Determine the number of WAPs needed
Choose the location(s) for your WAPs
Run Ethernet cables for PoE (<100m total distance from switch)
Install the mounting plate
Connect the cables and turn on the power
Verify that the Ethernet link and radio LEDs are functioning correctly
Log in to WMI
Review the WAP Configuration

Figure 17. Installation Workflow

See Also

Coverage and Capacity Planning

Common Deployment Options

Installing Your WAP

This section provides information about the physical installation of your WAP. For complete instructions, please see the Installation Guide for your model of WAP.

Choosing a Location

Based on coverage, capacity and deployment examples previously discussed, choose a location for the WAP that will provide the best results for your needs. The WAP was designed to be mounted on a ceiling where the unit is unobtrusive and wireless transmissions can travel unimpeded throughout open plan areas.

Choose a location that is central to your users (see the following diagram for correct placement.

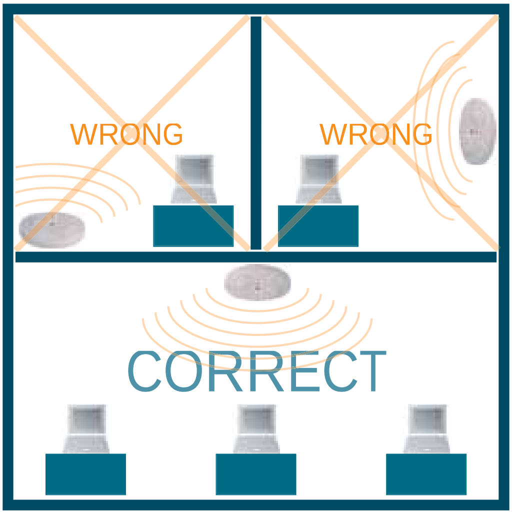


Figure 18. WAP Placement

Wiring Considerations

Before using the PoE to distribute power, see "Power over Ethernet (PoE)" on page 12.

Once you have determined the best location for your WAP, you must run cables to the location for the following services:

Power

No separate power cable is required to the WAP—WAPs use PoE (Power over Ethernet). See the Installation Guide for your WAP model for compatible power injectors or switches.

The total of all Cat 5e or Cat 6 cable segments from the Gigabit Ethernet switch to the power injector and then to a WAP PoE port must be less than 100m long. The WAP must be connected to PoE networks without routing cabling to the outside plant, to ensure that cabling is not exposed to lightning strikes or possible high voltage crossover.

Network

WAPs have one PoE port to supply power and data over the same cable. Please see the Installation Guide for your WAP model for detailed information about running cables to the WAP and connecting it.

When a network connection is established, the WAP can be managed from any of the available network connections, either Gigabit 1 or Gigabit 2.
The Avaya Console utility may be used locally to set up an IP address if necessary.

Important Note About Network Connections

! *The WAP's Ethernet ports should be plugged into an Ethernet switch, not an Ethernet hub—if a hub is used, we recommend that you connect only one Ethernet port.*

See Also

Installation Prerequisites
Installation Workflow
Mounting and Connecting the WAP
Power over Ethernet (PoE)

Mounting and Connecting the WAP

A detailed Installation Guide is available at support.avaya.com that describes mounting your WAP. Please follow the provided instructions carefully. Data and power connections to the WAP are also detailed in the Installation Guide. Please follow the cabling and connection instructions carefully.

Dismounting the WAP

For all WAP models, push up on the WAP (i.e., push it against the mounting plate). Then turn the WAP to the left to remove it. This is similar to dismounting a smoke detector.

Powering Up the WAP

When powering up, the WAP follows a specific sequence of LED patterns showing the boot progress, and following a successful boot will provide extensive status information.

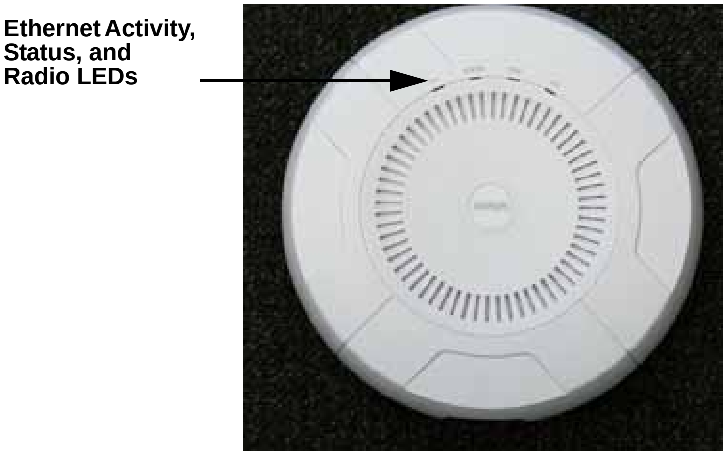


Figure 19. LED Locations

WAP LED settings may be altered or disabled entirely for diagnostic purposes or for personal preference. Changes are made via the WAP’s Command Line Interface or the Web Management Interface—refer to “LED Settings” on page 350.

WAP LED Operating Sequences

Use the following tables to review the operating sequences of the WAP’s LEDs.

- **“LED Boot Sequence” on page 56**
- **“LED Operation when WAP is Running” on page 57**

LED Boot Sequence

The normal boot LED sequence is as follows:

WAP Activity	Status LED	Radio LEDs
Power ON	Blinking GREEN	All OFF
Boot loader power ON self-test	Blinking GREEN	All ON
Image load from compact FLASH	Blinking GREEN	Spinning pattern (rotate all to ON, then all to OFF)
Image load failure	Blinking ORANGE	All OFF
Hand off to Avaya OS	Solid GREEN	All OFF
System software initialization	Solid GREEN	Walking pattern—(LED rotating one position per second)
Up and running	Solid GREEN	ON for radios that are up: OFF for radios that are down. Green or orange per table on the next page. Behavior may be changed using “LED Settings” on page 350.

LED Operation when WAP is Running

The normal LED operation when the WAP is running is shown in the table below. Note that behavior may be modified using "LED Settings" on page 350 or via the CLI.

LED Status	Reason
Radio LED is OFF	radio is down
Radio LED is solid ON	radio is up, but no associations and no traffic
Radio LED heartbeat	radio is up, with stations associated but no traffic
Radio LED flashing Flashing at 10 Hz Flashing at 5 Hz Flashing at 2.5 Hz	radio is up, passing traffic Traffic > 1500 packets / sec Traffic > 150 packets / sec Traffic > 1 packet / sec
Radio LED is GREEN	radio is operating in the 2.4 GHz band
Radio LED is ORANGE	radio is operating in the 5 GHz band
Radio LED flashing ORANGE to GREEN at 1 Hz	The radio is in monitor mode (standard intrude detect)
STATUS LED is GREEN ***	WAP is operational
GIG (Ethernet) LEDs are dual color **Ethernet LED is ORANGE** **Ethernet LED is GREEN**	 Transferring data at 1 Gbps Transferring data at 10 / 100 Mbps

See Also

Installation Prerequisites

Installation Workflow

Ongoing Management

WOS-

This enterprise-hosted platform automatically detects and provisions new Avaya devices deployed in your network via a zero touch provisioning approach similar to that described above. Create and configure a default profile for newly added WAPs—these new devices will automatically receive the configuration defined in your default profile.

If you are a WOS customer, we recommend that you manage your WAPs completely by WOS. Wait five minutes after powering up the WAP, then use WOS to view/manage this unit. If you change settings directly on the WAP, WOS may not sync up with these changes for up to 24 hours.

Note that the WAP must already be running Avaya OS release 7.0.0 or above to support zero-touch provisioning. Optional licenses can be deployed using WOS.

WAP Management Interfaces

User Interfaces

We recommend that you use the WOS for ongoing monitoring and fine-tuning of the network. (For WOS-E, you must set up a default profile and discovery first, to find new APs).

To check the configuration of individual WAPs locally, WAP settings may be viewed or configured through the Command Line Interface (CLI) using SSH, or on a browser with the Web Management Interface (WMI). You may use the CLI on any of the Gigabit Ethernet ports. You can use the WMI via any of the WAP’s Ethernet ports.

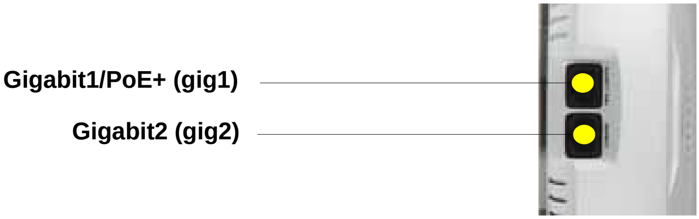


Figure 20. Network Interface Ports—WAP9122/9132 or WAP9123/9133

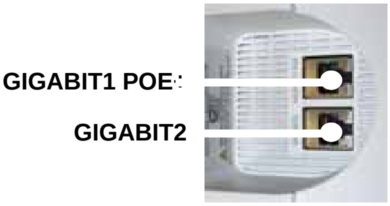


Figure 21. Network Interface Ports—WAP 9172/9173

The Avaya Console utility may also be used to communicate with WAPs locally. See "Securing Low Level Access to the WAP" on page 64.

Using the Ethernet Ports to Access the WAP

By default, the WAP's Ethernet interfaces use DHCP to obtain an IP address. If the WAP is booted and does not receive DHCP addresses on Gigabit Ethernet ports, then both Gigabit1 and its bonded pair port (if any) will default to 192.168.1.3 with a mask of 255.255.255.0.

If the WAP is connected to a network that provides DHCP addresses, the IP address can be determined by the following methods:

1. The simplest way to address the WAP is using its default hostname which is the WAP's serial number, found on the WAP label and shipping container (for example, A171417008D). If your network provides DHCP and DNS, then you can use this hostname.

2. Otherwise, examine the DHCP tables on the server and find the addresses assigned to the WAP (Avaya MAC addresses begin with **64:a7:dd** and are found on the WAP label and shipping container).

3. If the WAP cannot obtain an IP address via DHCP, the factory default uses a static IP address of 192.168.1.3 with a mask of 255.255.255.0 on its Gigabit POE port.

Take care to ensure that your network is not using the 192.168.1.3 *IP address prior to connecting the WAP to the network.*

To connect to the WAP, you must set your laptop to be in the same subnet as the WAP: set your laptop's IP address to be in the 192.168.1.x subnet, and set its subnet mask to 255.255.255.0. If this subnet is already in use on your network, you may connect your laptop directly to the WAP by connecting the laptop to the power injector's IN port temporarily (this port may be called the SWITCH port or the DATA port on your injector).

Starting the WMI

Use this procedure to log in to the WMI on a Web browser.

1. Establish a network connection and open your Web browser.

2. Connect to the WAP using its host name or IP address as described in the previous section.

   http://<hostname or IPaddress>

Logging In

Enter the default user name and password—the default user name is **admin**, and the default password is **admin**.

See Also

Installation Workflow
Performing the Express Setup Procedure
Powering Up the WAP

Licensing

Factory Installed Licenses

Avaya WAP9122/WAP9123 and WAO91XX Access Points are licensed for 802.11a/b/g/n. The WAP9132/WAP9133 Access Points are licensed for 802.11a/b/g/n/ac. All the Access Points are factory licensed for advanced software features—RF Performance Manager (RPM), RF Security Manager (RSM), and RF Analysis Manager (RSM).

Optional Licenses

11N to 11AC Upgrade License—WAP9122 and WAP9123 provide customers investment protection with the option to enable 802.11ac Capability on the 802.11a/b/g/n Radios via optional license purchase. WAO9122 Access Point does not support 11AC Upgrade License.

Application Control License—Avaya Application Control functionality can be enabled on all Avaya WAP91XX/WAO91XX Access Points via an optional license purchase.

License Certificate and License Activation Code

Upon fulfillment of the Purchase Order for the optional licenses, the customer will receive the License Certificate that entitles the customer to optional licenses on the specified number of Access Points. The License Certificate includes the License Activation Code that is required to generate the licenses on the Avaya WLAN Licensing Portal http://licenses.wifi.avaya.com.

Important: Keep the License Certificate safely for future reference.

Obtaining Software License Keys

To enable the optional licensed capability on the Access Points, you must first obtain software license keys from Avaya and apply them to the Access Points.

Instructions for Wireless Orchestration System Customers

1. Connect to WOS using a web browser and navigate to **Configure, Access Point Licenses, Export Licenses**.

2. Select the Access Points to which you wish to apply the new 802.11ac Upgrade or Application Control Licenses and click **Next**.
3. Review the **File Name**. Select **Export as CSV** and click the **Export** button. Note the name and location where the CSV file is saved.
4. Connect to Avaya's WLAN 9100 Licensing portal at http://licenses.wifi.avaya.com using a web browser.
5. Fill in the required customer contact details on the Licensing Page and select **Create/Generate Licenses for your 9100 series APs**.
6. Enter the **License Activation Code** listed in the lower right box of the License Certificate and choose **Upload a csv File that you exported from your WOS-E**.
7. Choose the CSV file exported from WOS in Step 3, and click **Upload**. Then click **Submit** at the bottom of the page.
8. The license file will be sent to the email address entered in the request.

Instructions for Customers without Wireless Orchestration System

1. Collect the Serial Number for each Access Point to be upgraded with an 802.11ac Upgrade or Application Control License. Get the Serial Number from the WMI/CLI or from the WAP’s label.
2. Connect to Avaya's WLAN 9100 Licensing portal at http://licenses.wifi.avaya.com using a Web Browser
3. Fill in the required customer contact details on the Licensing Page and select **Create/Generate Licenses for your 9100 series APs**.
4. Enter the **License Activation Code** listed in the lower right box of the License Certificate and choose **Enter Serial numbers manually**. Up to 50 AP Serial Numbers can be entered separated by commas or spaces.
5. The License File will be sent to the email address entered in the request.

Applying Software Licenses to Access Points

The license keys received via email must be applied to the Access Points to enable the optional capabilities / features.

Instructions for Customers with Wireless Orchestration System

1. Download the License File received to your personal computer. Note down the file name and location.
2. Connect to WOS using a web browser and navigate to **Configure, Access Point Licenses, Import Licenses**.
3. Choose the License File saved in Step 1 and click **Upload**. Click **Next** when the upload is complete.
4. Verify that the optional license feature is now included in the License Feature List. Click **Finish**.
5. Navigate to **Configure, Access Points, Deployed Licenses**. Confirm that the Access Points to which the license keys have been applied show that the optional feature is included.

Instructions for Customers without Wireless Orchestration System

1. Open the license file received via email.
2. Login to WMI on the WAP using a web browser and navigate to the **Express Setup** page.
3. Copy the License Key corresponding to the AP Serial Number from the license file opened in Step 1 and paste it under **License Key**. Click **Apply**.
4. Navigate to **Status, Access Point, Information** and verify that the new optional feature is included in the Licensed Features.
5. Repeat Steps 2—4 for every AP to which the optional license key has to be applied.

Performing the Express Setup Procedure

The Express Setup procedure establishes global configuration settings that enable basic WAP functionality. Changes made in this window will affect all radios. If you are not using WOS to perform your initial configuration, please see “Express Setup” on page 143. Also see “Ongoing Management” on page 58.

See Also

Ongoing Management
Installation Prerequisites
Installation Workflow
Logging In
Multiple SSIDs
Security

Securing Low Level Access to the WAP

Most local management of the WAP is done via the WMI or CLI—see “The Command Line Interface” on page 407. The WAP also has a lower level interface: boot loader, which allows access to more primitive commands. You won’t normally use boot loader unless instructed to do so by Avaya Customer Support. For proper security, you should replace the default boot loader login username and password with your own, as instructed below. boot loader has its own username and password, separate from the Avaya OS Admin User and Password (used for logging in to the WMI and CLI) that you may change on the Express Setup page (see Step 5 on page 147).

Avaya also provides the Avaya Console utility for connecting to Avaya WAPs that are not reachable via the normal access methods such as Secure Shell (SSH) or WMI. Avaya Console discovers WAPs on your network subnet by sending IP/ UDP broadcast packets. Once a WAP is discovered, Avaya Console can establish an encrypted console session to the WAP via the network even if the WAP IP configuration is incorrect. Avaya Console allows you to manage the WAP using CLI. Avaya Console also has an option for easily accessing boot loader.

In normal circumstances Avaya WAPs should be configured and managed through SSH or via the WMI. A connection is established using either the WAP hostname or DHCP-assigned IP address, or via the other options described in “Using the Ethernet Ports to Access the WAP” on page 59. Avaya Console may be needed in special circumstances as directed by Avaya Customer Support for troubleshooting WAP problems or IP connectivity. (In this case, refer to the *Using* *the Avaya Console for the WLAN 9100 Series* (NN47252-106) for detailed information.)

Avaya Console access to the WAP:

- You may enable or disable all Avaya Console access to the WAP as instructed in the procedure below. There are also options to allow access only to CLI (i.e., Avaya OS access) or only to boot loader.
- To avoid potentially being locked out of the WAP, Avaya Console should always be enabled at the boot loader level at least.

! *If you disable Avaya Console access to both boot loader and CLI, you must ensure that you do not lose track of the username and password to log in to CLI/WMI! In this situation, there is no way to recover from a lost password, other than returning the WAP to Avaya. If you have Avaya Console access to boot loader enabled, you can reset the password, but this recovery will require setting the unit to factory defaults with loss of all configuration data.*

Procedure for Securing Low Level WAP Access

Use the following steps to replace the default boot loader username and password, and optionally to change the type of Avaya Console management access that is allowed. These steps use CLI commands.

1. To access CLI via the WMI, click **CLI** under the **Tools** section on the left (for detailed instructions see “CLI” on page 398). Skip to Step 4 on page 65.

   To access CLI via SSH, see “Establishing a Secure Shell (SSH) Connection” on page 407. Then proceed to the next step.

2. At the **login as** prompt, log in to CLI using the username and password that you set in Step 5 on page 147, or the default value of **admin** / **admin** if you have not changed them.

3. Type **configure** to enter the CLI config mode.

4. If Avaya Console access at the boot loader level is to be allowed, use the following three commands to change the boot loader username and

password from the default values of **admin**/**admin**. In the example below, replace **newusername** and **newpassword** with your desired entries. Note that these entries are case-sensitive.

5. Enter the following commands if you wish to change Avaya Console access permission:

<management-status> may be one of:

- **on**—enables both CLI and boot loader access
- **off**—disables both CLI and boot loader access
- **aos-only**—enables only CLI (i.e. Avaya OS) access
- **boot-only**—enables only boot loader access

Note that there is a WMI setting for changing Avaya Console access, timeout period, and the UDP port used. This may be used instead of CLI if you wish. See "Management Control" on page 217. Note that you cannot change the boot loader username and password via the WMI.

The Web Management Interface

This topic provides an overview of the WAP's embedded Web Management Interface (WMI), used for establishing your network's configuration settings and wireless operating parameters. It also includes login instructions. The following topics are discussed:

- **Managing WAPs Locally or Using WOS**
- **An Overview**
- **Structure of the WMI**
- **User Interface**
- **Logging In**
- **Applying Configuration Changes**

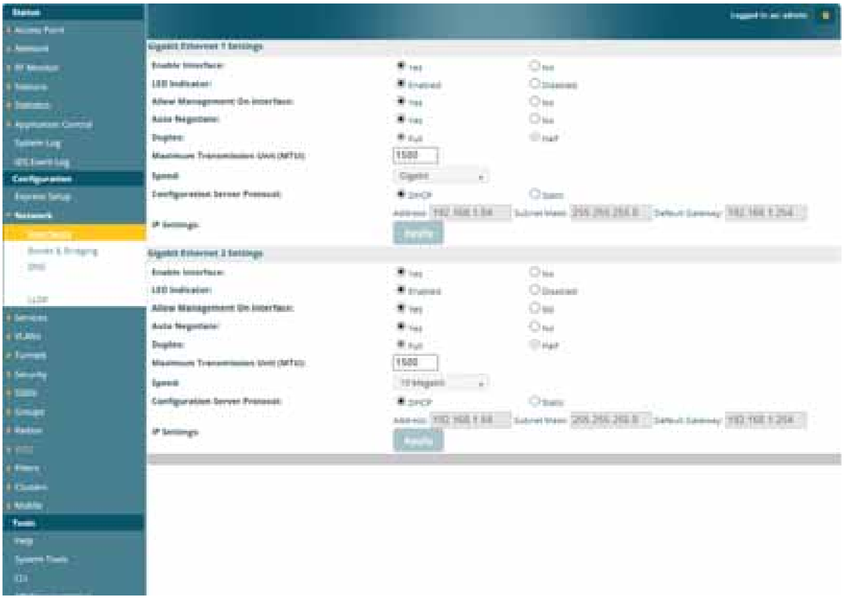
Managing WAPs Locally or Using WOS

For Avaya deployments of any size, we recommend that you use WOS to manage the network rather than directly managing each WAP individually. You may change settings directly on the WAP—but be aware that WOS may not sync up with these changes for up to 24 hours. All WOS versions automatically "rediscover" the wireless network once a day by default, and WOS will fetch updated settings into its database at that time.

To immediately sync up WOS with changes that you have made to a particular WAP, you may go to the WOS **Monitor** > **WAPs** or **Configure** > **WAPs** page. Select the WAP, and click the **Refresh** button to update WOS with your changes on a WAP. This causes WOS to read the current configuration of the WAP and update the WOS database with these values.

An Overview

The WMI is an easy-to-use graphical interface to your WAP. It allows you to configure the product to suit your individual requirements and ensure that the unit functions efficiently and effectively.



Gigabit Ethernet 1 Settings

Enable Interface: ● Yes ○ No

LED Indicator: ● Enabled ○ Disabled

Allow Management On Interface: ● Yes ○ No

Auto Negotiate: ● Yes ○ No

Duplex: ● Full ○ Half

Maximum Transmission Unit (MTU): 1500

Speed: Gigabit

Configuration Server Protocol: ● DHCP ○ Static

IP Settings: Address: 192.168.1.64 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.254

Gigabit Ethernet 2 Settings

Enable Interface: ● Yes ○ No

LED Indicator: ● Enabled ○ Disabled

Allow Management On Interface: ● Yes ○ No

Auto Negotiate: ● Yes ○ No

Duplex: ● Full ○ Half

Maximum Transmission Unit (MTU): 1500

Speed: 10 Megabit

Configuration Server Protocol: ● DHCP ○ Static

IP Settings: Address: 192.168.1.64 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.254

Figure 22. Web Management Interface

Structure of the WMI

The content of the WMI is organized by function and hierarchy, shown in the following table. Click on any item below to jump to the referenced destination.

- **Status Windows**
  - Access Point Status Windows
    - Access Point Summary
    - Access Point Information
    - Access Point Configuration
    - Admin History
  - Network Status Windows
    - Network Map
    - Spanning Tree Status
    - Routing Table
    - ARP Table
    - DHCP Leases
    - Connection Tracking / NAT
    - Network Assurance
  - RF Monitor Windows
    - Radio Monitoring
    - Radio Assurance
  - Station Status Windows
    - Stations
    - Location Map
    - RSSI
    - Signal-to-Noise Ratio (SNR)
    - Noise Floor
    - Max by AP
    - Station Assurance
- Statistics Windows
  - Radio Statistics Summary
  - Per-Radio Statistics
  - Network Statistics
  - VLAN Statistics
  - IDS Statistics
  - Filter Statistics
  - Station Statistics
  - Per-Station Statistics
- Application Control Windows
- System Log Window
- IDS Event Log Window

Configuration Windows

- Express Setup
- Network
  - Interfaces
  - Bonds and Bridging
  - DNS Settings
- Services
  - Time Settings (NTP)
  - NetFlow
  - Wi-Fi Tag
  - Location
  - System Log
  - SNMP
  - DHCP Server
  - Proxy Services
- VLANs
  - VLAN Management
- Security
  - Admin Management
  - Admin Privileges
  - Admin RADIUS
  - Management Control
  - Access Control List
  - Global Settings
  - External Radius
  - Internal Radius
  - Active Directory
  - Rogue Control List
  - OAuth 2.0 Management
- SSIDs
  - SSID Management
  - Active Radios
  - Per-SSID Access Control List
  - Honeypots

Configuration Windows (cont’d)

- Groups
  - Group Management
- Radios
  - Radio Settings
  - Global Settings
  - Global Settings .11an
  - Global Settings .11bgn
  - Global Settings .11n
  - Global Settings .11u
  - Global Settings .11ac
  - Advanced RF Settings
  - Hotspot 2.0
  - NAI Realms
  - NAI EAP
  - Intrusion Detection
  - LED Settings
  - DSCP Mappings
  - Roaming Assist
- WDS
  - WDS Client Links
- Filters
  - Filter Lists
  - Filter Management

Tool Windows

- System Tools
- CLI
- API Documentation
- Options
- Logout

User Interface

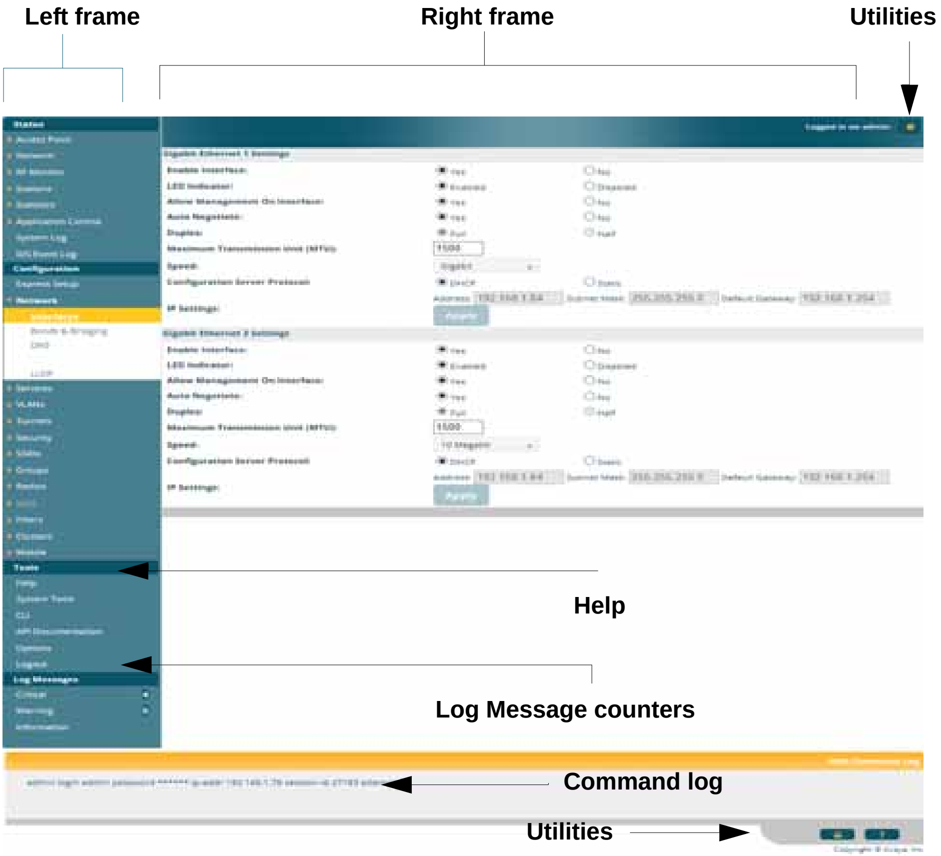


Figure 23. WMI: Frames

The WMI has been designed with simplicity in mind, making navigation quick and easy. In the following example, you'll see that windows are divided into left and right frames. (Figure 23)

The left frame contains two main elements:

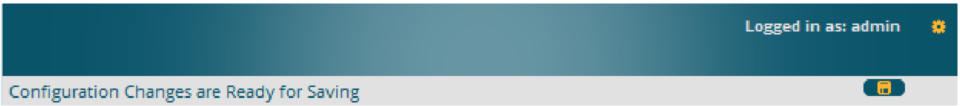
- The menu is organized into three major sections (**Status**, **Configuration**, **Tools**). Each has headings for major functions, such as Network, SSIDs, Security, etc. Click a heading, such as **Network**, to display a page showing a summary of its current configuration, as well as to show links for all of its associated WMI pages.

- Three **Log Messages** counters are located at the bottom of the menu. They provide a running total of messages generated by the Avaya OS Syslog subsystem during your session—organized into **Critical**, **Warning**, and **General** messages. Click on a counter to display the associated Syslog messages. Messages at the selected level or higher will be shown. For more information, please see "System Log Window" on page 137.

The right frame has four main elements:

- The header shows the WAP type in the upper right corner, along with the hostname (this defaults to the unit's serial number) and IP address. The Uptime shows the time since the WAP was last rebooted.

  Below this is the page title, and the user name you used to log in. On the right, click the Utilities button ✹ for a drop-down menu that allows you to **Refresh Page**, **Save** your changes, open the **Help** system, or **Logout**. If you have any unsaved changes, the **Save** button 💾 is displayed on the right, in the top bar.

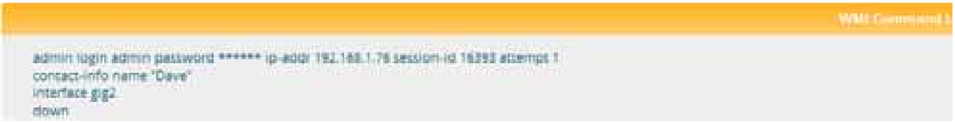


Configuration Changes are Ready for Saving

Figure 24. WMI Header

- The main window displays the status information or configuration page that you requested. This is where you review the WAP's current status and activity or enter changes if you wish.

- The Command Log shows the resulting commands for requests made through the WMI.



```
admin login admin password ****** ip-addr 192.168.1.76 session-id 16292 attempt 1
contact-info name "Dave"
interface gig2
down
```

Figure 25. WMI Command Log

- Utility buttons are located at the bottom right of each window— a **Print** button and a **Help** button.

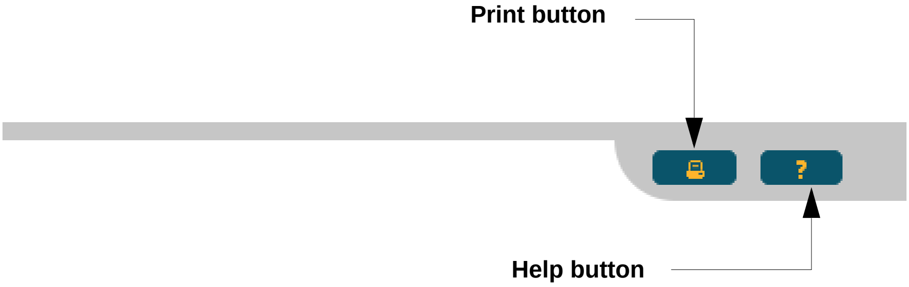


Figure 26. WMI: Utility Buttons

- Click the **Print** button to open a print dialog to send a copy of the active window to your local printer.
- Click the **Help** button to access the WAP’s online help system.

*Some pages or individual settings are only available if the WAP’s license includes appropriate Avaya **Advanced Feature Sets**. If a setting is unavailable (grayed out), then your license does not support the feature. See “Licensing” on page 61.*

Note that WMI provides an option that allows you to change its behavior. You may change:

- **Refresh Interval**—the refresh interval, if automatic refresh is selected.

See “Options” on page 405 for more information.

Logging In

Use this procedure to log in to the WMI via your Web browser.

1. Establish a network connection and open your Web browser.
2. If your network supports DHCP and DNS, enter the WAP’s default host name in the browser’s URL. The default host name is simply the WAP’s serial number (for example, A1714170008D).

   Otherwise, enter the WAP’s IP address. This may be determined as described in “Using the Ethernet Ports to Access the WAP” on page 59.
3. The default login to the WAP’s Web Management Interface is **admin** for both the user name and password.

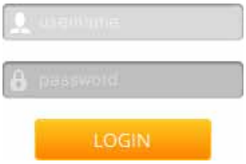


Figure 27. Logging In to the WAP

Applying Configuration Changes

In most of the WMI configuration windows, your changes to settings are applied to the WAP as you make them. In most cases, there is no separate Apply button to click to make the changes take effect. There are a few exceptions to this rule. In these cases, a particular section of a page may have its own **Apply Settings** button right below the settings.

In both cases described above, the changes that you have made are not saved to the latest configuration file in the WAP’s flash memory, so they will not be restored after a reboot. Click the **Save** button (located on the upper right of each page) in order to make sure that these changes will be applied after rebooting. This will save the entire current configuration, not only the changes on current WMI page.

Character Restrictions

When inputting strings in the WMI (for example, assigning SSIDs, host name, password, etc.), use common alphanumeric characters. Some of the fields in the WMI will not accept special characters, so use of the following characters should typically be avoided:

**&   <   >   '   “   /   **

Viewing Status on the WAP

These windows provide status information and statistics for your WAP using the product's embedded Web Management Interface (WMI). You cannot make configuration changes to your WAP from these windows. The following topics have been organized into functional areas that reflect the flow and content of the Status section of the navigation tree in the left frame of the WMI.

- **"Access Point Status Windows" on page 78**
- **"Network Status Windows" on page 85**
- **"RF Monitor Windows" on page 96**
- **"Station Status Windows" on page 107**
- **"Statistics Windows" on page 119**
- **"Application Control Windows" on page 130**
- **"System Log Window" on page 137**
- **"IDS Event Log Window" on page 138**

Configuration and Tools windows are not discussed here. For information on these windows, please see:

- **"Configuring the WAP" on page 141**
- **"Using Tools on the WAP" on page 383**

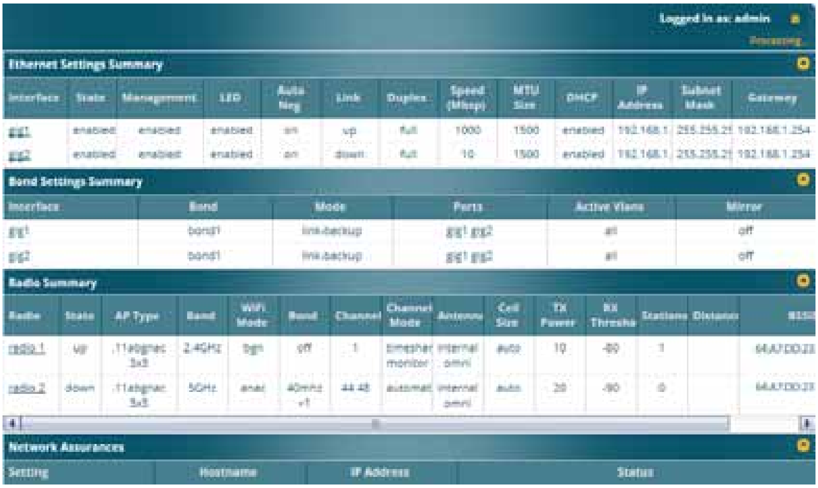
Access Point Status Windows

The following WAP Status windows are available:

- **Access Point Summary**—displays information on the configuration of all WAP interfaces, including radios.
- **Access Point Information**—provides version / serial number information for all WAP components.
- **Access Point Configuration**—shows all configuration information for the WAP in text format.
- **Admin History**—shows all current and past logins since the last reboot.

Access Point Summary

This is a status only window that provides a snapshot of the global configuration settings for all Wireless WAP network interfaces and radios. You must go to the appropriate configuration window to make changes to any of the settings displayed here—configuration changes cannot be made from this window. Clicking on an interface or radio will take you to the proper window for making configuration changes.



Logged in as: admin

Ethernet Settings Summary

Interface	State	Management	LED	Auto Neg	Link	Duplex	Speed (Mbsp)	MTU Size	DHCP	IP Address	Subnet Mask	Gateway
gig1	enabled	enabled	enabled	on	up	full	1000	1500	enabled	192.168.1	255.255.2!	192.168.1.254
gig2	enabled	enabled	enabled	on	down	full	10	1500	enabled	192.168.1	255.255.2!	192.168.1.254

Bond Settings Summary

Interface	Bond	Mode	Ports	Active Vlans	Mirror
gig1	bond1	link-backup	gig1 gig2	all	off
gig2	bond1	link-backup	gig1 gig2	all	off

Radio Summary

Radio	State	AP Type	Band	WiFi Mode	Bond	Channel	Channel Mode	Antenna	Cell Size	TX Power	RX Thresho	Stations	Distanc	BSSI
radio 1	up	.11abgnac 3x3	2.4GHz	bgn	off	1	timeshar monitor	internal omni	auto	10	-90	1		64:A7:DD:23
radio 2	down	.11abgnac 3x3	5GHz	anac	40mhz +1	44 48	automati	internal omni	auto	20	-90	0		64:A7:DD:23

Network Assurances

Setting	Hostname	IP Address	Status

Figure 28. WAP Summary

Content of the Access Point Summary Window

The Access Point Summary window is sub-divided into the **Ethernet Interfaces** section and the radio section, providing you with the following information:

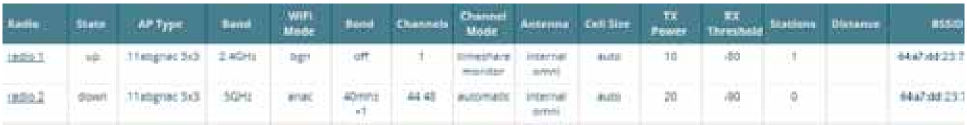
- **Ethernet Settings Summary**
  This section provides information about network interface devices. To make configuration changes to these devices, go to "Interfaces" on page 150.
  - **Interface**: Lists the network interfaces that are available on the WAP.
  - **State**: Shows the current state of each interface, either enabled or disabled.
  - **Mgmt**: Shows whether WAP management traffic is allowed on this interface.
  - **Auto Neg**: Shows whether auto-negotiation is in use on this interface, to determine settings for speed, parity bits, etc.
  - **LED**: Shows whether LED display of interface status is enabled.
  - **Link**: Shows whether the link on this interface is up or down.
  - **Duplex**: Shows whether full duplex mode is in use.
  - **Speed**: Shows the speed of this interface in Mbps.
  - **MTU Size**: Shows the Maximum Transmission Unit size that has been configured. This is the largest packet size (in bytes) that the interface can pass along.
  - **DHCP**: Shows whether DHCP on this port is enabled or disabled.
  - **IP Address**: Shows the current IP address assigned to each network interface device.
  - **Subnet Mask**: Shows the subnet mask, which defines the number of IP addresses that are available on the routed subnet where the WAP is located.
  - **Gateway**: Shows the IP address of the router that the WAP uses to transmit data to other networks.

- **Bond Settings Summary**
  This section provides information about the relationship that has been selected for the Gigabit ports. For detailed explanations and to make configuration changes, see “Bonds and Bridging” on page 153.

  - **Bond**: Lists all network bonds that have been configured.
  - **Mode**: Shows the type of relationship that has been selected for the Gigabit ports.
  - **Ports**: Shows the Gigabit ports that are part of this bond.
  - **Port Mode**: Shows the relationship that has been selected for the Ethernet ports. See “Bonds and Bridging” on page 153 for details
  - **Active VLANs**: Shows the VLANs that are active in this bond.
  - **Mirror**: Shows whether mirroring is enabled on this bond.

- **Radio Section**
  This section provides information about the radios that are contained within the WAP. How many radios are listed depends on which product model you are using. To make configuration changes to these radios, go to “Radio Settings” on page 284.

  - **Radio**: Lists the radios that are available on the WAP.
  - **State**: Shows the current state of each radio, either up or down. Radios that are down are shown in RED. Figure 29 shows an example where **radio2** is down.
  - **AP Type**: Shows the types of 802.11 clients supported by this radio (11/a/b/g/n) and the number of separate data streams transmitted and received by the antennas of each radio for 802.11n. For example, 3x3 means that the radio supports three transmit chains and three receive chains. See “Up to Eight Simultaneous Data Streams—Spatial Multiplexing” on page 33.



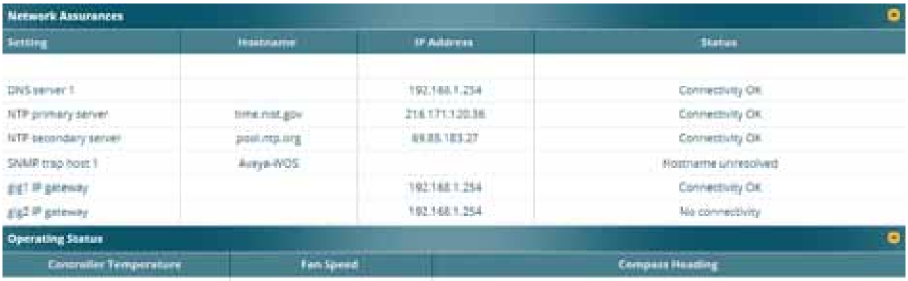
Radio	State	AP Type	Band	WiFi Mode	Bond	Channels	Channel Mode	Antenna	Cell Size	TX Power	RX Threshold	Stations	Distance	BSSID
radio 1	up	11abgnac 3x3	2.4GHz	bgn	off	1	timeshare monitor	internal omni	auto	10	-80	1		64:a7:dd:23:7
radio 2	down	11abgnac 3x3	5GHz	anac	40mhz +1	44 48	automatic	internal omni	auto	20	-90	0		64:a7:dd:23:1

Figure 29. Disabled Radio (Partial View)

- **Channel**: Shows which channel each radio is using, and the channel setting. To avoid co-channel interference, adjacent radios should not be using adjacent channels. To make channel selections for a specific radio, go to “Radio Settings” on page 284.
- **Wi-Fi Mode**: Shows the 802.11 client types that the radio has been configured to support.
- **Antenna**: Shows which antenna is being used by each radio.
- **Cell Size**: Indicates which cell size setting is currently active for each radio—small, medium, large, max, automatic, or manually defined by you.

  The cell size of a radio is a function of its transmit power and determines the radio’s overall coverage. To define cell sizes, go to “Radio Settings” on page 284. For additional information about cell sizes and the importance of planning for and defining the optimum cell sizes for your WAP, go to “Coverage and Capacity Planning” on page 25.
- **Tx Power**: Shows the transmit power for each radio.
- **Rx Threshold**: Shows the receive threshold for each radio.
- **Stations**: Informs you how many client stations are currently associated with each radio.
- **WDS Link/Distance**: The WDS Link on this radio (if any), and whether the link has been set to support Long Distance Links. See “WDS” on page 356.
- **MAC Address/BSSID**: Shows the MAC address for each radio.
- **Description**: The description (if any) that you set for this radio.

- **Network Assurance Section**
  This section shows the results of ongoing network assurance testing. This is the same as information shown in "Network Assurance" on page 94.



Network Assurances

Setting	Hostname	IP Address	Status
DNS server 1		192.168.1.254	Connectivity OK
NTP primary server	time.nist.gov	216.171.120.36	Connectivity OK
NTP secondary server	pool.ntp.org	69.85.183.27	Connectivity OK
SNMP trap host 1	Avaya-WOS		Hostname unresolved
gig1 IP gateway		192.168.1.254	Connectivity OK
gig2 IP gateway		192.168.1.254	No connectivity

Operating Status

Controller Temperature	Fan Speed	Compass Heading

Figure 30. Network Assurance and Operating Status

The WAP checks connectivity to network servers that you have configured (for example, DNS and NTP servers) on an ongoing basis. For each Setting, this list shows the server's **Host Name** (if any), **IP Address**, and **Status**.

Network assurance must be enabled on the WAP in order to perform these connectivity tests and display this information. See "Management Control" on page 217.

- **Operating Status Section**
  This section shows the WAP controller board's current internal temperatures, current fan speed, and compass heading. (Figure 30)

Notice that the Compass Heading field will only show a value if the WAP model is one that includes a built-in compass. In order for this reading to be correct, the WAP must be mounted with radio1 facing north. If the WAP does not have an integrated compass, this field will just show a dash.

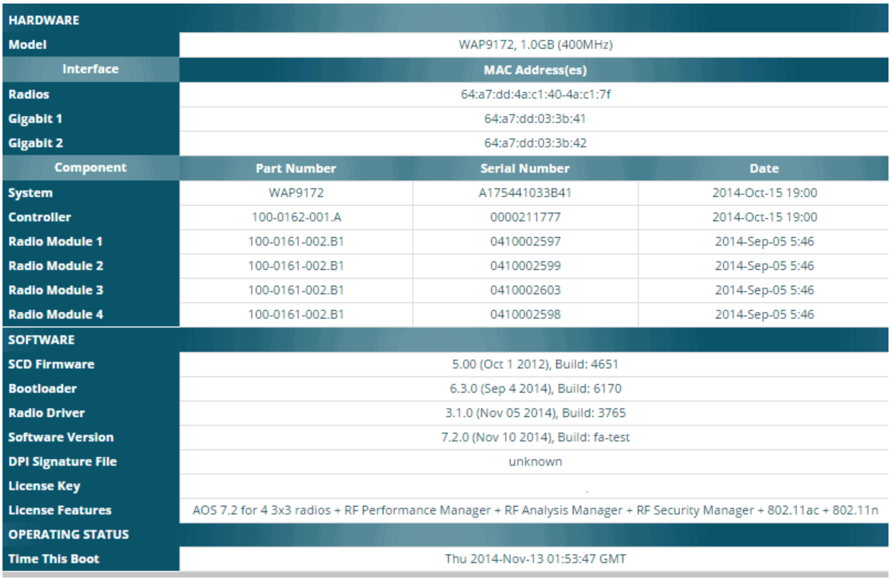
See Also

Management Control
Interfaces
Bonds and Bridging
Radio Settings

Access Point Information

This is a status only window that shows you the current firmware versions utilized by the WAP, serial numbers assigned to each module, MAC addresses, licensing information, and recent boot timestamps. It will also show current internal temperatures, fan speed, and compass heading if the WAP model supports these features.

Notice that the **License Features** row lists the features that are supported by your WAP's license. See "Licensing" on page 61.



HARDWARE			
Model	WAP9172, 1.0GB (400MHz)		
Interface	MAC Address(es)		
Radios	64:a7:dd:4a:c1:40-4a:c1:7f		
Gigabit 1	64:a7:dd:03:3b:41		
Gigabit 2	64:a7:dd:03:3b:42		
Component	Part Number	Serial Number	Date
System	WAP9172	A175441033B41	2014-Oct-15 19:00
Controller	100-0162-001.A	0000211777	2014-Oct-15 19:00
Radio Module 1	100-0161-002.B1	0410002597	2014-Sep-05 5:46
Radio Module 2	100-0161-002.B1	0410002599	2014-Sep-05 5:46
Radio Module 3	100-0161-002.B1	0410002603	2014-Sep-05 5:46
Radio Module 4	100-0161-002.B1	0410002598	2014-Sep-05 5:46
SOFTWARE			
SCD Firmware	5.00 (Oct 1 2012), Build: 4651		
Bootloader	6.3.0 (Sep 4 2014), Build: 6170		
Radio Driver	3.1.0 (Nov 05 2014), Build: 3765		
Software Version	7.2.0 (Nov 10 2014), Build: fa-test		
DPI Signature File	unknown		
License Key	-		
License Features	AOS 7.2 for 4 3x3 radios + RF Performance Manager + RF Analysis Manager + RF Security Manager + 802.11ac + 802.11n		
OPERATING STATUS			
Time This Boot	Thu 2014-Nov-13 01:53:47 GMT		

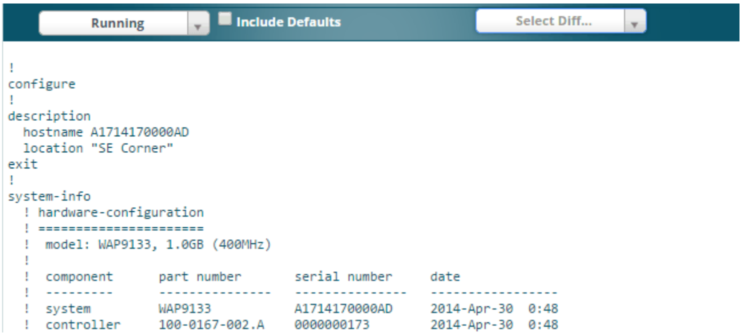
Figure 31. WAP Information

You cannot make configuration changes in this window, but if you are experiencing issues with network services, you may want to print the content of this window for your records.

Access Point Configuration

This is a status only window that allows you to display the configuration settings assigned to the WAP, based on the following filter options:

- **Running**—displays the current configuration (the one running now).
- **Saved**—displays the saved configuration from this session.
- **Lastboot**—displays the configuration as it was after the last reboot.
- **Factory**—displays the configuration established at the factory.



```
!
configure
!
description
  hostname A1714170000AD
  location "SE Corner"
exit
!
system-info
  ! hardware-configuration
  ! ======================
  !  model: WAP9133, 1.0GB (400MHz)
  !
  !  component      part number      serial number     date
  !  ---------      ---------------  ---------------   -----------------
  !  system         WAP9133          A1714170000AD     2014-Apr-30  0:48
  !  controller     100-0167-002.A   0000000173        2014-Apr-30  0:48
```

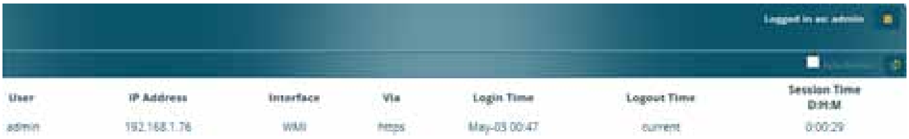
Figure 32. Show Configuration

If you want to see just the differences between the Running, Saved, Lastboot, and Factory configurations, you can do this by choosing a configuration option from the **Select Config** pull-down menu then selecting an alternative configuration option from the **Select Diff** pull-down menu.

To include the default configuration settings in the output, choose the configuration then click the **Include Defaults** check box. If **Include Defaults** is disabled, then only the changes from the default configuration are shown.

Admin History

It is useful to know who else is currently logged in to a WAP while you're configuring it, or who has logged in since the WAP booted. This status-only window shows you all administrator logins to the WAP that have occurred since the last reboot. To determine who is currently logged in, check which entries say **active** in the **Logout Time** column.



User	IP Address	Interface	Via	Login Time	Logout Time	Session Time D:H:M
admin	192.168.1.76	WMI	https	May-03 00:47	current	0:00:29

Figure 33. Admin Login History

Network Status Windows

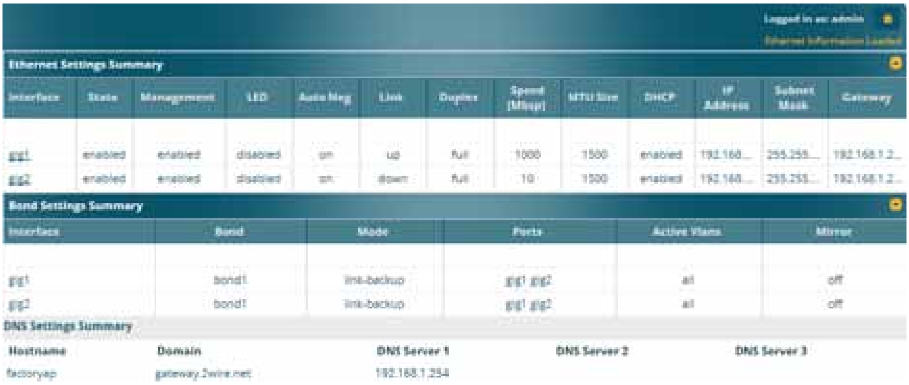
The following Network Status windows are available:

- **Network**—displays a summary of network interface settings.
- **Network Map**—displays information about this WAP and neighboring WAPs that have been detected.
- **Spanning Tree Status**—displays the spanning tree status of network links on this WAP.
- **Routing Table**—displays information about routing on this WAP.
- **ARP Table**—displays information about Address Resolution Protocol on this WAP.
- **DHCP Leases**—displays information about IP addresses (leases) that the WAP has allocated to client stations.
- **Connection Tracking/NAT**—lists connections that have been established for client stations.
- **Fabric Attach List—**lists devices on the WAP’s network that support the Link Layer Discovery Protocol (LLDP).
- **Network Assurance**—shows results of connectivity tests for network servers.

- **Undefined VLANs**—shows VLANs present on an 802.1Q connection to the WAP, that are not configured in the WAP's VLAN list.

Network

This window provides a snapshot of the configuration settings currently established for WAP’s wired interfaces. This includes the Gigabit interfaces and their bonding settings. DNS Settings are summarized as well. You can click on any item in the **Interface** or **Bond** columns to go to the associated configuration window.



Ethernet Settings Summary

Interface	State	Management	LED	Auto Neg	Link	Duplex	Speed (Mbsp)	MTU Size	DHCP	IP Address	Subnet Mask	Gateway
gig1	enabled	enabled	disabled	on	up	full	1000	1500	enabled	192.168...	255.255...	192.168.1.2...
gig2	enabled	enabled	disabled	on	down	full	10	1500	enabled	192.168...	255.255...	192.168.1.2...

Bond Settings Summary

Interface	Bond	Mode	Ports	Active Vlans	Mirror
gig1	bond1	link-backup	gig1 gig2	all	off
gig2	bond1	link-backup	gig1 gig2	all	off

DNS Settings Summary

Hostname	Domain	DNS Server 1	DNS Server 2	DNS Server 3
factoryap	gateway.2wire.net	192.168.1.254		

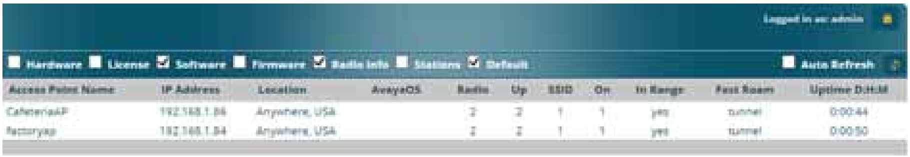
Figure 34. Network Settings

WMI windows that allow you to change or view configuration settings associated with the network interfaces include:

- **“Interfaces” on page 150**
- **“Bonds and Bridging” on page 153**
- **“DNS Settings” on page 160**

Network Map

This window offers detailed information about this WAP and all neighboring WAPs, including how the WAPs have been set up within your network.



Logged in as: admin

□ Hardware □ License ☑ Software □ Firmware ☑ Radio Info □ Stations ☑ Default □ Auto Refresh

Access Point Name	IP Address	Location	AvayaOS	Radio	Up	SSID	On	In Range	Fast Roam	Uptime D:H:M
CafeteriaAP	192.168.1.86	Anywhere, USA		2	2	1	1	yes	tunnel	0:00:44
factoryap	192.168.1.84	Anywhere, USA		2	2	1	1	yes	tunnel	0:00:50

Figure 35. Network Map

The Network Map has a number of options at the top of the page that allow you to customize your output by selecting from a variety of information that may be displayed. You may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon ☝. Click **Refresh** to update the information at any time. Click **Auto Refresh** to instruct the WAP to refresh this window automatically.

Content of the Network Map Window

By default, the network map shows the following status information for each WAP:

- **Access Point Name**: The host name assigned to the WAP. To establish the host name, go to "Express Setup" on page 143. You may click the host name to access WMI for this WAP.
- **IP Address**: The WAP's IP address. You may click the address to access WMI for this WAP. If DHCP is enabled, the WAP's IP address is assigned by the DHCP server. If DHCP is disabled, you must assign a static IP address. To enable DHCP or to assign a static IP address for the WAP, go to "Express Setup" on page 143.
- **Location**: The location assigned to the WAP. To establish the location information, go to "Express Setup" on page 143.
- **Avaya OS**: The software version running on the WAP.
- **Radio**: The number of radios on the WAP.

- **(Radio) Up**: Informs you how many radios are currently up and running. To enable or disable all radios, go to “Express Setup” on page 143. To enable or disable individual radios, go to “Radio Settings” on page 284.
- **SSID**: Informs you how many SSIDs have been assigned for the WAP. To assign an SSID, go to “SSID Management” on page 254.
- **(SSID) On**: Informs you how many SSIDs are enabled. To enable or disable SSIDs, go to “SSID Management” on page 254.
- **In Range**: Informs you whether the WAP is within wireless range of another Wireless WAP.
- **Fast Roam**: Informs you whether or not the Avaya fast roaming feature is enabled. This feature utilizes the Avaya Roaming Protocol ensuring fast and seamless roaming capabilities between radios or WAPs at both Layer 2 and Layer 3. To enable or disable fast roaming, go to “Global Settings” on page 290.
- **Uptime (D:H:M)**: Informs you how long the WAP has been up and running (in Days, Hours and Minutes).

To see additional information, select from the following checkboxes at the bottom of the page. This will show the columns described below.

Hardware

- **Model**: The model number of each WAP, plus the amount of RAM memory and the speed of the processor.
- **Serial**: Displays the serial number of each WAP.

License

- **License**: The license key of each WAP.
- **Licensed Features**: Lists the features enabled by the key.

Software (enabled by default)

- Enable / disable display of the WAP OS column.

Firmware

- **Boot Loader**: The software version number of the boot loader on each WAP.
- **SCD Firmware**: The software version number of the SCD firmware on each WAP.

Radio Info (enabled by default)

- Enable / disable display of the Radio / Up columns.

Stations

- **Stations**: Tells you how many stations are currently associated to each WAP. To de-authenticate a station, go to "Stations" on page 108.

  The columns to the right (**H**, **D**, **W**, and **M**) show the highest number of stations that have been associated over various periods of time: the previous hour, day, week, and month.

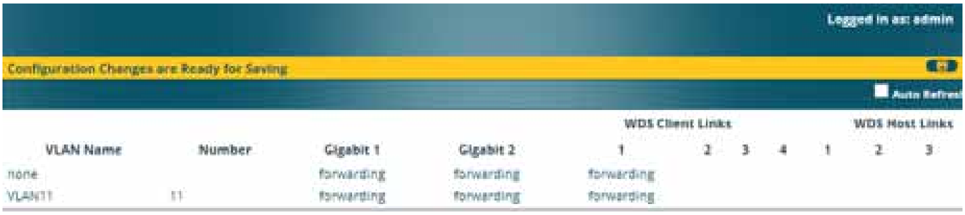
Default

- Sets the columns displayed to the default settings. By default, only Software and Radio Info are selected.

Spanning Tree Status

Multiple active paths between stations can cause loops in the network. If a loop exists in the network topology, the potential exists for the duplication of messages. The spanning tree protocol is a link management protocol that provides path redundancy while preventing undesirable loops. For a wireless network to function properly, only one active path can exist between two stations.

To facilitate path redundancy, the spanning tree protocol defines a tree that spans all stations in the network and forces certain redundant data paths into a standby (blocked) state. If one segment in the spanning tree becomes unreachable, the spanning tree algorithm reconfigures the network topology and reestablishes the link by activating the standby path. The spanning tree function is transparent to client stations.



				WDS Client Links				WDS Host Links		
VLAN Name	Number	Gigabit 1	Gigabit 2	1	2	3	4	1	2	3
none		forwarding	forwarding	forwarding						
VLAN11	11	forwarding	forwarding	forwarding						

Figure 36. Spanning Tree Status

This window shows the spanning tree status (forwarding or blocked) for path segments that terminate on the Gigabit ports and WDS links of this WAP. You may sort the rows based on the **VLAN Name** or **Number** columns by clicking the column header. Click **Refresh** to update the information at any time. Click **Auto Refresh** to instruct the WAP to refresh this window automatically.

See Also

Network

Interfaces

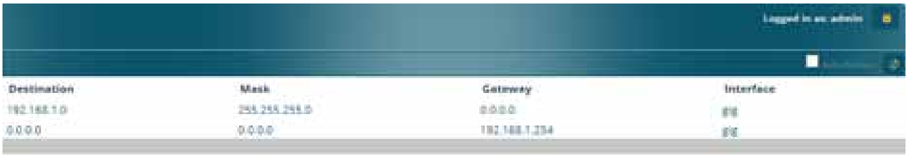
Network Status Windows

VLANs

WDS

Routing Table

This status-only window lists the entries in the WAP's routing table. The table provides the WAP with instructions for sending each packet to its next hop on its route across the network.



Destination	Mask	Gateway	Interface
192.168.1.0	255.255.255.0	0.0.0.0	[illegible]
0.0.0.0	0.0.0.0	192.168.1.254	[illegible]

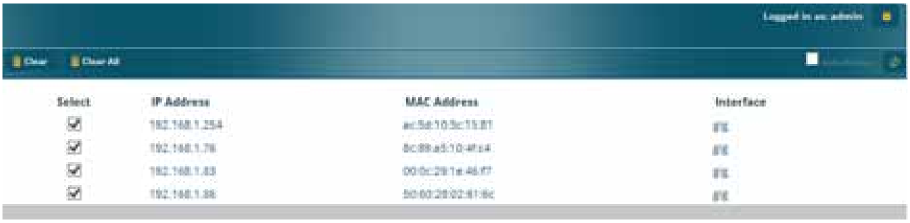
Figure 37. Routing Table

See Also

VLANs

ARP Table

This status-only window lists the entries in the WAP's ARP table. For a device with a given IP address, this table lists the device's MAC address. It also shows the WAP interface through which this device may be reached. The table typically includes devices that are on the same local area network segment as the WAP.



Select	IP Address	MAC Address	Interface
☑	192.168.1.254	ac:5d:10:3c:15:81	[illegible]
☑	192.168.1.76	8c:89:a5:10:4f:c4	[illegible]
☑	192.168.1.83	00:0c:29:1e:46:f7	[illegible]
☑	192.168.1.86	50:60:28:02:61:6c	[illegible]

Figure 38. ARP Table

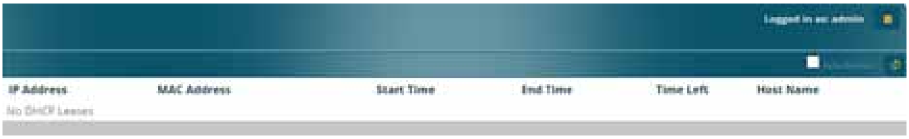
See Also

Routing Table

ARP Filtering

DHCP Leases

This status-only window lists the IP addresses (leases) that the WAP has allocated to client stations. For each, it shows the IP address assigned from one of the defined DHCP pools, and the MAC address and host name of the client station. The start and end time of the lease show how long the allocation is valid. The same IP address is normally renewed at the expiration of the current lease.



Logged in as: admin

□

IP Address	MAC Address	Start Time	End Time	Time Left	Host Name
No DHCP Leases					

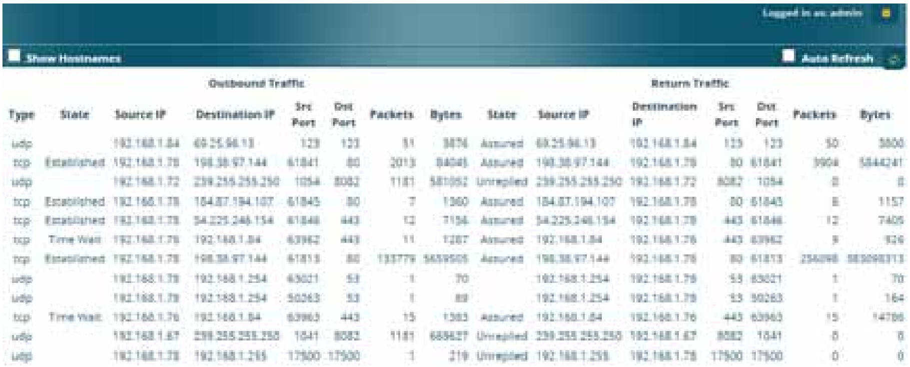
Figure 39. DHCP Leases

See Also

DHCP Server

Connection Tracking/NAT

This status-only window lists the session connections that have been created on behalf of clients. This table may also be used to view information about current NAT sessions.



Logged in as: admin

□ Show Hostnames

□ Auto Refresh

		Outbound Traffic						Return Traffic						
Type	State	Source IP	Destination IP	Src Port	Dst Port	Packets	Bytes	State	Source IP	Destination IP	Src Port	Dst Port	Packets	Bytes
udp		192.168.1.84	69.25.96.13	123	123	51	3876	Assured	69.25.96.13	192.168.1.84	123	123	50	3800
tcp	Established	192.168.1.78	198.38.97.144	61841	80	2013	84045	Assured	198.38.97.144	192.168.1.78	80	61841	3904	5844241
udp		192.168.1.72	239.255.255.250	1054	8082	1181	581052	Unreplied	239.255.255.250	192.168.1.72	8082	1054	0	0
tcp	Established	192.168.1.78	184.87.194.107	61845	80	7	1360	Assured	184.87.194.107	192.168.1.78	80	61845	8	1157
tcp	Established	192.168.1.78	54.225.246.154	61846	443	12	7136	Assured	54.225.246.154	192.168.1.78	443	61846	12	7405
tcp	Time Wait	192.168.1.78	192.168.1.84	63962	443	11	1287	Assured	192.168.1.84	192.168.1.78	443	63962	9	926
tcp	Established	192.168.1.78	198.38.97.144	61813	80	133779	5659505	Assured	198.38.97.144	192.168.1.78	80	61813	256098	383090313
udp		192.168.1.78	192.168.1.254	63021	53	1	70		192.168.1.254	192.168.1.78	53	63021	1	70
udp		192.168.1.78	192.168.1.254	50263	53	1	89		192.168.1.254	192.168.1.78	53	50263	1	164
tcp	Time Wait	192.168.1.78	192.168.1.84	63963	443	15	1383	Assured	192.168.1.84	192.168.1.78	443	63963	15	14786
udp		192.168.1.67	239.255.255.250	1041	8082	1181	688627	Unreplied	239.255.255.250	192.168.1.67	8082	1041	0	0
udp		192.168.1.78	192.168.1.255	17500	17500	1	219	Unreplied	192.168.1.255	192.168.1.78	17500	17500	0	0

Figure 40. Connection Tracking

Click the **Show Hostnames** checkbox at the top of the page to display name information (if any) for the source and destination location of the connection. The Hostname columns will replace traffic statistics columns.

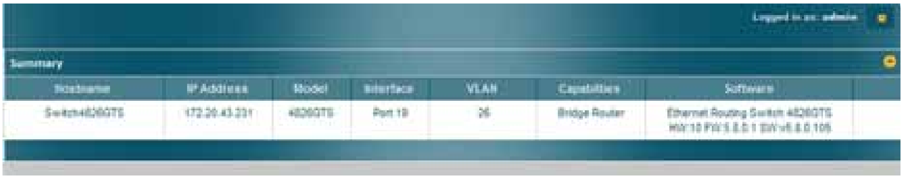
You may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon 👆. Click **Refresh** to update the information at any time. Click **Auto Refresh** to instruct the WAP to refresh this window automatically.

See Also

Filters

Fabric Attach List

This status-only window lists devices on the WAP's network that support the Link Layer Discovery Protocol (LLDP). This allows you to see Avaya switches that you are using to supply power and data to your WAPs.



Hostname	IP Address	Model	Interface	VLAN	Capabilities	Software
Switch4826GTS	172.20.43.231	4826GTS	Port 19	26	Bridge Router	Ethernet Routing Switch 4826GTS HW:10 FW:5.8.0.1 SW:v5.8.0.105

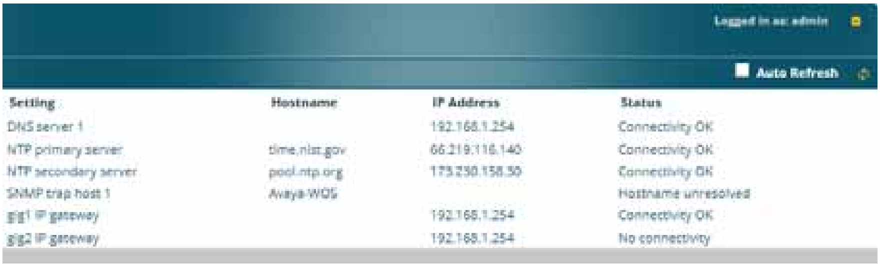
Figure 41. LLDP List

The WAP performs discovery on the network on an ongoing basis. This list shows the devices that have been discovered—devices on the network that have LLDP running. For each, it shows the device's host name, IP address, and model name, the device interface that is connected to the network (i.e., the port that was discovered), and the network capabilities of the device (switch, router, supported protocols, etc.).

LLDP must be enabled on the WAP in order to gather and display this information. For details and some restrictions, see "Fabric Attach Settings" on page 162.

Network Assurance

This status-only window shows the results of ongoing network assurance testing.



Setting	Hostname	IP Address	Status
DNS server 1		192.168.1.254	Connectivity OK
NTP primary server	time.nist.gov	66.219.116.140	Connectivity OK
NTP secondary server	pool.ntp.org	173.230.158.30	Connectivity OK
SNMP trap host 1	Avaya-WOS		Hostname unresolved
gig1 IP gateway		192.168.1.254	Connectivity OK
gig2 IP gateway		192.168.1.254	No connectivity

Figure 42. Network Assurance

The WAP checks connectivity to network servers that you have configured (for example, DNS and NTP servers) on an ongoing basis. For each server, this list shows the server's host name (if any), IP address, and status.

Network assurance must be enabled on the WAP in order to perform these connectivity tests and display this information. See "Management Control" on page 217.

See Also

Management Control

Undefined VLANs

This status-only window lists VLANs that are detected on the WAP's trunk ports (i.e., wired ports), but have not been configured on the WAP. See "VLANs" on page 191.

Undefined VLANs

None

Figure 43. Undefined VLANs

This feature alerts you to the fact that an 802.1Q trunk to the WAP has VLANs that are not being properly handled on the WAP. To reduce unnecessary traffic, only VLANs that are actually needed on the WAP should normally be on the trunk, e.g., the management VLAN and SSID VLANs. In some cases such as multicast forwarding for Apple Bonjour you may want to extend other VLANs to the WAP, in order to forward Bonjour or other multicast packets (see "Advanced Traffic Optimization" on page 295).

See Also

VLANs

RF Monitor Windows

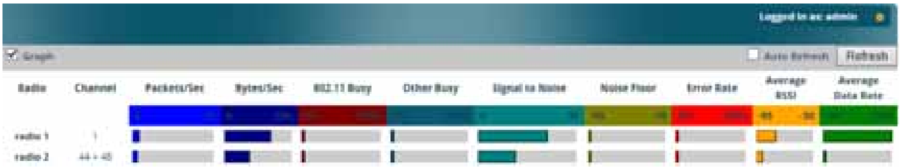
Every Wireless WAP includes an integrated RF spectrum analyzer as a standard feature. The spectrum analyzer allows you to characterize the RF environment by monitoring throughput, signal, noise, errors, and interference levels continually per channel. This capability uses the assigned threat-sensor (monitor) radio. The associated software is part of the Avaya OS.

The following RF Status windows are available:

- **Radio Monitoring**—displays current statistics and RF measurements for each of the WAP’s radios.
- **Spectrum Analyzer**—displays current statistics and RF measurements for each of the WAP’s channels.
- **Rogues**—displays rogue APs that have been detected by the WAP.
- **Channel History**—charts ongoing statistics and RF measurements for one selected channel over time.
- **Radio Assurance**—displays counts of types of problems that caused each radio to reset.

Radio Monitoring

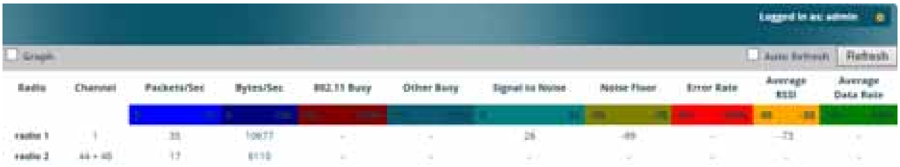
The RF Monitor—Radio Monitoring window displays traffic statistics and RF readings observed by each WAP radio. Note that the data is an instantaneous snapshot for the radio—it is not an average or a cumulative total. To graph these values over time for a particular channel, see “Channel History” on page 103. For detailed information on the measurements displayed, please see “Spectrum Analyzer Measurements” on page 100.



Radio	Channel	Packets/Sec	Bytes/Sec	802.11 Busy	Other Busy	Signal to Noise	Noise Floor	Error Rate	Average RSSI	Average Data Rate
radio 1	1									
radio 2	44 + 48									

Figure 44. RF Monitor—Radios

Figure 44 presents the data as a graphical display, enabled by selecting the **Graph** checkbox on the upper left. If this option is not selected, data is presented as a numerical table.



Radio	Channel	Packets/Sec	Bytes/Sec	802.11 Busy	Other Busy	Signal to Noise	Noise Floor	Error Rate	Average RSSI	Average Data Rate
radio 1	1	35	10677	-	-	26	-89	-	-73	-
radio 2	44 + 48	17	6110	-	-	-	-	-	-	-

Figure 45. RF Monitor—Radios

You may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon ☝. Click **Refresh** to update the information at any time. Click **Auto Refresh** to instruct the WAP to refresh this window automatically.

Spectrum Analyzer

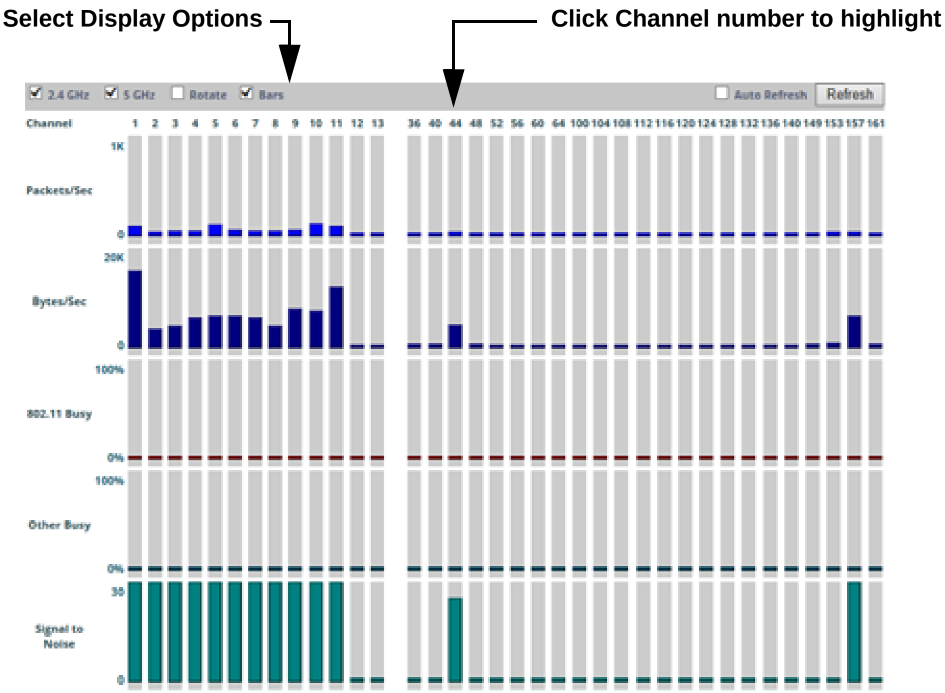
The RF measurements for this feature are obtained by the monitor radio. You ***must*** *have a radio set to* ***monitor*** *mode for any data to be available. See "Radio Settings" on page 284.*

Spectrum Analysis is only available for the WAO9122 WAP.

Spectrum analysis on Wireless WAPs is a distributed capability that automatically covers the entire wireless network, since a sensor is present in every unit. WAPs monitor the network 24/7 and analyze interference anywhere in the network from your desk. There's no need to walk around with a device as with traditional spectrum analyzers, thus you don't have to be in the right place to find outside sources that may cause network problems or pose a security threat. The WAP monitors all 802.11 radio bands (a/b/g/n), not just those currently used for data transmission.

The RF Spectrum Analyzer window displays instantaneous traffic statistics and RF readings for all channels, as measured by the WAP's monitor radio. This differs from the RF Monitor-Radio Monitoring window, which displays values measured by each radio for its current assigned channel. For the spectrum analyzer, the monitor radio is in a listen-only mode, scanning across all wireless channels. Each channel is scanned in sequence, for a 250 millisecond interval per channel. The spectrum analyzer window presents the data as a graphical display of vertical bar graphs for each statistic as shown in Figure 46 (the default presentation), or horizontally as bar graphs or numerical RF measurements. The measurements displayed are explained in "Spectrum Analyzer Measurements" on page 100.

As an aid to viewing data for a particular channel, click the channel number. The channel will be highlighted down the page (or across the page for a rotated view, in both text and graph modes). Click additional channels to highlight them for easy comparison. To remove the highlighting from a channel, click the channel number again. Click **Refresh** to update the information at any time. Click **Auto Refresh** to instruct the WAP to refresh this window automatically.



Select Display Options

Click Channel number to highlight

Figure 46. RF Spectrum Analyzer

The Spectrum Analyzer offers several display options:

- To display horizontal bar graphs, click the **Rotate** checkbox at the bottom of the data window.
- In the rotated view, if you wish to view data as a numerical table, click the **Text** checkbox. Click again to return to a graphical display. The text option is only available in the rotated view.
- When viewing a graphical display, click **Bars** to have the bar graphs displayed against a gray background—you may find this easier on the eyes. This operation is not available when Text is selected.
- You may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon ☝. Sorting is only available in the rotated view.

- At the bottom left of the frame, you may select whether to display only 2.4 GHz channels, 5 GHz channels, or both (the default is both). Note that the data is an instantaneous snapshot—it is not an average or a cumulative total.

Spectrum Analyzer Measurements

The spectrum analyzer displays the following information:

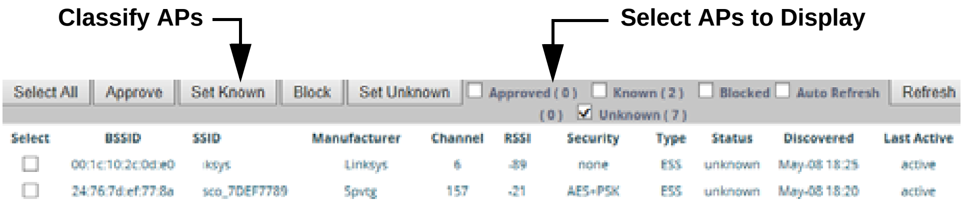
- **Packets/Sec:** Total number of wireless packets per second on the channel, both valid and errored packets.
- **Bytes/Sec:** Total number of wireless bytes per second on the channel, valid packets only.
- **802.11 Busy:** Percentage of time that 802.11 activity is seen on the channel.
- **Other Busy:** Percentage of time that the channel is unavailable due to non-802.11 activity.

  The total busy time (802.11 Busy plus Other Busy) will never total more than 100%. The remaining time (100% minus total busy time) is quiet time—the time that no activity was seen on the channel.
- **Signal to Noise:** Average SNR (signal to noise ratio) seen on the channel, calculated from the signal seen on valid 802.11 packets less the noise floor level. A dash value “**-**“means no SNR data was available for the interval.
- **Noise Floor:** Average noise floor reading seen on the channel (ambient noise). A dash value “**-**“means no noise data was available for the interval.
- **Error Rate:** Percentage of the total number of wireless packets seen on the channel that have CRC errors. The Error rate percentage may be high on some channels since the monitor radio is set to receive at a very sensitive level, enabling it to hear packets from devices at far distances.
- **Average RSSI:** Average RSSI level seen on 802.11 packets received on the channel. A dash value “**-**“means no RSSI data was available for the interval.
- **Average Data Rate:** Average data rate over time (per byte, not per packet) seen on 802.11 packets received on the channel. A dash value “**-**“means

no data rate information was available for the interval. A higher date rate (above 6 Mbps) typically indicates user data traffic on the channel. Otherwise, the data rate reflects control packets at the lower basic rates.

Rogues

This window displays all detected access points, according to the classifications you select from the checkboxes at the top—**Blocked**, **Unknown**, **Known**, or **Approved**. This includes ad hoc access points (station-to-station connections). For more information about intrusion detection, rogue APs, and blocking, please see “About Blocking Rogue APs” on page 346.



Classify APs

Select APs to Display

Select	BSSID	SSID	Manufacturer	Channel	RSSI	Security	Type	Status	Discovered	Last Active
□	00:1c:10:2c:0d:e0	iksys	Linksys	6	-89	none	ESS	unknown	May-08 18:25	active
□	24:76:7d:ef:77:8a	sco_7DEF7789	Spvtg	157	-21	AES+PSK	ESS	unknown	May-08 18:20	active

Figure 47. Intrusion Detection / Rogue AP List

The Intrusion Detection window provides the easiest method for classifying rogue APs as Blocked, Known, Approved, or Unknown. Choose one or more APs using the checkbox in the **Select** column, then use the buttons on the upper left to classify them with the following actions: **Approve**, **Set Known**, **Block**, or **Set Unknown**.

You can sort the results based on the following parameters by clicking the desired column header:

- SSID
- BSSID
- Manufacturer
- Channel
- RSSI
- Security
- Type
- Status
- Discovered
- Last Active

You can refresh the list at any time by clicking on the **Refresh** button, or click in the **Auto Refresh** check box to instruct the WAP to refresh the list automatically.

See Also

Network Map
Rogue Control List
SSIDs
SSID Management

Channel History

Channel History is only available for the WAO9122 WAP.

The RF Monitor—Channel History window focuses on traffic statistics and RF readings observed for just one channel that you select in the **Channel** field. A new set of readings is added every 10 seconds for a 5 GHz channel, or every 5 seconds for a 2.4 GHz channel. For descriptions of the measurements displayed, please see "Spectrum Analyzer Measurements" on page 100.

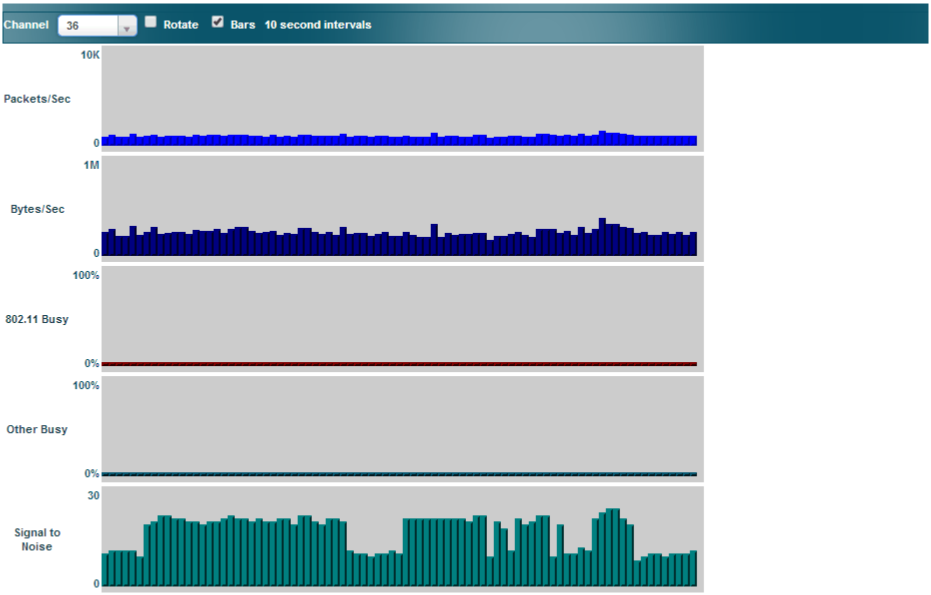
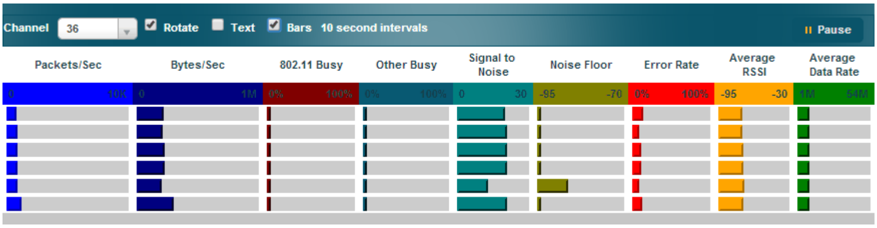


Figure 48. RF Monitor—Channel History

New data appears at the left, with older readings shifting to the right. To make the data appear as a bar chart, click the **Bar** checkbox which will shade the background.

You also have the option of clicking the **Rotate** checkbox to give each statistic its own column. In other words, the graph for each statistic will grow down the page as new readings display at the top.

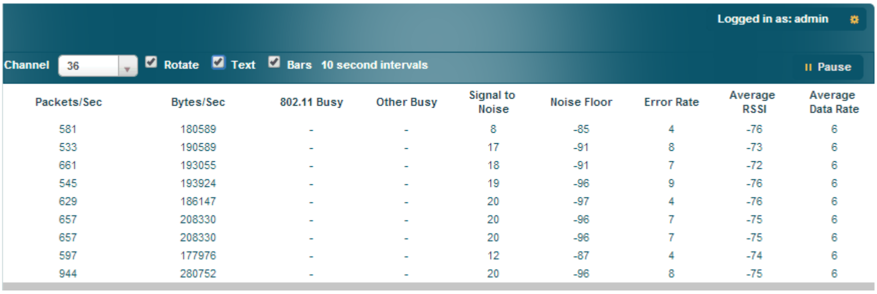


Channel 36 ☑ Rotate □ Text ☑ Bars 10 second intervals

Figure 49. RF Monitor—Channel History (Rotated)

If you select **Rotate** and **Text** together, data is presented as a numerical table.

Click **Pause** to stop collecting data, or **Resume** to continue.



Logged in as: admin

Channel 36 ☑ Rotate ☑ Text ☑ Bars 10 second intervals

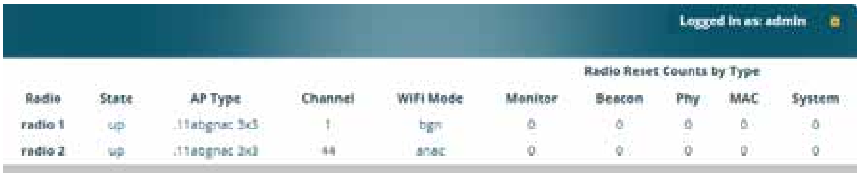
Packets/Sec	Bytes/Sec	802.11 Busy	Other Busy	Signal to Noise	Noise Floor	Error Rate	Average RSSI	Average Data Rate
581	180589	-	-	8	-85	4	-76	6
533	190589	-	-	17	-91	8	-73	6
661	193055	-	-	18	-91	7	-72	6
545	193924	-	-	19	-96	9	-76	6
629	186147	-	-	20	-97	4	-76	6
657	208330	-	-	20	-96	7	-75	6
657	208330	-	-	20	-96	7	-75	6
597	177976	-	-	12	-87	4	-74	6
944	280752	-	-	20	-96	8	-75	6

Figure 50. RF Monitor—Channel History (Text)

Radio Assurance

When Radio Assurance mode is enabled, the monitor radio performs loopback tests on the WAP’s radios. When problems are encountered, the WAP can take various actions to correct them by performing different levels of reset on the affected radio. This window shows which resets, if any, have been performed on which radios since the last reboot.

The WAP’s response to radio problems is controlled by the **Radio Assurance Mode** selected, as described in “RF Resilience” on page 331. If you have selected **Failure Alerts & Repairs** (with or without reboots), then the WAP can take corrective action if a problem is detected. Note that radio assurance requires RF Monitor Mode to be enabled in Advanced RF Settings to turn on self-monitoring functions. It also requires a radio to be set to monitoring mode. For a detailed discussion of the operation of this feature and the types of resets performed, see “Radio Assurance” on page 498.



					Radio Reset Counts by Type				
Radio	State	AP Type	Channel	WiFi Mode	Monitor	Beacon	Phy	MAC	System
radio 1	up	.11abgnac 3x3	1	bgn	0	0	0	0	0
radio 2	up	.11abgnac 3x3	44	anac	0	0	0	0	0

Figure 51. Radio Assurance

For each of the WAP’s radios, this window shows the radio’s state, its type (IEEE 802.11 type, and antenna type—2x2 or 3x3), the assigned channel, and the selected 802.11 wireless mode. To the right, the table shows counts for the number of times, if any, that radio assurance has performed each of the following types of resets since the last reboot, as described in Radio Assurance:

- Monitor
- Beacon
- Phy
- MAC
- System (i.e., reboot the WAP)

See Also

Radios

Avaya Advanced RF Analysis Manager (RAM)

RF Resilience

Radio Assurance

Station Status Windows

The following Station Status windows are available:

- **Stations**—this list describes all stations associated to the WAP.
- **Location Map**—displays a map showing the approximate locations of all stations associated to the WAP.
- **RSSI**—for each associated station, this displays the Received Signal Strength Indicator at each of the WAP's radios.
- **Signal-to-Noise Ratio (SNR)**—for each associated station, this displays the SNR at each of the WAP's radios.
- **Noise Floor**—for each associated station, this displays the ambient noise (silence) value at each of the WAP's radios.
- **Max by AP**—for each radio, this shows the historical maximum number of stations that have been associated to it over various periods of time.
- **Station Assurance**— displays stations that are having connectivity problems.

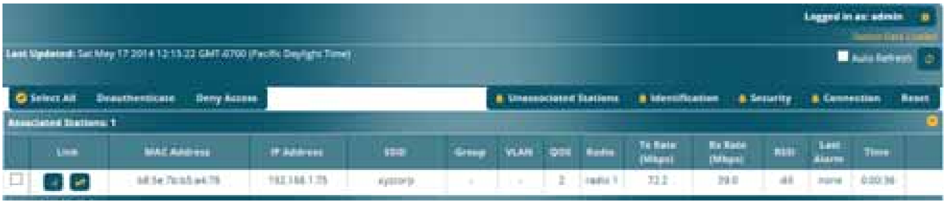
Stations

This window shows client stations currently visible to the WAP. You may choose to view only stations that have **Associated** to the WAP, or include stations that are **Unassociated** by selecting the appropriate buttons above the list. The list always shows the MAC address of each station, its IP address, the SSID used for the association, the Group (if any) that this station belongs to, its VLAN, its QoS, the radio used for the association, transmit and receive rates, the RSSI for each station, and how long each association has been active (up time).

In the Link column, click the details button .ıl to jump to a detailed statistics page for this station. Click ⇄ to see Application Control information.

You may click other buttons above the list to show a number of additional columns:

- **Identification**: shows more identifying information for the station—its **User Name, Host Name, Manufacturer, Device Type,** and **Device Class** (for example, notebook, iPad, etc.).
- **Security**: includes security settings used by the connection—**Encryption** type, **Cipher** used, and Key **Management** used by the station.
- **Connection Info**: shows the **Band** (5GHz or 2.4 GHz) used. Shows an additional RF measurement that affects the quality of the connection: **SNR** (signal to noise ratio).
- **Reset**: click this button to return the display to showing just the default columns.



Last Updated: Sat May 17 2014 12:15:22 GMT-0700 (Pacific Daylight Time)

Associated Stations: 1

	Link	MAC Address	IP Address	SSID	Group	VLAN	QOS	Radio	Tx Rate (Mbps)	Rx Rate (Mbps)	RSSI	Last Alarm	Time
□		b8:5e:7b:b5:a4:79	192.168.1.75	xyzcorp	-	-	2	radio 1	72.2	39.0	-48	none	0:00:36

Figure 52. Stations

You may sort the rows based on any column that has an active column header. Click again to reverse the sort order. You may select one or more specific stations and perform one of the following actions by clicking the associated button:

- **Deny Access:** Sends a de-authentication frame to the selected station and explicitly denies it access by adding its MAC address to the Deny List in the Access Control List window. To permit access again, go to "Access Control List" on page 227 and delete the station from the **Deny** list.
- **Deauthenticate:** Sends a de-authentication frame to the selected station. The station may re-authenticate.

Click on the **Refresh** button to refresh the station list, or click in the **Auto Refresh** check box to instruct the WAP to refresh this window automatically.

See Also

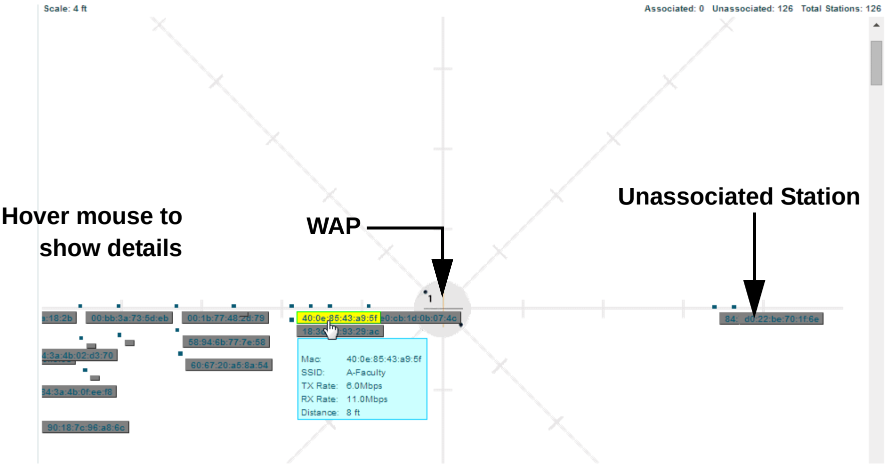
Access Control List

Station Status Windows

Station Statistics

Location Map

The Location Map shows the approximate locations of stations relative to this WAP. The location of each station is computed based on the RSSI of its signal as received by the WAP. The distance is adjusted based on the environment setting that you selected. You may display just the stations associated to this WAP, unassociated stations (shown in gray), or both. The station count is shown on the right, above the map. You may also choose to display only 5 GHz stations (shown in orange) or 2.4 GHz stations (shown in green), or both.



Scale: 4 ft

Associated: 0 Unassociated: 126 Total Stations: 126

Mac: 40:0e:85:43:a9:5f
SSID: A-Faculty
TX Rate: 6.0Mbps
RX Rate: 11.0Mbps
Distance: 8 ft

Figure 53. Location Map

The map and WAP are shown as if you were looking down on the WAP from above, say from a skylight on the roof. Thus the positions of the radios are a mirror image of the way they are typically drawn when looking at the face of the WAP. Radios are marked on the map to show the orientation of the WAP.

A station is identified by the type of **Preferred Label** that you select: **Netbios Name**, **IP Address**, **MAC Address**, or **Manufacturer**. If multiple stations are near each other, they will be displayed slightly offset so that one station does not completely obscure another. You may minimize a station that is not of interest by clicking it. There is also a **Minimize All** button.

You may replace the range-finder background image above with your own custom image of the floor plan of the area served by the WAP—see “Working with the Custom Image” on page 113

Hover the mouse over a station to show detailed information. For a station that is associated to this WAP, the details include:

- The **Radio, Channel**, and **SSID** to which the station is associated.
- The **MAC** and **IP** address and **Netbios** name of the station.
- The **TX Rate** and **RX Rate** of this connection.
- The approximate **Distance** of this station from the WAP. The distance is estimated using the received signal strength and your environment setting. The environment determines the typical signal attenuation due to walls and other construction that affect signal reception.

Controls and items displayed on the Location Map window

The Location Map has its own scroll bars in addition to the browser’s scroll bars. If you narrow the browser window, the map’s scroll bar may be hidden. Use the browser’s bottom scroll bar if you need to move it into view.

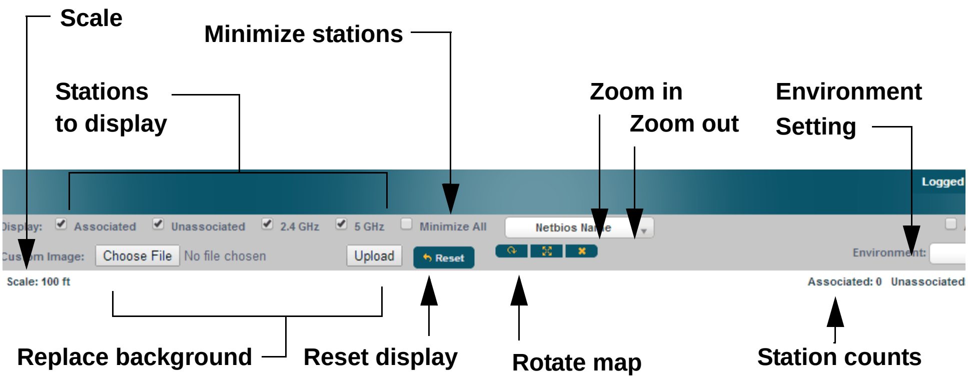


Figure 54. Controls for Location Map

- **Display Associated/Unassociated**: Select whether to display stations that are associated to the WAP, stations that are not associated, or both.

- **Display 2.4 GHz/5 GHz**: Select whether to display 802.11bgn stations, or 802.11an stations, or both.
- **Preferred Label**: This field is located on the top of the window towards the right. It shows the type of label to be displayed for stations: NetBIOS is the default, else, an IP or MAC address will be used, in that order.
- **Auto Refresh:** Instructs the WAP to refresh this window automatically.
- **Refresh:** Updates the stations displayed.

- **Custom Image**: Use this feature to replace the default background image with your own image of the floor plan of your location. Click the **Browse** button and browse to the desired file on your computer. This may be a .gif, .jpg, .jpeg., .png, .htm, or .html file. The scale of the file should be 100 feet per inch. Then click **Upload** (see below). For more information on using the custom, image, see "Working with the Custom Image" on page 113.
- **Upload**: After browsing to the desired custom image, click the **Upload** button to install it. The map is redisplayed with your new background. No hash marks (for the map scale) are added to the image display.
- **Reset**: Click this button to restore the map display to the factory settings. All attributes are restored—including the stations selected for display, the scale, the rotation, and the background map.
- **Rotate**: Click this button to rotate the orientation of the entire map. It rotates the map 45^0 counter-clockwise.
- **Enlarge**: Click this button to enlarge (zoom in on) the map. The displayed **Scale** is updated with the new scale for the map.
- **Reduce**: Click this button to reduce (zoom out on) the map. The displayed **Scale** is updated with the new scale for the map.
- **Environment**: This field is located on the top right of the window. Select the type of environment for this WAP's deployment: **Indoor open** (few walls or obstructions), **Indoor walled** (typical wall or cubicle construction), or **Indoor dense** (many walls or obstructions, or unusually dense walls).

- **Scale**: This view-only value shows the approximate distance represented by each hash mark on the default map background.
- **Associated**, **Unassociated**, **Total Stations**: These view-only values show the station counts observed by the WAP.

See Also

Station Status Windows

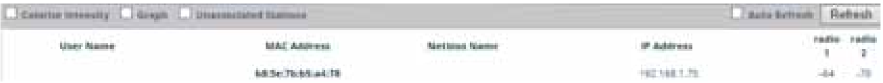
Working with the Custom Image

After you have uploaded a custom image (see **Custom Image** and **Upload** in "Controls and items displayed on the Location Map window" on page 111), you should move the display of the WAP on your map to correspond with its actual location at your site.

To move the WAP on the map, simply click it, then drag and drop it to the desired location. The WAP will continue to follow the mouse pointer to allow you to make further changes to its location. When you are satisfied with its location, click the WAP again to return to normal operation.

RSSI

For each station that is associated to the WAP, the RSSI (Received Signal Strength Indicator) window shows the station's RSSI value as measured by each radio. In other words, the window shows the strength of the station's signal at each radio. You may choose to display **Unassociated Stations** as well with a checkbox at the bottom of the window.



User Name	MAC Address	Netbios Name	IP Address	radio 1	radio 2
	68:5e:7b:b5:a4:78		192.168.1.75	-64	-78

Figure 55. Station RSSI Values

By default, the RSSI is displayed numerically. You may display the relative strength using color if you select **Colorize Intensity**, with the strongest signals indicated by the most intense color. (Figure 55) If you select **Graph**, then the RSSI is shown on a representation of the WAP, either colorized or numerically based on your selection. The stations are listed to the left of the WAP—click on a station to show its RSSI values on the WAP.

In either graphical or tabular view, you may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon ☝. Click on the **Refresh** button to refresh the station list, or click in the **Auto Refresh** check box to instruct the WAP to refresh this window automatically.

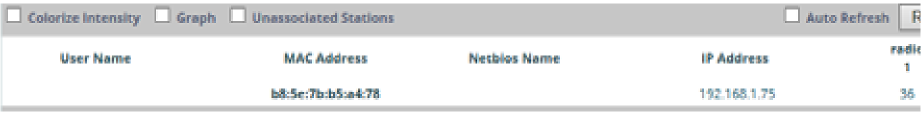
See Also

Station Status Windows

RF Monitor Windows

Signal-to-Noise Ratio (SNR)

For each station that is associated to the WAP, the Signal-to-Noise Ratio (SNR) window shows the station's SNR value as measured by each radio. In other words, the window shows the SNR of the station's signal at each radio. The signal-to-noise ratio can be very useful for determining the cause of poor performance at a station. A low value means that action may need to be taken to reduce sources of noise in the environment and/or improve the signal from the station.



□ Colorize Intensity □ Graph □ Unassociated Stations □ Auto Refresh R

User Name	MAC Address	Netbios Name	IP Address	radi 1
	b8:5e:7b:b5:a4:78		192.168.1.75	36

Figure 56. Station Signal-to-Noise Ratio Values

You may choose to display **Unassociated Stations** as well with a checkbox at the bottom of the window.

By default, the SNR is displayed numerically. (Figure 56) You may display the relative value using color if you select **Colorize Intensity**, with the highest SNR indicated by the most intense color. If you select **Graph**, then the SNR is shown on a representation of the WAP, either colorized or numerically based on your selection. The stations are listed to the left of the WAP—click on a station to show its SNR values on the WAP.

In either graphical or tabular view, you may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon 👆. Click on the **Refresh** button to refresh the station list, or click in the **Auto Refresh** check box to instruct the WAP to refresh this window automatically.

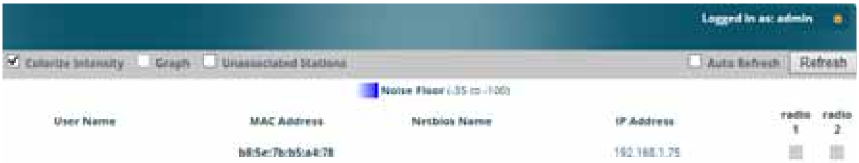
See Also

Station Status Windows

RF Monitor Windows

Noise Floor

For each station that is associated to the WAP, the Noise Floor window shows the ambient noise affecting a station's signal as measured by each radio. The noise floor is the RSSI value when the station is not transmitting, sometimes called a Silence value. In other words, the window shows the noise floor of the station's signal at each radio. The noise floor value can be very useful for characterizing the environment of a station to determine the cause of poor performance. A relatively high value means that action may need to be taken to reduce sources of noise in the environment.



User Name	MAC Address	Netbios Name	IP Address	radio 1	radio 2
	b8:5e:7b:b5:a4:78		192.168.1.75	▨	▨

Figure 57. Station Noise Floor Values

You may choose to display **Unassociated Stations** as well with a checkbox at the bottom of the window.

By default, the noise floor is displayed numerically. (Figure 57) You may display the relative value using color if you select **Colorize Intensity**, with the highest noise indicated by the most intense color. If you select **Graph**, then the ambient noise is shown on a representation of the WAP, either colorized or numerically based on your selection. The stations are listed to the left of the WAP—click on a station to show its values on the WAP.

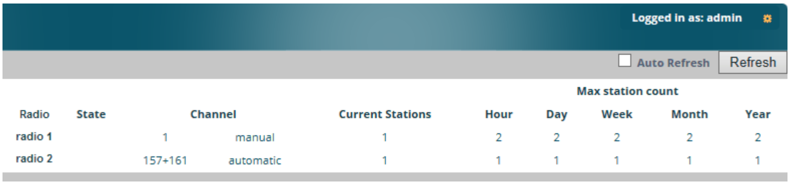
In either graphical or tabular view, you may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon 👆. Click on the **Refresh** button to refresh the station list, or click in the **Auto Refresh** check box to instruct the WAP to refresh this window automatically.

See Also

Station Status Windows
RF Monitor Windows

Max by AP

This status-only window shows the maximum number of client stations that have historically been associated to the WAP. For each radio, the list shows the radio's state and channel number, the current number of stations associated, and the highest number of stations that have been associated over various periods of time: hour, day, week, month, and year. In other words, the Max Station Count shows the "high water mark" over the selected period of time—the maximum count of stations for the selected period, rather than a cumulative count of all stations that have associated. This information aids in network administration and in planning for additional capacity.



					Max station count				
Radio	State	Channel		Current Stations	Hour	Day	Week	Month	Year
radio 1		1	manual	1	2	2	2	2	2
radio 2		157+161	automatic	1	1	1	1	1	1

Figure 58. Max by Radio

You may click a radio to go to the Radio Settings window. Click on the **Refresh** button to refresh the station list, or click **Auto Refresh** to instruct the WAP to refresh this window automatically.

See Also

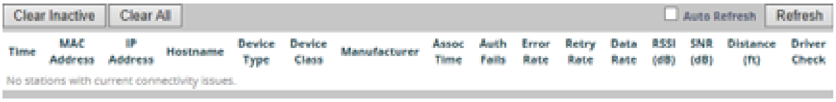
Radios

Station Status Windows

Station Assurance

Station assurance monitors the quality of the connections that users are experiencing on the wireless network. This window shows client stations that have had connectivity issues. You may enable or disable the station assurance feature and set thresholds for the problems that it checks, such as excessive packet retry or packet error rates, or stations that are unable to stay associated to the WAP. Please see "Station Assurance" on page 336 for more information about these settings. When the WAP detects that a station has reached the threshold value for one or more of the issues checked, it adds the station to this page. In addition, an event is triggered, a trap is generated, and a Syslog message is logged.

For each station, this list shows the MAC address, its IP address, its host name, its device type, device class, and manufacturer. It also shows the values of the various statistics that were monitored for problems as described in "Station Assurance" on page 336: associated time, authentication failures, packet error rate, packet retry rate, packet data rate, RSSI, signal to noise ratio (SNR), and distance.



Time	MAC Address	IP Address	Hostname	Device Type	Device Class	Manufacturer	Assoc Time	Auth Fails	Error Rate	Retry Rate	Data Rate	RSSI (dB)	SNR (dB)	Distance (ft)	Driver Check

No stations with current connectivity issues.

Figure 59. Station Assurance

You may click the **Clear Inactive** button to remove stations that are no longer connected to the WAP from the list. Click the **Clear All** button to remove all entries and start fresh to add problem stations to the list as they are detected. Click on the **Refresh** button to refresh the station list, or click **Auto Refresh** to instruct the WAP to refresh this window automatically.

See Also

Radios

Station Status Windows

Station Assurance

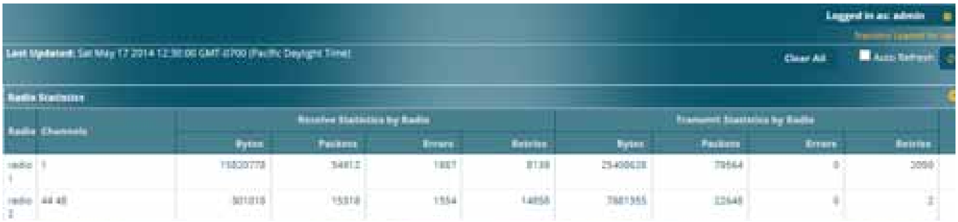
Statistics Windows

The following WAP Statistics windows are available:

- **Radio Statistics Summary**—provides an overview of the statistical data associated with all radios. Expands to show links for displaying detailed statistics for individual radios.
- **Per-Radio Statistics**—provides detailed statistics for an individual radio.
- **Network Statistics**—displays statistical data associated with each network (Ethernet) interface.
- **VLAN Statistics**—provides statistical data associated with your assigned VLANs.
- **WDS Statistics**—provides statistical data for all WDS client and host links.
- **IDS Statistics**—provides statistical data for intrusion detection.
- **Filter Statistics**—provides statistical data for all configured filters.
- **Station Statistics**—provides statistical data associated with each station.

Radio Statistics Summary

This is a status only window that provides an overview of the statistical data associated with all radios. It also shows the channel used by each radio. For detailed statistics for a specific radio, see "Per-Radio Statistics" on page 120. Click the **Unicast Stats Only** checkbox on the lower left to filter the results, or clear the checkbox to show statistics for all wireless traffic.



Last Updated: Sat May 17 2014 12:30:00 GMT-0700 (Pacific Daylight Time)

Radio Statistics

Radio	Channels	Receive Statistics by Radio				Transmit Statistics by Radio			
		Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
radio 1	1	15020778	34812	1807	8138	25400628	79564	0	2098
radio 2	44 48	501018	15318	1554	14858	7881355	22648	0	2

Figure 60. Radio Statistics Summary Page

You can **Refresh** the data (update the window with the latest information) or **Clear** the data (reset all content to zero and begin counting again) at any time by clicking on the appropriate button. You can also click in the **Auto Refresh** check box to instruct the WAP to refresh this window automatically.

See Also

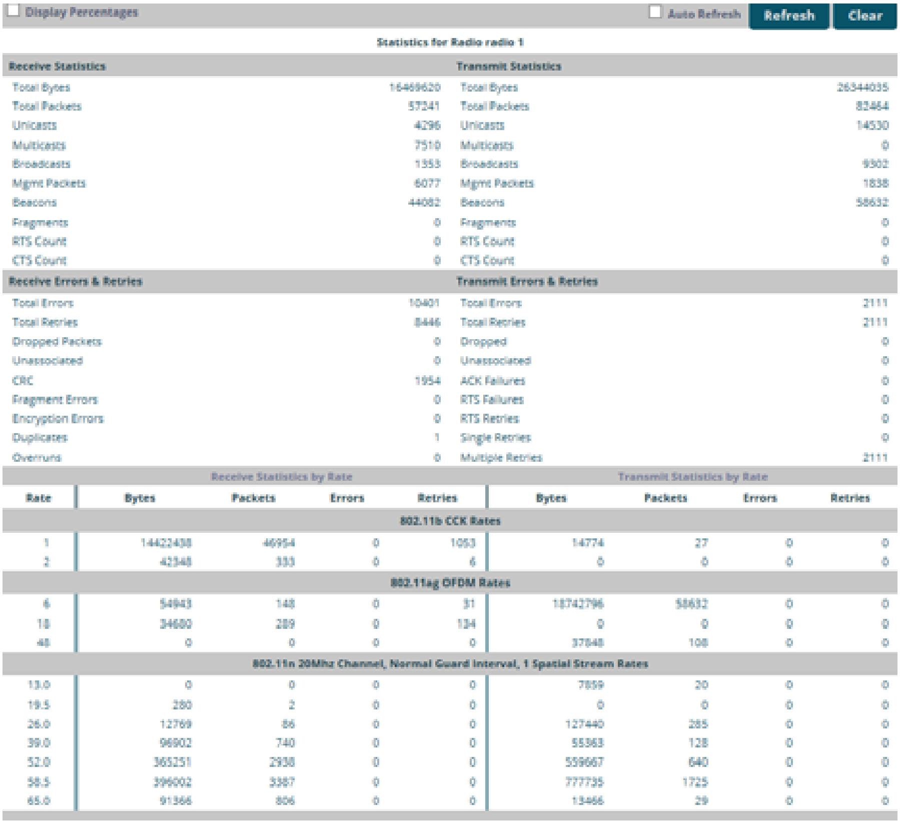
System Log Window
Global Settings
Global Settings .11an
Global Settings .11bgn
Radios

Per-Radio Statistics

This is a status only window that provides detailed statistics for the selected radio. Scroll the window down to see a breakout of the statistics by connection rate. For a summary of statistics for all radios, see "Radio Statistics Summary" on page 119. Use the **Display Percentages** checkbox at the upper left to select the output format—check this option to express each statistic as a percentage of the total at the top of the column, or leave it blank to display raw numbers.

Receive Error statistics include:

- **Total Retries**: the count of packets that were sent more than once before being received correctly.
- **CRC error**: the count of packets that were corrupted on the air and were dropped. Some level of CRC errors are expected in wireless networks. Note that all radios operate in a mode where they are listening to everything all the time, which means they will see many CRC errors.
- **Fragment Errors**: the count of packets that were incomplete.
- **Encryption Errors:** the count of packets that had encryption problems.
- **Duplicates**: the count of packets that were received more than once. The duplicate packets are dropped.
- **Dropped Packets**: the count of packets that were dropped due to various receive errors, including being received when all receive queues were full. These packets are dropped after being received.
- **Overruns**: indicate the number of times that First-In-First-Out (FIFO) overflow errors occur.



Statistics for Radio radio 1

Receive Statistics		Transmit Statistics	
Total Bytes	16469620	Total Bytes	26344035
Total Packets	57241	Total Packets	82464
Unicasts	4296	Unicasts	14530
Multicasts	7510	Multicasts	0
Broadcasts	1353	Broadcasts	9302
Mgmt Packets	6077	Mgmt Packets	1838
Beacons	44082	Beacons	58632
Fragments	0	Fragments	0
RTS Count	0	RTS Count	0
CTS Count	0	CTS Count	0
Receive Errors & Retries		**Transmit Errors & Retries**	
Total Errors	10401	Total Errors	2111
Total Retries	8446	Total Retries	2111
Dropped Packets	0	Dropped	0
Unassociated	0	Unassociated	0
CRC	1954	ACK Failures	0
Fragment Errors	0	RTS Failures	0
Encryption Errors	0	RTS Retries	0
Duplicates	1	Single Retries	0
Overruns	0	Multiple Retries	2111

	Receive Statistics by Rate				Transmit Statistics by Rate			
Rate	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
802.11b CCK Rates								
1	14422438	46954	0	1053	14774	27	0	0
2	42348	333	0	6	0	0	0	0
802.11ag OFDM Rates								
6	54943	148	0	31	18742796	58632	0	0
18	34600	289	0	134	0	0	0	0
48	0	0	0	0	37848	108	0	0
802.11n 20Mhz Channel, Normal Guard Interval, 1 Spatial Stream Rates								
13.0	0	0	0	0	7859	20	0	0
19.5	280	2	0	0	0	0	0	0
26.0	12769	86	0	0	127440	285	0	0
39.0	96902	740	0	0	55363	128	0	0
52.0	365251	2938	0	0	559667	640	0	0
58.5	396002	3387	0	0	777735	1725	0	0
65.0	91366	806	0	0	13466	29	0	0

Figure 61. Individual Radio Statistics Page

You can **Refresh** the data (update the window with the latest information) or **Clear** the data (reset all content to zero and begin counting again) at any time by clicking on the appropriate button. You can also click in the **Auto Refresh** check box to instruct the WAP to refresh this window automatically.

See Also

System Log Window

Global Settings

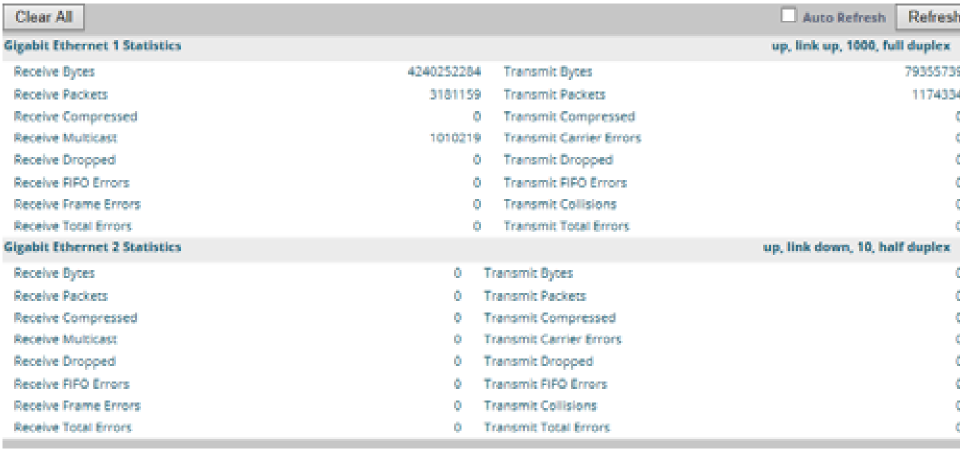
Global Settings .11an

Global Settings .11bgn

Radios

Network Statistics

This is a status only window that allows you to review statistical data associated with each network (Ethernet) interface and its activity. You can **Refresh** the data (update the window with the latest information) or **Clear** the data (reset all content to zero and begin counting again) at any time by clicking on the appropriate button. You can also click in the **Auto Refresh** check box to instruct the WAP to refresh this window automatically. If you are experiencing problems on the WAP, you may also want to print this window for your records



Gigabit Ethernet 1 Statistics			**up, link up, 1000, full duplex**
Receive Bytes	4240252284	Transmit Bytes	7935573
Receive Packets	3181159	Transmit Packets	1174334
Receive Compressed	0	Transmit Compressed	0
Receive Multicast	1010219	Transmit Carrier Errors	0
Receive Dropped	0	Transmit Dropped	0
Receive FIFO Errors	0	Transmit FIFO Errors	0
Receive Frame Errors	0	Transmit Collisions	0
Receive Total Errors	0	Transmit Total Errors	0
Gigabit Ethernet 2 Statistics			**up, link down, 10, half duplex**
Receive Bytes	0	Transmit Bytes	0
Receive Packets	0	Transmit Packets	0
Receive Compressed	0	Transmit Compressed	0
Receive Multicast	0	Transmit Carrier Errors	0
Receive Dropped	0	Transmit Dropped	0
Receive FIFO Errors	0	Transmit FIFO Errors	0
Receive Frame Errors	0	Transmit Collisions	0
Receive Total Errors	0	Transmit Total Errors	0

Figure 62. Network Statistics

See Also

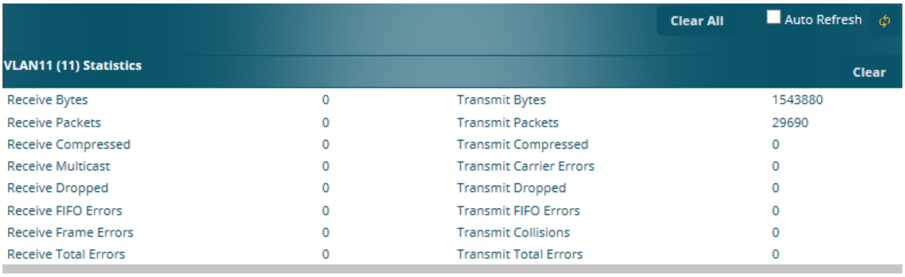
DHCP Server

DNS Settings

Network Interfaces

VLAN Statistics

This is a status only window that allows you to review statistical data associated with your assigned VLANs. You can refresh the information that is displayed on this page at any time by clicking on the **Refresh** button, or select the **Auto Refresh** option for this window to refresh automatically. The **Clear All** button at the lower left allows you to clear (zero out) all VLAN statistics.



VLAN11 (11) Statistics

Receive Bytes	0	Transmit Bytes	1543880
Receive Packets	0	Transmit Packets	29690
Receive Compressed	0	Transmit Compressed	0
Receive Multicast	0	Transmit Carrier Errors	0
Receive Dropped	0	Transmit Dropped	0
Receive FIFO Errors	0	Transmit FIFO Errors	0
Receive Frame Errors	0	Transmit Collisions	0
Receive Total Errors	0	Transmit Total Errors	0

Figure 63. VLAN Statistics

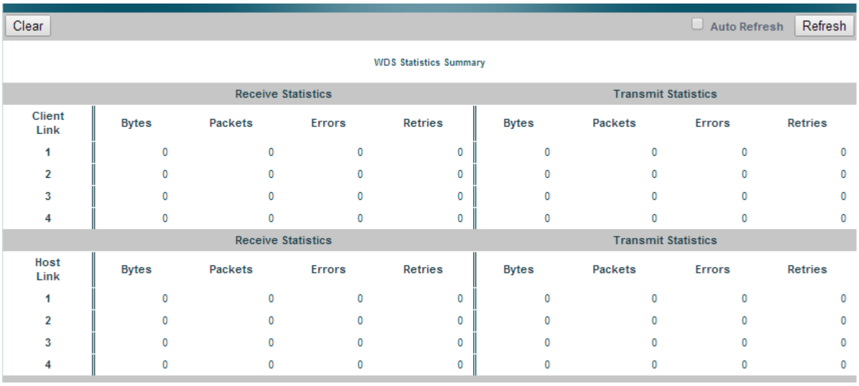
See Also

VLAN Management

VLANs

WDS Statistics

The main WDS Statistics window provides statistical data for all WDS client and host links. To access data about a specific WDS client or host link, simply click on the desired link in the left frame to access the appropriate window. You may also choose to view a sum of the statistics for all client links, all host links, or all links (both client and host links).



WDS Statistics Summary

	Receive Statistics				Transmit Statistics			
Client Link	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0

	Receive Statistics				Transmit Statistics			
Host Link	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0

Figure 64. WDS Statistics

See Also

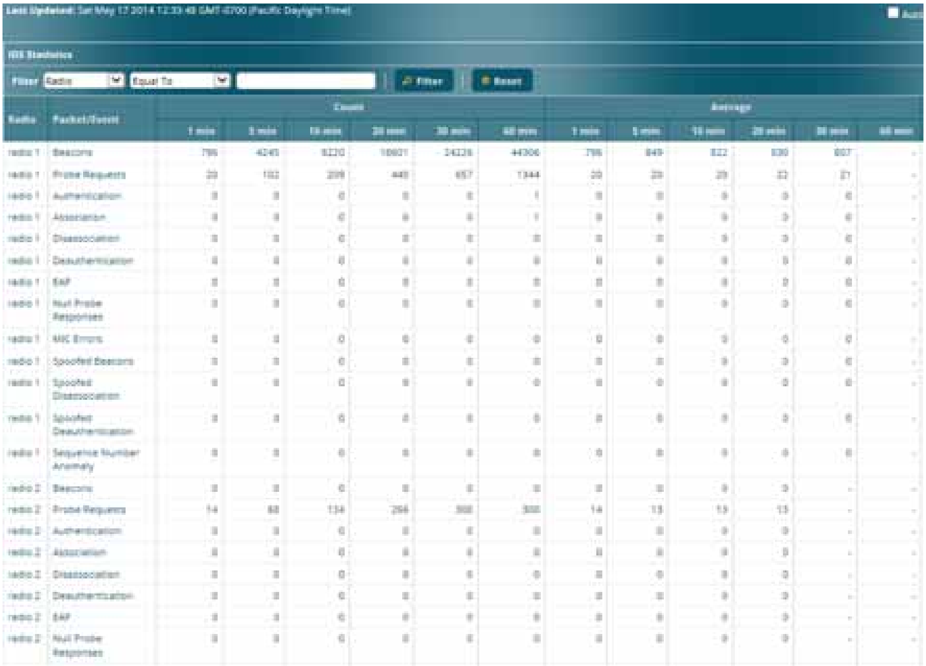
SSID Management

WDS

IDS Statistics

The WAP employs a number of IDS/IPS (Intrusion Detection System/Intrusion Prevention System) strategies to detect and prevent malicious attacks on the wireless network. This status-only window provides detailed intrusion detection statistics for the selected radio.

You must have **Intrusion Detection Mode** enabled to collect IDS statistics. See “Intrusion Detection” on page 343. Information about IDS events is discussed in the “IDS Event Log Window” on page 138.



Last Updated: Sat May 17 2014 12:33:40 GMT-0700 (Pacific Daylight Time) ☐ Auto

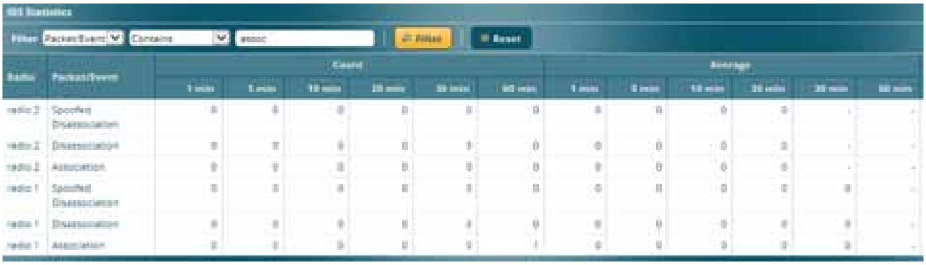
IDS Statistics

Filter: Radio | Equal To | [ ] | Filter | Reset

Radio	Packet/Event	Count						Average					
		1 min	5 min	10 min	20 min	30 min	60 min	1 min	5 min	10 min	20 min	30 min	60 min
radio 1	Beacons	795	4245	8220	16601	24226	44306	795	849	822	830	807	-
radio 1	Probe Requests	23	102	209	440	657	1344	23	20	20	22	21	-
radio 1	Authentication	0	0	0	0	0	1	0	0	0	0	0	-
radio 1	Association	0	0	0	0	0	1	0	0	0	0	0	-
radio 1	Disassociation	0	0	0	0	0	0	0	0	0	0	0	-
radio 1	Deauthentication	0	0	0	0	0	0	0	0	0	0	0	-
radio 1	EAP	0	0	0	0	0	0	0	0	0	0	0	-
radio 1	Null Probe Responses	0	0	0	0	0	0	0	0	0	0	0	-
radio 1	MIC Errors	0	0	0	0	0	0	0	0	0	0	0	-
radio 1	Spoofed Beacons	0	0	0	0	0	0	0	0	0	0	0	-
radio 1	Spoofed Disassociation	0	0	0	0	0	0	0	0	0	0	0	-
radio 1	Spoofed Deauthentication	0	0	0	0	0	0	0	0	0	0	0	-
radio 1	Sequence Number Anomaly	0	0	0	0	0	0	0	0	0	0	0	-
radio 2	Beacons	0	0	0	0	0	0	0	0	0	0	-	-
radio 2	Probe Requests	14	68	134	264	300	300	14	13	13	13	-	-
radio 2	Authentication	0	0	0	0	0	0	0	0	0	0	-	-
radio 2	Association	0	0	0	0	0	0	0	0	0	0	-	-
radio 2	Disassociation	0	0	0	0	0	0	0	0	0	0	-	-
radio 2	Deauthentication	0	0	0	0	0	0	0	0	0	0	-	-
radio 2	EAP	0	0	0	0	0	0	0	0	0	0	-	-
radio 2	Null Probe Responses	0	0	0	0	0	0	0	0	0	0	-	-

Figure 65. IDS Statistics Page

Use the filter feature to show only information for a selected radio or for selected event types. Select the type of **Filter**: **Radio** to select radios, or **Packet/Event** to select particular attack types. Select the type of string matching, for example, **Begins with** or **Contains**. Then enter the string to be matched and click the **Filter** button.



Radio	Packet/Event	Count						Average					
		1 min	5 mins	10 mins	20 mins	30 mins	60 mins	1 min	5 mins	10 mins	20 mins	30 mins	60 mins
radio 2	Spoofed Disassociation	0	0	0	0	0	0	0	0	0	0	-	-
radio 2	Disassociation	0	0	0	0	0	0	0	0	0	0	-	-
radio 2	Association	0	0	0	0	0	0	0	0	0	0	-	-
radio 1	Spoofed Disassociation	0	0	0	0	0	0	0	0	0	0	0	-
radio 1	Disassociation	0	0	0	0	0	0	0	0	0	0	0	-
radio 1	Association	0	0	0	0	0	1	0	0	0	0	0	-

Figure 66. Filtered IDS Statistics

Many of the column headers may be clicked to sort the entries in ascending or descending order based on that column. You can **Refresh** the data (update the window with the latest information) at any time by clicking the **Refresh** button ⟳ on the upper right. You can also click in the **Auto Refresh** check box to instruct the WAP to refresh this window automatically.

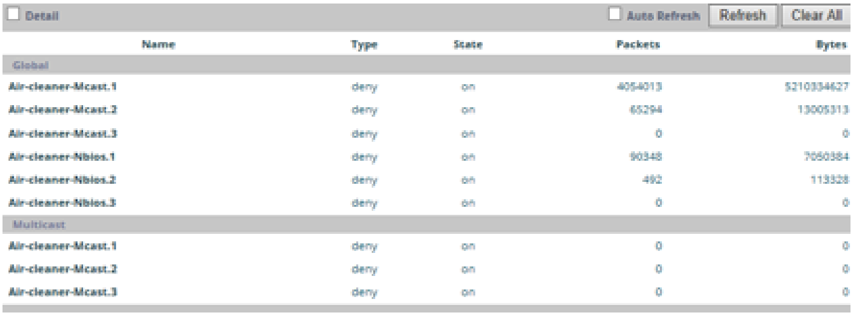
See Also

Intrusion Detection

IDS Event Log Window

Filter Statistics

The Filter Statistics window provides statistical data for all configured filters. The name, state (enabled—on or off), and type (allow or deny) of each filter is shown. For enabled filters, this window shows the number of packets and bytes that met the filter criteria. Click on a column header to sort the rows based on that column. Click on a filter name to edit the filter settings.



Name	Type	State	Packets	Bytes
Global				
Air-cleaner-Mcast.1	deny	on	4054013	5210334627
Air-cleaner-Mcast.2	deny	on	65294	13005313
Air-cleaner-Mcast.3	deny	on	0	0
Air-cleaner-Nbios.1	deny	on	90348	7060384
Air-cleaner-Nbios.2	deny	on	492	113328
Air-cleaner-Nbios.3	deny	on	0	0
Multicast				
Air-cleaner-Mcast.1	deny	on	0	0
Air-cleaner-Mcast.2	deny	on	0	0
Air-cleaner-Mcast.3	deny	on	0	0

Figure 67. Filter Statistics

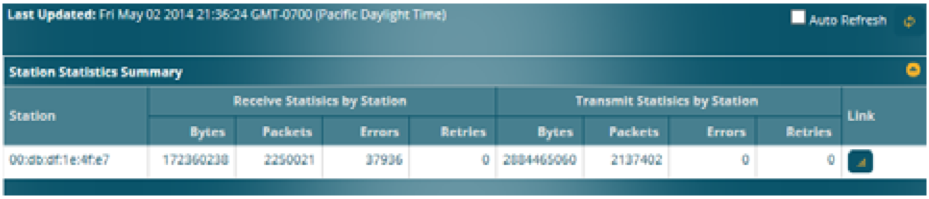
See Also

Filters

Application Control Windows

Station Statistics

This status-only window provides an overview of statistical data for all stations. Stations are listed by MAC address, and Receive and Transmit statistics are summarized for each. For detailed statistics for a specific station, click the desired MAC address in the **Station** column or click the details button 📶 in the station's **Link** column, and see "Per-Station Statistics" on page 129.


Last Updated: Fri May 02 2014 21:36:24 GMT-0700 (Pacific Daylight Time)

Station Statistics Summary

Station	Receive Statisics by Station				Transmit Statisics by Station				Link
	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries	
00:db:df:1e:4f:e7	172360238	2250021	37936	0	2884465060	2137402	0	0	📶

Figure 68. Station Statistics

Click on a column header to sort the rows based on that column. You can **Refresh** the data (update the window with the latest information) at any time by clicking the refresh button ↻ . You can also click in the **Auto Refresh** check box to instruct the WAP to refresh this window automatically.

See Also

Per-Station Statistics

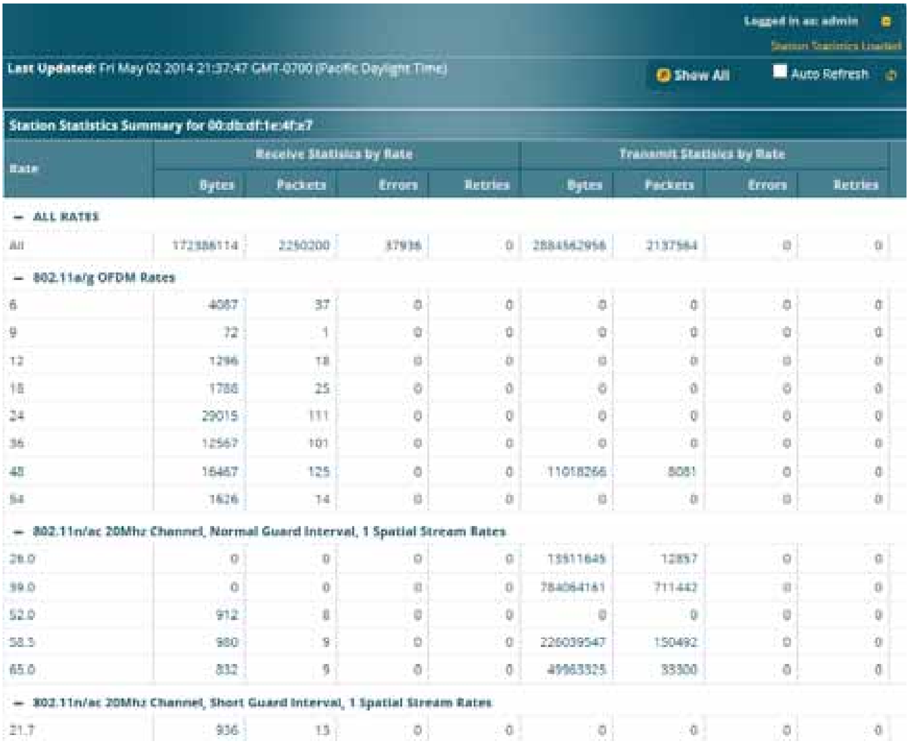
Stations

Per-Station Statistics

This window provides detailed statistics for the selected station. This window is accessed from the Station Statistics window—click the MAC address of the desired entry in the **Station** column to display its Per-Station Statistics window.

Receive and Transmit statistics are listed by **Rate**—this is the data rate in Mbps. For a summary of statistics for all stations, see "Station Statistics" on page 127.

You can **Refresh** the data (update the window with the latest information) at any time by clicking on the appropriate button. You can also click in the **Auto Refresh** check box to instruct the WAP to refresh this window automatically.



Last Updated: Fri May 02 2014 21:37:47 GMT-0700 (Pacific Daylight Time)

Station Statistics Summary for 00:db:df:1e:4f:e7

Rate	Receive Statistics by Rate				Transmit Statistics by Rate			
	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
− ALL RATES								
All	172386114	2250200	37936	0	2884562956	2137564	0	0
− 802.11a/g OFDM Rates								
6	4067	37	0	0	0	0	0	0
9	72	1	0	0	0	0	0	0
12	1296	18	0	0	0	0	0	0
18	1788	25	0	0	0	0	0	0
24	29015	111	0	0	0	0	0	0
36	12567	101	0	0	0	0	0	0
48	16467	125	0	0	11018266	8081	0	0
54	1626	14	0	0	0	0	0	0
− 802.11n/ac 20Mhz Channel, Normal Guard Interval, 1 Spatial Stream Rates								
26.0	0	0	0	0	13511645	12857	0	0
39.0	0	0	0	0	784064161	711442	0	0
52.0	912	8	0	0	0	0	0	0
58.5	980	9	0	0	226039547	150492	0	0
65.0	832	9	0	0	49963325	33300	0	0
− 802.11n/ac 20Mhz Channel, Short Guard Interval, 1 Spatial Stream Rates								
21.7	936	13	0	0	0	0	0	0

Figure 69. Individual Station Statistics Page

See Also

Station Statistics

Application Control Windows

This feature is only available if the WAP license includes ***Application Control****. See “Licensing” on page 61.*

The Application Control feature provides real-time visibility of application usage by users across the wireless network. Network usage has changed enormously in the last few years, with the increase in smart phone and tablet usage stressing networks. Increasing traffic from legitimate business needs such as cloud- and web-based applications, streaming media and VoIP must be handled with an adequate quality of experience.

Application Control is discussed in the following topics:

- **About Application Control**—an overview of this feature.
- **Application Control**—displays information about applications running on the wireless network.
- **Stations (Application Control)**—displays a list of stations. Click one to analyze application control information for only that station.

About Application Control

The WAP uses Deep Packet Inspection (DPI) to determine what applications are being used and by whom, and how much bandwidth they are consuming. These applications are rated by their degree of risk and productiveness. Filters can be used to implement per-application policies that keep network usage focused on productive uses:

- Usage of non-productive and risky applications like BitTorrent can be restricted using Filters.
- Traffic for mission-critical applications like VoIP and Scopia may be given higher priority (QoS).
- Non- critical traffic from applications like YouTube may be given lower priority (QoS).
- Traffic flows for specific applications may be controlled by sending them into VLANs that are designated for that type of traffic.

Application Control can track application usage over time to monitor trends. Usage may be tracked by WAP, VLAN, or station. Many hundreds of applications are recognized and grouped into a number of categories. The distributed architecture of WAPs allows Application Control to scale naturally as you grow the network.

About Risk and Productivity

Application Control ranks applications in terms of their levels of risk and productivity.

Productivity indicates how appropriate an application is for business purposes. The higher the rating number, the more business-oriented an application is.

- 1—Primarily recreational
- 2—Mostly recreational
- 3—Combination of business and recreational purposes
- 4—Mainly used for business
- 5—Primarily used for business

Risk indicates how likely an application is to pose a threat to the security of your network. The higher the rating number, the more risky an application is.

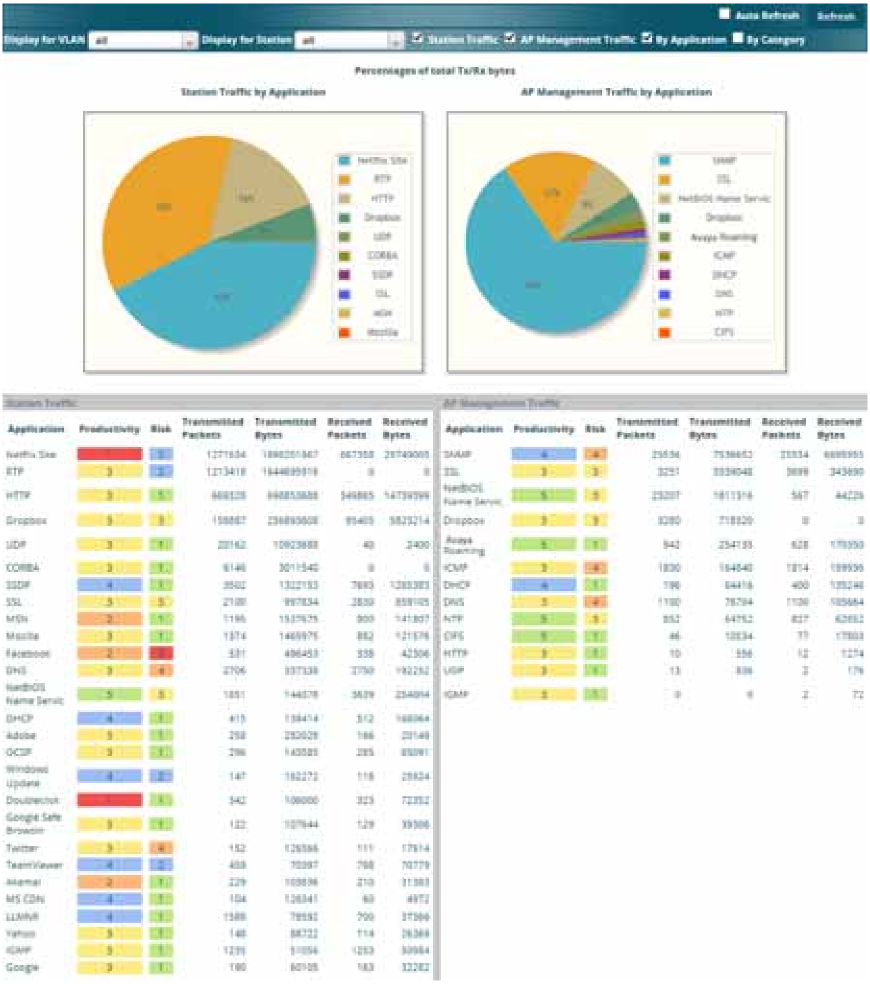
- 1—No threat
- 2—Minimal threat
- 3—Some risk - may be misused
- 4—High risk - may be malware or allow data leaks
- 5—Very high risk - threat circumvents firewalls or avoids detection

Keeping Application Control Current

Applications are recognized using a signature file which may be updated using the System Tools page as new applications become popular (see "Application Control Signature File Management" on page 393).

Application Control

This display-only window provides a snapshot of the application usage on your WAP. In order to view the Application Control window, the WAP must have a license that supports this feature, and you must have enabled the **Application Control** option on the **Filter Lists** page (see “Filter Lists” on page 364).



Station Traffic

Application	Productivity	Risk	Transmitted Packets	Transmitted Bytes	Received Packets	Received Bytes
Netflix Site	1	2	1271634	1890201867	667358	29749005
RTP	3	2	1213418	1844695919	0	0
HTTP	3	1	668528	846853688	349865	14739599
Dropbox	3	3	158887	236893608	95405	5825214
UDP	3	1	20162	10923888	40	2400
CORBA	3	1	6146	3011540	0	0
SSDP	4	1	3502	1322153	7693	1283383
SSL	3	3	2100	997834	2839	859105
MSN	2	1	1195	1537675	900	141807
Mozilla	3	1	1374	1465975	882	121576
Facebook	2	5	531	406453	338	42306
DNS	3	4	2706	337338	2750	192252
NetBIOS Name Servic	5	3	1851	144078	3629	234094
DHCP	4	1	415	138414	312	168064
Adobe	3	1	258	252028	166	20148
OCSP	3	1	296	143583	285	85091
Windows Update	4	2	147	182272	118	28924
Doubleclick	1	1	342	108000	323	72352
Google Safe Browsin	3	1	122	107644	129	39306
Twitter	3	4	152	126566	111	17614
TeamViewer	4	2	459	70397	798	70779
Akamai	2	1	229	103636	210	31383
MS CDN	4	1	104	126341	60	4972
LLMNR	4	1	1589	79592	700	37366
Yahoo	3	1	148	88722	114	26369
IGMP	3	1	1235	51056	1253	50984
Google	3	1	180	60105	163	32282

AP Management Traffic

Application	Productivity	Risk	Transmitted Packets	Transmitted Bytes	Received Packets	Received Bytes
SNMP	4	4	23536	7536652	23334	6695955
SSL	3	3	3251	3339048	3699	343690
NetBIOS Name Servic	5	3	25207	1811316	567	44226
Dropbox	3	3	3280	718320	0	0
Avaya Roaming	5	1	942	254135	628	170350
ICMP	3	4	1830	164640	1814	159936
DHCP	4	1	196	64416	400	135246
DNS	3	4	1100	78794	1120	105664
NTP	5	3	852	64752	827	62852
CIFS	5	1	46	10034	77	17803
HTTP	3	1	10	556	12	1274
UDP	3	1	13	836	2	176
IGMP	3	1	0	0	2	72

Figure 70. Application Control

The Application Control window has three sections:

- **Selection Criteria** allow you to choose the type of data to show, and to filter for a single VLAN or station.
- **Pie Charts** present a color coded at-a-glance view of the top ten applications being used by the network.
- **Traffic Tables** beneath the pie charts list the applications in use along with traffic statistics. Unique **Productivity** and **Risk** ratings let you easily assess the nature of applications in use, so that you can take action using Filter Management.

Selection Criteria

At the top of the window, the options in the gray ribbon allow you to customize the display with the following choices:

- **Display for VLAN**: Use the drop-down list if you wish to select just one VLAN to analyze, or leave the default value of **all** to see data from all VLANs.
- **Display for Station**: Use the drop-down list if you wish to select just one station to analyze (stations are listed by their MAC address), or leave the default value of **all** to see data from all stations. You may also use the Stations window to select a station to display. See "Stations (Application Control)" on page 136.
- **Station Traffic**: Check this box if you wish to analyze traffic from stations, listing the applications that they are using.
- **WAP Management Traffic**: Check this box if you wish to analyze management traffic on this WAP, including the load due to functions such as Avaya Roaming. Tracking traffic into the WAP on the management side can alert you to nefarious activity—and even to traffic on the wired network that would best be blocked before it hits the WAP. You may display both station and WAP management traffic, if you wish.
- **By Application**: Check this box if you wish to analyze and list traffic by what specific applications are in use, such as Scopia or BitTorrent.

- **By Category**: Check this box if you wish to analyze and list traffic by the types of applications in use, such as Games or Collaboration.
- **Auto Refresh** instructs the WAP to periodically refresh this window automatically. Use the **Refresh** button to refresh the window right now.

Pie Charts

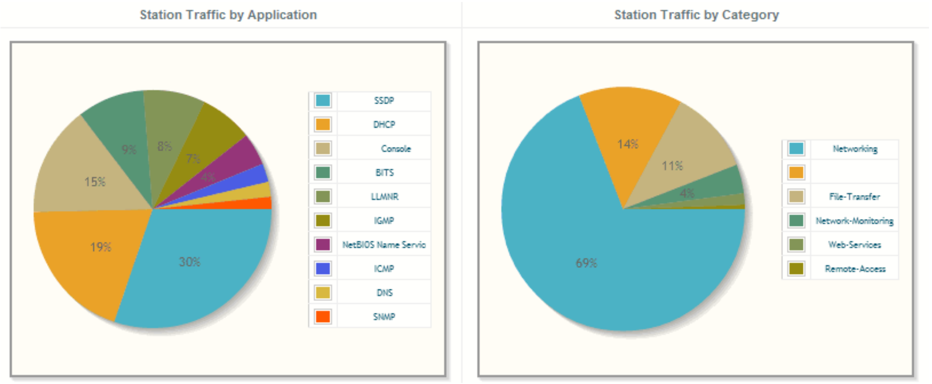
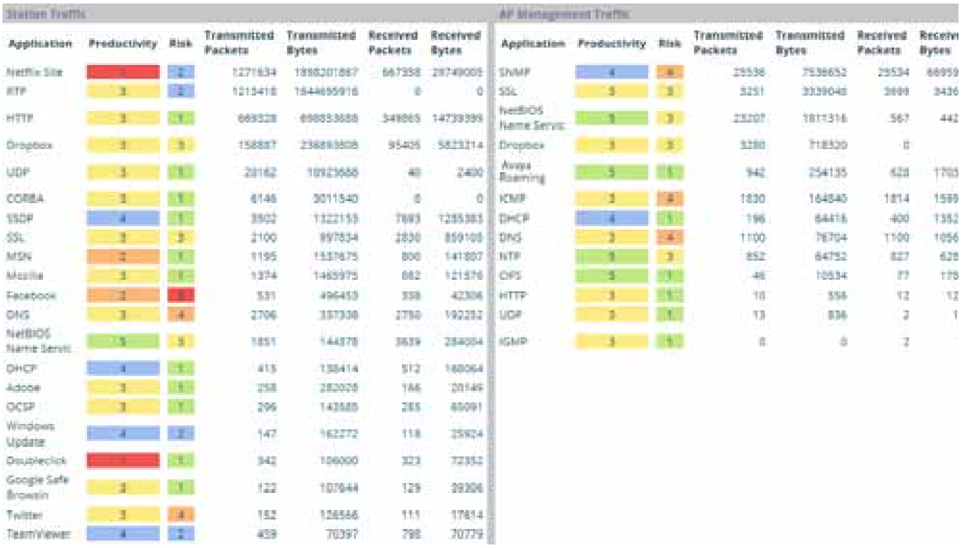


Figure 71. Application Control (Pie Charts)

These charts provide a quick way to determine how your wireless bandwidth is being used. There are charts for **Station Traffic** and/or WAP **Management Traffic**, depending on which checkboxes you selected. Similarly, there are charts for **By Application** and/or **By Category**, depending on your selections. The top ten applications or categories are listed, by percentage of bandwidth usage.

Traffic Tables



Station Traffic

Application	Productivity	Risk	Transmitted Packets	Transmitted Bytes	Received Packets	Received Bytes
Netflix Site	1	2	1271634	1898201887	667358	28749005
RTP	3	2	1213418	1844695916	0	0
HTTP	3	1	669328	698853688	349065	14739399
Dropbox	3	3	158887	238893808	95405	5823214
UDP	3	1	20162	10923688	40	2400
CORBA	3	1	6146	3011540	0	0
SSDP	4	1	3902	1322153	7693	1285383
SSL	3	3	2100	997834	2830	859105
MSN	2	1	1195	1537675	800	141807
Mozilla	3	1	1374	1465975	682	121576
Facebook	2	5	531	496453	358	42306
DNS	3	4	2706	337338	2750	192252
NetBIOS Name Servi	5	3	1851	144578	3639	284004
DHCP	4	1	415	138414	512	168064
Adobe	3	1	258	282028	166	20146
OCSP	3	1	296	143585	285	65091
Windows Update	4	2	147	162272	118	25924
Doubleclick	1	1	342	106000	323	72352
Google Safe Browsin	3	1	122	107644	129	29306
Twitter	3	4	152	126566	111	17614
TeamViewer	4	2	459	70397	798	70779

AP Management Traffic

Application	Productivity	Risk	Transmitted Packets	Transmitted Bytes	Received Packets	Receiv Bytes
SNMP	4	4	25536	7536652	25534	66959
SSL	3	3	5251	3339048	3699	3436
NetBIOS Name Servic	5	3	23207	1811316	567	442
Dropbox	3	3	5280	718520	0	
Avaya Roaming	5	1	942	254135	628	1703
ICMP	3	4	1830	164840	1814	1599
DHCP	4	1	196	64416	400	1352
DNS	3	4	1100	76704	1100	1056
NTP	5	3	852	64752	827	628
CIFS	5	1	46	10534	77	178
HTTP	3	1	16	556	12	12
UDP	3	1	13	836	2	1
IGMP	3	1	8	0	2	

Figure 72. Application Control (Station Traffic)

These tables provide detailed information about how your wireless bandwidth is being used. There are tables for **Station Traffic** and/or WAP **Management Traffic**, depending on which checkboxes you selected. Similarly, there are tables for **By Application** and/or **By Category**, depending on your selections.

In addition to showing traffic statistics, there are two unique and highly useful columns. **Risk** estimates the likelihood of an application causing problems for your business, such as a file-sharing utility introducing viruses or exposing you to legal problems. Risk is rated from 1 (low risk: for example, Google) to 5 (high risk: for example, BitTorrent). Risky applications (rated at 4 or 5) are flagged for your attention by highlighting the entry in pale red. **Productivity** estimates the value of an activity to your business, from 1 (unproductive: for example, Y8 gaming) to 5 (productive: for example, Scopia).

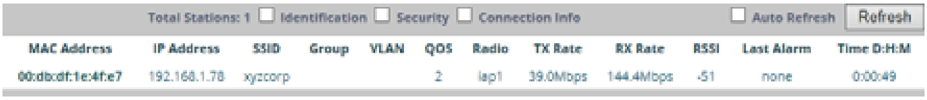
You may click the heading of any column to sort based on that column. Click again to sort in the reverse order. For instance, sort on **Risk** to find problem applications, or sort on **Productivity** to find applications that should be given increased or decreased handling priority.

When you find risky or unproductive applications consuming bandwidth on the network, you can easily create Filters to control them. See "Filter Management" on page 367. You may use filters to:

- Block problematic traffic, such as BitTorrent or Y8.
- Prioritize mission critical traffic—by increasing the QoS assigned to the traffic. See "Understanding QoS Priority on the WAP" on page 249.
- Lower the priority of less productive traffic—use filters to decrease the QoS assigned to traffic for applications like YouTube and Facebook.

Stations (Application Control)

This status-only window shows client stations currently visible to the WAP. The MAC address in the first column is a link. Click on a selected station, and the Application Control window opens with the **Display for Station** field set to that station, to perform a detailed analysis of its application usage.



Total Stations: 1 □ Identification □ Security □ Connection Info □ Auto Refresh Refresh

MAC Address	IP Address	SSID	Group	VLAN	QOS	Radio	TX Rate	RX Rate	RSSI	Last Alarm	Time D:H:M
00:db:df:1e:4f:e7	192.168.1.78	xyzcorp			2	iap1	39.0Mbps	144.4Mbps	-51	none	0:00:49

Figure 73. Stations (Application Control)

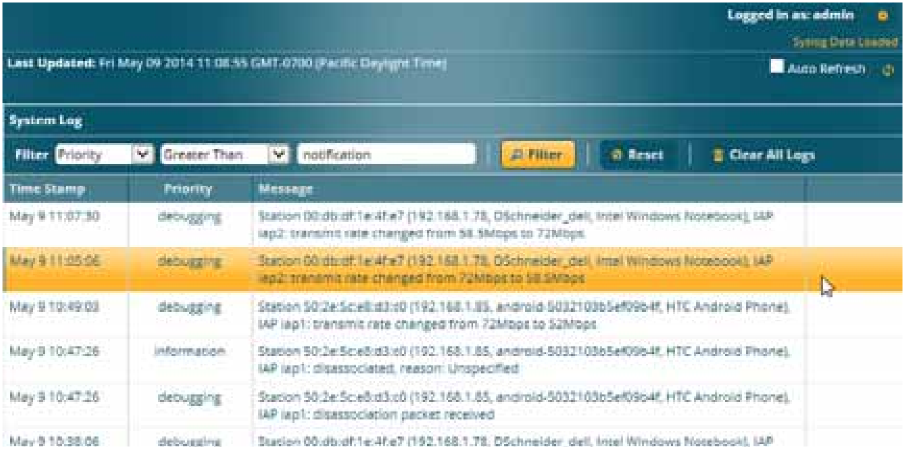
The rest of the fields and display options on this window (including the **Identification**, **Security**, and **Connection Info** checkboxes) are as described in "Stations" on page 108.

System Log Window

This is a status only window that allows you to review the system log, where system alerts and messages are displayed. Although there are no configuration options available in this window, you do have the usual choice of deciding how the event messages are sorted by clicking in the column header for the desired field (Time Stamp, Priority, or Message).

- **Time Stamp**—sorts the list based on the time the event occurred.
- **Priority**—sorts the list based on the priority assigned to the message.
- **Message**—sorts the list based on the message category

The displayed messages may be filtered by using the **Filter Priority** option, which allows control of the minimum priority level displayed. For example, you may choose (under **Services >System Log**) to log messages at or above Debug level but use **Filter Priority** to display only those at Information level and above.



Last Updated: Fri May 09 2014 11:08:55 GMT-0700 (Pacific Daylight Time)

☐ Auto Refresh

Filter: Priority | Greater Than | notification

Time Stamp	Priority	Message
May 9 11:07:30	debugging	Station 00:db:df:1e:4f:e7 (192.168.1.78, DSchneider_dell, Intel Windows Notebook), IAP iap2: transmit rate changed from 58.5Mbps to 72Mbps
May 9 11:05:06	debugging	Station 00:db:df:1e:4f:e7 (192.168.1.78, DSchneider_dell, Intel Windows Notebook), IAP iap2: transmit rate changed from 72Mbps to 58.5Mbps
May 9 10:49:03	debugging	Station 50:2e:5c:e8:d3:c0 (192.168.1.85, android-50321036b5ef09b4f, HTC Android Phone), IAP iap1: transmit rate changed from 72Mbps to 52Mbps
May 9 10:47:26	information	Station 50:2e:5c:e8:d3:c0 (192.168.1.85, android-50321036b5ef09b4f, HTC Android Phone), IAP iap1: disassociated, reason: Unspecified
May 9 10:47:26	debugging	Station 50:2e:5c:e8:d3:c0 (192.168.1.85, android-50321036b5ef09b4f, HTC Android Phone), IAP iap1: disassociation packet received
May 9 10:38:06	debugging	Station 00:db:df:1e:4f:e7 (192.168.1.78, DSchneider_dell, Intel Windows Notebook), IAP

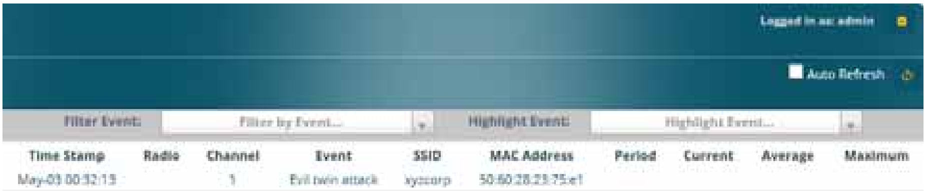
Figure 74. System Log (Alert Level Highlighted)

Use the **Highlight Priority** field if you wish to highlight messages at the selected priority level. Click on the **Refresh** button to refresh the message list, or click on the **Clear All** button at the upper left to delete all messages. You can also click in the **Auto Refresh** check box to instruct the WAP to refresh this window automatically.

IDS Event Log Window

This status only window displays the Intrusion Detection System (IDS) Event log, listing any detected attacks on your network. For descriptions of the types of attacks detected, as well as the settings to fine-tune IDS on the WAP, please see "Intrusion Detection" on page 343.

The displayed messages may be filtered by using the **Filter Event** setting, which allows you to select just one type of intrusion to display. For example, you may choose to display only beacon flood attacks.



Time Stamp	Radio	Channel	Event	SSID	MAC Address	Period	Current	Average	Maximum
May-03 00:32:15		1	Evil twin attack	xyzcorp	50:60:28:23:75:e1				

Figure 75. IDS Event Log

Use the **Highlight Event** field if you wish to highlight all events of one particular type in the list. Click on a column header to sort the rows based on that column. Click on the **Refresh** button to refresh the message list, or click the **Auto Refresh** check box to instruct the WAP to refresh this window automatically.

Although there are no configuration options available in this window, you do have the usual choice of deciding how the event messages are sorted by clicking in the column header for the desired field.

- **Time Stamp**—the time that the event occurred.
- **Radio**—the affected radio.
- **Channel**—the affected channel.
- **Event**—the type of attack, as described in Intrusion Detection.
- **SSID**—the SSID that was attacked.
- **MAC Address**—the MAC address of the attacker.

- **Period**—the length of the window used to determine whether the count of this type of event exceeded the threshold.
- **Current**—the count of this type of event for the current period.
- **Average**—the average count per period of this type of event.
- **Maximum**—the maximum count per period of this type of event.

Configuring the WAP

The following topics include procedures for configuring the WAP using the product's embedded Web Management Interface (WMI). Procedures have been organized into functional areas that reflect the flow and content of the WMI. The following WMI windows allow you to establish configuration parameters for your WAP, and include:

- **"Express Setup" on page 143**
- **"Network" on page 149**
- **"Services" on page 164**
- **"VLANs" on page 191**
- **"Tunnels" on page 199**
- **"Security" on page 204**
- **"SSIDs" on page 246**
- **"Groups" on page 275**
- **"Radios" on page 282**
- **"WDS" on page 356**
- **"Filters" on page 363**
- **"Clusters" on page 373**
- **"Mobile" on page 378**

After making changes to the configuration settings of a WAP you must click the **Save** button 🖫 at the top of the configuration window, otherwise the changes you make will not be applied the next time the WAP is rebooted.

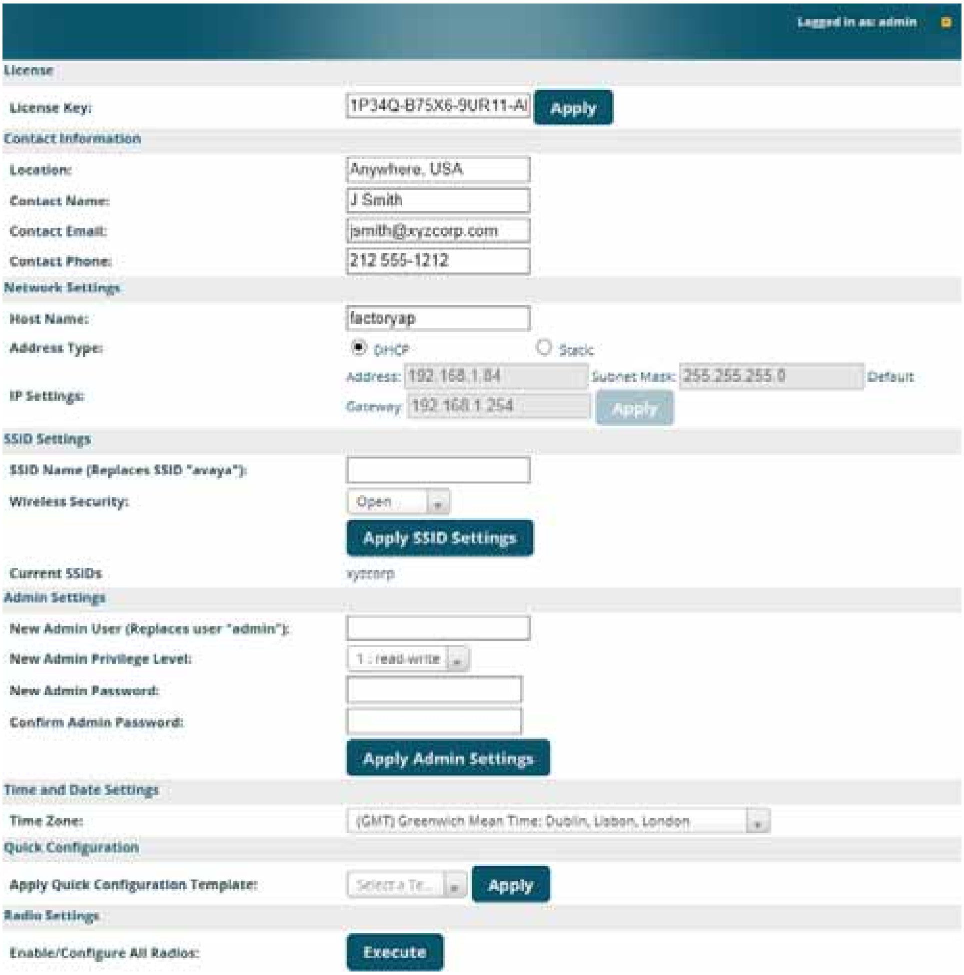
Some pages or individual settings are only available if the WAP's license includes appropriate features. If a setting is unavailable (grayed out), then your license or your WAP model does not support the feature. See "Licensing" on page 61.

This chapter only covers using the configuration windows on the WAP. To view status or use system tools on the WAP, please see:

- **"Viewing Status on the WAP" on page 77**
- **"Using Tools on the WAP" on page 383**

Express Setup

Initial WAP configuration via WOS sets items such as SSIDs and security, as described in "Ongoing Management" on page 58. This page allows you to see many of these values, or change them locally.



License

License Key: 1P34Q-B75X6-9UR11-Al

Contact Information

Location: Anywhere, USA

Contact Name: J Smith

Contact Email: jsmith@xyzcorp.com

Contact Phone: 212 555-1212

Network Settings

Host Name: factoryap

Address Type: ● DHCP ○ Static

IP Settings: Address: 192.168.1.84 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.254

SSID Settings

SSID Name (Replaces SSID "avaya"):

Wireless Security: Open

Current SSIDs xyzcorp

Admin Settings

New Admin User (Replaces user "admin"):

New Admin Privilege Level: 1 : read-write

New Admin Password:

Confirm Admin Password:

Time and Date Settings

Time Zone: (GMT) Greenwich Mean Time: Dublin, Lisbon, London

Quick Configuration

Apply Quick Configuration Template: Select a Te...

Radio Settings

Enable/Configure All Radios:

Figure 76. WMI: Express Setup

When finished, click the **Save** button 💾 if you wish to make your changes permanent.

Procedure for Performing an Express Setup

1. **License Key**: The factory installed license key is listed here. If you need to enable 802.11ac on WAP9122/WAP9123 or enable Application Control for all models, enter it here. See "Licensing" on page 61.
2. Configure the **Contact Information** settings.
   a. **Location**: Enter a brief but meaningful description that accurately defines the physical location of the WAP. In an environment where multiple units are installed, clear definitions for their locations are important if you want to identify a specific unit.

   b. **Contact Name**: Enter the name and contact information of the person who is responsible for administering the WAP at the designated location.

   c. **Contact Email**: Enter the email address of the admin contact you entered in Step 3.

   d. **Contact Phone**: Enter the telephone number of the admin contact you entered in Step 3.
3. Configure the **Network** settings. Please see "Interfaces" on page 150 for more information.
   a. **Host Name**: Specify a unique host name for this WAP. The host name is used to identify the WAP on the network. Use a name that will be meaningful within your network environment, up to 64 alphanumeric characters. The default is the WAP's serial number.

   b. **Address Type**: Choose **DHCP** to instruct the WAP to use DHCP to assign IP addresses to the WAP's Ethernet interfaces, or choose **Static** if you intend to enter IP addresses manually. If you choose the Static IP option, you must enter the following **IP Settings**:

   c. **IP Settings**: If you choose the **Static** IP addressing option, enter the following:

- **Address**: Enter a valid IP address for this WAP. To use a remote connection (Web, SNMP, or SSH), a valid IP address must be used.
- **Subnet Mask**: Enter a valid IP address for the subnet mask (the default is 255.255.255.0). The subnet mask defines the number of IP addresses that are available on the routed subnet where the WAP is located.
- **Default Gateway**: Enter a valid IP address for the default gateway. This is the IP address of the router that the WAP uses to forward data to other networks.
- Click the **Apply** button for this interface when done making IP changes.

For improved security, you should also take the additional steps described in "Securing Low Level Access to the WAP" on page 64.

4. **SSID Settings**: This section specifies the wireless network name and security settings.

   a. **SSID Name** is a unique name that identifies a wireless network. The default SSID is **avaya**. Entering a value in this field will replace the this default SSID with the new name.

   For additional information about SSIDs, go to the Multiple SSIDs section of "Frequently Asked Questions" on page 490.

   b. **Wireless Security**: Select the desired wireless security scheme (Open, WEP or WPA). Make your selection from the choices available in the pull-down list.

   - **Open**—This option offers no data encryption and is not recommended, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTy.
   - **WEP** (Wired Equivalent Privacy)—An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. WEP generates secret shared encryption keys that both

source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.

- **WPA** (Wi-Fi Protected Access)—A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP or AES as an encryption method and 802.1x for authentication. WPA is the stronger of the two wireless security schemes.
- **WPA2** (Wi-Fi Protected Access 2)—WPA2 is the follow-on security method to WPA for wireless networks and provides stronger data protection and network access control. It offers Enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Like WPA, WPA2 is designed to secure all versions of 802.11 devices, including 802.11a, 802.11b, 802.11g, and 802.11n, multi-band and multi-mode.
- **WPA-Both** (WPA and WPA2)—This option makes use of both WPA and WPA2.

For more information about security, including a full review of all security options and settings, go to "Understanding Security" on page 205.

c. **WEP Encryption Key/WPA Passphrase**: Depending on the wireless security scheme you selected, enter a unique WEP key or WPA passphrase. This field and the one below only appear if you select a **Wireless Security** option other than **Open**.

d. **Confirm Encryption Key/Passphrase**: If you entered a WEP key or WPA passphrase, confirm it here.

e. Click **Apply SSID Settings** when done.

f. **Current SSIDs**: This lists all of the currently defined SSIDs for you (regardless of whether they are enabled or not).

5. **Admin Settings:** This section allows you to change the default admin username, password, and privileges for the WAP. You may change the password and leave the user name as is, but we suggest that you change both to improve WAP security.

   a. **New Admin User (Replaces user "admin")**: Enter the name of a new administrator user account. Be sure to record the new account name and password, because the default **admin** user will be deleted! Note that the WAP also offers the option of authenticating administrators using a RADIUS server (see "Admin Management" on page 210).

   b. **New Admin Privilege Level**: By default, the new administrator will have read / write privileges on the WAP (i.e., the new user will be able to change the configuration of the WAP). If you wish the new account to have different privileges, select the desired level from the drop-down list. For more information about user privileges, please see "Admin Privileges" on page 212. Take care to make sure to leave yourself enough read / write privileges on at least one account to be able to administer the WAP.

   c. **New Admin Password**: Enter a new administration password for managing this WAP. If you forget this password, you must reset the WAP to its factory defaults so that the password is reset to **admin** (its default setting).

   d. **Confirm Admin Password**: If you have entered a new administration password, confirm the new password here.

   e. Click **Apply Admin Settings** when done.

6. **Time and Date Settings:** System time is synchronized using NTP (Network Time Protocol) by default. Use the drop-down list to select the **Time Zone**.

7. **Quick Configuration:** This offers predefined configuration options such as **Classroom** and **High-Density** that capture best practices from years of field experience. If one of the options in the drop-down list is appropriate

to your deployment, select it and click **Apply**. For example, the **High-Density** option uses best practices to configure the WAP for high density settings such as lecture halls, convention centers, stadiums, etc.

8. **Radio Settings:**

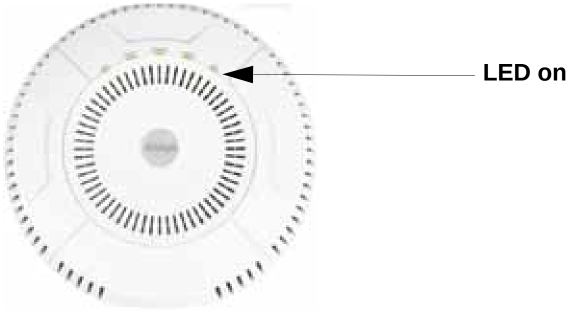


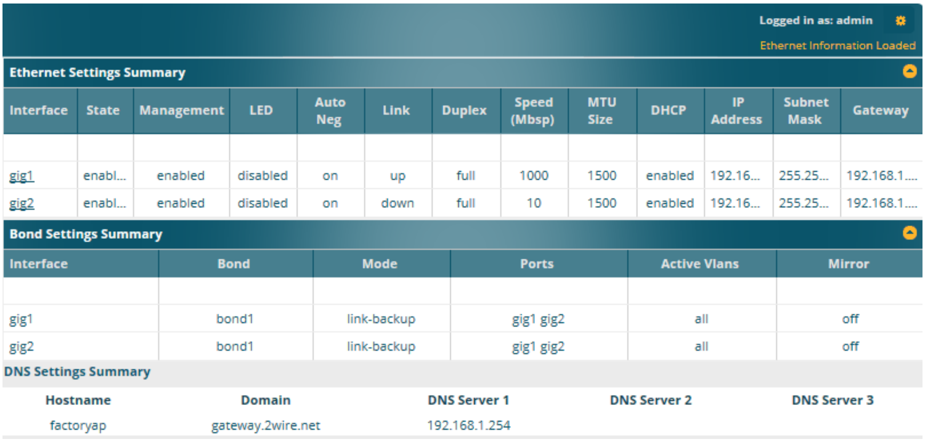
Figure 77. LEDs are Switched On

Enable/Configure All Radios: Click on the **Execute** button to enable and auto configure all radios (a message displays the countdown time—in seconds—to complete the auto-configuration task). When enabled, the radio's LED is switched on.

9. Click the **Save** button 💾 at the upper right to make your changes permanent, i.e., these settings will still be in effect after a reboot.

Network

This is a status-only window that provides a snapshot of the configuration settings currently established for the Ethernet interfaces. DNS Settings and other settings are summarized as well. You must go to the appropriate configuration window to make changes to any of the settings displayed here (configuration changes cannot be made from this window). You can click on any item in the **Interface** column to “jump” to the associated configuration window.



Logged in as: admin

Ethernet Information Loaded

Ethernet Settings Summary

Interface	State	Management	LED	Auto Neg	Link	Duplex	Speed (Mbsp)	MTU Size	DHCP	IP Address	Subnet Mask	Gateway
gig1	enabl...	enabled	disabled	on	up	full	1000	1500	enabled	192.16...	255.25...	192.168.1....
gig2	enabl...	enabled	disabled	on	down	full	10	1500	enabled	192.16...	255.25...	192.168.1....

Bond Settings Summary

Interface	Bond	Mode	Ports	Active Vlans	Mirror
gig1	bond1	link-backup	gig1 gig2	all	off
gig2	bond1	link-backup	gig1 gig2	all	off

DNS Settings Summary

Hostname	Domain	DNS Server 1	DNS Server 2	DNS Server 3
factoryap	gateway.2wire.net	192.168.1.254		

Figure 78. Network Interfaces

WMI windows that allow you to change or view configuration settings associated with the network interfaces include:

- “Interfaces” on page 150
- “Bonds and Bridging” on page 153
- “DNS Settings” on page 160
- “Fabric Attach Settings” on page 162

See Also

DNS Settings

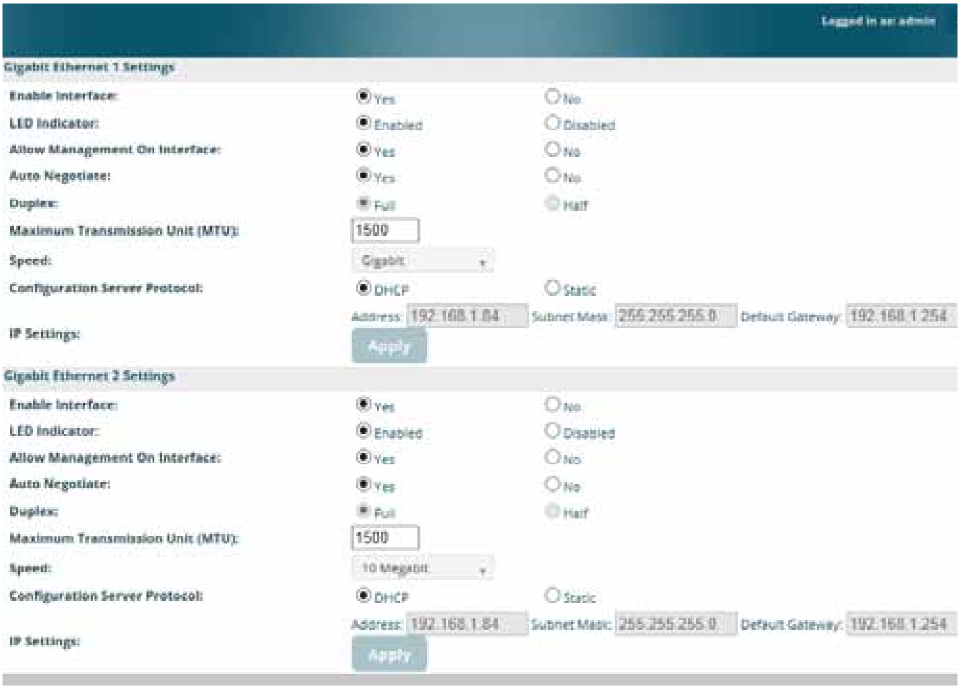
Interfaces

Network Status Windows

Spanning Tree Status
Network Statistics

Interfaces

This window allows you to establish configuration settings for the WAP's Ethernet network interfaces.



Logged in as: admin

Gigabit Ethernet 1 Settings

Enable Interface:	● Yes	○ No
LED Indicator:	● Enabled	○ Disabled
Allow Management On Interface:	● Yes	○ No
Auto Negotiate:	● Yes	○ No
Duplex:	● Full	○ Half
Maximum Transmission Unit (MTU):	1500	
Speed:	Gigabit	
Configuration Server Protocol:	● DHCP	○ Static
IP Settings:	Address: 192.168.1.84 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.254 Apply	

Gigabit Ethernet 2 Settings

Enable Interface:	● Yes	○ No
LED Indicator:	● Enabled	○ Disabled
Allow Management On Interface:	● Yes	○ No
Auto Negotiate:	● Yes	○ No
Duplex:	● Full	○ Half
Maximum Transmission Unit (MTU):	1500	
Speed:	10 Megabit	
Configuration Server Protocol:	● DHCP	○ Static
IP Settings:	Address: 192.168.1.84 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.254 Apply	

Figure 79. Network Settings

When finished making changes, click the **Save** button 💾 if you wish to make your changes permanent. When the status of a port changes, a Syslog entry is created describing the change.

Network Interface Ports

For the location of network interface ports on a WAP, see the illustrations in "User Interfaces" on page 58.

Procedure for Configuring the Network Interfaces

Configure the **Gigabit** network interfaces. The fields for each of these interfaces are the same, and include:

1. **Enable Interface:** Choose **Yes** to enable this network interface, or choose No to disable the interface.
2. **LED Indicator**: Choose **Enabled** to allow the LED for this interface to blink with traffic on the port, or choose **Disabled** to turn the LED off. The LED will still light during the boot sequence, then turn off. This option is only available for the Gigabit interfaces.
3. **Allow Management on Interface**: Choose **Yes** to allow management of this WAP via the selected network interface, or choose **No** to deny all management privileges for this interface.

For improved security, you should also take the additional steps described in "Securing Low Level Access to the WAP" on page 64.

4. **Auto Negotiate**: This feature allows the WAP to negotiate the best transmission rates automatically. Choose **Yes** to enable this feature, or choose **No** to disable this feature—the default is enabled. If you disable the Auto Negotiate feature, you must define the Duplex and Speed options manually (otherwise these options are not available). Both sides of the link **must** have the same values for the following settings, or the connection will have errors.
   a. **Duplex**: Full-duplex mode transmits data in two directions simultaneously (for example, a telephone is a full-duplex device because both parties can talk and be heard at the same time). Half-duplex allows data transmission in one direction at a time only (for example, a walkie-talkie is a half-duplex device). If the Auto-Negotiate feature is disabled, you can manually choose **Half** or **Full** duplex for your data transmission preference.
   b. **MTU**: The Maximum Transmission Unit size. This is the largest packet size (in bytes) that the interface can pass along.

c. **Speed**: If the Auto-Negotiate feature is disabled, you must manually choose the data transmission speed from the pull-down list. For the Gigabit interfaces the options are **10 Megabit** or **100 Megabit**. (Note that 1000 Megabit speed can only be set by Auto-Negotiation.)

5. **Configuration Server Protocol / IP Settings**: Choose **DHCP** to instruct the WAP to use DHCP when assigning IP addresses to the WAP, or choose **Static IP** if you intend to enter IP addresses manually. If you select the Static IP option you must specify the IP address, IP subnet mask and default gateway.

   a. **Address**: If you selected the Static IP option, enter a valid IP address for the WAP. To use any of the remote connections (Web, SNMP, or SSH), a valid IP address must be established.

   b. **Subnet Mask**: If you selected the Static IP option, enter a valid IP address for the subnet mask (the default for Class C is 255.255.255.0). The subnet mask defines the number of IP addresses that are available on the routed subnet where the WAP is located.

   c. **Default Gateway**: If you selected the Static IP option, enter a valid IP address for the default gateway. This is the IP address of the router that the WAP uses to send data to other networks. (You don’t need to enter the gateway if it is on the same subnet as the WAP.)

   d. Click the **Apply** button for this interface when done making IP changes.

6. When done configuring all interfaces as desired, click the **Save** button 💾 if you wish to make your changes permanent.

See Also

Bonds and Bridging

DNS Settings

Network

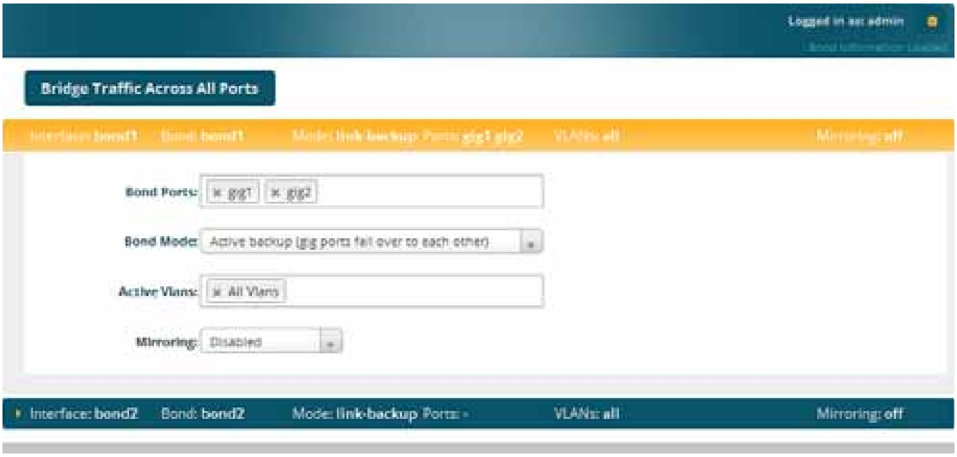
Network Statistics

Spanning Tree Status

Bonds and Bridging

On models with more than one Gigabit port these ports may be bonded, i.e. configured to work together in sets. For example, one port may provide active backup or load balancing for another, or other options as described in this section.

A special option lets you configure bridging between the Gigabit ports on a WAP that has two of these ports.



Interface: bond1 Bond: bond1 Mode: link-backup Ports: gig1 gig2 VLANs: all Mirroring: off

Bond Ports: gig1 gig2

Bond Mode: Active backup (gig ports fail over to each other)

Active Vlans: All Vlans

Mirroring: Disabled

Interface: bond2 Bond: bond2 Mode: link-backup Ports: - VLANs: all Mirroring: off

Figure 80. Network Bonds and Bridging

You may use the mirror option to have all the traffic that is ingressing and egressing one bond be transmitted by the bond you are configuring. For example, if you configure Bond2 to mirror Bond1, then all traffic going in and out of Bond1's Gigabit ports will be transmitted out of Bond2's Gigabit ports. This way of duplicating one bond's traffic to another bond is very useful for troubleshooting with a network analyzer.

If a set of Gigabit ports have been bonded, the IP address, IP mask, IP gateway, IP DHCP, and Management settings are shared between bonded ports. Any changes you make to these settings on one member will be reflected in the settings of the other members. Other settings may be configured individually.

Procedure for Configuring Network Bonds

Configure the bonding behavior of the **Gigabit** network interfaces. The fields for each of these bonds are the same, and include:

1. **Bridge Traffic Across All Ports:** Click this for Layer 2 bridging between *all* Gigabit ports. (Figure 81)

Bridging traffic

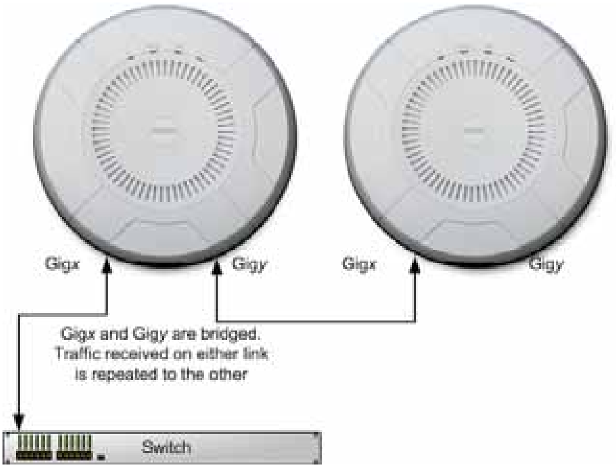


Figure 81. Bridging Traffic

Traffic received on Gig*x* is transmitted by Gig*y*; similarly, traffic received on Gig*y* is transmitted by Gig*x*. The WAP acts as a wired bridge—this allows WAPs to be chained and still maintain wired connectivity.

Each WAP in a chain must have power supplied to its PoE port from a compatible power injector or powered switch port. ***A WAP does not supply power to another WAP.***

When bridging is enabled, it configures the following bond settings for each bond. Do not make any manual changes to these settings afterwards if you wish to continue bridging.

- **Bond Mode is** set to **Active Backup** (the default value).
- Each port is in its own bond, by itself.
- **Bond Mirror** is **Off**.
- You will typically need to enable use of Spanning Tree manually, to prevent network loops.
- **Active VLANs** is set to **All**.

A bridge between ports **Gig1** and **Gig2** sets **Bond1** to contain only **Gig1**. **Bond2** contains only **Gig2**.

If you are bridging a chain of more than two WAPs, the endpoint WAP is not actually bridging. It can be left with the default settings—**Bond1** is set to **Active Backup**, and will contain **Gig1** and **Gig2**.

Skip to Step 7 on page 159.

2. If you are not enabling bridging, configure the bonding behavior of the **Gigabit** network interfaces as described in the following steps. The fields for each of these bonds are the same.

3. **Bond Mode**: Select the desired behavior for a set of bonded Gigabit Ethernet ports from the following options.

   The modes below describe the relationship between a set of Gigabit ports—for example, load balancing or active backup. Use the **Bond Ports** field to select the ports that are bonded (set in Step 4). You may also include just one single port in a bond—this is useful for mirroring one Gigabit port to another port (Step c on page 158). In this discussion, we call two ports that are bonded **Gig*x*** and **Gig*y***.

   a. **Active Backup (gig ports fail over to each other)**—This mode provides fault tolerance and is the default mode. Gig*x* acts as the primary link. Gig*y* is the backup link and is passive. Gig*y* assumes the IP properties of Gig*x*. If Gig*x* fails, the WAP automatically fails over to Gig*y*. When a failover occurs in this mode, Gig*y* issues gratuitous ARPs to allow it to substitute for Gig*x* at Layer 3 as well as Layer 2. See Figure 82 (a).

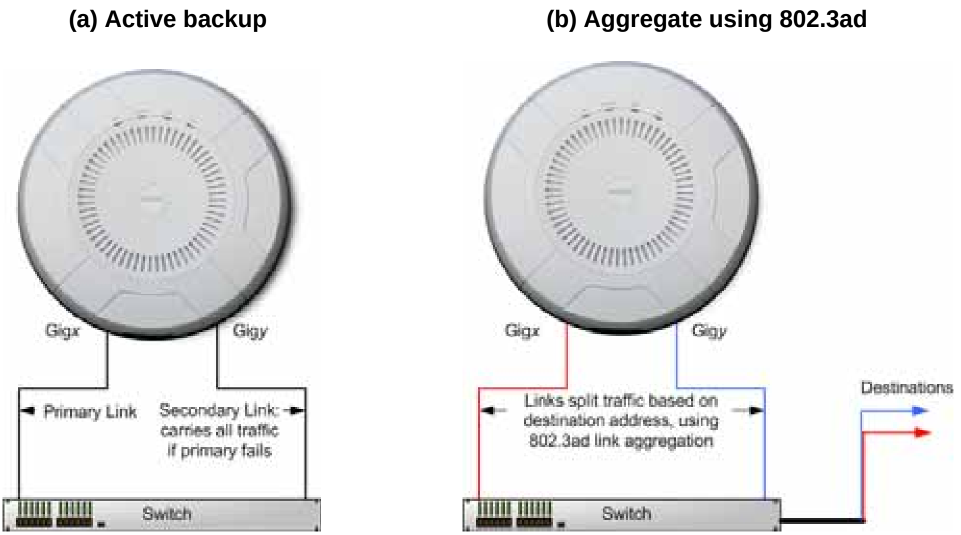

(a) Active backup
Gigx
Gigy
Primary Link
Secondary Link: carries all traffic if primary fails
Switch
(b) Aggregate using 802.3ad
Gigx
Gigy
Links split traffic based on destination address, using 802.3ad link aggregation
Destinations
Switch

Figure 82. Port Modes (a, b)

b. **Aggregate Traffic from gig ports using 802.3ad**—The WAP sends network traffic across all member Gigabit ports to increase link speed to the network. These ports act as a single logical interface, using a load balancing algorithm to balance traffic across the ports. For non-IP traffic (such as ARP), the last byte of the destination MAC address is used to do the calculation. If the packet is a fragment or not TCP or UDP, the source and destination IP addresses are used to do the calculation. If the packet is TCP or UDP over IP then the source IP address, destination IP address, source port number and destination port number are all used to do the calculation. The network switch must also support 802.3ad. If a port fails, the connection degrades gracefully—the other port still transmits. See Figure 82 (b).

c. **Transmit Traffic on all gig ports**—Transmits incoming traffic on all Gigabit ports. Any traffic received on Gigabit ports is sent to the onboard processor. This mode provides fault tolerance. See Figure 83 (c).

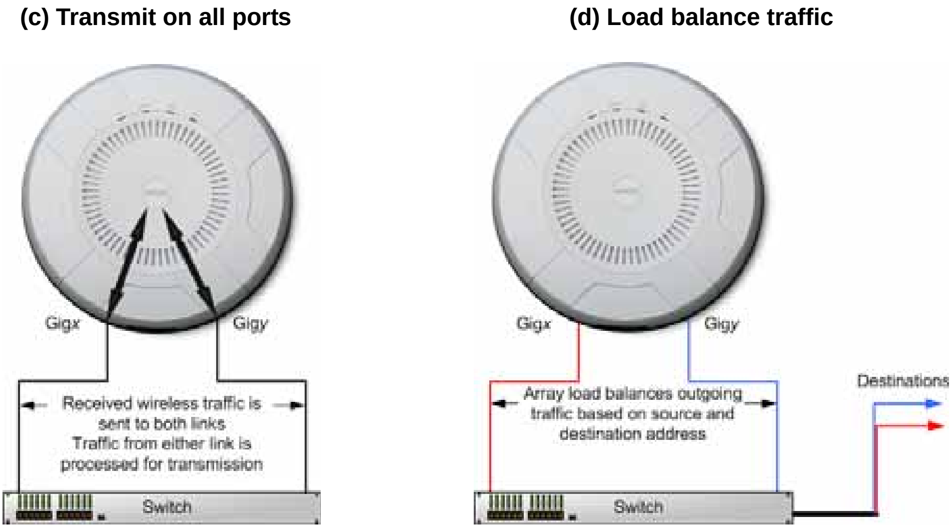

(c) Transmit on all ports
(d) Load balance traffic
Gigx
Gigy
Received wireless traffic is sent to both links
Traffic from either link is processed for transmission
Switch
Gigx
Gigy
Array load balances outgoing traffic based on source and destination address
Destinations
Switch

Figure 83. Port Modes (c, d)

d. **Load balance traffic between gig ports**—This option provides trunking, similar to option (b)—**Aggregate Traffic from gig1 & gig2 using 802.3ad**, but it does not use 802.3ad and it uses a different load balancing algorithm to determine the outgoing Gigabit port. The outgoing port used is based on an exclusive OR of the source and destination MAC address. Like option (b), this mode also provides load balancing and fault tolerance. See Figure 83 (d).

4. **Bond Ports**: Select the ports to be members of this bond for the behavior specified by **Bond Mode**. By default, Bond1 contains Gig1 and Gig2. You may set up a bond with a single port, for example, if you wish to mirror one Gigabit port to another.

   When you check off a port to be a member of a bond, that port is automatically removed from any other bonds that contain it.

5. **Active VLANs**: **Active VLANs** shows the VLANs that you have selected to be passed through this port. Create and manage the list of VLANs that are allowed to be passed through this port. Traffic will be dropped for VLANs that are not in this list. The default setting is to pass All VLANs.

    a. To add a VLAN to the list of allowed VLANs, click this field and select the desired VLAN from the drop-down list. To allow all VLANs (current or future) to be passed, select **All VLANs**.

    b. To allow only the set of currently defined VLANs (see "VLANs" on page 191) to be passed, select **All Current VLANs**. Essentially, this "fixes" the Active VLANs list to contain the currently defined VLANs, and only this set, until you make explicit changes to the Active VLANs list. If you create new VLANs, they will not be passed unless you take action to add them to the list.

    c. To remove a VLAN from the list of allowed VLANs, click the **X** before its name.

6. **Mirroring**—Specify one of the active bonds (Bond*x*) that is to be mirrored by this bond (Bond*y*). (Figure 84) All wireless traffic received on the WAP is transmitted out both Bond*x* and Bond*y*. All traffic received on Bond*x* is passed on to the onboard processor as well as out Bond*y*. All traffic received on Bond*y* is passed on to the onboard processor as well as out Bond*x*. This allows a network analyzer to be plugged into Bond*y* to capture traffic for troubleshooting, while the bonded ports provide network connectivity for data traffic.

    If each bond contains just one port, then you have the simple case of one port mirroring another.

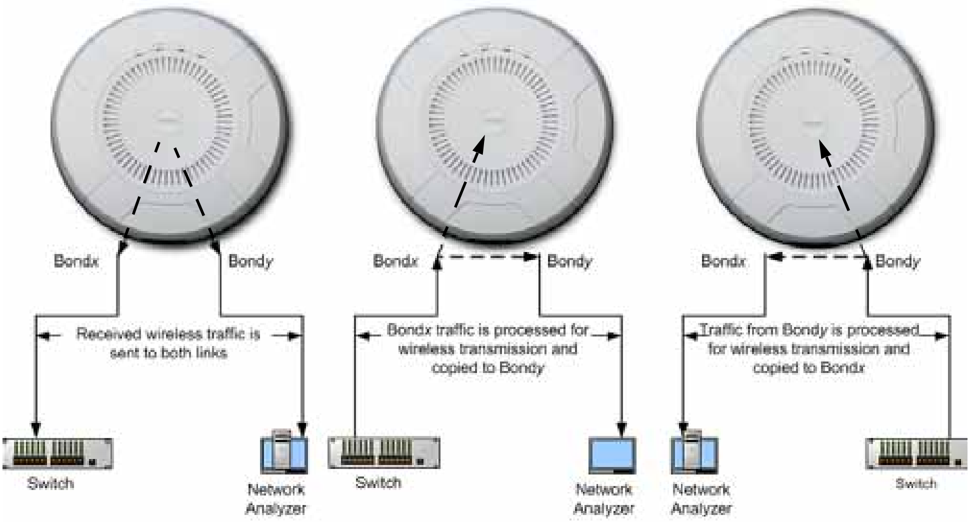

Bondx
Bondy
Received wireless traffic is sent to both links
Switch
Network Analyzer
Bondx
Bondy
Bondx traffic is processed for wireless transmission and copied to Bondy
Switch
Network Analyzer
Bondx
Bondy
Traffic from Bondy is processed for wireless transmission and copied to Bondx
Network Analyzer
Switch

Figure 84. Mirroring Traffic

7. When done configuring bonds and bridging as desired, click the **Save** button 💾 if you wish to make your changes permanent.

See Also

Interfaces

DNS Settings

Network

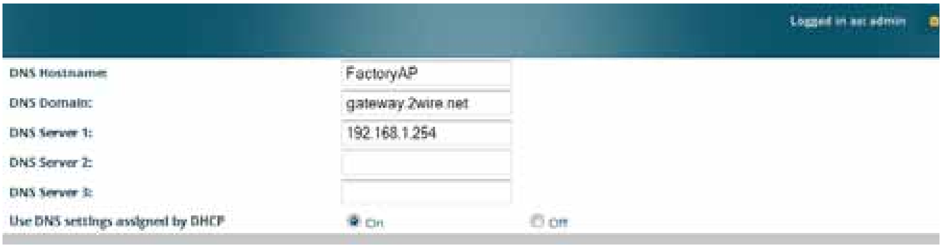
Network Statistics

Spanning Tree Status

DNS Settings

This window allows you to establish your DNS (Domain Name System) settings. The WAP uses these DNS servers to resolve host names into IP addresses. The WAP also registers its own Host Name with these DNS servers, so that others may address the WAP using its name rather than its IP address. An option allows you to specify that the WAP's DNS servers will be assigned via a DHCP server on the wired network.

Note that the DNS servers defined here are not used by wireless clients—servers for stations associated to the WAP are defined along with DHCP pools. See "DHCP Server" on page 178. At least one DNS server must be set up if you want to offer clients associating with the WAP the ability to use meaningful host names instead of numerical IP addresses. When finished, click the **Save** button if you wish to make your changes permanent.



DNS Hostname: FactoryAP

DNS Domain: gateway.2wire.net

DNS Server 1: 192.168.1.254

DNS Server 2:

DNS Server 3:

Use DNS settings assigned by DHCP ● On ○ Off

Figure 85. DNS Settings

Procedure for Configuring DNS Servers

1. **DNS Host Name:** Enter a valid DNS host name.
2. **DNS Domain**: Enter the DNS domain name.
3. **DNS Server 1**: Enter the IP address of the primary DNS server.
4. **DNS Server 2** and **DNS Server 3**: Enter the IP address of the secondary and tertiary DNS servers (if required).
5. **Use DNS settings assigned by DHCP**: If you are using DHCP to assign the WAP's IP address, you may turn this option **On**. The WAP will then obtain its DNS domain and server settings from the network DHCP

server that assigns an IP address to the WAP, rather than using the DNS Server fields above. You may also configure that DHCP server to assign a host name to the WAP.

6. Click the **Save** button 💾 if you wish to make your changes permanent.

See Also

DHCP Server
Network
Interfaces
Network Statistics
Spanning Tree Status

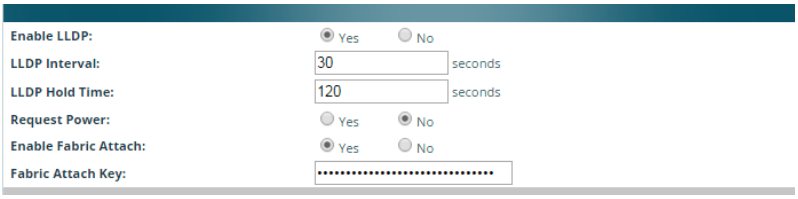
See Also

Network
Interfaces
Network Statistics

Fabric Attach Settings

This page controls Avaya Fabric Attach settings and LLDP settings. Link Layer Discovery Protocol (LLDP) is a Layer 2 network protocol used to share information (such as the device manufacturer and model, network capabilities, and IP address) with other directly connected network devices. WAPs can both advertise their presence by sending LLDP announcements, and gather and display information sent by neighbors (see “Fabric Attach List” on page 93).

This window allows you to establish your Fabric Attach and LLDP settings. When finished, use the Save button 💾 if you wish to make your changes permanent.



Enable LLDP:	● Yes ○ No
LLDP Interval:	30 seconds
LLDP Hold Time:	120 seconds
Request Power:	○ Yes ● No
Enable Fabric Attach:	● Yes ○ No
Fabric Attach Key:	••••••••••••••••••••••••••••••••

Figure 86. Fabric Attach Settings

Procedure for Configuring Fabric Attach Settings

1. **Enable LLDP:** When LLDP is enabled, the WAP sends out LLDP announcements of the WAP’s presence, and gathers LLDP data sent by neighbors. When disabled, it does neither. LLDP is enabled by default.

2. **LLDP Interval**: The WAP sends out LLDP announcements advertising its presence at this interval. The default is 30 seconds.

3. **LLDP Hold Time**: LLDP information received from neighbors is retained for this period of time before aging out of the WAP’s neighbor list. Thus, if a neighbor stops sending announcements, it will no longer appear on the Fabric Attach List window after LLDP Hold Time seconds from its last announcement. The default is 120 seconds.

4. **Request Power**: You must enable LLDP before enabling this feature. If Request Power is set to **Yes** and LLDP discovers a device port that supplies power to this WAP (on a powered switch, for example), the WAP

checks that the port is able to supply the peak power that is required by this WAP model. The Request Power feature does this by requesting this peak power (in watts) from the PoE source, and it expects the PoE source to reply with the amount of power allocated. If the WAP does not receive a response confirming that the power allocated by the PoE source is equal to or greater than the power requested, then the WAP issues a Syslog message and keeps the radios down for ten minutes. The radios may be enabled manually after this—see “Radio Settings” on page 284.

Using this feature provides a more graceful way of handling an underpowered situation on a Wi-Fi device. When the radios are turned off, WOS can notify you, rather than having to hunt down an intermittent problem.

Request Power is available on WLAN 9100 models that support IEEE802.3at power. It is especially useful for the WAP9172, which requests 30W (this is above the IEEE 802.3at maximum of 25.5W). Note that Request Power is not available on the WAP9173.

5. **Enable Fabric Attach**: WAPs support the Avaya Fabric Attach feature to simplify network deployment. Click **Yes** to enable the WAP as a Fabric Attach client device. This feature is enabled by default. Fabric Attach uses LLDP packets for communication, and requires LLDP to be enabled.
6. **Fabric Attach Key**: This is the message authentication key used by Fabric Attach. This can be used to establish a new key of length 1 to 32 octets.

See Also

Fabric Attach List

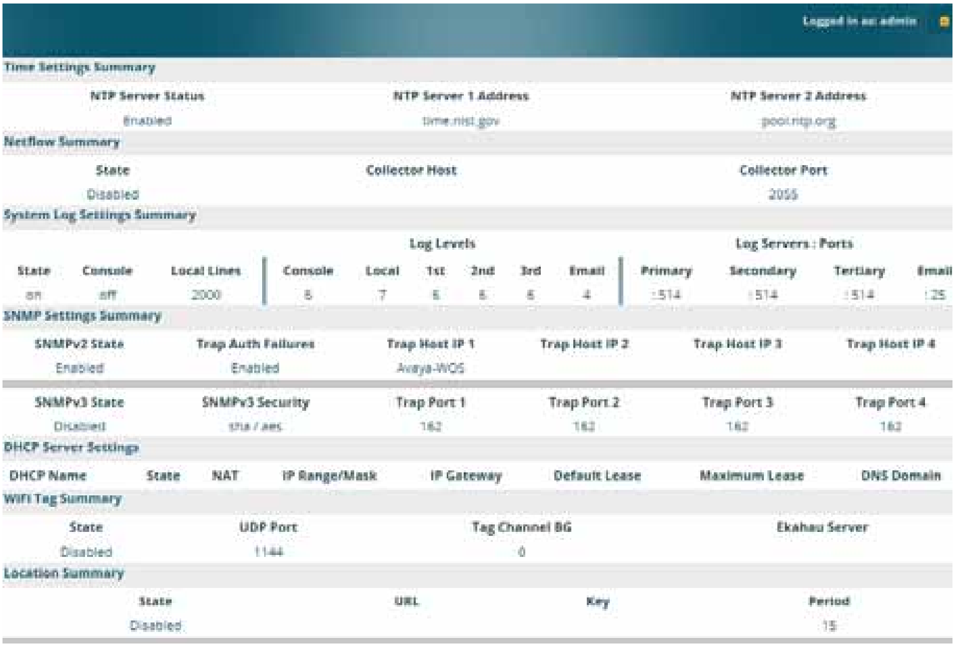
Network

Interfaces

Network Statistics

Services

This is a status-only window that allows you to review the current settings and status for services on the WAP, including DHCP, SNMP, Syslog, and Network Time Protocol (NTP) services. For example, for the DHCP server, it shows each DHCP pool name, whether the pool is enabled, the IP address range, the gateway address, lease times, and the DNS domain being used. There are no configuration options available in this window, but if you are experiencing issues with network services, you may want to print this window for your records.



Time Settings Summary

NTP Server Status	NTP Server 1 Address	NTP Server 2 Address
Enabled	time.nist.gov	pool.ntp.org

Netflow Summary

State	Collector Host	Collector Port
Disabled		2055

System Log Settings Summary

			Log Levels						Log Servers : Ports			
State	Console	Local Lines	Console	Local	1st	2nd	3rd	Email	Primary	Secondary	Tertiary	Email
on	off	2000	6	7	6	6	6	4	:514	:514	:514	:25

SNMP Settings Summary

SNMPv2 State	Trap Auth Failures	Trap Host IP 1	Trap Host IP 2	Trap Host IP 3	Trap Host IP 4
Enabled	Enabled	Avaya-WOS			

SNMPv3 State	SNMPv3 Security	Trap Port 1	Trap Port 2	Trap Port 3	Trap Port 4
Disabled	sha / aes	162	162	162	162

DHCP Server Settings

DHCP Name	State	NAT	IP Range/Mask	IP Gateway	Default Lease	Maximum Lease	DNS Domain

WiFi Tag Summary

State	UDP Port	Tag Channel BG	Ekahau Server
Disabled	1144	0	

Location Summary

State	URL	Key	Period
Disabled			15

Figure 87. Services

The following sections discuss configuring services on the WAP:

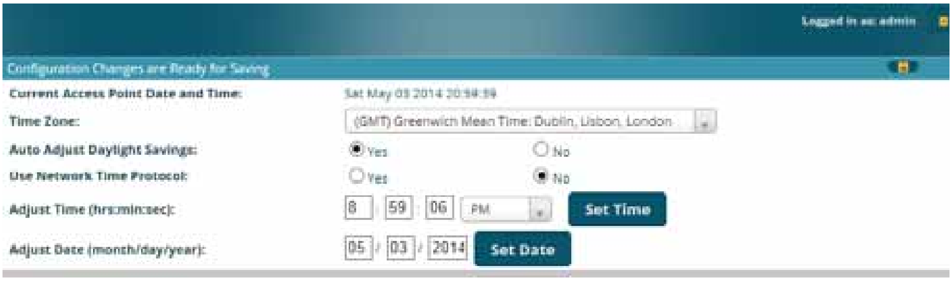
- **"Time Settings (NTP)" on page 165**
- **"NetFlow" on page 167**
- **"Wi-Fi Tag" on page 168**
- **"Location" on page 169**

- **"System Log" on page 171**
- **"SNMP" on page 175**
- **"DHCP Server" on page 178**
- **"Proxy Services" on page 180**

Time Settings (NTP)

This window allows you to manage the WAP's time settings, including synchronizing the WAP's clock with a universal clock from an Network Time Protocol (NTP) server. We recommend that you use NTP for proper operation of SNMP in WOS, since a lack of synchronization will cause errors to be detected. Synchronizing the WAP's clock with an NTP server also ensures that Syslog time-stamping is maintained across all units.

It is possible to use authentication with NTP to ensure that you are receiving synchronization from a known source. For example, the instructions for requesting a key for the NIST Authenticated NTP server are available at http://www.nist.gov/pml/div688/grp00/upload/ntp_instructions.pdf. The WAP allows you to enter optional authentication information.



Current Access Point Date and Time: Sat May 03 2014 20:59:59

Time Zone: (GMT) Greenwich Mean Time: Dublin, Lisbon, London

Auto Adjust Daylight Savings: ● Yes ○ No

Use Network Time Protocol: ○ Yes ● No

Adjust Time (hrs:min:sec): 8 : 59 : 06 PM

Adjust Date (month/day/year): 05 / 03 / 2014

Figure 88. Time Settings (Manual Time)

Procedure for Managing the Time Settings

1. **Current WAP Date and Time:** Shows the current time.
2. **Time Zone**: Select the time zone you want to use (normally your local time zone) from the pull-down list.

3. **Auto Adjust Daylight Savings**: Check this box to have the system adjust for daylight savings automatically, else leave it unchecked (default).

4. **Use Network Time Protocol:** Select whether to set time manually or use NTP to manage system time.

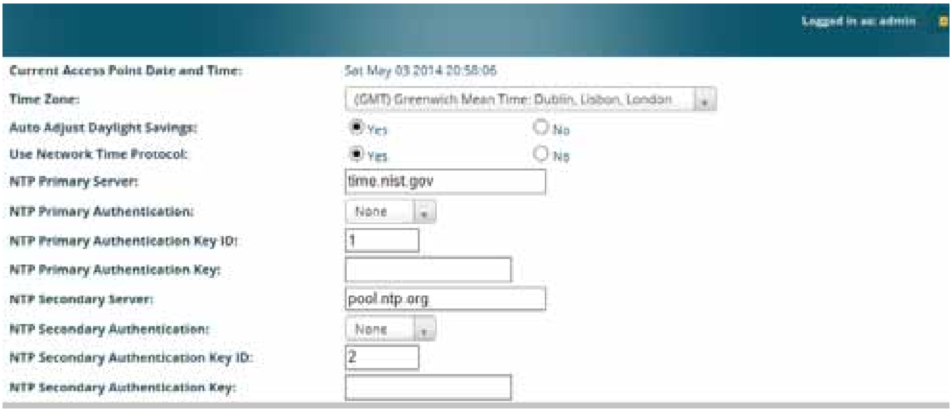
5. **Setting Time Manually**

   a. **Adjust Time (hrs:min:sec)**: If you are not using NTP, use this field if you want to adjust the current system time. Enter a revised time (hours, minutes, seconds, am / pm) in the corresponding fields. Click **Set Time** to apply the changes.

   b. **Adjust Date (month/day/year)**: If you are not using NTP, use this field if you want to adjust the current system date. Enter a revised date (month, day and year) in the corresponding fields. Click **Set Date** to apply the changes.

6. **Using an NTP Server**

   a. **NTP Primary Server**: If you are using NTP, enter the IP address or domain name of the NTP server.



Current Access Point Date and Time:	Sat May 03 2014 20:58:06	
Time Zone:	(GMT) Greenwich Mean Time: Dublin, Lisbon, London	
Auto Adjust Daylight Savings:	● Yes	○ No
Use Network Time Protocol:	● Yes	○ No
NTP Primary Server:	time.nist.gov	
NTP Primary Authentication:	None	
NTP Primary Authentication Key ID:	1	
NTP Primary Authentication Key:		
NTP Secondary Server:	pool.ntp.org	
NTP Secondary Authentication:	None	
NTP Secondary Authentication Key ID:	2	
NTP Secondary Authentication Key:		

Figure 89. Time Settings (NTP Time Enabled)

b. **NTP Primary Authentication**: (optional) If you are using authentication with NTP, select the type of key: **MD5** or **SHA1**. Select **None** if you are not using authentication (this is the default).

c. **NTP Primary Authentication Key ID**: Enter the key ID, which is a decimal integer.

d. **NTP Primary Authentication Key**: Enter your key, which is a string of characters.

e. **NTP Secondary Server**: Enter the IP address or domain name of an optional secondary NTP server to be used in case the WAP is unable to contact the primary server. You may use the authentication fields as described above if you wish to set up authentication for the secondary server.

See Also

Express Setup

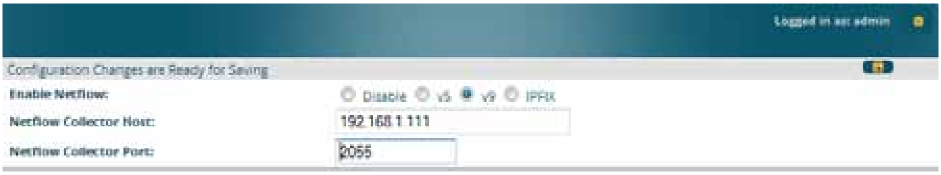
Services

SNMP

System Log

NetFlow

This window allows you to enable or disable the sending of NetFlow information to a designated collector. NetFlow is a proprietary but open network protocol for collecting IP traffic information. When NetFlow is enabled, the WAP will send IP flow information (traffic statistics) to the designated collector.



Logged in as: admin

Configuration Changes are Ready for Saving

Enable Netflow: ○ Disable ○ v5 ● v9 ○ IPFIX

Netflow Collector Host: 192.168.1.111

Netflow Collector Port: 2055

Figure 90. NetFlow

NetFlow sends per-flow network traffic information from the WAP. Network managers can use a NetFlow collector to view the statistics on a per-flow basis and use this information to make key decisions. Knowing how many packets and bytes are sent to and from certain IP addresses or across specific network interfaces allows administrators to track usage by various areas. Traffic flow information may be used to engineer networks for better performance.

Procedure for Configuring NetFlow

1. **Enable NetFlow:** Select one of the Netflow versions to enable NetFlow functionality: **v5**, **v9**, or **IPFIX**. Internet Protocol Flow Information Export (IPFIX) is an IETF protocol (www.ietf.org**)** performing many of the same functions as Netflow. Choose **Disable** if you wish to disable this feature.

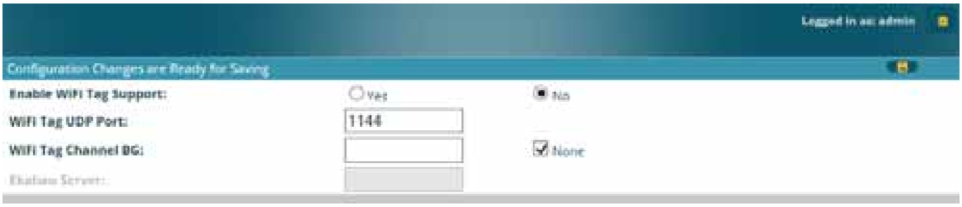
If you select IPFIX, 64 bit counters are supported starting with Release 7.1. IPFIX uses IF-MIB, whose ifXTables support 64 bit counters.

2. **NetFlow Collector Host (Domain or IP)**: If you enabled NetFlow, enter the domain name or IP address of the collector.

3. **NetFlow Collector Port**: If you enabled NetFlow, enter the port on the collector host to which to send data.

Wi-Fi Tag

This window enables or disables Wi-Fi tag capabilities. When enabled, the WAP listens for and collects information about Wi-Fi RFID tags sent on the designated channel. These tags are transmitted by specialized tag devices (for example, AeroScout or Ekahau tags). A Wi-Fi tagging server then queries the WAP for a report on the tags that it has received. The Wi-Fi tagging server uses proprietary algorithms to determine locations for devices sending tag signals.



Enable WiFi Tag Support:	○ Yes	● No
WiFi Tag UDP Port:	1144	
WiFi Tag Channel BG:		☑ None
Ekahau Server:		

Figure 91. Wi-Fi Tag

Procedure for Configuring Wi-Fi Tag

1. **Enable Wi-Fi Tag:** Choose **Yes** to enable Wi-Fi tag functionality, or choose **No** to disable this feature.

2. **Wi-Fi Tag UDP Port**: If Wi-Fi tagging is enabled, enter the UDP port that the Wi-Fi tagging server will use to query the WAP for data. When queried, the WAP will send back information on tags it has observed. For each, the WAP sends information such as the MAC address of the tag transmitting device, and the RSSI and noise floor observed.

3. **Wi-Fi Tag Channel BG**: If you enabled Wi-Fi tagging, enter the 802.11 channel on which the WAP will listen for tags. The tag devices must be set up to transmit on this channel. Only one channel may be configured, and it must be an 802.11b/g channel in the range of Channel 1 to 11.

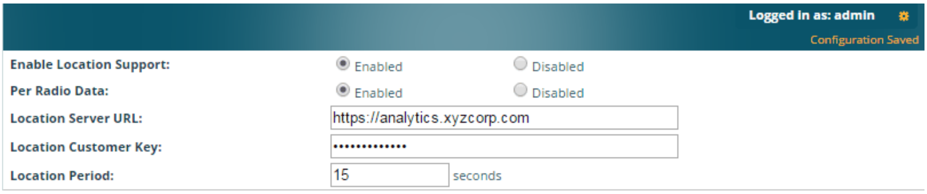
4. **Ekahau Server**: If you enabled Wi-Fi tagging and you are using an Ekahau server, enter its IP address or hostname. Ekahau Wi-Fi Tag packets received by the WAP will be encapsulated as expected by Ekahau, and forwarded to the server.

Location

The WAP offers an integrated capability for capturing and uploading visitor analytics data, eliminating the need to install a standalone sensor network. This data can be used to characterize information such as guest or customer traffic and location, visit duration, and frequency. Use this Location window to configure the WAP to send collected data to an analytics server, such as Euclid.

When Location Support is enabled, the WAP collects information about stations, including the station ID and manufacturer, time and length of the visit and related time interval statistics, and signal strength and its related statistics. Data collected from stations comprises only basic device information that is broadcast by Wi-Fi enabled devices. Devices that are only detected are included, as well as those that actually connect to the WAP. Multiple data points may be sent for a station— data is sent for each radio that sees a probe request from the station. The WAP sending the data also sends its own ID so that the server knows where the visitors were detected. Data messages are uploaded via HTTPS, and they are encrypted if a

Location Customer Key has been entered. Data is sent as JSON (JavaScript Object Notation) objects, as described in “Location Service Data Formats” on page 503.



Logged in as: admin

Configuration Saved

Enable Location Support:	● Enabled	○ Disabled
Per Radio Data:	● Enabled	○ Disabled
Location Server URL:	https://analytics.xyzcorp.com	
Location Customer Key:	•••••••••••••	
Location Period:	15 seconds	

Figure 92. Location

Procedure for Configuring Location

1. **Enable Location Support:** Choose **Enabled** to enable the collection and upload of visitor analytic data, or choose **Disabled** to disable this feature.

2. **Per Radio Data**: Choose **Enabled** to enable the collection and upload of visitor analytic data on a per-radio basis, or choose **Disabled** to disable this feature.

3. **Location Server URL**: If Location Support is enabled, enter the URL of the location / analytics server. If this URL contains the string **euclid**, then the WAP knows that data is destined for a Euclid location server.

   For a Euclid analytics server, use the URL that was assigned to you as a customer by Euclid. The WAP will send JSON-formatted messages in the form required by Euclid via HTTPS.

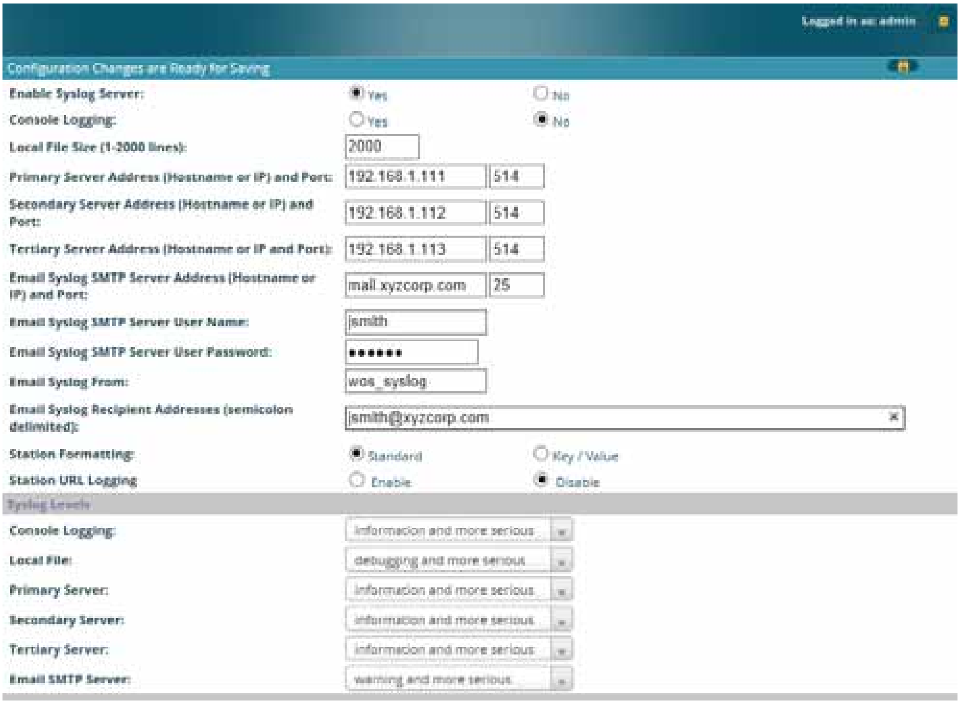
   For any other location analytics server, enter its URL. The WAP will send JSON-formatted messages in the form described in “Location Service Data Formats” on page 503.

4. **Location Customer Key**: (optional) If a **Location Customer Key** has been entered, data is sent encrypted using AES with that key.

5. **Location Period**: If you enabled Location Support, specify how often data is to be sent to the server, in seconds.

System Log

This window allows you to enable or disable the Syslog server, define primary, secondary, and tertiary servers, set up email notification, and set the level for Syslog reporting for each server and for email notification—the Syslog service will send Syslog messages at the selected severity or above to the defined Syslog servers and email address. An option allows you to use a Splunk application to analyze WAP events by sending data in key:value pairs, as described in "About Using Splunk for Avaya WAPs" on page 174.



Enable Syslog Server:	● Yes	○ No
Console Logging:	○ Yes	● No
Local File Size (1-2000 lines):	2000	
Primary Server Address (Hostname or IP) and Port:	192.168.1.111	514
Secondary Server Address (Hostname or IP) and Port:	192.168.1.112	514
Tertiary Server Address (Hostname or IP and Port):	192.168.1.113	514
Email Syslog SMTP Server Address (Hostname or IP) and Port:	mail.xyzcorp.com	25
Email Syslog SMTP Server User Name:	jsmith	
Email Syslog SMTP Server User Password:	••••••	
Email Syslog From:	wos_syslog	
Email Syslog Recipient Addresses (semicolon delimited):	jsmith@xyzcorp.com	
Station Formatting:	● Standard	○ Key / Value
Station URL Logging	○ Enable	● Disable
Syslog Levels		
Console Logging:	information and more serious	
Local File:	debugging and more serious	
Primary Server:	information and more serious	
Secondary Server:	information and more serious	
Tertiary Server:	information and more serious	
Email SMTP Server:	warning and more serious	

Figure 93. System Log

Procedure for Configuring Syslog

1. **Enable Syslog Server:** Choose **Yes** to enable Syslog functionality, or choose **No** to disable this feature.

2. **Console Logging**: If you enabled Syslog, select whether or not to echo Syslog messages to the console as they occur. If you enable console logging, be sure to set the Console Logging level (see Step 9 below).

3. **Local File Size** (1-2000 lines): Enter a value in this field to define how many Syslog records are retained locally on the WAP's internal Syslog file. The default is 2000.

4. **Primary Server Address (Hostname or IP) and Port**: If you enabled Syslog, enter the hostname or IP address of the primary Syslog server. You may also change the port used on the server if you do not wish to use 514, the default port.

5. **Secondary/Tertiary Server Address (Hostname or IP) and Port**: (Optional) If you enabled Syslog, you may enter the hostname or IP address of one or two additional Syslog servers to which messages will also be sent. You may also change the port used on each server if you do not wish to use 514, the default port. You may set one of the server addresses to the address of a server for Splunk (see "About Using Splunk for Avaya WAPs" on page 174).

6. **Email Notification**: (Optional) The following parameters allow you to send an email to a designated address each time a Syslog message is generated. The email will include the text of the Syslog message.

   a. **Email Syslog SMTP Server Address (Hostname or IP) and Port**: The hostname or the IP address of the SMTP server to be used for sending the email. Note that this specifies the mail server, **not** the email recipient. You may also change the port used on the server if you do not wish to use 25, the default SMTP port.

   b. **Email Syslog SMTP User Name**: Specify a user name for logging in to an account on the mail server designated in Step a.

   c. **Email Syslog SMTP User Password**: Specify a password for logging in to an account on the mail server designated in Step a.

   d. **Email Syslog SMTP From**: Specify the "From" email address to be displayed in the email.

e. **Email Syslog SMTP Recipient Addresses**: Specify the entire email address of the recipient of the email notification. You may specify additional recipients by separating the email addresses with semicolons (;).

7. **Station Formatting**: If you are sending event information to a Splunk server, select **Key/Value** to send data in Splunk's expected format, otherwise leave this at the default value of **Standard**. See "About Using Splunk for Avaya WAPs" on page 174.

8. **Station URL Logging**: When enabled, Syslog messages are sent for each URL that each station visits. Only HTTP destinations (port 80) are logged; HTTPS destinations (port 443) are not logged. All URLs in a domain are logged, so for example, if an HTTP request to yahoo.com generates requests to 57 other URLs, all are logged. Furthermore, each visit to the same URL generates an additional log message. No deep packet inspection is performed by the URL logging, so no Application Control information is included in the Syslog message.

   The following information is included in the syslog message:

   - Date / Time
   - Source Device MAC and IP address
   - Destination Port
   - Destination Site address (e.g., 20.20.20.1)
   - The specific URL (e.g., http://20.20.20.1.24/online/images/img2.jpg)

   Station URL Logging is disabled by default.

9. **Syslog Levels**: For each of the Syslog destinations, choose your preferred level of Syslog reporting from the pull-down list. Messages with criticality at the selected level and above will be shown. The default level varies depending on the destination.

   a. **Console Logging**: For messages to be echoed to the console, the default level is **Critical and more serious**. This prevents large numbers of non-critical messages from being displayed on the console. If you set this level too low, the volume of messages may make it very difficult to work with the CLI or view other output on the console.

b. **Local File**: For records to be stored on the WAP's internal Syslog file, choose your preferred level of Syslog reporting from the pull-down list. The default level is **Debugging and more serious**.

c. **Primary Server**: Choose the preferred level of Syslog reporting for the primary server. The default level is **Debugging and more serious**.

d. **Secondary/Tertiary Server**: Choose the preferred level of reporting for the secondary/tertiary server. The default level is **Information and more serious**. (Optional)

e. **Email SMTP Server**: Choose the preferred level of Syslog reporting for the email notifications. The default level is **Warning and more serious**. This prevents your mailbox from being filled up with a large number of less severe messages such as informational messages.

10. Click the **Save** button 💾 if you wish to make your changes permanent.

About Using Splunk for Avaya WAPs

Splunk may be used to provide visibility into client experience and analyze usage on WAPs. You may develop a Splunk application to present this operational intelligence at a glance (www.splunk.com).

To use Splunk, set up your Splunk server with your Splunk application, if you have one. Configure the WAP to send data to Splunk by setting a **Primary**, **Secondary**, or **Tertiary Server Address** to the IP address or hostname of your Splunk server. Then set **Station Formatting** to **Key/Value** to send data in Splunk's expected format.

You may specify Server Addresses for Syslog servers and a Splunk server on the same WAP. Selecting the **Key/Value** option will not cause any problems with Syslog.

See Also

System Log

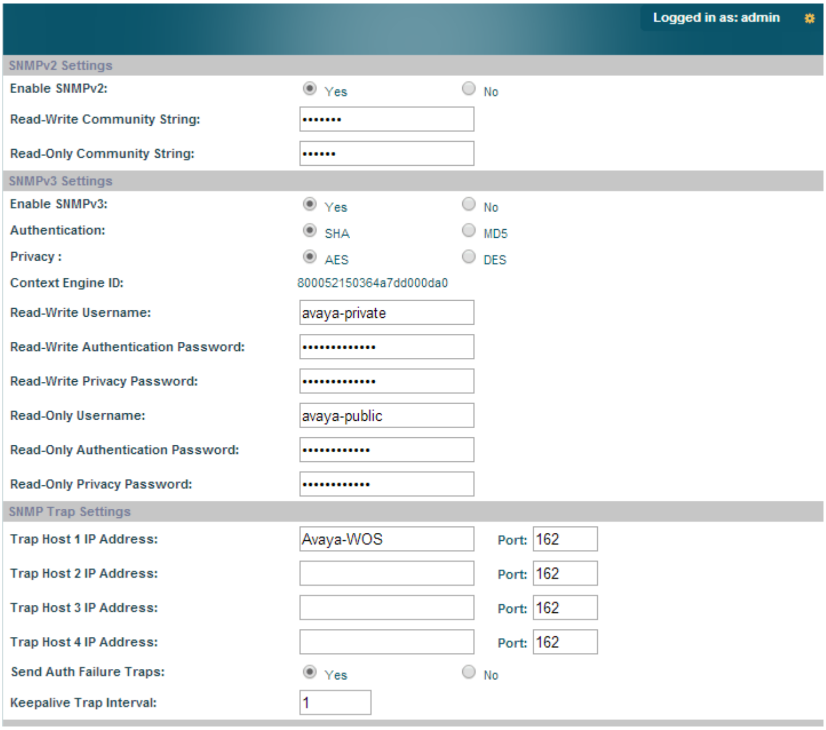
Services

SNMP

Time Settings (NTP)

SNMP

This window allows you to enable or disable SNMP v2 and SNMP v3 and define the SNMP parameters. SNMP allows remote management of the WAP by the WOS and other SNMP management tools. SNMP v3 was designed to offer much stronger security. You may enable either SNMP version, neither, or both.



SNMPv2 Settings			
Enable SNMPv2:	● Yes	○ No	
Read-Write Community String:	•••••••		
Read-Only Community String:	••••••		
SNMPv3 Settings			
Enable SNMPv3:	● Yes	○ No	
Authentication:	● SHA	○ MD5	
Privacy :	● AES	○ DES	
Context Engine ID:	800052150364a7dd000da0		
Read-Write Username:	avaya-private		
Read-Write Authentication Password:	•••••••••••••		
Read-Write Privacy Password:	•••••••••••••		
Read-Only Username:	avaya-public		
Read-Only Authentication Password:	••••••••••••		
Read-Only Privacy Password:	••••••••••••		
SNMP Trap Settings			
Trap Host 1 IP Address:	Avaya-WOS	Port:	162
Trap Host 2 IP Address:		Port:	162
Trap Host 3 IP Address:		Port:	162
Trap Host 4 IP Address:		Port:	162
Send Auth Failure Traps:	● Yes	○ No	
Keepalive Trap Interval:	1		

Figure 94. SNMP

Complete SNMP details for the WAP, including trap descriptions, are found in the Avaya MIB, available at support.avaya.com.

> ***NOTE:** If you are managing your WAPs with WOS (the Wireless LAN Orchestration System), it is very important to make sure that your SNMP settings match those that you have configured for WOS. WOS uses both SNMP v2 and v3.*

Procedure for Configuring SNMP

SNMPv2 Settings

1. **Enable SNMPv2:** Click the checkbox to the left of the **Enabled** label to enable or disable SNMP v2 functionality. When used in conjunction with the Wireless LAN Orchestration System, SNMP v2 (**not** SNMP v3) must be enabled on each WAP to be managed with WOS. The default for this feature is Enabled.

2. **SNMP Read-Write Community String**: Enter the read-write community string. The default is **private**.

3. **SNMP Read-Only Community String**: Enter the read-only community string. The default is **public**.

SNMPv3 Settings

4. **Enable SNMPv3**: Click the checkbox to the left of the **Enabled** label to enable or disable SNMP v3 functionality. The default for this feature is Disabled.

5. **Authentication**: Select the desired method for authenticating SNMPv3 packets: Secure Hash Algorithm (**SHA**) or Message Digest Algorithm 5 (**MD5**).

6. **Privacy**: Select the desired method for encrypting data: Data Encryption Standard (**DES)** or the stronger Advanced Encryption Standard (**AES)**.

7. **Context Engine ID**: The unique identifier for this SNMP server. We recommend that you do not change this value. The Context Engine ID must be set if data collection is to be done via a proxy agent. This ID helps the proxy agent to identify the target agent from which data is to be collected.

8. **SNMP Read-Write Username**: Enter the read-write user name. This username and password allow configuration changes to be made on the WAP. The default is **avaya-private**.

9. **SNMP Read-Write Authentication Password**: Enter the read-write password for authentication (i.e., logging in). The default is **avaya-private**.

10. **SNMP Read-Write Privacy Password**: Enter the read-write password for privacy (i.e., a key for encryption). The default is **avaya-private**.

11. **SNMP Read-Only Username**: Enter the read-only user name. This username and password do not allow configuration changes to be made on the WAP. The default is **avaya-public**.

12. **SNMP Read-Only Authentication Password**: Enter the read-only password for authentication (i.e., logging in). The default is **avaya-public**.

13. **SNMP Read-Only Privacy Password**: Enter the read-only password for privacy (i.e., a key for encryption). The default is **avaya-public**.

SNMP Trap Settings

14. **SNMP Trap Host IP Address**: Enter the **IP Address** or hostname, as well as the **Port** number, of an SNMP management station that is to receive SNMP traps. You may specify up to four hosts that are to receive traps. Note that by default, **Trap Host 1** sends traps to **Avaya-WOS**. Thus, the WAP will automatically communicate its presence to WOS (as long as the network is configured correctly to allow this host name to be resolved—note that DNS is not normally case-sensitive).

    For a definition of the traps sent by WAPs, you may download the Avaya MIB from support.avaya.com. Search for the string **TRAP** in the MIB file.

15. **Send Auth Failure Traps**: Click the checkbox to the left of the **Enabled** label to enable or disable log authentication failure traps.

16. **Keepalive Trap Interval** (minutes): Traps are sent out at this interval to indicate the presence of the WAP on the network. Keepalive traps are required for proper operation with WOS. To disable keepalive traps, set the value to **0**.

17. Click the **Save** button if you wish to make your changes permanent.

See Also

Services

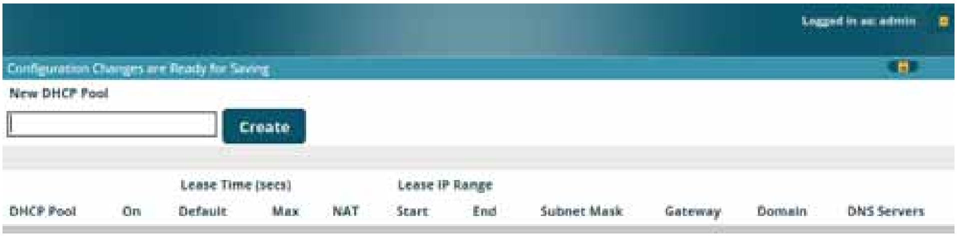
System Log

Time Settings (NTP)

DHCP Server

This window allows you to create, enable, modify and delete DHCP (Dynamic Host Configuration Protocol) address pools. DHCP allows the WAP to provide wireless clients with IP addresses and other networking information. The DHCP server will not provide DHCP services to the wired side of the network. If you do not use the DHCP server on the WAP, then your wired network must be configured to supply DHCP addresses and gateway and DNS server addresses to wireless clients.

When you create a DHCP pool, you must define the DHCP lease time (default and maximum), the IP address ranges (pools) that the DHCP server can assign, and the gateway address and DNS servers to be used by clients.



		Lease Time (secs)			Lease IP Range					
DHCP Pool	On	Default	Max	NAT	Start	End	Subnet Mask	Gateway	Domain	DNS Servers

Figure 95. DHCP Management

DHCP usage is determined in several windows—see SSID Management, Group Management, and VLAN Management.

Procedure for Configuring the DHCP Server

1. **New Internal DHCP Pool**: Enter a name for the new DHCP pool, then click on the **Create** button. The new pool ID is added to the list of available DHCP pools. You may create up to 16 DHCP pools.
2. **On**: Click this checkbox to make this pool of addresses available, or clear it to disable the pool.
3. **Lease Time—Default**: This field defines the default DHCP lease time (in seconds). The factory default is 300 seconds, but you can change the default at any time.
4. **Lease Time—Max**: Enter a value (in seconds) to define the maximum allowable DHCP lease time. The default is 300 seconds.
5. **Network Address Translation (NAT)**: Check this box to enable the Network Address Translation feature. The NATed address uses the IP address of the WAP's outbound gigabit Ethernet interface.
6. **Lease IP Range—Start**: Enter an IP address to define the start of the IP range that will be used by the DHCP server. The default is 192.168.1.100.
7. **Lease IP Range—End**: Enter an IP address to define the end of the IP range that will be used by the DHCP server. The DHCP server will only use IP addresses that fall between the start and end range that you define on this page. The default is 192.168.1.200.
8. **Subnet Mask**: Enter the subnet mask for this IP range for the DHCP server. The default is 255.255.255.0.
9. **Gateway**: If necessary, enter the IP address of the gateway.
10. **Domain**: Enter the DNS domain name. See "DNS Settings" on page 160.
11. **DNS Servers** (1 to 3): Enter the IP address of the primary DNS server, secondary DNS server and tertiary DNS server. These DNS server addresses will be passed to stations when they associate, along with the

assigned IP address. Note that if you leave these blank, no DNS information is sent to the stations. DHCP will **not** default to sending the DNS servers that are configured in DNS Settings. See also, “DNS Settings” on page 160.

12. Click the **Save** button if you wish to make your changes permanent.

See Also

DHCP Leases

DNS Settings

Network Map

Proxy Services

APs do not support HTTP/S proxy. You will receive an error message if you attempt to configure this feature.

If your organization uses a proxy server such as Blue Coat or Netbox Blue to control Internet access, use this page to configure proxy forwarding on the WAP. Options are provided for proxying user traffic and WAP management traffic.

Proxy services for user traffic are discussed in the following topics:

- “About Proxy Forwarding” on page 181
- “Proxy Forwarding for HTTPS” on page 182
- “Summary of Proxy Forwarding Behavior on the WAP” on page 183
- “Configuring Proxy Forwarding on Clients for HTTPS” on page 184
- “Procedure for Configuring Proxy Forwarding on the WAP” on page 188

Proxy services for management traffic are discussed in the following topics:

- “About Using a Proxy Client for Management Traffic” on page 188
- “Procedure for Configuring Proxy Client for Management Traffic” on page 189

About Proxy Forwarding

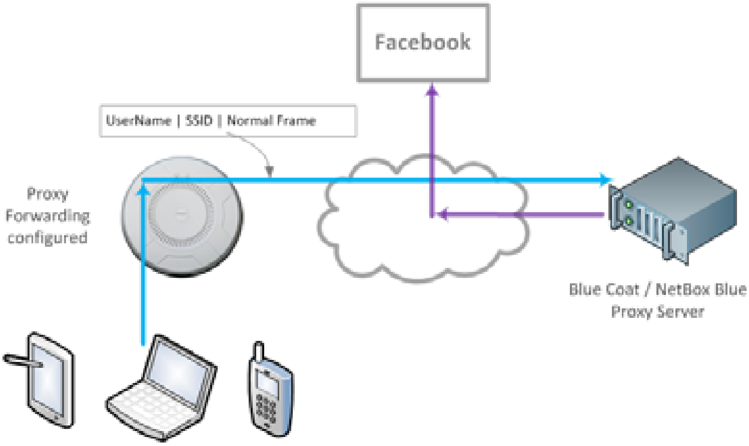

Facebook
UserName | SSID | Normal Frame
Proxy Forwarding configured
Blue Coat / NetBox Blue Proxy Server

Figure 96. Proxy Forwarding Example

When you configure proxy forwarding settings on the WAP, it forwards each HTTP request to the proxy server (for example, Blue Coat) at the specified URL, which checks if the policies that you have set up on the server are satisfied. If so, the proxy server sends the request on to the desired web site. An example is shown in Figure 96. The user of the laptop tries to open Facebook on a browser. The WAP forwards this request to the proxy server that you have specified, after adding a prefix with the **user's ID** and the **SSID** (the SSID serves as a user group; for unauthenticated clients, the MAC address serves as the user name). The proxy server checks whether its configured policies permit this access for this user and SSID. If so, the frame is forwarded to the desired web site.

SSID and client User Name restrictions permit the following characters.
— Blue Coat permits only alphanumerics and + and /.
— Netbox Blue permits only alphanumerics and dot, hyphen, underscore, and space characters.

Proxy forwarding on the WAP is designed for proxy servers such as Blue Coat and Netbox Blue whose purpose is restricting Internet access to sites, applications and content, and the monitoring and reporting of this activity. It is not used for enhanced performance utilizing content caching.

Blue Coat policy configuration:
The AuthConnector utility is not used with the Avaya implementation. Traffic must first be passed through the portal to dynamically add the User to Blue Coat's list of recognized Users, based on the User header inserted in the packets. When configuring Blue Coat Content Filtering policy, you may select "Users from Reporting". Only the User value can be used in this manner. The Group header value is not dynamically added to Blue Coat's Group list, and it can't be added manually.

Netbox Blue policy configuration:
Users and Groups are manually configured on the server. Users are manually assigned to Groups, and policy is applied on a per-Group basis.

Proxy forwarding on the WAP is configured as described in "Procedure for Configuring Proxy Forwarding on the WAP" on page 188. This proxies all HTTP traffic to the specified server. If you wish to proxy HTTPS traffic as well, you must take the additional steps described below.

Proxy Forwarding for HTTPS

There are two usage scenarios for proxy forwarding:

- Use proxy forwarding for HTTP traffic only: set up the WAP per "Procedure for Configuring Proxy Forwarding on the WAP" on page 188. HTTPS traffic is unaffected and proceeds in the usual way.
- Use proxy forwarding for both HTTP and HTTPS traffic: set up the WAP per "Procedure for Configuring Proxy Forwarding on the WAP" on page 188. Then you must set up browsers on client stations (laptops, smart phones, tablets, ...) to proxy both HTTP and HTTPS traffic to the WAP. Each client must also download and install the SSL certificate from the Blue Coat or Netbox Blue proxy server. Follow the procedure below to perform these steps on each client. Note that when a proxy is set up and used for HTTPS, HTTP traffic will also use the proxy server, so configure both as instructed in "Configuring Proxy Forwarding on Clients for HTTPS" on page 184.

Summary of Proxy Forwarding Behavior on the WAP

If proxy forwarding is **not** enabled in the WAP and the client browser is **not** configured to use a proxy:

- HTTP traffic (port 80) and HTTPS traffic (port 443) pass transparently through the WAP in the usual way.

If proxy forwarding **is** enabled for Blue Coat or Netbox Blue and the client browser is **not** configured to use a proxy (i.e., you do not wish to proxy secure traffic):

- The browser still uses HTTP (port 80) and this traffic is captured and proxied by the WAP.
- The browser still uses HTTPS (port 443) and this traffic is passed transparently through the WAP.
- If proxy forwarding is not working correctly, HTTP traffic (port 80) is blocked.

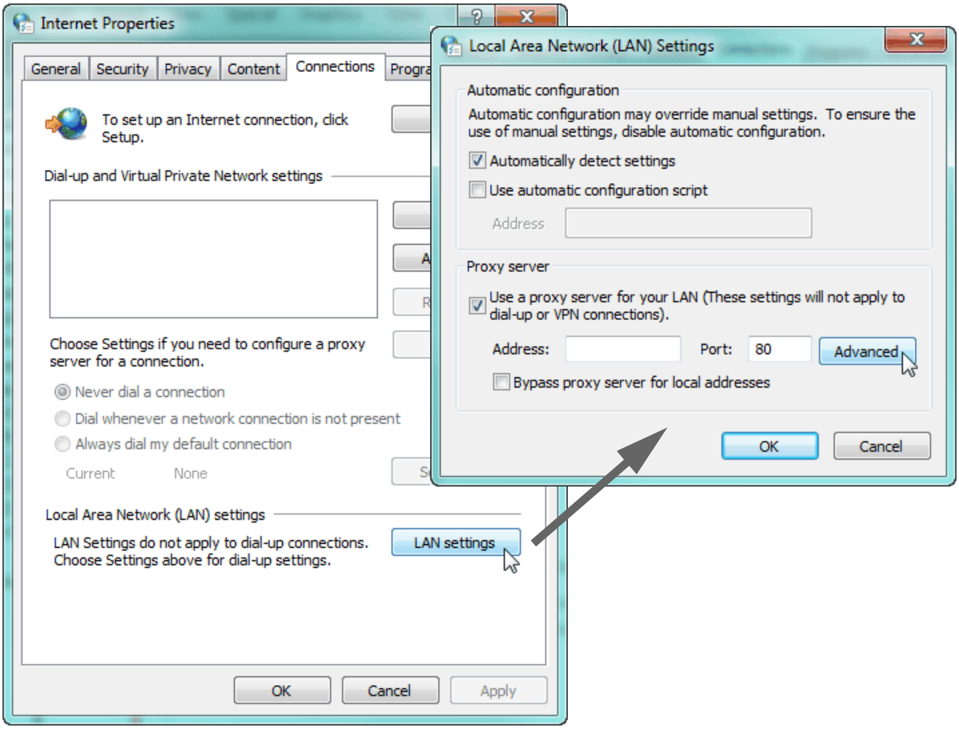
If proxy forwarding **is** enabled for Blue Coat or Netbox Blue and the client browser **is** configured to use a proxy:

- The browser is configured to proxy HTTPS to port 4388.
- The browser automatically proxies HTTP traffic to the **same** port that is used for HTTPS traffic—port 4388.
- All HTTP/HTTPS traffic is captured by the WAP and proxied to Blue Coat or Netbox Blue per your settings.
- If WAP proxy forwarding is not working correctly (for example, if the configuration is incorrect), all HTTP/HTTPS/4388 traffic is blocked.

Configuring Proxy Forwarding on Clients for HTTPS

To set the proxy server on an Apple laptop, skip to Step 3.

1. For Windows laptops, click the desktop **Start** button. In the **Search programs and files** field, enter **Configure proxy server**. The Internet Properties dialog is displayed. (Figure 97) Click the **LAN Settings** button. The Local Area Network dialog displays.



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings
□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: 80

□ Bypass proxy server for local addresses

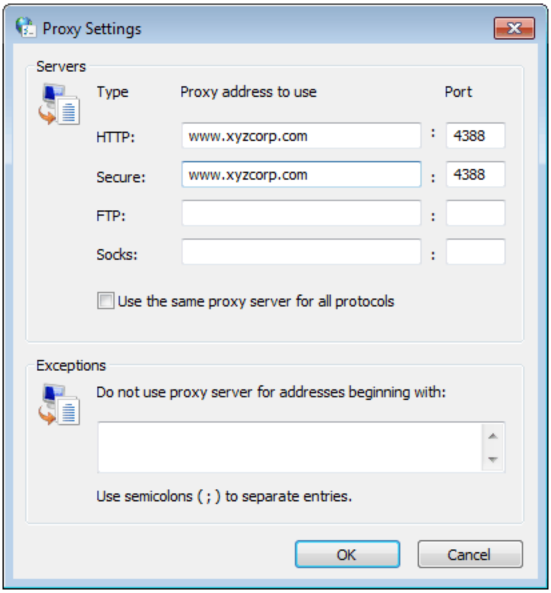
Figure 97. Set up a Proxy Server on each Client (Windows)

2. In the Proxy Server section, click the **Advanced** button. The Proxy Settings dialog displays. (Figure 98)

   For **HTTPS:** Enter any valid address, such as your company's web site in the **Proxy address to use** field. For example, **www.xyzcorp.com** as shown in Figure 94. This field is not actually used, but Windows needs it to be a valid address or domain name. You **must** set the **Port** to **4388**. This is **very important**! This is the WAP port that should receive all HTTPS traffic if you are using a proxy server.

For **HTTP:** HTTP traffic will automatically use the same port that you have configured for HTTPS: 4388. We suggest that you enter your company's web site, **Port 4388** here to make it obvious that HTTP traffic is being proxied in this way.

Continue to Step 5.



HTTP: www.xyzcorp.com : 4388

Secure: www.xyzcorp.com : 4388

FTP: :

Socks: :

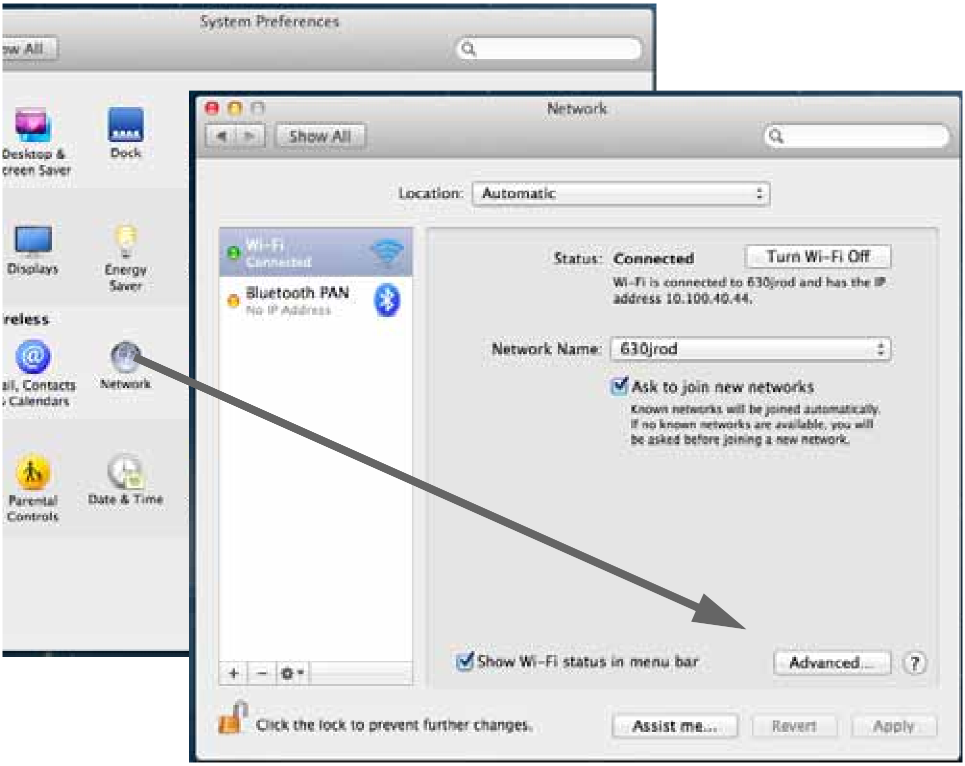
☐ Use the same proxy server for all protocols

Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

Figure 98. Specify Proxy Servers (Windows)

3. For Apple laptops, open **System Preferences** and select **Network**. The Network dialog is displayed. (Figure 99) Click the **Advanced** button.



Location: Automatic

Status: Connected

Wi-Fi is connected to 630jrod and has the IP address 10.100.40.44.

Network Name: 630jrod

☑ Ask to join new networks

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

☑ Show Wi-Fi status in menu bar

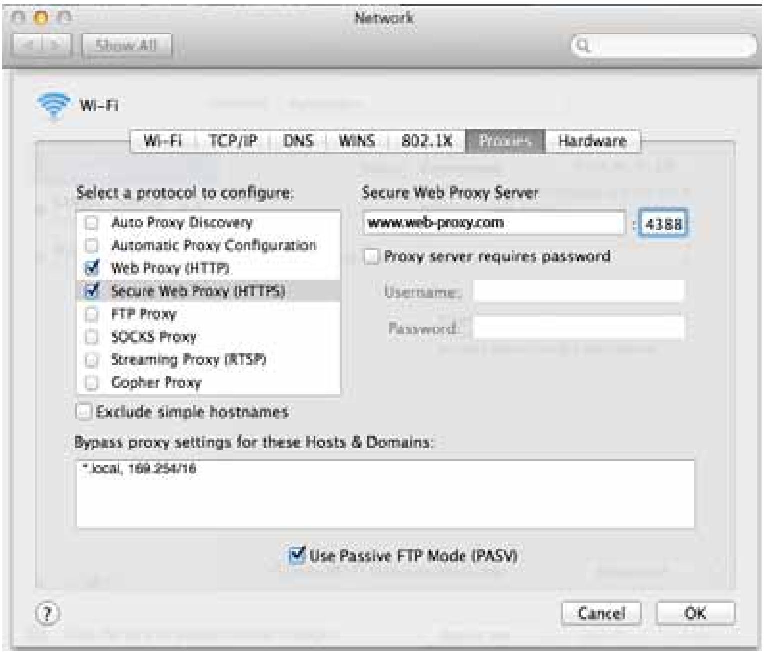
Click the lock to prevent further changes.

Figure 99. Set up a Proxy Server on each Client (Apple)

4. Select the **Proxies** tab. (Figure 100)

   Check **Secure Web Proxy (HTTPS):** Under **Secure Web Proxy Server**, you can enter any valid address. We suggest that you enter **www.avaya.com**. (This field is not actually used, but it must be a valid address or domain name). You **must** set the **Port** to **4388**. This is **very** important! This is the WAP port that must receive all HTTPS traffic if you are using a proxy server for HTTPS.

Check **Web Proxy (HTTP):** Under **Web Proxy Server**, we suggest that you enter **www.avaya.com Port 4388** to make it obvious that HTTP traffic is being proxied in this way.



Select a protocol to configure:

- □ Auto Proxy Discovery
- □ Automatic Proxy Configuration
- ☑ Web Proxy (HTTP)
- ☑ Secure Web Proxy (HTTPS)
- □ FTP Proxy
- □ SOCKS Proxy
- □ Streaming Proxy (RTSP)
- □ Gopher Proxy

□ Exclude simple hostnames

Bypass proxy settings for these Hosts & Domains:

*.local, 169.254/16

Secure Web Proxy Server

www.web-proxy.com : 4388

□ Proxy server requires password

Username:

Password:

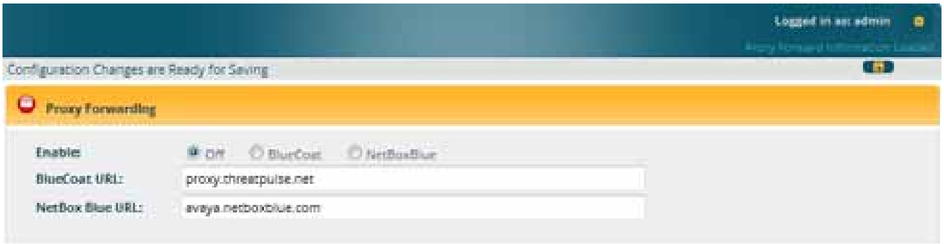
☑ Use Passive FTP Mode (PASV)

Figure 100. Specify Proxy Servers (Apple)

5. **SSL Certificate**: you must download and install the security certificate from your proxy server—Blue Coat or Netbox Blue. It must be installed on each of your client devices.

Procedure for Configuring Proxy Forwarding on the WAP

1. **Enable:** If you wish to use proxy forwarding, select the proxy server type**—Blue Coat** or **Netbox Blue**.



Logged in as: admin

Configuration Changes are Ready for Saving

Proxy Forwarding

Enable: ● Off ○ BlueCoat ○ NetBoxBlue

BlueCoat URL: proxy.threatpulse.net

NetBox Blue URL: avaya.netboxblue.com

Figure 101. Proxy Forwarding

2. **BlueCoat URL**: If you selected **Blue Coat** above, enter the URL of the proxy server, for example, **http://proxy.threatpulse.net**.

3. **Netbox Blue URL**: If you selected **Netbox Blue** above, enter the actual URL of the proxy server, for example, **avaya.netboxblue.com**. Note that this default URL is not an actual proxy server—this prevents you from unintentionally forwarding traffic.

About Using a Proxy Client for Management Traffic

Some deployments require that all Internet traffic, including management traffic, use proxy services. For instance, some school systems require *all* traffic to use a proxy server. The WAP generates management traffic to implement essential functions such as licensing / activation. The WAP allows you to configure clients that are used to proxy such management traffic.

If your deployment requires proxying the WAP's management traffic, rather than allowing that traffic to go directly out to the Internet, you will need to configure the following clients:

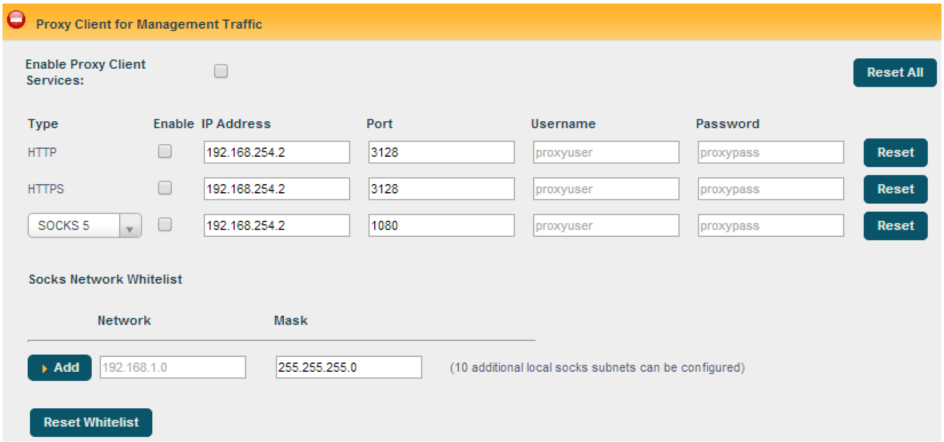
- **HTTP** and **HTTPS**: This traffic sends traps and fetches configurations from WOS. You must enter the IP address and subnet mask of the proxy server. If this server requires authentication, you may enter a user name and password as well.

- **SOCKS**: Other management functions use this form of socket to send traffic. Currently, two versions of SOCKS are broadly used on the Internet – Version 4 and Version 5. The service defaults to Version 5 if no version is declared.

  The SOCKS proxy client requires a whitelist of networks that will not be proxied. At the least, this must include the loopback address and the subnet where the proxy server lives. Additional defined subnets should include DNS servers and authentication servers.

Procedure for Configuring Proxy Client for Management Traffic

1. **Enable:** For each proxy client, you must **Enable** it if you wish to use it.



Proxy Client for Management Traffic

Enable Proxy Client Services: □

Type	Enable	IP Address	Port	Username	Password	
HTTP	□	192.168.254.2	3128	proxyuser	proxypass	Reset
HTTPS	□	192.168.254.2	3128	proxyuser	proxypass	Reset
SOCKS 5	□	192.168.254.2	1080	proxyuser	proxypass	Reset

Socks Network Whitelist

	Network	Mask	
Add	192.168.1.0	255.255.255.0	(10 additional local socks subnets can be configured)

Figure 102. Proxy Client for Management Traffic

2. **IP Address/Port**: For each proxy client, enter the IP Address and Port of the proxy server. For the **HTTP** and **HTTPS** proxy clients, you may specify a fully qualified domain name (FQDN) or an IP address. For SOCKS, an FQDN is not allowed—an IP address is required. The default Port settings are standard defaults for these ports.

3. **Username/Password**: For each proxy client, if the proxy server requires authentication, enter the Username and Password here.

4. **SOCKS 4/ SOCKS 5:** Select the version of SOCKS in use on your proxy server. The default is SOCKS 5.

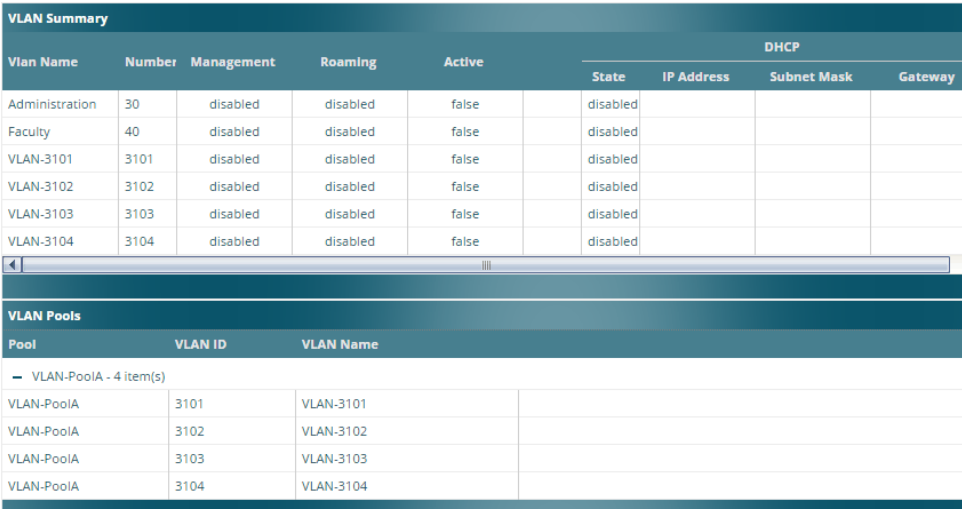
5. **Socks Network Whitelist**: Enter a whitelist of subnetworks that must not be proxied. Specify each subnet by entering its **Network** address and its subnet **Mask**, then click **Add**. At the least, create entries for the loopback address and the subnet where the proxy server lives. You should also enter subnets that include your DNS servers and authentication servers.

VLANs

This is a status-only window that allows you to review the current status of configured VLANs and VLAN Pools. VLANs are virtual LANs used to create broadcast domains. VLAN pools are provided for special situations where clients are to be assigned one of a set of VLANs that are treated as a pool. See “VLAN Pools” on page 193.

You should create VLAN entries on the WAP for all of the VLANs in your wired network if you wish to make traffic from those VLANs available on the wireless network. Each tagged VLAN should be associated with a wireless SSID (see “VLAN Management” on page 194). The WAP will discard any VLAN-tagged packets arriving on its wired ports, unless the same VLAN has been defined on the WAP. See “Undefined VLANs” on page 95.

In addition to listing all VLANs, this window shows your settings for the Default Route VLAN and the Native (Untagged) VLAN (Step 1 page 195).



VLAN Summary

Vlan Name	Number	Management	Roaming	Active		DHCP			
						State	IP Address	Subnet Mask	Gateway
Administration	30	disabled	disabled	false		disabled			
Faculty	40	disabled	disabled	false		disabled			
VLAN-3101	3101	disabled	disabled	false		disabled			
VLAN-3102	3102	disabled	disabled	false		disabled			
VLAN-3103	3103	disabled	disabled	false		disabled			
VLAN-3104	3104	disabled	disabled	false		disabled			

VLAN Pools

Pool	VLAN ID	VLAN Name
− VLAN-PoolA - 4 item(s)		
VLAN-PoolA	3101	VLAN-3101
VLAN-PoolA	3102	VLAN-3102
VLAN-PoolA	3103	VLAN-3103
VLAN-PoolA	3104	VLAN-3104

Figure 103. VLANs

Understanding Virtual Tunnels

Avaya WAPs support Layer 2 tunneling. This allows a WAP to use tunnels to transport traffic for one or more SSID-VLAN pairs onto a single destination network through the Layer 3 core network. Tunnels may be implemented with:

- Virtual Tunnel Server (VTS)—see below.

You may specify a tunnel for a VLAN as described below and in "Procedure for Managing VLANs" on page 195. These tunnels are typically set up to be encrypted. Alternatively, the GRE tunnels created in "Tunnel Management" on page 200 are not encrypted, offering much higher throughput and improved scaling. If tunneled traffic is not traversing public networks, GRE is recommended. While VLAN tunnels and GRE can be used on the same AP simultaneously, more than one tunnel shouldn't be configured to tunnel the same traffic.

Virtual Tunnel Server (VTS)

Tunneling capability is provided by a Virtual Tunnel Server. You supply the server and deploy it in your network using open-source VTun software, available from vtun.sourceforge.net. To enable the WAP to use tunneling for a VLAN, simply enter the IP address, port and secret for the tunnel server as described in Step 13 on page 198.

VTun may be configured for a number of different tunnel types, protocols, and encryption types. For use with WAPs, we recommend the following configuration choices:

- Tunnel Type: Ether (Ethernet tunnel)
- Protocol: UDP
- Encryption Type: select one of the encryption types supported by VTun (AES and Blowfish options are available)
- Keepalive: yes

VTS Client-Server Interaction

The WAP is a client of the Virtual Tunnel Server. When you specify a VTS for an active VLAN-SSID pair, the WAP contacts the VTS. The server then creates a tunnel session to the WAP. VTun encapsulated packets will cross the Layer 3 network from the WAP to the VTS. When packets arrive at the VTS, they will be de-encapsulated and the resultant packets will be passed to your switch with 802.1q VLAN tags for final Layer 2 processing. The process occurs in reverse for packets traveling in the other direction.

We recommend that you enable the VTun keep-alive option. This will send a keep-alive packet once per second to ensure that the tunnel remains active. Tunnels can be configured to come up on demand but this is a poor choice for wireless, since tunnel setup can take roughly 5-20 seconds and present a problem for authentication.

VLAN Pools

A VLAN pool is a set of VLANs. Using a pool allows a client associating to an AP to be assigned to one of the VLANs in the pool rather than to a particular VLAN. This is useful in special networking situations. For example, a large hotel uses four Internet access gateways to capture Wi-Fi users. Each gateway uses one VLAN. On the hotel’s APs, we create a VLAN pool with the four gateway VLANs. When a client connects to an AP, it is assigned to one of the VLANs in the pool. This distributes users approximately evenly among the gateways, roughly balancing their loads.

Each client device is assigned to a pool VLAN with a computation based on the lower digits of its MAC address, so that the device will always be assigned to the same VLAN. This ensures that a client roaming from one AP to the next will be handled properly. Note that the VLAN assigned is also based on the VLANs in the pool, so that if changes are made to the pool, the client device may be assigned to a different VLAN.

You may specify a VLAN pool rather than a particular VLAN for SSIDs or for user groups. See “Procedure for Managing SSIDs” on page 255 or “Procedure for Managing Groups” on page 277.

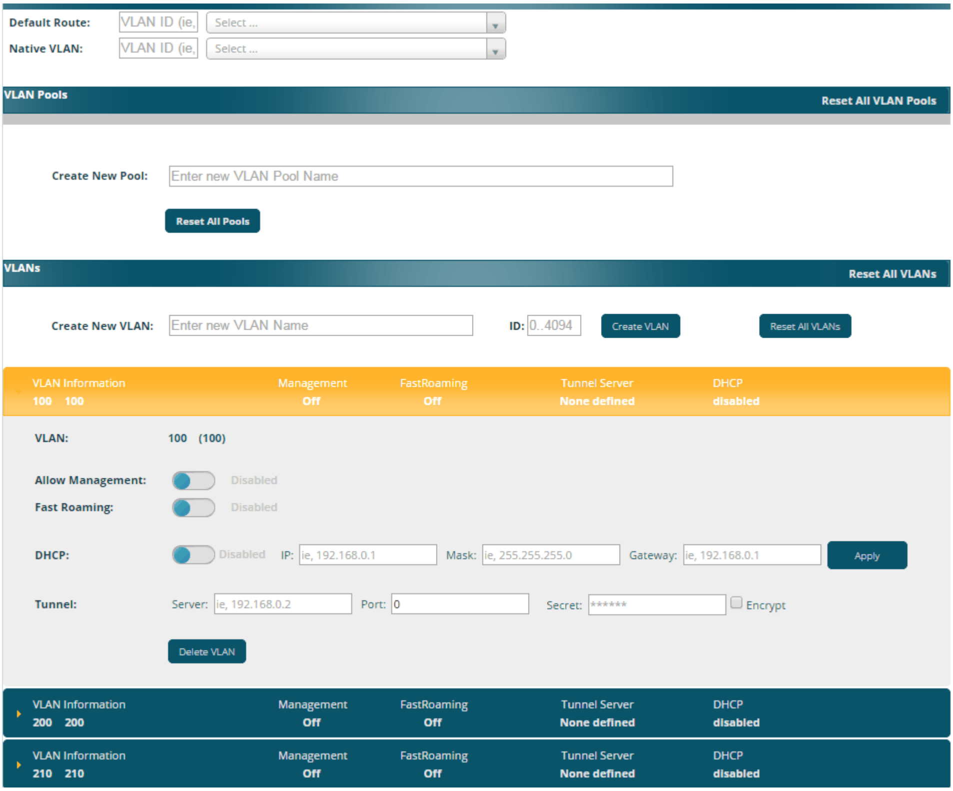
You may create up to 16 VLAN pools, and each may contain up to the maximum number of VLANS that may be created on the AP. If a user has a VLAN assigned via RADIUS authentication, then this VLAN will be used rather than one from the

VLAN pool. If a user has a VLAN assigned via a Group, then this VLAN will be used rather than one from the VLAN pool.

To set up a VLAN pool, see the next section.

VLAN Management

This window allows you to set up VLANs and VLAN Pools. After creating a new VLAN (added to the list of VLANs), you can modify the configuration parameters of an existing VLAN or delete a selected VLAN. For Avaya OS 7.0 and later releases, you may create up to 64 VLANs (up to 32 on WAO9122).



Default Route: VLAN ID (ie, Select ...

Native VLAN: VLAN ID (ie, Select ...

VLAN Pools — Reset All VLAN Pools

Create New Pool: Enter new VLAN Pool Name

Reset All Pools

VLANs — Reset All VLANs

Create New VLAN: Enter new VLAN Name ID: 0..4094 Create VLAN Reset All VLANs

VLAN Information	Management	FastRoaming	Tunnel Server	DHCP
100 100	Off	Off	None defined	disabled

VLAN: 100 (100)

Allow Management: Disabled

Fast Roaming: Disabled

DHCP: Disabled IP: ie, 192.168.0.1 Mask: ie, 255.255.255.0 Gateway: ie, 192.168.0.1 Apply

Tunnel: Server: ie, 192.168.0.2 Port: 0 Secret: ****** ☐ Encrypt

Delete VLAN

VLAN Information	Management	FastRoaming	Tunnel Server	DHCP
200 200	Off	Off	None defined	disabled
210 210	Off	Off	None defined	disabled

Figure 104. VLAN Management

*The WAP supports dynamic VLAN assignments specified by RADIUS policy settings. When RADIUS sends these assignments, the WAP dynamically assigns wireless stations to VLANs as requested. VLAN tags on traffic are passed through the WAP (i.e., VLAN tags are not stripped). Once a station has been dynamically moved to a new VLAN, it will be shown in the Stations window as a member of the new VLAN. (**Figure 52 on page 108**)*

It is critical to configure all VLANs to be used on the WAP, even those that will be dynamically assigned.

Procedure for Managing VLANs

1. **Default Route:** This option sets a default route from the WAP. The WAP supports a default route on native and tagged interfaces. Once the default route is configured the WAP will attempt to use Address Resolution Protocol (ARP) to find the default router. ARP finds the MAC address of a device with a given IP address by sending out a broadcast message requesting this information. This option allows you to choose a default VLAN route from the pull-down list. The IP Gateway must be established for this function to work. After changing the **Default Route**, you *must* click the **Save** button 💾 *and then reboot.*

Note: Avaya recommends to separate AP management traffic from Wireless Station traffic. Leaving Default Route and Native VLAN fields empty results in all WAP management traffic going out untagged using the Gig Interface. Wireless Client Traffic will be Tagged with the VLAN ID Associated to the SSID.

For Avaya Edge switches, the Port tagging mode should be "UntagPvidOnly" in this configuration. The port PVID should be set to the AP Management VLAN.

If a WAP is configured to send Management Traffic as Tagged Traffic by enabling management on one of the VLAN created on the WAP and not setting the Native VLAN, then the Port tagging mode on the Avaya Edge switch port tagging mode should be "TagAll" with PVID set to the VLAN that is enabled for management.

2. **Native VLAN**: This option sets whether the WAP management is tagged or untagged. If you select a Native VLAN, then that VLAN will use an untagged (Native) link. Otherwise, the WAP will use 802.1Q tagging and a specific VLAN ID with management enabled for management of the WAP.

VLAN Pools

3. See "VLAN Pools" on page 193 for a discussion of VLAN pools. To add a new pool, type its name in **Create New Pool**, and click ENTER. The new VLAN pool entry is added to the list.

4. First, create all of the VLANs that will belong to this pool. See Step 5 below.

   Click in the field for the new pool to display a list of VLANs. Add the desired VLANs to this pool, one at a time. This field also provides a search feature—type in a string, and a list will display all VLANs whose names contain that string in any position (VLAN names are searched, but not VLAN numbers). Click the **Apply** button on the right when done adding VLANs. Note that the same VLAN can be added to more than one pool. Be sure to consider any network implications of using the same VLAN in multiple pools.

Click **Reset** if you want to remove all of the VLANs from this pool, i.e., to empty it. Click **Remove** to delete this pool. You may use **Reset All Pools** on the bottom to delete all pools.

VLANs

5. **Create New VLAN**: Enter a name for the new VLAN in this field. **ID**: Enter a number for this VLAN (0-4094). Click the **Create VLAN** button. The new VLAN appears in the list. Entries are sorted alphabetically by VLAN name. Select the new entry to modify any of the settings below.

6. **Fabric Attach**: Check this box to allow this VLAN to participate in Fabric Attach. This feature is enabled by default, and should normally be used for VLANs.

   If Fabric Attach is in use on the network, it should only be disabled for a VLAN in special situations. For example, in order to support the Honeypot feature which requires a local VLAN to drop client traffic, you should disable Fabric Attach for the VLAN associated with the Honeypot SSID. This VLAN will be local to the AP and the service request for this VLAN should not be sent to the Fabric Attach switch. See also, “High Density 2.4G Enhancement—Honeypot SSID” on page 253 and “Fabric Attach Settings” on page 162.

7. **Management**: Move the slider if you want to allow AP management over this VLAN.

8. **Fast Roaming**: Move the slider if you want to allow roaming over this VLAN.

9. **DHCP**: Move the slider if you want the DHCP server to assign the IP address, subnet mask and gateway address for this VLAN automatically, otherwise you must go to the next step and assign these parameters manually.

10. **IP Address**: If the DHCP option is disabled, enter a valid IP address for this VLAN association.

11. **Subnet Mask**: If the DHCP option is disabled, enter the subnet mask IP address for this VLAN association.

12. **Gateway**: If the DHCP option is disabled, enter the IP gateway address for this VLAN association.

13. **Tunnel Server**: If this VLAN is to be tunneled, enter the IP address or host name of the tunnel server that will perform the tunneling. For more information on virtual tunnels, please see "Understanding Virtual Tunnels" on page 192.

14. **Tunnel Server Port**: If this VLAN is to be tunneled, enter the port number of the tunnel server.

15. **New Secret**: Enter the password expected by the tunnel server.

16. **Delete VLAN**: To delete the selected VLAN, simply click the **Delete** button to remove the VLAN from the list.

17. Click the **Save** button 💾 if you wish to make your changes permanent.

See Also

VLAN Statistics

VLANs

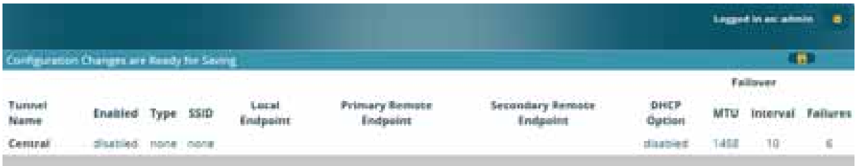
Tunnels

Tunnels

This read-only window allows you to review the tunnels that have been defined on the WAP. It lists all tunnels and their settings, including the type of authentication and the local and remote endpoints for each tunnel.

Tunnels are discussed in these sections:

- About Avaya Tunnels
- Tunnel Management
- SSID Assignments
- VLAN Assignments



Logged in as: admin

Configuration Changes are Ready for Saving

								Failover		
Tunnel Name	Enabled	Type	SSID	Local Endpoint	Primary Remote Endpoint	Secondary Remote Endpoint	DHCP Option	MTU	Interval	Failures
Central	disabled	none	none				disabled	1400	10	6

Figure 105. Tunnel Summary

About Avaya Tunnels

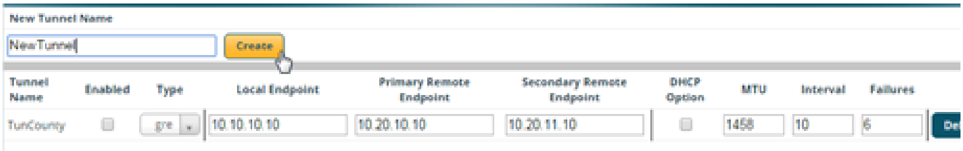
Avaya WAPs offer GRE (Generic Routing Encapsulation) tunneling with VLAN support. This allows a WAP to use tunnels to bridge Layer 2 traffic for one or more SSIDs onto a single destination network through the Layer 3 network. You may specify particular VLANs on an SSID to be tunneled, or tunnel all of the VLANs that are on this SSID. GRE tunneling is quite flexible, and can encapsulate many network layer protocols. As a result, it can support a variety of applications. For example, a Wi-Fi hotspot can allow guest logins and use the tunnel to give guests direct access to the Internet, without allowing access to the local network. In a small office, you may define a tunnel to connect users to the corporate office network. Tunnels may also used when providing cellular offload capability. For non-GRE tunnels associated with particular VLANs, see "Understanding Virtual Tunnels" on page 192.

Tunnels may be implemented with VTS —see "Virtual Tunnel Server (VTS)" on page 192.

To create a tunnel, you specify the **Local Endpoint**, which should be one of the WAP's wired ports, and the **Primary Remote Endpoint**. A **Secondary Remote Endpoint** may also be specified in case of a failure at the first endpoint. Traffic for the designated VLANs on an SSID is sent in GRE encapsulated packets across the Layer 3 network from the WAP to the remote endpoint. When packets arrive, the encapsulation is stripped and the resultant packets are passed to your switch with 802.1q VLAN tags for final Layer 2 processing. The process occurs in reverse for packets traveling in the other direction.

Tunnel Management

This window allows you to create tunnels.



New Tunnel Name

NewTunnel

Tunnel Name	Enabled	Type	Local Endpoint	Primary Remote Endpoint	Secondary Remote Endpoint	DHCP Option	MTU	Interval	Failures
TunCounty	□	gre	10.10.10.10	10.20.10.10	10.20.11.10	□	1458	10	6

Figure 106. Tunnel Management

Procedure for Managing Tunnels

1. **New Tunnel Name**: Enter a name for the new tunnel in this field, then click on the **Create** button. The new tunnel is added to the list. You may crate up to 250 Layer 3 tunnels.

2. **Enabled**: The new tunnel is created in the disabled state. Click this checkbox to enable it.

3. **Type**: Enter the type of tunnel, **none** or **gre**.

4. **Local Endpoint**: Enter the IP address of the WAP Gigabit or 10 Gigabit port where the tunnel is to begin.

5. **Primary Remote Endpoint**: Enter the IP address of the remote endpoint of the tunnel.

6. **Secondary Remote Endpoint**: This provides a failover capability. If the primary tunnel fails, traffic is switched over to the secondary tunnel. Enter the IP address of the remote endpoint of the secondary tunnel.

7. **DHCP Option**: When this option is enabled, the WAP snoops station DHCP requests and inserts relay agent information (Option 82, in the CIRCUIT-ID sub-option) into these DHCP packets. Information inserted includes WAP BSSID, SSID name, and SSID encryption type. You may use this option here or on the SSID Management page, but not in both places. Information is inserted as a colon-separated text string in the CIRCUIT ID value field in this format: [AP_MAC];[SSID];[ENC]

[AP_MAC]	length = 17 (aa:bb:cc:dd:ee:ff)
[SSID]	length = length of SSID name
[ENC]	length = 1 (encryption type: 'o' = open, 's' = non-open)

Note that this is a different format than is used for Option 82 with SSIDs.

8. **MTU**: Set maximum transmission unit (MTU) size.

9. **Interval**: The tunnel mechanism will ping the current remote endpoint periodically to ensure that it is still reachable. Enter the ping interval (in seconds).

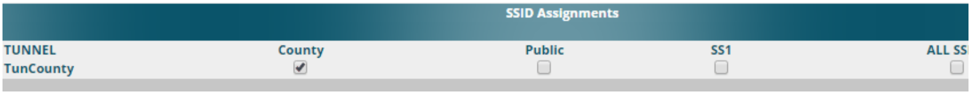
10. **Failures**: Enter the number of consecutive ping failures that will cause the WAP to consider the tunnel to be down. tunnel to failover to the other remote endpoint.

11. Click the **Save** button 💾 if you wish to make your changes permanent.

12. Proceed to SSID Assignments to define the SSIDs for which each tunnel will bridge data. You may create up to 16 tunnels. Assign one or more SSIDs to each tunnel. You may restrict the tunnel to handling traffic for particular VLANs on each SSID if you wish, as described in VLAN Assignments.

SSID Assignments

This window allows you to select the SSIDs to be bridged by each tunnel. Station traffic for SSIDs assigned will be bridged through the tunnel, but you may restrict which VLANs are tunneled for each SSID (see VLAN Assignments, below). By default, all VLANs will be tunneled. When VLAN traffic is tunneled, it will be tagged accordingly.



SSID Assignments

TUNNEL	County	Public	SS1	ALL SS
TunCounty	☑	☐	☐	☐

Figure 107. Tunnel SSID Assignments

Procedure for Assigning SSIDs

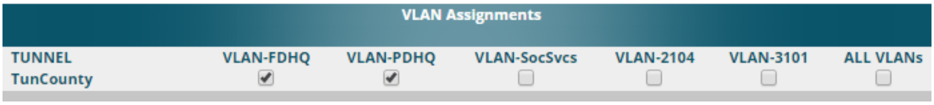
This window lists the tunnels and SSIDs that you have defined.

1. For each tunnel, select the SSIDs that are to be bridged to the remote endpoint. Clear the checkbox for any SSID that you no longer wish to include in the tunnel. You may use the **ALL SSIDs** checkbox to toggle between selecting all SSIDs, or none.

2. Click the **Save** button 💾 to make your changes permanent.

VLAN Assignments

When you assign an SSID to a tunnel, all VLANs on that SSID will be transported to the tunnel by default. This window allows you to select specific VLANs to be bridged by each tunnel. A VLAN's station traffic bridged through a tunnel will be tagged accordingly. Station traffic for a VLAN that is not tunneled is forwarded to the local subnet, i.e., dropped off locally at the edge of the switch network to which the AP is connected.



VLAN Assignments

TUNNEL	VLAN-FDHQ	VLAN-PDHQ	VLAN-SocSvcs	VLAN-2104	VLAN-3101	ALL VLANs
TunCounty	☑	☑	□	□	□	□

Figure 108. Tunnel VLAN Assignments

Procedure for Assigning SSIDs

This window lists the tunnels and VLANs that you have defined.

1. For each tunnel, select the VLANs that are to be bridged to the remote endpoint. Clear the checkbox for any VLAN that you no longer wish to include in the tunnel. You may use the **ALL VLANs** checkbox to toggle between selecting all VLANs, or none. Note that if you add any VLANs to this list, then they will be the **only** VLANs transported on this tunnel. Also note that many VLANs may be in use on an SSID if they are assigned to stations dynamically by a RADIUS server or by user groups (see "Groups" on page 275).

2. Click the **Save** button 💾 to make your changes permanent.

See Also

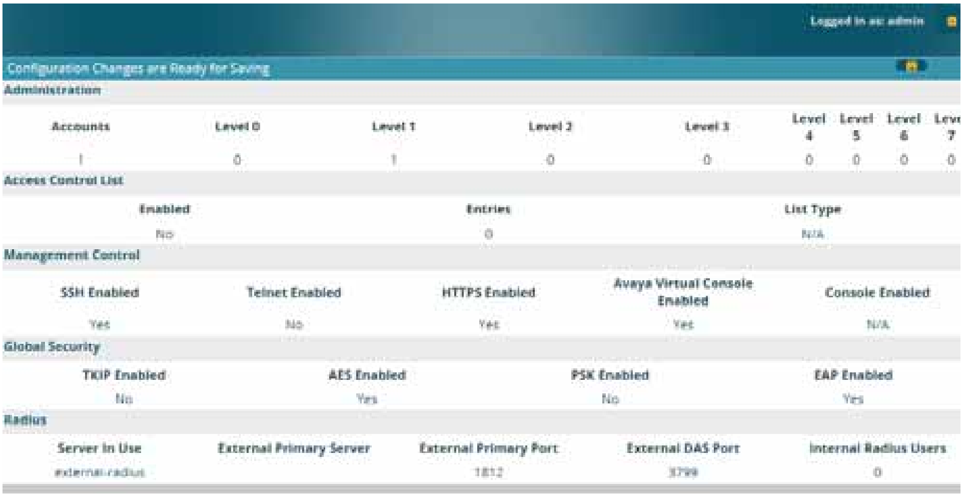
Tunnels

VLANs

SSIDs

Security

This status-only window allows you to review the WAP’s security parameters. It includes the assigned network administration accounts, Access Control List (ACL) values, management settings, encryption and authentication protocol settings, and RADIUS configuration settings. There are no configuration options available in this window, but if you are experiencing issues with security, you may want to print this window for your records.



Administration

Accounts	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5	Level 6	Leve 7
1	0	1	0	0	0	0	0	0

Access Control List

Enabled	Entries	List Type
No	0	N/A

Management Control

SSH Enabled	Telnet Enabled	HTTPS Enabled	Avaya Virtual Console Enabled	Console Enabled
Yes	No	Yes	Yes	N/A

Global Security

TKIP Enabled	AES Enabled	PSK Enabled	EAP Enabled
No	Yes	No	Yes

Radius

Server In Use	External Primary Server	External Primary Port	External DAS Port	Internal Radius Users
external-radius		1812	3799	0

Figure 109. Security

For additional information about wireless network security, refer to:

- **“Security Planning” on page 42**
- **“Understanding Security” on page 205**
- **The Security section of “Frequently Asked Questions” on page 490**

For information about secure use of the WMI, refer to:

- **“Certificates and Connecting Securely to the WMI” on page 208**
- **“Using the WAP’s Default Certificate” on page 209**
- **“Using an External Certificate Authority” on page 210**
- **“About Creating Admin Accounts on the RADIUS Server” on page 214**

- **"About Creating User Accounts on the RADIUS Server" on page 233**

Security settings are configured with the following windows:

- **"Admin Management" on page 210**
- **"Admin Privileges" on page 212**
- **"Admin RADIUS" on page 214**
- **"Management Control" on page 217**
- **"Access Control List" on page 227**
- **"Global Settings" on page 229**
- **"External Radius" on page 232**
- **"Internal Radius" on page 236**
- **"Active Directory" on page 238**
- **"Rogue Control List" on page 242**
- **"OAuth 2.0 Management" on page 244**

Understanding Security

The WAP incorporates many configurable security features. After initially installing a WAP, always change the default administrator password (the default is admin), and choose a strong replacement password (containing letters, numbers and special characters). When appropriate, issue read-only administrator accounts.

Other security considerations include:

- **SSH versus Telnet**: Be aware that Telnet is not secure over network connections and should be used only with a direct serial port connection. When connecting to the unit's Command Line Interface (CLI) over a network connection, you must use a Secure SHell version 2 (SSH-2) utility. SSH-2 provides stronger security than SSH-1. The most commonly used freeware providing SSH tools is PuTTY.
- **Configuration auditing**: The optional WOS offers powerful management features for small or large wireless deployments, and can audit your configuration settings automatically. In addition, using the WOS eliminates the need for an FTP server.

- **Choosing an encryption method**: Wireless data encryption prevents eavesdropping on data being transmitted or received over the airwaves. The WAP allows you to establish the following data encryption configuration options:
    - **Open**—this option offers no data encryption and is not recommended, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTy.
    - **Wired Equivalent Privacy (WEP)**—this option provides minimal protection (though much better than using an open network). An early standard for wireless data encryption and supported by all Wi-Fi certified equipment, WEP is vulnerable to hacking and is therefore not recommended for use by Enterprise networks.
    - **Wi-Fi Protected Access (WPA** and **WPA2)**—these are much stronger encryption modes than WEP, using Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) to encrypt data.

      WPA solves security issues with WEP. It also allows you to establish encryption keys on a per-user-basis, with key rotation for added security. In addition, TKIP provides Message Integrity Check (MIC) functionality and prevents active attacks on the wireless network.

      AES is the strongest encryption standard and is used by government agencies; however, old legacy hardware may not be capable of supporting the AES mode (it probably won't work on older wireless clients). Because AES is the strongest encryption standard currently available, WPA2 with AES is highly recommended for Enterprise networks.

  Any of the above encryption methods can be used and a WAP can support multiple encryption methods simultaneously, but only one method may be selected per SSID (except that selecting **WPA-Both** allows WPA and WPA2 to be used at the same time on the same SSID).

Otherwise, if multiple security methods are needed, you must define multiple SSIDs.

The encryption mode (WEP, WPA, etc.) is selected in the **SSIDs >SSID Management** window (see "SSID Management" on page 254). The encryption standard used with WPA or WPA2 (AES or TKIP) is selected in the **Security>Global Settings** window under **WPA Settings** (see "Global Settings" on page 229).

- **Choosing an authentication method**: User authentication ensures that users are who they say they are. For this purpose, the WAP allows you to choose between the following user authentication methods:
  - **Pre-Shared Key**—users must manually enter a key (passphrase) on the client side of the wireless network that matches the key stored by the administrator in the WAP.

    This method should be used only for smaller networks when a RADIUS server is unavailable. If PSK must be used, choose a strong passphrase containing between 8 and 63 characters (20 is preferred). Always use a combination of letters, numbers and special characters. Never use English words separated by spaces.
  - **RADIUS 802.1x with EAP**—802.1x uses a RADIUS server to authenticate large numbers of clients, and can handle different Extensible Authentication Protocol (EAP) authentication methods, including EAP-TLS, EAP-TTLS, EAP-PEAP, and LEAP-Passthrough. The RADIUS server can be internal (provided by the WAP) or external. An external RADIUS server offers more functionality and security, and is recommended for large deployments. When using this method, user names and passwords must be entered into the RADIUS server for user authentication.
  - **MAC Address Access Control Lists (ACLs)**—MAC address ACLs provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network. Access Control Lists work well when there are a limited number of users—in this case, enter the MAC address of each user in the Allow list. In

the event of a lost or stolen MAC adapter, enter the affected MAC address in the Deny list. The WAP will accept up to 1,000 ACL entries.

- **PCI DSS**—to implement the requirements of these security standards on the WAP, please see "Auditing PCI DSS" on page 509.

Certificates and Connecting Securely to the WMI

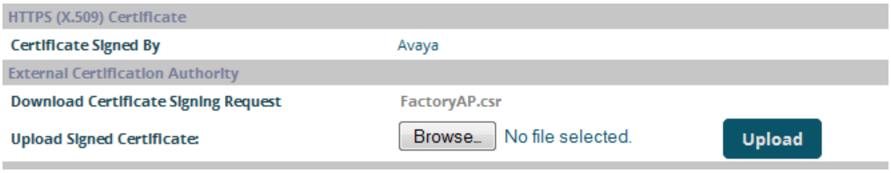
When you point your browser to the WAP to connect to the WMI, the WAP presents an X.509 security certificate to the browser to establish a secure channel. One significant piece of information in the certificate is the WAP's host name. This ties the certificate to a particular WAP and ensures the client that it is connecting to that host.

Certificate Authorities (CAs) are entities that digitally sign certificates, using their own certificates (for example, VeriSign is a well-known CA). When the WAP presents its certificate to the client's browser, the browser looks up the CA that signed the certificate to decide whether to trust it. Browsers ship with a small set of trusted CAs already installed. If the browser trusts the certificate's CA, it checks to ensure the host name (and IP address) match those on the certificate. If any of these checks fail, you get a security warning when connecting to the WMI.

The WAP ships with a default certificate that is signed by the Avaya CA. You may choose to use this certificate, or to use a certificate issued by the CA of your choice, as described in the following sections:

- Using the WAP's Default Certificate
- Using an External Certificate Authority

Using the WAP’s Default Certificate



HTTPS (X.509) Certificate		
Certificate Signed By	Avaya	
External Certification Authority		
Download Certificate Signing Request	FactoryAP.csr	
Upload Signed Certificate:	Browse... No file selected.	Upload

Figure 110. Import Avaya Certificate Authority

The WAP’s certificate is signed by an Avaya CA that is customized for your WAP and its current host name. By default, browsers will not trust the WAP’s certificate. You may import the Avaya certificate to instruct the browser to trust the Avaya CA on all future connections to WAPs. The certificate for the Avaya CA is available on the WAP, so that you can import it into your browser’s cache of trusted CAs (right alongside VeriSign, for example). On the Management Control window of the WMI you will see the **avaya-ca.crt** file.

By clicking and opening this file, you can follow your browser’s instructions and import the Avaya CA into your CA cache (see “HTTPS (X.509) Certificate” on page 223 for more information). This instructs your browser to trust any of the certificates signed by the Avaya CA, so that when you connect to any of our WAPs you should no longer see the warning about an untrusted site. Note however, that this only works if you use the host name when connecting to the WAP. If you use the IP address to connect, you get a lesser warning saying that the certificate was only meant for ‘hostname’.

Since a WAP’s certificate is based on the WAP’s host name, any time you change the host name the WAP’s CA will regenerate and sign a new certificate. This happens automatically the next time you reboot after changing the host name. If you have already installed the Avaya CA on a browser, this new WAP certificate should automatically be trusted.

When you install the Avaya CA in your browser, it will trust a certificate signed by any Avaya WAP, as long as you connect using the WAP’s host name.

Using an External Certificate Authority

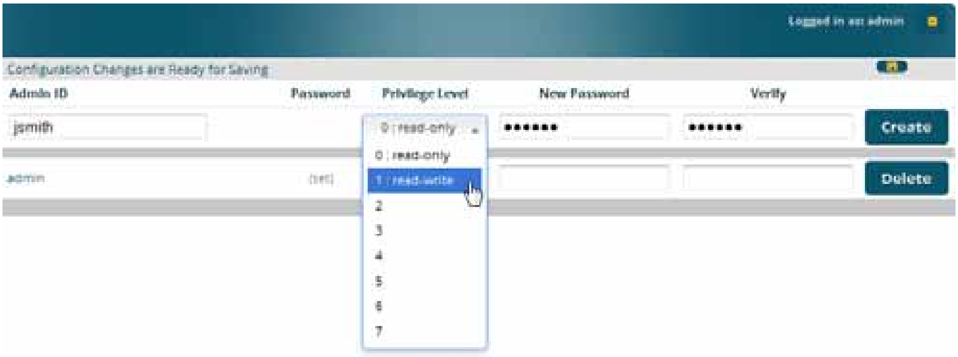
If you prefer, you may install a certificate on your WAP signed by an outside CA.

The WAP's certificate is used for security when stations attempt to associate to an SSID that has Web Page Redirect (captive portal) enabled. In this case, it is preferable for the WAP to present a certificate from an external CA that is likely to be trusted by most browsers. When a WPR login page is presented, the user will not see a security error if the WAP's certificate was obtained from an external CA that is already trusted by the user's browser.

WMI provides options for creating a Certificate Signing Request that you can send to an external CA, and for uploading the signed certificate to the WAP after you obtain it from the CA. This certificate will be tied to the WAP's host name and private key. See "External Certificate Authority" on page 225 for more details.

Admin Management

This window allows you to manage network administrator accounts (create, modify and delete). It also allows you to limit account access to a read only status. When finished, click the **Save** button 💾 if you wish to make your changes permanent.



Logged in as: admin

Configuration Changes are Ready for Saving

Admin ID	Password	Privilege Level	New Password	Verify	
jsmith		0 : read-only	••••••	••••••	Create
admin	(set)				Delete

Figure 111. Admin Management

Procedure for Creating or Modifying Network Administrator Accounts

1. **Admin ID:** Enter the login name for a new network administrator ID. The length of the ID must be between 5 and 50 characters, inclusive.

2. **Read/Write**: Choose **1:read-write** if you want to give this administrator ID full read / write privileges, or choose **0:read-only** to restrict this user to read only status. In the read only mode, administrators cannot save changes to configurations. Or you may select one of your custom-defined privilege levels (see “Admin Privileges” on page 212).

3. **New Password**: Enter a password for this ID. The length of the password must be between 5 and 50 characters, inclusive.

4. **Verify**: Re-enter the password in this field to verify that you typed the password correctly. If you do not re-enter the correct password, an error message is displayed).

5. Click on the **Create** button to add this administrator ID to the list.

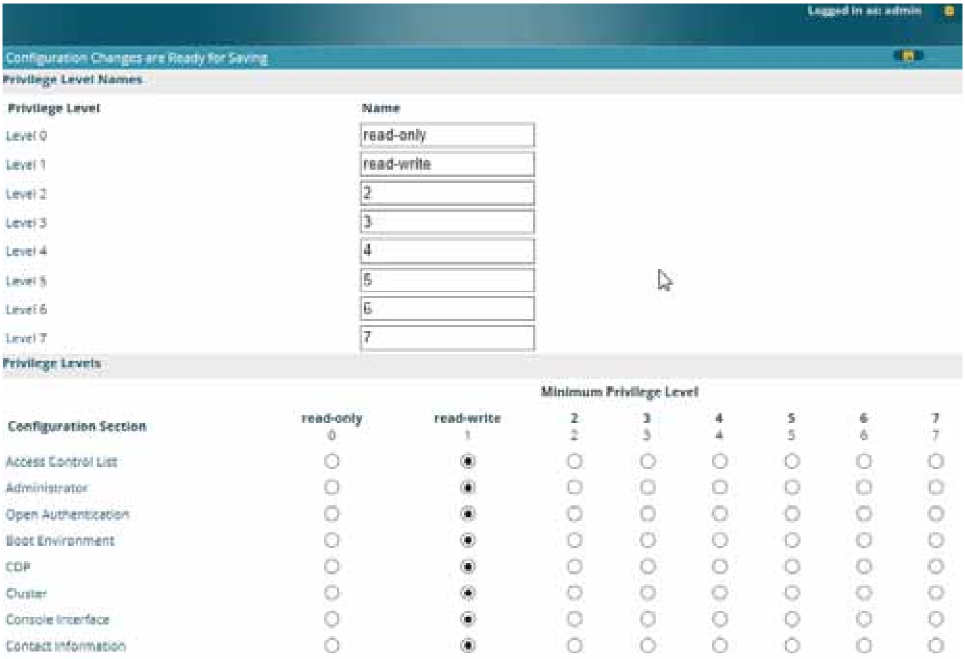
6. Click the **Save** button 💾 if you wish to make your changes permanent.

See Also

Admin Privileges
External Radius
Global Settings
Internal Radius
Management Control

Admin Privileges

This window provides a detailed level of control over the privileges of WAP administrators. Administrators may be assigned one of eight **Privilege Levels**. You may define the privilege level of each major feature (**Configuration Section**) that may be configured on the WAP. For example, say that you set the privilege level to 4 for Reboot WAP, Security, Radius Server, and SNMP, and you leave all other configuration sections at the default privilege level of 1. In this case, any administrator with a privilege level of 4 or higher may perform any operation on the WAP, while an administrator with a privilege level lower than 4 but at least 1 may perform any operation except those whose level was set to 4. An error message will be displayed if an operation is attempted without a sufficient privilege level.



Configuration Changes are Ready for Saving

Privilege Level Names

Privilege Level	Name
Level 0	read-only
Level 1	read-write
Level 2	2
Level 3	3
Level 4	4
Level 5	5
Level 6	6
Level 7	7

Privilege Levels

	Minimum Privilege Level							
Configuration Section	read-only 0	read-write 1	2 2	3 3	4 4	5 5	6 6	7 7
Access Control List	○	●	○	○	○	○	○	○
Administrator	○	●	○	○	○	○	○	○
Open Authentication	○	●	○	○	○	○	○	○
Boot Environment	○	●	○	○	○	○	○	○
CDP	○	●	○	○	○	○	○	○
Cluster	○	●	○	○	○	○	○	○
Console Interface	○	●	○	○	○	○	○	○
Contact Information	○	●	○	○	○	○	○	○

Figure 112. Admin Privileges

Privilege level 0 is **read-only**. As a minimum, all administrators have permission for read access to all areas of WAP configuration. Higher privilege levels may be used to define additional privileges for specific configuration sections.

If you are using an Admin RADIUS server to define administrator accounts, please see “RADIUS Vendor Specific Attribute (VSA) for Avaya” on page 500 to set the privilege level for each administrator.

Procedure for Configuring Admin Privileges

1. **Privilege Level Names** (optional): You may assign a **Name** to each Privilege Level. The name may be used to describe the access granted by this level. By default, levels **0** and **1** are named **read-only** and **read-write**, respectively, and levels **2** through **7** have the same name as their level number.

2. **Privilege Levels**: Use this section to assign a **Minimum Privilege Level** to selected **Configuration Sections** as desired. By default, all sections are assigned level 1. When you select a higher privilege level for a configuration section, then only administrators who have at least that privilege level will be able to make configuration changes to that section.

3. You may click ^ at the bottom of any row to toggle the values in the entire column to either on or off.

4. Click the **Save** button 💾 if you wish to make your changes permanent.

See Also

External Radius
Groups
Admin Management
Admin RADIUS
Security

Admin RADIUS

This window allows you to set up authentication of network administrators via RADIUS. Using RADIUS to control administrator accounts for logging in to WAPs has these benefits:

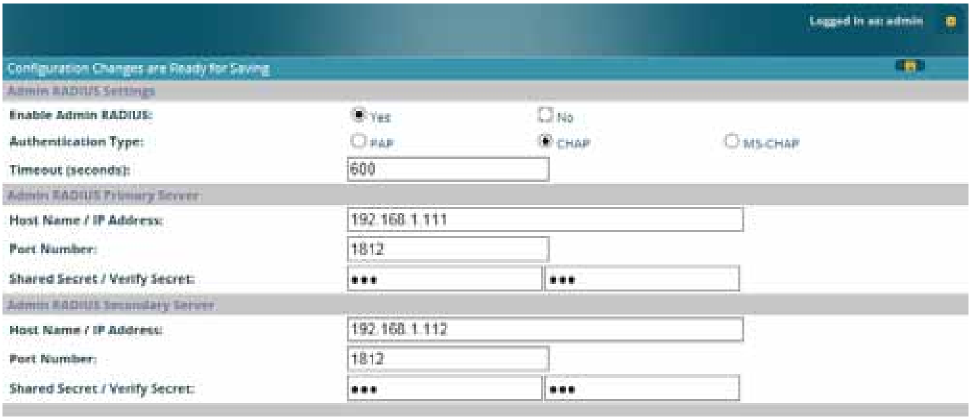
- Centralized control of administrator accounts.
- Less effort—you don't have to set up user names and passwords on each WAP; just enter them once on the RADIUS server and then all of the WAPs can pull from the RADIUS server.
- Enforced policies—you may set password rules (e.g., passwords must contain at least one number and be at least 12 characters in length), and you may set expiration times for passwords.

Admin RADIUS settings override any local administrator accounts configured on the Admin Management window. If you have Admin RADIUS enabled, all administrator authentication is done via the configured RADIUS servers.

About Creating Admin Accounts on the RADIUS Server

Permissions for RADIUS administrator accounts are controlled by the RADIUS **Avaya-Admin-Role** attribute. This is a Vendor Specific Attribute (VSA). To define the privileges permitted to an administrator account, set the value of its Avaya-Admin-Role attribute to the desired **Privilege Level Name** string, as defined in “Admin Privileges” on page 212. For more information about the RADIUS VSAs used by Avaya, see “RADIUS Vendor Specific Attribute (VSA) for Avaya” on page 500.

When configuring administrator accounts on the RADIUS server, you must observe the same restrictions for length and legal characters as when creating these accounts on the WAP using the Admin Management window: the user name and password must be between 5 and 50 characters, inclusive.



Logged in as: admin

Configuration Changes are Ready for Saving

Admin RADIUS Settings

Enable Admin RADIUS:	● Yes	○ No	
Authentication Type:	○ PAP	● CHAP	○ MS-CHAP
Timeout (seconds):	600		

Admin RADIUS Primary Server

Host Name / IP Address:	192.168.1.111	
Port Number:	1812	
Shared Secret / Verify Secret:	●●●	●●●

Admin RADIUS Secondary Server

Host Name / IP Address:	192.168.1.112	
Port Number:	1812	
Shared Secret / Verify Secret:	●●●	●●●

Figure 113. Admin RADIUS

Procedure for Configuring Admin RADIUS

Use this window to enable/disable administrator authentication via RADIUS, and to set up primary and secondary servers to use for authentication of administrators attempting to log in to the WAP.

1. **Admin RADIUS Settings:**

   a. **Enable Admin RADIUS**: Click **Yes** to enable the use of RADIUS to authenticate administrators logging in to the WAP. You will need to specify the RADIUS server(s) to be used.

   b. **Authentication Type**: Select the protocol used for authentication of administrators, **CHAP** or **PAP** (the default).

   - Password Authentication Protocol (PAP), is a simple protocol. PAP transmits ASCII passwords over the network “in the clear” (unencrypted) and is therefore considered insecure.
   - Challenge-Handshake Authentication Protocol (CHAP) is a more secure protocol. The login request is sent using a one-way hash function.

c. **Timeout (seconds)**: Define the maximum idle time (in seconds) before the RADIUS server's session times out. The default is 600 seconds.

2. **Admin RADIUS Primary Server**: This is the RADIUS server that you intend to use as your primary server.

   a. **Host Name / IP Address**: Enter the IP address or domain name of this external RADIUS server.

   b. **Port Number**: Enter the port number of this RADIUS server. The default is 1812.

   c. **Shared Secret / Verify Secret**: Enter the shared secret that this RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

   The shared secret that you define must match the secret used by the RADIUS server.

3. **Admin RADIUS Secondary Server** (optional): If desired, enter an alternative external RADIUS server. If the primary RADIUS server becomes unreachable, the WAP will "failover" to the secondary RADIUS server (defined here).

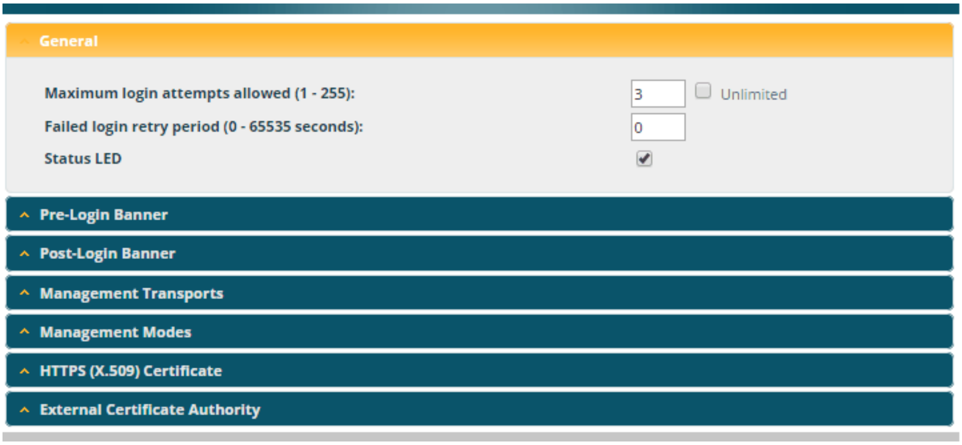
   a. **Host Name / IP Address**: Enter the IP address or domain name of this RADIUS server.

   b. **Port Number**: Enter the port number of this RADIUS server. The default is 1812.

   c. **Shared Secret / Verify Secret**: Enter the shared secret that this RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

Management Control

This window allows you to enable or disable the WAP management interfaces and set their inactivity time-outs. The range is 300 (default) to 100,000 seconds.



General

Maximum login attempts allowed (1 - 255): 3 □ Unlimited

Failed login retry period (0 - 65535 seconds): 0

Status LED ☑

Figure 114. Management Control

Procedure for Configuring Management Control

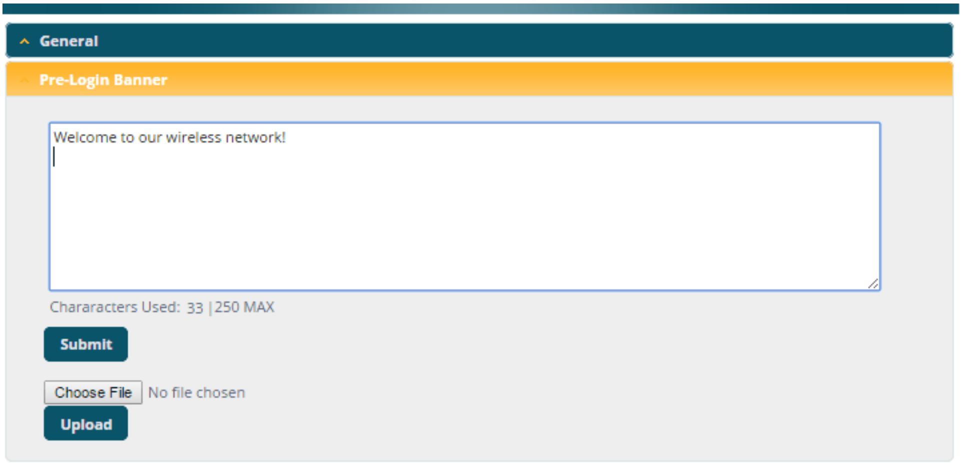
1. **Management Settings:**

   a. **Maximum login attempts allowed (1-255)**: After this number of consecutive failing administrator login attempts via ssh or telnet, the **Failed login retry period** is enforced. The default is 3.

   b. **Failed login retry period (0-65535 seconds)**: After the maximum number (defined above) of consecutive failing administrator login attempts via ssh or telnet, the administrator's IP address is denied access to the WAP for the specified period of time (in seconds). The default is 0.

   c. **Pre-login Banner**: Text that you enter here will be displayed below the WMI login prompt. (Figure 115) Click the **Submit** button when done typing.

      If you wish to display more than 256 characters of text (for instance, to display usage restrictions for the wireless network), you may upload a text file. Click **Choose File** and browse to the file. Click **Upload** when done.



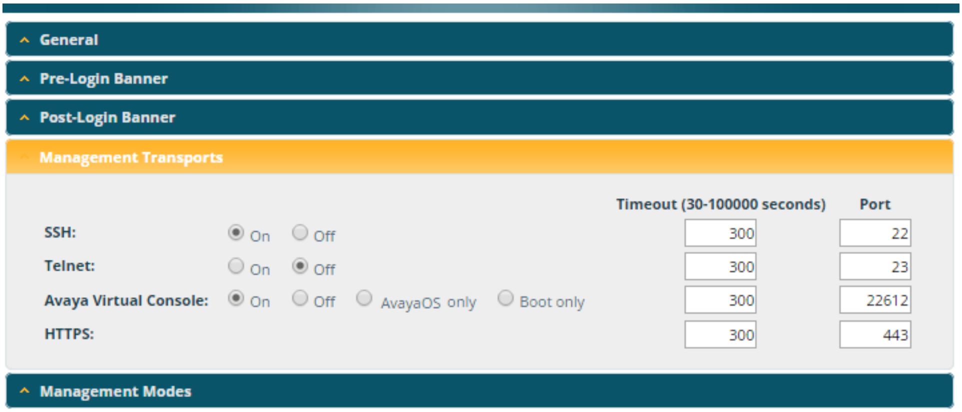
Welcome to our wireless network!

Chararacters Used: 33 | 250 MAX

Figure 115. Pre-login Banner

d. **Post-login Banner**: Text that you enter here will be displayed in a message box after a user logs in to the WMI.

If you wish to display more than 256 characters of text, upload a text file. Click **Choose File** and browse to the file, then click **Upload**.



		Timeout (30-100000 seconds)	Port
SSH:	● On ○ Off	300	22
Telnet:	○ On ● Off	300	23
Avaya Virtual Console:	● On ○ Off ○ AvayaOS only ○ Boot only	300	22612
HTTPS:		300	443

Figure 116. Management Transports

2. **SSH**

   a. **On/Off**: Choose **On** to enable management of the WAP over a Secure Shell (SSH-2) connection, or **Off** to disable this feature. Be aware that only SSH-2 connections are supported by the WAP. SSH clients used for connecting to the WAP must be configured to use SSH-2.

   b. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your SSH connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

   c. **Port**: Enter a value in this field to define the port used by SSH. The default port is 22.

3. **Telnet:**

   a. **On/Off**: Choose **On** to enable WAP management over a Telnet connection, or **Off** to disable this feature. SSH offers a more secure connection than Telnet, and is recommended over Telnet.

   b. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your Telnet connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

c. **Port**: Enter a value in this field to define the port used by Telnet. The default port is 23.

4. **Avaya Console**

The Avaya Console utility connects to WAPs. Please see "Securing Low Level Access to the WAP" on page 64 for more information about Avaya Console. You can enable or disable Avaya Console access to the WAP as instructed below.

__Warning__: If you disable Avaya Console access completely, you __must__ ensure that you do not lose track of the username and password to log in to CLI/WMI! There is no way to recover from a lost password, other than returning the WAP to Avaya.

a. **On/Off**: Choose **On** to enable Avaya Console access to the WAP at the Avaya OS (CLI) and Avaya Boot Loader (boot loader) levels, or **Off** to disable access at both levels. Avaya Console access is **On** by default.

b. **Avaya OS only**: Choose this radio button to enable Avaya Console access at the Avaya OS level only (i.e., Avaya Console can access CLI only). Access to the WAP at the Avaya Boot Loader (boot loader) level is disabled.

c. **Boot only**: Choose this radio button to enable Avaya Console access at the Avaya Boot Loader (boot loader) level only. Avaya OS level (CLI) access to the WAP is disabled.

d. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your Avaya Console connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

e. **Port**: Enter a value in this field to define the port used by Avaya Console. The default port is 22612.

5. **Console**

   a. **On/Off**: Choose **On** to enable management of the WAP via a serial connection, or choose **Off** to disable this feature.

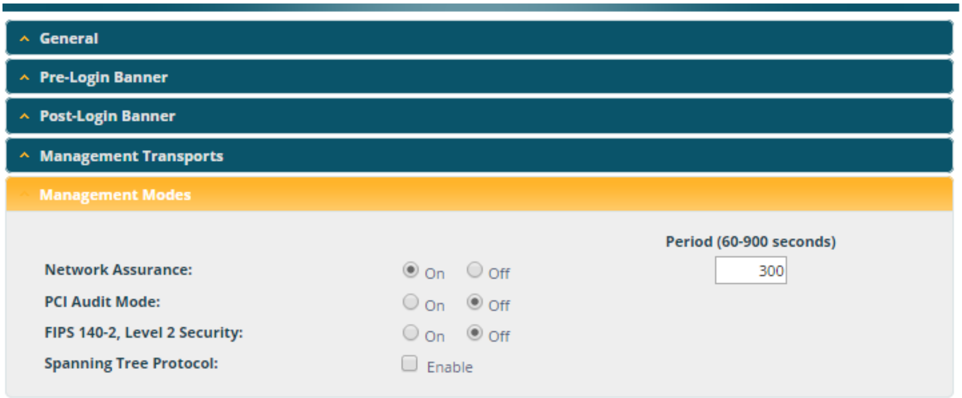
   b. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your serial connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

6. **HTTPS**

   a. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your HTTPS connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds. Management via HTTPS (i.e., the Web Management Interface) cannot be disabled on this window. To disable management over HTTPS, you must use the Command Line Interface.

   b. **Port**: Enter a value in this field to define the port used by SSH. The default port is 443.

7. **Management Modes**



Period (60-900 seconds)

Network Assurance: ● On ○ Off 300

PCI Audit Mode: ○ On ● Off

FIPS 140-2, Level 2 Security: ○ On ● Off

Spanning Tree Protocol: □ Enable

Figure 117. Management Modes

a. **Network Assurance**: Click the **On** button to enable this mode. Network assurance checks network connectivity to each server that you configure, such as the NTP server, RADIUS servers, SNMP trap hosts, etc. By proactively identifying network resources that are unavailable, the network manager can be alerted of problems potentially before end-users notice an issue. The distributed intelligence of WAPs provides this monitoring at multiple points across the network, adding to the ability to isolate the problem and expedite the resolution

   Connectivity is checked when you configure a server. If a newly configured server is unreachable, you will be notified directly and a Syslog entry is created. Configured servers are checked once per **Period** which by default is 300 seconds (five minutes). Servers are checked regardless of whether they are configured as IP addresses or host names.

   If a server becomes unreachable, a Syslog message is generated. When the server again becomes reachable, another Syslog message is generated.

   To view the status of all configured servers checked by this feature, please see “Network Assurance” on page 94.

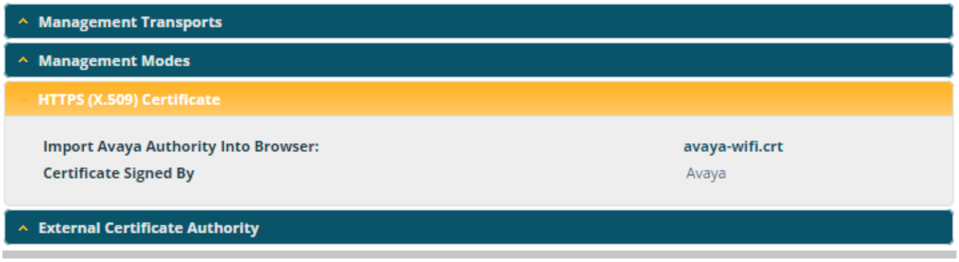
b. **PCI Audit Mode**: Click the **On** button to enable this mode, which is provided as an aid to setting up WAPs to pass PCI DSS audit requirements. In PCI Audit Mode, the WAP checks whether its configuration is appropriate for auditing PCI DSS wireless security. This mode does not change any other settings, but will inform you of any incorrect settings that exist. Furthermore, the WAP will monitor changes that you make to its configuration in CLI or the WMI. PCI Mode will warn you (and issue a Syslog message) if the change is inappropriate for PCI DSS. A warning is issued when a non-compliant change is first applied to the WAP, and also if you attempt to save a configuration that is non-compliant. Use this command in conjunction with “The Avaya WAP PCI Compliance Configuration” on page 511 to ensure that you are using the WAP in accordance with the PCI DSS requirements. For more information, see "Auditing PCI DSS" on page 509.

The pci-audit command checks items such as:

- Telnet is disabled.
- Admin RADIUS is enabled (admin login authentication is via RADIUS server).
- An external Syslog server is in use.
- All SSIDs must set encryption to WPA or better (which also enforces 802.1x authentication)

c. **Spanning Tree Protocol**: this protocol is used in Layer 2 networks to turn off ports when necessary to prevent network loops. It is **Off** by default, and is turned on automatically if you are using WDS to interconnect WAPs using wireless links. Use the **On** button to enable spanning tree if your network topology requires it. See "Spanning Tree Status" on page 90.

8. **HTTPS (X.509) Certificate**



Import Avaya Authority Into Browser: avaya-wifi.crt
Certificate Signed By: Avaya

Figure 118. HTTPS (X.509) Certificate

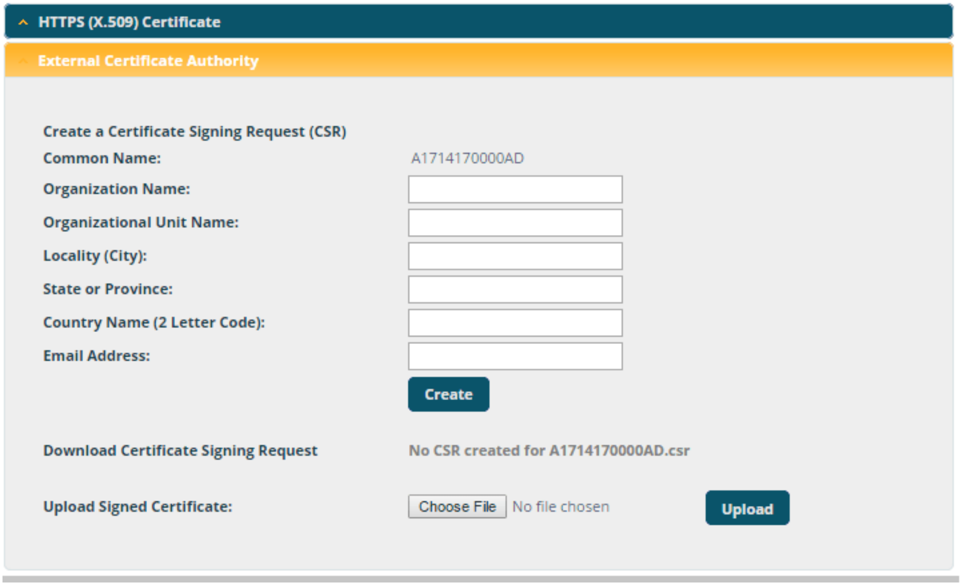
a. **Import Avaya Authority into Browser**: This feature imports the Avaya Certificate Authority (CA) into your browser (for a discussion, please see "Certificates and Connecting Securely to the WMI" on page 208). Click the link (**avaya-ca.crt**), and then click **Open** to view or install the current Avaya CA certificate. Click **Install Certificate** to start your browser's Certificate Install Wizard. We recommend that you use this process to install Avaya as a root authority in your browser.

When you assign a **Host Name** to your WAP using the Express Setup window, then the next time you reboot the WAP (or restart the HTTPS service by turning it off and on again using the CLI), it automatically creates a security certificate for that host name. That certificate uses Avaya as the signing authority. Thus, in order to avoid having certificate errors on your browser when using WMI:

- You must have assigned a host name to the WAP and rebooted at some time after that.
- Use **Import Avaya Authority into Browser**
- Access WMI by using the host name of the WAP rather than its IP address.

b. **HTTPS (X.509) Certificate Signed By**: This read-only field shows the signing authority for the current certificate.

9. External Certificate Authority



HTTPS (X.509) Certificate

External Certificate Authority

Create a Certificate Signing Request (CSR)

Common Name:	A1714170000AD
Organization Name:	
Organizational Unit Name:	
Locality (City):	
State or Province:	
Country Name (2 Letter Code):	
Email Address:	
Download Certificate Signing Request	No CSR created for A1714170000AD.csr
Upload Signed Certificate:	No file chosen

Figure 119. External Certificate Authority

This step and Step 10 allow you to obtain a certificate from an external authority and install it on a WAP. “Using an External Certificate Authority” on page 210 discusses reasons for using an external CA.

For example, to obtain and install a certificate from VeriSign on the WAP, follow these steps:

- If you don’t already have the certificate from the external (non-Avaya) Certificate Authority, see Step 10 to create a request for a certificate.
- Use option (a) to review the request and copy its text to send to VeriSign.
- When you receive the new certificate from VeriSign, upload it to the WAP using option (b).

External Certification Authority has the following options:

a. **Download Certificate Signing Request**: After creating a certificate signing request (.csr file—Step 10), click the **View** button to review it. If it is satisfactory, click the name of the .csr file to display the text of the request. You can then copy this text and use it as required by the CA. You may also click on the filename of the .csr file to download it to your local computer.

b. **Upload Signed Certificate**: To use a custom certificate signed by an authority other than Avaya, use the **Browse** button to locate the certificate file, then click **Upload** to copy it to the WAP. The WAP's web server will be restarted and will pick up the new certificate. This will terminate any current web sessions, and you will need to reconnect and re-login to the WAP.

10. **To create a Certificate Signing Request**

a. Fill in the fields in this section: **Common Name, Organization Name, Organizational Unit Name, Locality (City), State or Province, Country Name,** and **Email Address**. Spaces may be used in any of the fields, except for Common Name, Country Name, or Email Address. Click the **Create** button to create the certificate signing request. See Step 9 above to use this request.

11. Click the **Save** button 💾 if you wish to make your changes permanent.

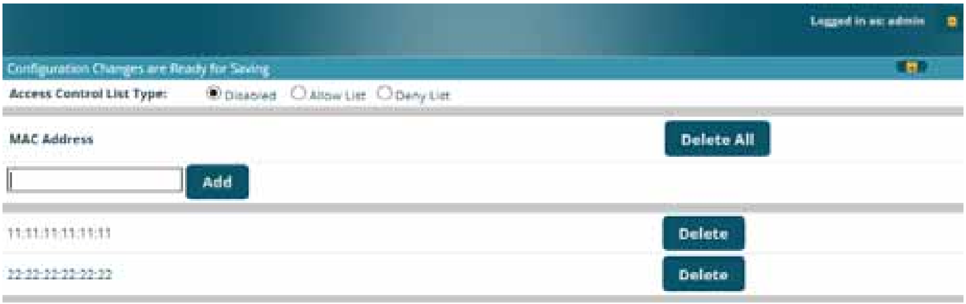
See Also

Interfaces - to enable / disable management over an Ethernet interface
Global Settings - to enable / disable management over radios
Admin Management
External Radius
Global Settings
Internal Radius
Access Control List
Security

Access Control List

This window allows you to enable or disable the use of the global Access Control List (ACL), which controls whether a station with a particular MAC address may associate to the WAP. You may create station access control list entries and delete existing entries, and control the type of list.

There is only one global ACL, and you may select whether its type is an Allow List or a Deny List, or whether use of the list is disabled.



Logged in as: admin

Configuration Changes are Ready for Saving

Access Control List Type: ● Disabled ○ Allow List ○ Deny List

MAC Address

11:11:11:11:11:11

22-22-22-22-22-22

Figure 120. Access Control List

There is also a per-SSID ACL (see "Per-SSID Access Control List" on page 270). If the same MAC address is listed in both the global ACL and in an SSID's ACL, and if either ACL would deny that station access to that SSID, then access will be denied.

Procedure for Configuring Access Control Lists

1. **Access Control List Type:** Select **Disabled** to disable use of the Access Control List, or select the ACL type—either **Allow List** or **Deny List**.

   - **Allow List**: Only allows the listed MAC addresses to associate to the WAP. All others are denied.
   - **Deny List**: Denies the listed MAC addresses permission to associate to the WAP. All others are allowed.

   In addition to these lists, other authentication methods (for example, RADIUS) are still enforced for users.

2. **MAC Address**: If you want to add a MAC address to the ACL, enter the new MAC address here, then click on the **Add** button. The MAC address is added to the ACL. You may use a wildcard (*) for one or more digits to match a range of addresses. You may create up to 1000 entries.
3. **Delete**: You can delete selected MAC addresses from this list by clicking their **Delete** buttons.
4. Click the **Save** button 💾 if you wish to make your changes permanent.

See Also

External Radius

Global Settings

Internal Radius

Management Control

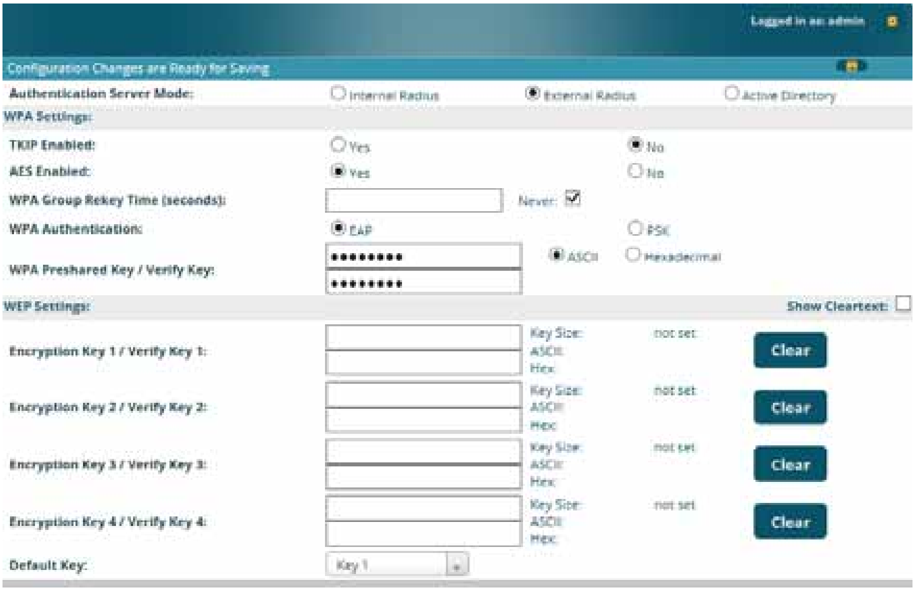
Security

Station Status Windows (list of stations that have been detected by the WAP)

Global Settings

This window allows you to establish the security parameters for your wireless network, including WEP, WPA, WPA2 and RADIUS authentication. When finished, click the **Save** button if you wish to make your changes permanent.

For additional information about wireless network security, refer to “Security Planning” on page 42 and “Understanding Security” on page 205.



Authentication Server Mode: ○ Internal Radius ● External Radius ○ Active Directory

WPA Settings:

TKIP Enabled: ○ Yes ● No

AES Enabled: ● Yes ○ No

WPA Group Rekey Time (seconds): Never: ☑

WPA Authentication: ● EAP ○ PSK

WPA Preshared Key / Verify Key: ●●●●●●●● / ●●●●●●●● ● ASCII ○ Hexadecimal

WEP Settings: Show Cleartext: □

Encryption Key 1 / Verify Key 1: Key Size: not set ASCII Hex

Encryption Key 2 / Verify Key 2: Key Size: not set ASCII Hex

Encryption Key 3 / Verify Key 3: Key Size: not set ASCII Hex

Encryption Key 4 / Verify Key 4: Key Size: not set ASCII Hex

Default Key: Key 1

Figure 121. Global Settings (Security)

Procedure for Configuring Network Security

1. **Authentication Server Mode**: Choose the type of Authentication Server that you will use for authenticating wireless users:

   - **Internal RADIUS** defines wireless user accounts locally on the WAP. See “Internal Radius” on page 236.
   - **External RADIUS** defines wireless user accounts on a RADIUS server external to the WAP. See “External Radius” on page 232.

- **Active Directory** defines wireless user accounts on an Active Directory server external to the WAP. See “Active Directory” on page 238.

WPA Settings

These settings are used if the **WPA** or **WPA2** encryption type is selected on the **SSIDs >SSID Management** window or the **Express Setup** window (on this window, encryption type is set in the **SSID Settings: Wireless Security** field).

2. **TKIP Enabled**: Choose **Yes** to enable TKIP (Temporal Key Integrity Protocol), or choose **No** to disable TKIP.

TKIP encryption does not support high throughput rates for 802.11n, per the IEEE 802.11n specification.

3. **AES Enabled**: Choose **Yes** to enable AES (Advanced Encryption Standard), or choose **No** to disable AES. If both AES and TKIP are enabled, the station determines which will be used.
4. **WPA Group Rekey Time (seconds)**: Enter a value to specify the group rekey time (in seconds). The default is **Never**.
5. **WPA Preshared Key / Verify Key**: If you enabled PSK, enter a passphrase here, then re-enter the passphrase to verify that you typed it correctly.

WEP Settings

These settings are used if the **WEP** encryption type is selected on the **SSIDs > SSID Management** window or the **Express Setup** window (on this window, encryption type is set in the **SSID Settings: Wireless Security** field).

Click the **Show Cleartext** button to make the text that you type in to the Key fields visible.

WEP encryption does not support high throughput rates or features like frame aggregation or block acknowledgments for 802.11n, per the IEEE 802.11n specification.

WEP should never be used for WDS links on WAPs.

6. **Encryption Key 1 / Verify Key 1:**

   Key Size: Key length is automatically computed based on the Encryption Key that you enter

   - 5 ASCII characters (10 hex) for 40 bits (WEP-64)
   - 13 ASCII characters for (26 hex) 104 bits (WEP-128)

   Encryption Key 1 / Verify Key 1: Enter an encryption key in ASCII or hexadecimal. The ASCII and translated hexadecimal values will appear to the right if you selected the **Show Cleartext** button.

   Re-enter the key to verify that you typed it correctly. You may include special ASCII characters, except for the double quote symbol (“).

7. **Encryption Key 2 to 4/ Verify Key 2 to 4/ Key Mode/Length** (optional): If desired, enter up to four encryption keys, in the same way that you entered the first key.

8. **Default Key**: Choose which key you want to assign as the default key. Make your selection from the pull-down list.

9. Click the **Save** button 💾 if you wish to make your changes permanent.

> *After configuring network security, the configuration must be applied to an SSID for the new functionality to take effect.*

See Also

Admin Management

External Radius

Internal Radius

Access Control List

Management Control

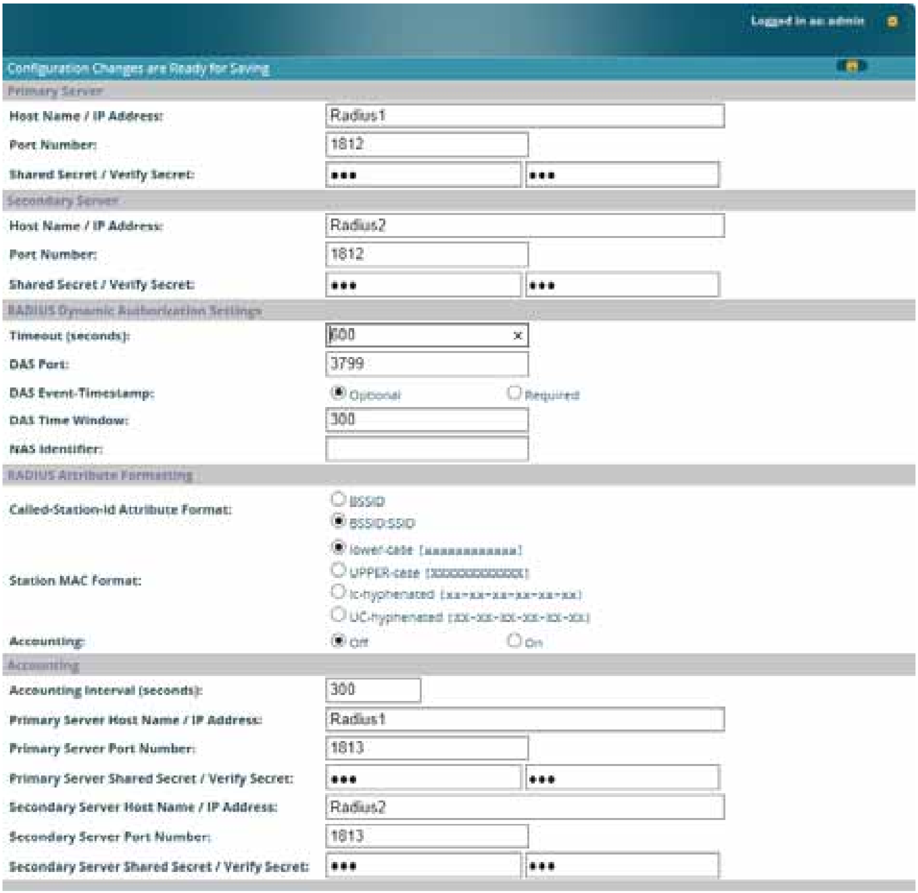
Security

Security Planning

SSID Management

External Radius

This window allows you to define the parameters of an external RADIUS server for user authentication. To set up an external RADIUS server, you must choose **External Radius** as the **Authentication Server Mode** in "Global Settings" on page 229.



Logged in as: admin

Configuration Changes are Ready for Saving

Primary Server		
Host Name / IP Address:	Radius1	
Port Number:	1812	
Shared Secret / Verify Secret:	●●●	●●●
Secondary Server		
Host Name / IP Address:	Radius2	
Port Number:	1812	
Shared Secret / Verify Secret:	●●●	●●●
RADIUS Dynamic Authorization Settings		
Timeout (seconds):	600	
DAS Port:	3799	
DAS Event-Timestamp:	● Optional	○ Required
DAS Time Window:	300	
NAS Identifier:		
RADIUS Attribute Formatting		
Called-Station-Id Attribute Format:	○ BSSID ● BSSID:SSID	
Station MAC Format:	● lower-case [aaaaaaaaaaaa] ○ UPPER-case [XXXXXXXXXXXX] ○ lc-hyphenated [xx-xx-xx-xx-xx-xx] ○ UC-hyphenated [XX-XX-XX-XX-XX-XX]	
Accounting:	● Off	○ On
Accounting		
Accounting Interval (seconds):	300	
Primary Server Host Name / IP Address:	Radius1	
Primary Server Port Number:	1813	
Primary Server Shared Secret / Verify Secret:	●●●	●●●
Secondary Server Host Name / IP Address:	Radius2	
Secondary Server Port Number:	1813	
Secondary Server Shared Secret / Verify Secret:	●●●	●●●

Figure 122. External RADIUS Server

If you want to include user group membership in the RADIUS account information for users, see "Understanding Groups" on page 275. User groups allow you to easily apply a uniform configuration to a user on the WAP.

About Creating User Accounts on the RADIUS Server

An attribute of user (wireless client) accounts is controlled by RADIUS Vendor Specific Attributes (VSAs) defined by Avaya. In particular, use the VSA named **Avaya-Admin-Role** to set the privilege level for an account. For more information about the RADIUS VSAs used by Avaya, see "RADIUS Vendor Specific Attribute (VSA) for Avaya" on page 500.

Procedure for Configuring an External RADIUS Server

1. **Primary Server:** This is the external RADIUS server that you intend to use as your primary server.

   a. **Host Name / IP Address**: Enter the IP address or domain name of this external RADIUS server.

   b. **Port Number**: Enter the port number of this external RADIUS server. The default is 1812.

   c. **Shared Secret / Verify Secret**: Enter the shared secret that this external RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

   The shared secret that you define must match the secret used by the external RADIUS server.

2. **Secondary Server** (optional): If desired, enter an alternative external RADIUS server. If the primary RADIUS server becomes unreachable, the WAP will "failover" to the secondary RADIUS server (defined here).

   a. **Host Name / IP Address**: Enter the IP address or domain name of this external RADIUS server.

   b. **Port Number**: Enter the port number of this external RADIUS server. The default is 1812.

   c. **Shared Secret / Verify Secret**: Enter the shared secret that this external RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

3. **Settings (RADIUS Dynamic Authorization)**: Some RADIUS servers have the ability to contact the WAP (referred to as an NAS, see below) to terminate a user with a Disconnect Message (DM). Or RADIUS may send a Change-of-Authorization (CoA) Message to the WAP to change a user’s privileges due to changing session authorizations. This implements RFC 5176—Dynamic Authorization Extensions to RADIUS.

   a. **Timeout (seconds)**: Define the maximum idle time before the RADIUS server’s session times out. The default is 600 seconds.

   b. **DAS Port**: RADIUS will use the DAS port on the WAP for Dynamic Authorization Extensions to RADIUS. The default port is **3799**.

   c. **DAS Event-Timestamp**: The Event-Timestamp Attribute provides a form of protection against replay attacks. If you select **Required**, both the RADIUS server and the WAP will use the Event-Timestamp Attribute and check that it is current within the **DAS Time Window**. If the Event-Timestamp is not current, then the DM or CoA Message will be silently discarded.

   d. **DAS Time Window**: This is the time window used with the **DAS Event-Timestamp**, above.

   e. **NAS Identifier**: From the point of view of a RADIUS server, the WAP is a client, also called a Network Access Server (NAS). Enter the NAS Identifier (IP address) that the RADIUS servers expect the WAP to use—normally the IP address of the WAP’s Gigabit1 port.

4. **RADIUS Attribute Formatting Settings**: Some RADIUS servers, especially older versions, expect information to be sent to them in a legacy format. These settings are provided for the unusual situation that requires special formatting of specific types of information sent to the RADIUS server. Most users will not need to change these settings.

   a. **Called-Station-Id Attribute Format**: Define the format of the **Called-Station-Id** RADIUS attribute sent from the WAP—**BSSID:SSID** (default) or **BSSID**. This identifies the WAP that is attempting to authenticate a client. **BSSID** is the MAC address of the radio receiving the client signal. The **BSSID:SSID** option additionally identifies the SSID to which the client wishes to connect.

b. **Station MAC Format**: Define the format of the **Station MAC** RADIUS attribute sent from the WAP—lower-case or upper-case, hyphenated or not. The default is lower-case, not hyphenated.

5. **Accounting Settings**:

Note that RADIUS accounting start packets sent by the WAP will include the client station's Framed-IP-Address attribute.

The RADIUS attribute Type-50 Acct-Multi-Session-Id is included in all RADIUS accounting messages generated by Avaya OS. This attribute is used, for example, by Aruba ClearPass to facilitate functions such as onboarding and guest access when stations are roaming between WAPs.

a. **Accounting Interval (seconds)**: Specify how often Interim records are to be sent to the server. The default is 300 seconds.

b. **Primary Server Host Name / IP Address**: Enter the IP address or domain name of the primary RADIUS accounting server that you intend to use.

c. **Primary Port Number**: Enter the port number of the primary RADIUS accounting server. The default is 1813.

d. **Primary Shared Secret / Verify Secret**: Enter the shared secret that the primary RADIUS accounting server will be using, then re-enter the shared secret to verify that you typed it correctly.

e. **Secondary Server Host Name / IP Address** (optional): If desired, enter an IP address or domain name for an alternative RADIUS accounting server. If the primary server becomes unreachable, the WAP will “failover” to this secondary server (defined here).

f. **Secondary Port Number**: If using a secondary accounting server, enter its port number. The default is 1813.

g. **Secondary Shared Secret / Verify Secret**: If using a secondary accounting server, enter the shared secret that it will be using, then re-enter the shared secret to verify that you typed it correctly.

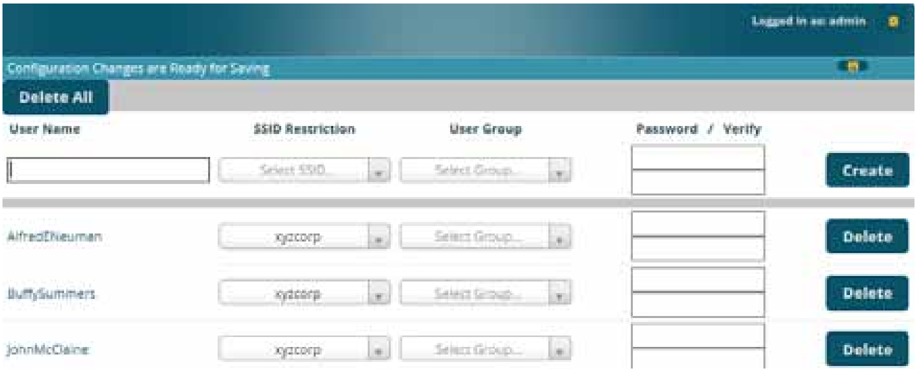
6. Click the **Save** button if you wish to make your changes permanent.

See Also

Admin Management
Global Settings
Internal Radius
Access Control List
Management Control
Security
Understanding Groups

Internal Radius

This window allows you to define the parameters for the WAP's internal RADIUS server for user authentication. However, the internal RADIUS server will only authenticate wireless clients that want to associate to the WAP. This can be useful if an external RADIUS server is not available. To set up the internal RADIUS server, you must choose **Internal Radius** as the **Authentication Server Mode** in "Global Settings" on page 229.



Logged in as: admin

Configuration Changes are Ready for Saving

Delete All

User Name	SSID Restriction	User Group	Password / Verify	
	Select SSID...	Select Group...		Create
AlfredENeuman	xyzcorp	Select Group...		Delete
BuffySummers	xyzcorp	Select Group...		Delete
JohnMcClaine	xyzcorp	Select Group...		Delete

Figure 123. Internal RADIUS Server

Clients using PEAP may have difficulty authenticating to the WAP using the Internal RADIUS server due to invalid security certificate errors. To prevent this problem, the user may disable the ***Validate Server Certificate*** *option on the station. Do this by displaying the station's wireless devices and then displaying the properties of the desired wireless interface. In the security properties, disable* ***Validate server certificate****. In some systems, this may be found by setting the authentication method to PEAP and changing the associated settings.*

Procedure for Creating a New User

1. **User Name:** Enter the name of the user that you want to authenticate to the internal RADIUS server. You may enter up to 1000 users (up to 480 on two-radio APs).

2. **SSID Restriction**: (Optional) If you want to restrict this user to associating to a particular SSID, choose an SSID from the pull-down list.

3. **User Group**: (Optional) If you want to make this user a member of a previously defined user group, choose a group from the pull-down list. This will apply all of the user group's settings to the user. See "Understanding Groups" on page 275.

4. **Password**: (Optional) Enter a password for the user.

5. **Verify**: (Optional) Retype the user password to verify that you typed it correctly.

6. Click on the **Create** button to add the new user to the list.

Procedure for Managing Existing Users

1. **SSID Restriction:** (Optional) If you want to restrict a user to associating to a particular SSID, choose an SSID from its pull-down list.

2. **User Group**: (Optional) If you want to change the user's group, choose a group from the pull-down list. This will apply all of the user group's settings to the user. See "Understanding Groups" on page 275.

3. **Password**: (Optional) Enter a new password for the selected user.

4. **Verify Password**: (Optional) Retype the user password to verify that you typed it correctly.
5. If you want to delete one or more users, click their **Delete** buttons.
6. Click the **Save** button 💾 if you wish to make your changes permanent.

See Also

Admin Management
External Radius
Global Settings
Access Control List
Management Control
Security
Understanding Groups

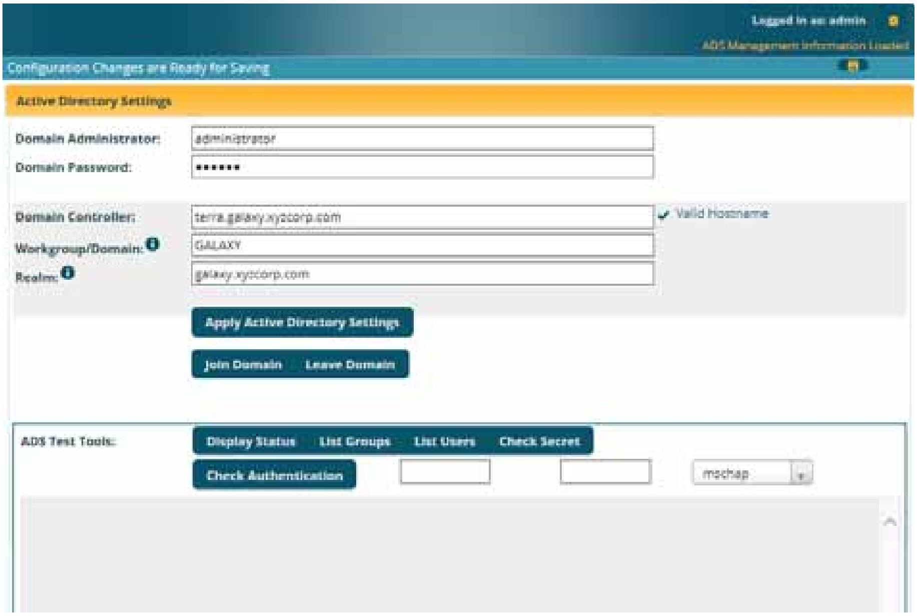
Active Directory

APs do not support Active Directory. You will receive an error message if you attempt to configure this feature.

This window allows you to configure 802.1x user authentication without needing to set up and use an External Radius server. The WAP performs authentication by utilizing an Active Directory server that you have deployed within your network domain.

This window configures the settings required to connect to the Active Directory server. Additionally, Active Directory Test Tools are provided to ease the process of validating proper communication between the Active Directory server and the WAP.

To use the Active Directory settings on this page you must choose **Active Directory** as the **Authentication Server Mode** in “Global Settings” on page 229.



Logged in as: admin

ADS Management Information Loaded

Configuration Changes are Ready for Saving

Active Directory Settings

Domain Administrator: administrator

Domain Password: ••••••

Domain Controller: terra.galaxy.xyzcorp.com ✓ Valid Hostname

Workgroup/Domain: GALAXY

Realm: galaxy.xyzcorp.com

Figure 124. Active Directory Server

Procedure for Use of an Active Directory Server

1. Choose **Active Directory** as the **Authentication Server Mode** in "Global Settings" on page 229.

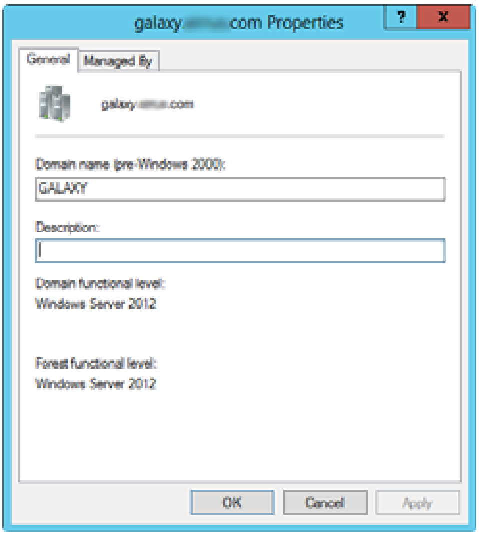
2. **Domain Administrator**: Enter the administrator account name for access to the domain controller. The WAP will use this (together with the password) to create a machine account on the domain for the WAP. This can be the name of any account that can join a machine to the domain.

3. **Domain Password**: The password for the **Domain Administrator** entered above.

4. **Domain Controller**: Enter the hostname to access the domain controller. This must be a fully qualified domain name (FQDN). This cannot be entered as an IP address. The WAP will check that it is able to access the controller and place a checkmark to the right of the entry to indicate that it has been validated. Note that the checkmark only appears after you

have made a change requiring validation (i.e., entering a new hostname or changing an existing entry to a different hostname). If you return to this page at a later time, the checkmark will not be present.

5. **Workgroup/Domain**: Enter the Pre-Windows 2000 Domain name. This can be found by opening the Active Directory **Users and Computers**. Right click the domain in the left hand window and select **Properties**. This will display the **Domain name** that should be entered.



galaxy[redacted]com Properties

galaxy[redacted]com

Domain name (pre-Windows 2000):
GALAXY

Description:

Domain functional level:
Windows Server 2012

Forest functional level:
Windows Server 2012

Figure 125. Finding the Domain Name from Active Directory

6. **Realm**: Realm name (may be the same as the domain name). **Workgroup** and **Realm** are both required. To find the Realm, open a command window on the server and type

```
echo %userdnsdomain%
```

This will display the Realm.

7. Click **Apply Active Directory Settings** to use these settings.

8. You must click **Join Domain** to ask the domain controller to join the WAP to the domain. The WAP is added to the list of computers in the workgroup. The status of the request will be displayed in the area below

the Test Tools. The domain controller will give the WAP a secret that may be used as a key to fetch information. The secret may be checked with the **Check Secret** test tool, below. You may click **Leave Domain** to ask the domain controller to remove the WAP from the domain and revoke its secret.

9. You may use the tools below to check that the WAP is able to access and use the Active Directory successfully, or to troubleshoot any problems.

Active Directory Test Tools

10. **Display Status**: Displays detailed status information for the Active Directory.

11. **List Groups**: Shows the groups defined in the Active Directory for this **Workgroup**.

12. **List Users**: Shows the users defined in the Active Directory for this **Workgroup**.

13. **Check Secret**: The continued validity of the secret granted by **Join Domain** may be checked with this test tool.

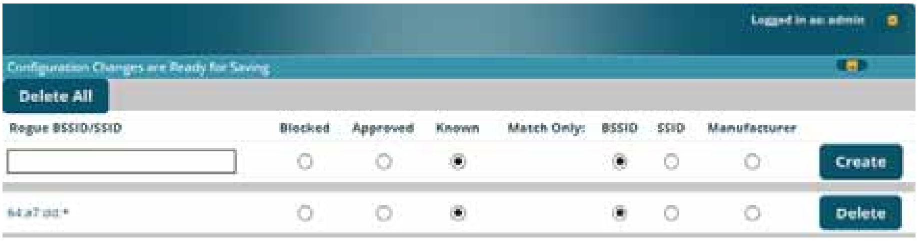
14. **Check Authentication**: Enter a **User** name and **Password**. Select the **Type** of encryption to be used (**MSCHAP**, **NTLM**, **PAP**, or **PEAP-MSCHAPv2**), to check that it will work with the Active Directory server. Then click **Check Authentication** to validate that the WAP can authenticate the user with the selected type of encryption.

See Also

Admin Management
External Radius
Internal Radius
Security
Understanding Groups

Rogue Control List

This window allows you to set up a control list for rogue APs, based on a type that you define. You may classify rogue APs as blocked, so that the WAP will take steps to prevent stations from associating with the blocked AP. See "About Blocking Rogue APs" on page 346. The WAP can keep up to 5000 list entries.



Configuration Changes are Ready for Saving

Rogue BSSID/SSID	Blocked	Approved	Known	Match Only:	BSSID	SSID	Manufacturer	
	○	○	●		●	○	○	Create
64:a7:dd:*	○	○	●		●	○	○	Delete

Figure 126. Rogue Control List

Procedure for Establishing Rogue AP Control

1. **Rogue BSSID/SSID:** Enter the BSSID, SSID, or manufacturer string to match for the new rogue control entry. The **Match Only** radio buttons specify what to match (e.g., the MAC address, SSID, or manufacturer).

   You may use the "*" character as a wildcard to match any string at this position. For example, **64:a7:dd:*** matches any string that starts with **64:a7:dd:**. Avaya WAPs start with any of the following:

   - 64:a7:dd:*
   - b0-ad-aa:*
   - cc:f9:54:*
   - f8-15-47:*
   - 00:1b:4f:*
   - 2c:f4:c5:*
   - 5c:e2:86:*
   - 58:16:26:*
   - 70:52:c5:*

- 70:38:ee:*

By default, the Rogue Control List contains entries corresponding to this list and apply the classification **Known** to all Avaya WAPs.

2. **Rogue Control Classification**: Enter the classification for the specified rogue AP(s), either **Blocked**, **Known** or **Approved**.
3. **Match Only**: Select the match criterion to compare the **Rogue BSSID/ SSID** string against: **BSSID**, **Manufacturer**, or **SSID**. The BSSID field contains the MAC address.
4. Click **Create** to add this rogue AP to the Rogue Control List.
5. **Rogue Control List**: If you want to edit the control type for a rogue AP, just click the radio button for the new type for the entry: **Blocked**, **Known** or **Approved**.
6. To delete rogue APs from the list, click their **Delete** buttons.
7. Click the **Save** button 💾 if you wish to make your changes permanent.

See Also

Network Map

SSIDs

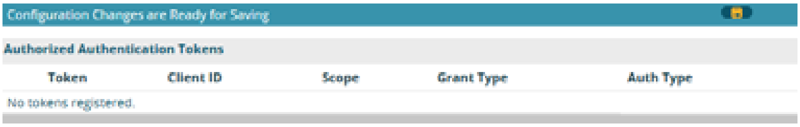
SSID Management

OAuth 2.0 Management

This window displays a list of tokens granted by the WAP for access to its RESTful API (see “API Documentation” on page 400 for a description of the features available in the API). OAuth 2.0 is used to provide the tokens. The list will be blank until tokens have been issued as described below. You may revoke (delete) existing tokens from the list, if desired.

WAPs use the OAuth 2.0 standard’s client credential grant model. This allows you to use administrator account credentials to obtain a token to access RESTful API on an individual WAP. Please note that the WAP will issue only **one** token on behalf on of any administrator account at any given time. If you have a need for multiple tokens, then the WAP will need multiple administrator accounts.

Follow the steps below to obtain a token and use the RESTful API.



Configuration Changes are Ready for Saving

Authorized Authentication Tokens

Token	Client ID	Scope	Grant Type	Auth Type
No tokens registered.				

Figure 127. OAuth 2.0 Management - Token List

Procedure for Obtaining a Token and Accessing RESTful API on the WAP

1. **Present User Credentials for a Permanent Token**

   A user-developed application must register by presenting the following information to the URL below:

   ```
   https://[WAP hostname or IP address]/oauth/authorize
   ```

   - **grant_type**: password
   - **username**: username of an administrator account on the WAP.
   - **client_id**: username of an administrator account on the WAP (username and client_id must match).
   - **password**: password for the same administrator account on the WAP

   The OAuth Authorization API provides a permanent token that the application may use to access the RESTful API. This token remains valid until the administrator revokes the token on the **OAuth 2.0 Management** page, unless the token file somehow becomes corrupted or is removed from the WAP's file system.

The token will be removed if the original account associated with it is deleted.

2. **Access the RESTful API**

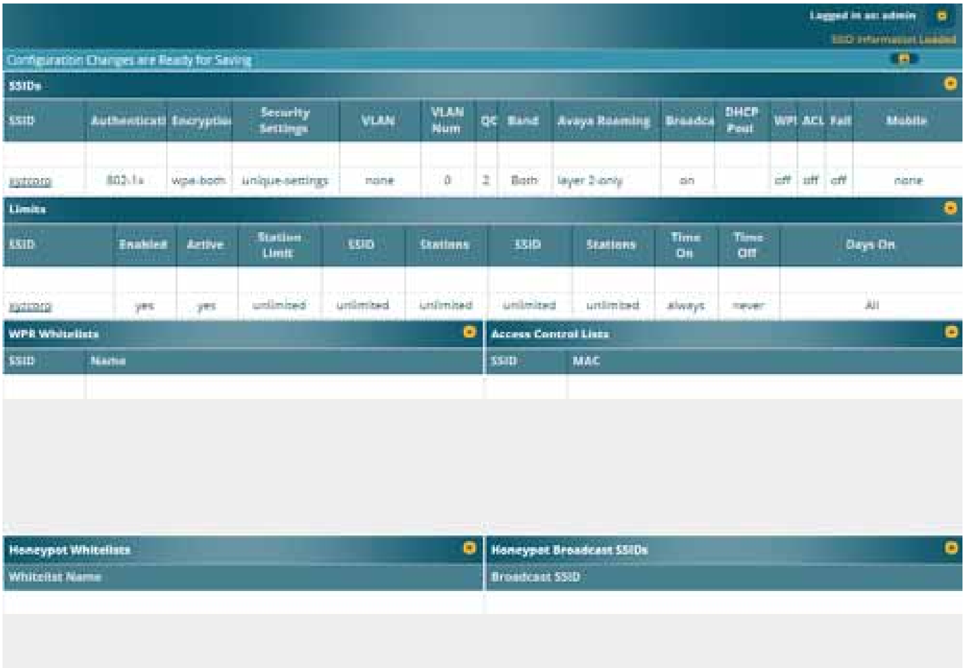
Once registration is completed and a permanent token has been provided, your application may access the API using the **client_id** and the token at the following URL:

```
https://[WAP hostname or IP address]/api/v3/[api-name]
```

Please see "API Documentation" on page 400 for a description of the features available in the API.

SSIDs

This status-only window allows you to review SSID (Service Set IDentifier) assignments. It includes the SSID name, whether or not an SSID is visible on the network, any security and QoS parameters defined for each SSID, associated VLAN IDs, radio availability, and DHCP pools defined per SSID. Click on an SSID's name to jump to the edit page for the SSID. There are no configuration options available on this page, but if you are experiencing problems or reviewing SSID management parameters, you may want to print this page for your records.



SSIDs

SSID	Authenticati	Encryptio	Security Settings	VLAN	VLAN Num	QC	Band	Avaya Roaming	Broadca	DHCP Pool	WPI	ACL	Fall	Mobile
systorg	802.1x	wpa-both	unique-settings	none	0	2	Both	layer 2-only	on		off	off	off	none

Limits

SSID	Enabled	Active	Station Limit	SSID	Stations	SSID	Stations	Time On	Time Off	Days On
systorg	yes	yes	unlimited	unlimited	unlimited	unlimited	unlimited	always	never	All

WPR Whitelists

SSID	Name

Access Control Lists

SSID	MAC

Honeypot Whitelists

Whitelist Name

Honeypot Broadcast SSIDs

Broadcast SSID

Figure 128. SSIDs

The read-only **Limits** section of the SSIDs window allows you to review any limitations associated with your defined SSIDs. For example, this window shows the current state of an SSID (enabled or not), how much SSID and station traffic is allowed, time on and time off, days on and off, and whether each SSID is currently active or inactive.

For information to help you understand SSIDs and how multiple SSIDs are managed by the WAP, go to “Understanding SSIDs” on page 247 and the Multiple SSIDs section of “Frequently Asked Questions” on page 490. For a description of how QoS operates on the WAP, see “Understanding QoS Priority on the WAP” on page 249.

SSIDs are managed with the following windows:

- **“SSID Management” on page 254**
- **“Active Radios” on page 269**
- **“Per-SSID Access Control List” on page 270**
- **“Honeypots” on page 272**

SSIDs are discussed in the following topics:

- **“Understanding SSIDs” on page 247**
- **“Understanding QoS Priority on the WAP” on page 249**
- **“High Density 2.4G Enhancement—Honeypot SSID” on page 253**

Understanding SSIDs

The SSID (Service Set Identifier) is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. SSIDs are case-sensitive and can contain up to 32 alphanumeric characters (do not include spaces when defining SSIDs).

Multiple SSIDs

A BSSID (Basic SSID) refers to an individual access point radio and its associated clients. The identifier is the MAC address of the access point radio that forms the BSS. A group of BSSs can be formed to allow stations in one BSS to communicate to stations in another BSS via a backbone that interconnects each access point.

The Extended Service Set (ESS) refers to the group of BSSIDs that are grouped together to form one ESS. The ESSID (often referred to as SSID or “wireless network name”) identifies the Extended Service Set. Clients must associate to a single ESS at any given time. Clients ignore traffic from other Extended Service Sets that do not have the same SSID.

Legacy access points typically support one SSID per access point. WAPs support the ability to define and use multiple SSIDs simultaneously.

Using SSIDs

The creation of different wireless network names allows system administrators to separate types of users with different requirements. The following policies can be tied to an SSID:

- The wireless security mode needed to join this SSID.
- The wireless Quality of Service (QoS) desired for this SSID.
- The wired VLAN associated with this SSID.

As an example, one SSID named **accounting** might require the highest level of security, while another named **guests** might have low security requirements.

Another example may define an SSID named **voice** that supports voice over Wireless LAN phones with the highest Quality of Service (QoS) definition. This SSID might also forward traffic to specific VLANs on the wired network.

See Also

SSID Management
SSIDs
Understanding SSIDs

Understanding QoS Priority on the WAP

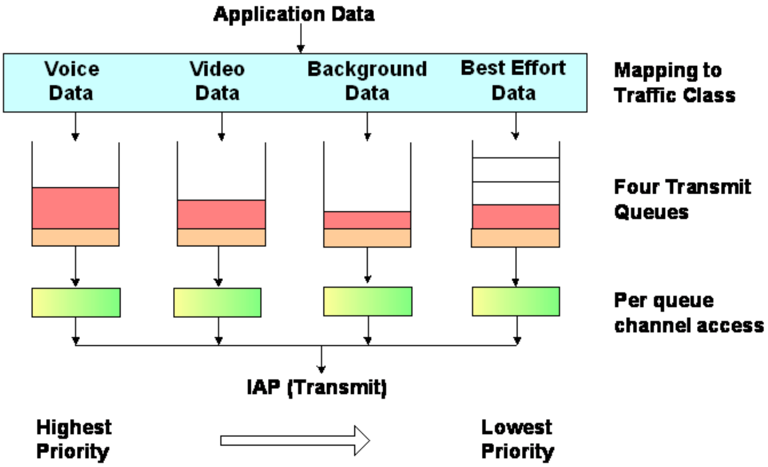


Figure 129. Four Traffic Classes

The WAP's Quality of Service Priority feature (QoS) allows traffic to be prioritized according to your requirements. For example, you typically assign the highest priority to voice traffic, since this type of traffic requires delay to be under 10 ms. The WAP has four separate queues for handling wireless traffic at different priorities, and thus it supports four traffic classes (QoS levels).

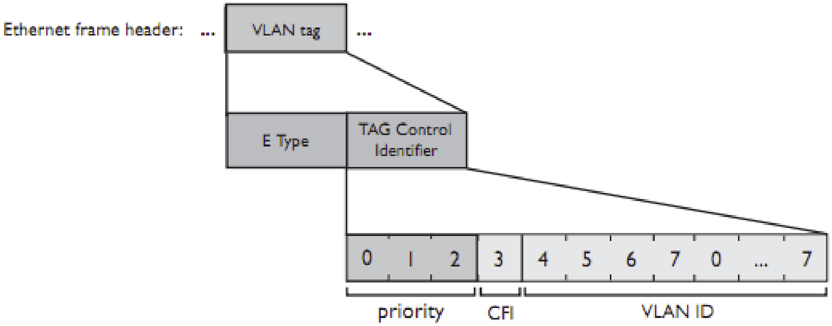


Figure 130. Priority Level—IEEE 802.1p (Layer 2)

IEEE802.1p uses three bits in an Ethernet frame header to define eight priority levels at the MAC level (Layer 2) for wired networks. Each data packet may be tagged with a priority level, i.e., a **user priority** tag. Since there are eight possible user priority levels and the WAP implements four wireless QoS levels, user priorities are mapped to QoS as described below.

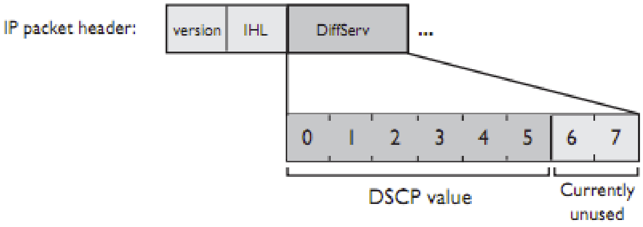


Figure 131. Priority Level—DSCP (DiffServ - Layer 3)

Differentiated Services Code Point or DiffServ (DSCP) uses 6 bits in the IPv4 or IPv6 packet header, defined in RFC2474 and RFC2475. The DSCP value classifies a Layer 3 packet to determine the Quality of Service (QoS) required. DSCP replaces the outdated Type of Service (TOS) field.

The description below describes how both of these priority levels are mapped to the WAP’s four traffic classes.

End-to-End QoS Handling

Wired QoS - Ethernet Port:

- Egress: Outgoing wired packets are IEEE 802.1p tagged at the Ethernet port for upstream traffic, thus enabling QoS at the edge of the network.

FROM WAP QoS (Wireless)	**TO** Priority Tag 802.1p (Wired)
1 (Lowest priority)	1
0	0
2 (Default)	5

FROM WAP QoS (Wireless)	**TO** Priority Tag 802.1p (Wired)
3 (Highest priority)	6

- Ingress: Incoming wired packets are assigned QoS priority based on their SSID and 802.1p tag (if any), as shown in the table below. This table follows the mapping recommended by IEEE802.11e.

FROM Priority Tag 802.1p (Wired)	**TO** WAP QoS (Wireless)	Typical Use
0	0	Best Effort
1	1 (Lowest priority)	Background—explicitly designated as low-priority and non-delay sensitive
2	1	Spare
3	0	Excellent Effort
4	2	Controlled Load
5	2	Video
6	3	Voice - requires delay <10ms
7 (Highest priority)	3 (Highest priority)	Network control

Wireless QoS - Radios:

- Each SSID can be assigned a separate QoS priority (i.e., traffic class) from 0 to 3, where 3 is highest priority and 2 is the default. See “SSID Management” on page 254. If multiple SSIDs are used, packets from the SSID with higher priority are transmitted first.

- The WAP supports IEEE802.11e Wireless QoS for downstream traffic. Higher priority packets wait a shorter time before gaining access to the air and contend less with all other 802.11 devices on a channel.
- How QoS is set for a packet in case of conflicting values:

  a. If an SSID has a QoS setting, and an incoming wired packet's user priority tag is mapped to a higher QoS value, then the higher QoS value is used.

  b. If a group or filter has a QoS setting, this overrides the QoS value above. See "Groups" on page 275, and "Filters" on page 363.

  c. Voice packets have the highest priority (see Voice Support, below).

  d. If **DSCP to QoS Mapping Mode** is enabled, the IP packet is mapped to QoS level 0 to 3 as specified in the DSCP Mappings table. This value overrides any of the settings in cases a to c above.

  In particular, by default:

  - DSCP 8 is set to QoS level 1.
  - DSCP 40 is typically used for video traffic and is set to QoS level 2.
  - DSCP 48 is typically used for voice traffic and is set to QoS level 3—the highest level
  - All other DSCP values are set to QoS level 0 (the lowest level—Best Effort).

Packet Filtering QoS classification

- Filter rules can be used to redefine the QoS priority level to override defaults. See "Filter Management" on page 367. This allows the QoS priority level to be assigned based on protocol, source, or destination.

Voice Support

- The QoS priority implementation on the WAP gives voice packets the highest priority to support voice applications.

High Density 2.4G Enhancement—Honeypot SSID

Some situations pose problems for all wireless APs. For example, iPhones will remember every SSID and flood the airwaves with probes, even when the user doesn't request or desire this behavior. In very high density deployments, these probes can consume a significant amount of the available wireless bandwidth.

The WAP "honeypot" SSID targets this problem. Simply create an SSID named **honeypot** (lower-case) on the WAP, with no encryption or authentication (select **None/Open**). Once this SSID is created and enabled, it will respond to any station probe looking for a named open SSID (unencrypted and unauthenticated) that is *not* configured on the WAP. It will make the station go through its natural authentication and association process. See "Honeypots" on page 272.

The following SSIDs are excluded from being honeypotted:

- Explicitly whitelisted SSIDs. See "Honeypots" on page 272.
- SSIDs that are encrypted and / or authenticated.
- SSIDs that are configured on this WAP, whether or not they are enabled.

Traffic for a station connected to the honeypot SSID may be handled in various ways using other WAP features:

- Traffic may be directed to WPR (captive portal) to display a splash page or offer the user the opportunity to sign in to your service (see "Web Page Redirect (Captive Portal) Configuration" on page 263);
- Traffic may be filtered (see "Filters" on page 363);
- or it may be dead-ended by defining a specific dead-end VLAN on the honeypot SSID to "trap" stations (see "VLANs" on page 191).

Use the honeypot feature carefully as it could interfere with legitimate SSIDs and prevent clients from associating to another available network. You may define a whitelist of allowed SSIDs which are not to be honeypotted. See "Honeypots" on page 272. Th Honey pots page also allows you to change the SSID name that is broadcast for the honeypot SSID.

SSID Management

This window allows you to manage SSIDs (create, edit, schedule, rename, and delete), assign security parameters and VLANs on a per SSID basis, and configure the Web Page Redirect (WPR captive portal) functionality.

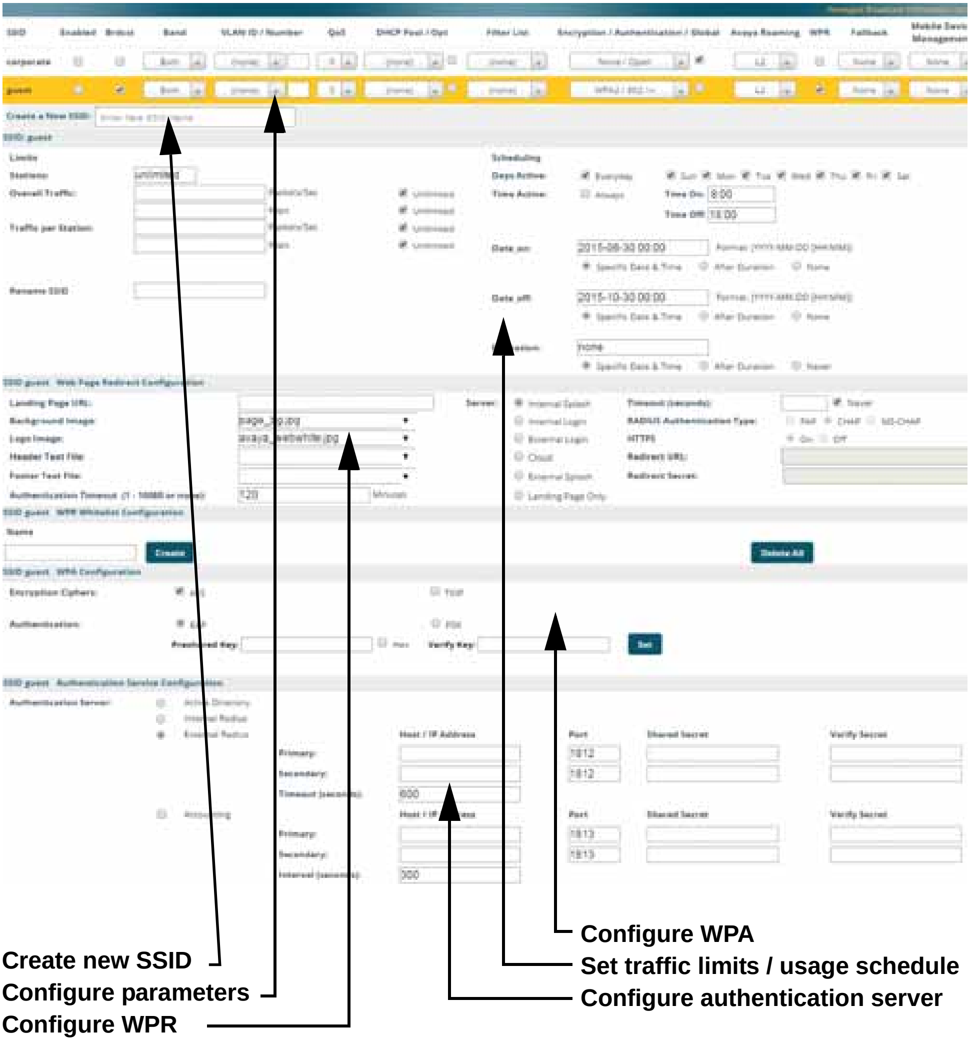

Create new SSID
Configure parameters
Configure WPR
Configure WPA
Set traffic limits / usage schedule
Configure authentication server

Figure 132. SSID Management

Procedure for Managing SSIDs

1. **New SSID:** To create a new SSID, enter a new SSID name. SSID names are case sensitive and may only consist of the characters A-Z, a-z, 0-9, dash, and underscore. You may create up to 16 SSIDs (up to 6 on the WAO9122). You may create a special SSID named **honeypot** (lower-case) to reduce the amount of unnecessary traffic caused by stations probing for open SSID names that they have learned in the past—see "High Density 2.4G Enhancement—Honeypot SSID" on page 253. In this case, a **Honeypot Service Whitelist Configuration** section will appear below (see Step 1 on page 273).

   To rename an SSID or schedule a range of dates during which it may be used, see "SSID Limits and Scheduling" on page 260.

SSID List (top of page)

2. **SSID**: Shows all currently assigned SSIDs. When you create a new SSID, the SSID name appears in this table. Click any SSID in this list to select it.
3. **Enabled**: Check this box to activate this SSID or clear it to deactivate it. Once the SSID is enabled, its availability is also controlled by settings in "SSID Limits and Scheduling" on page 260.
4. **Brdcast**: Check this box to make the selected SSID visible to all clients on the network. Although the WAP will not broadcast SSIDs that are hidden, clients can still associate to a hidden SSID if they know the SSID name to connect to it. Clear this box if you do not want this SSID to be visible on the network.
5. **Band**: Choose which wireless band the SSID will be beaconed on. Select either **5 GHz**—802.11an, **2.4 GHz**—802.11bgn or **Both**.
6. **VLAN ID / Number**: (Optional) From the pull-down list, select a VLAN or VLAN Pool that you want this traffic to be forwarded to on the wired network. Select **numeric** to enter the number of a previously defined VLAN in the **Number** field. See "VLANs" on page 191 and "VLAN Pools" on page 193.

7. **QoS**: (Optional) Select a value in this field for QoS (Quality of Service) priority filtering. The QoS value must be one of the following:

   - 0—The lowest QoS priority setting, where QoS makes its best effort at filtering and prioritizing data, video and voice traffic without compromising the performance of the network. Use this setting in environments where traffic prioritization is not a concern.
   - 1—Medium, with QoS prioritization aggregated across all traffic types.
   - 2—High, normally used to give priority to video traffic.
   - 3—The highest QoS priority setting, normally used to give priority to voice traffic.

   The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID traffic, as described in "Understanding QoS Priority on the WAP" on page 249. The default value for this field is 2.

8. **DHCP Pool**: If you want to associate an internal DHCP pool to this SSID, choose the pool from the pull--down list. An internal DHCP pool must be created before it can be assigned. To create an internal DHCP pool, go to "DHCP Server" on page 178.

9. **DHCP Option**: When this option is enabled, the WAP snoops station DHCP requests and inserts relay agent information into these DHCP packets (option 82, in the CIRCUIT-ID sub-option). Information inserted includes WAP MAC address and SSID name. Information is inserted as a colon-separated text string in the CIRCUIT ID value field, in this format: [AP_MAC]:[SSID]

[AP_MAC]	length = 17 (aa-bb-cc-dd-ee-ff)
[SSID]	length = length of SSID name

   Example: `aa-bb-cc-dd-ee-ff:mySSID`

   Note that the MAC address uses ***dashes*** as separators, and that format is different than that used for Option 82 with Tunnels.

10. **Filter List**: If you wish to apply a set a filters to this SSID's traffic, select the desired Filter List. See "Filters" on page 363.

11. **Authentication**: The following authentication options are available (only valid encryption / authentication combinations are offered):

    - **Open:** This option provides no authentication and is not recommended.
    - **RADIUS MAC:** Uses an external RADIUS server to authenticate stations onto the wireless network, based on the user's MAC address. Accounting for these stations is performed according to the accounting options that you have configured specifically for this SSID or globally (see Step 13 below).

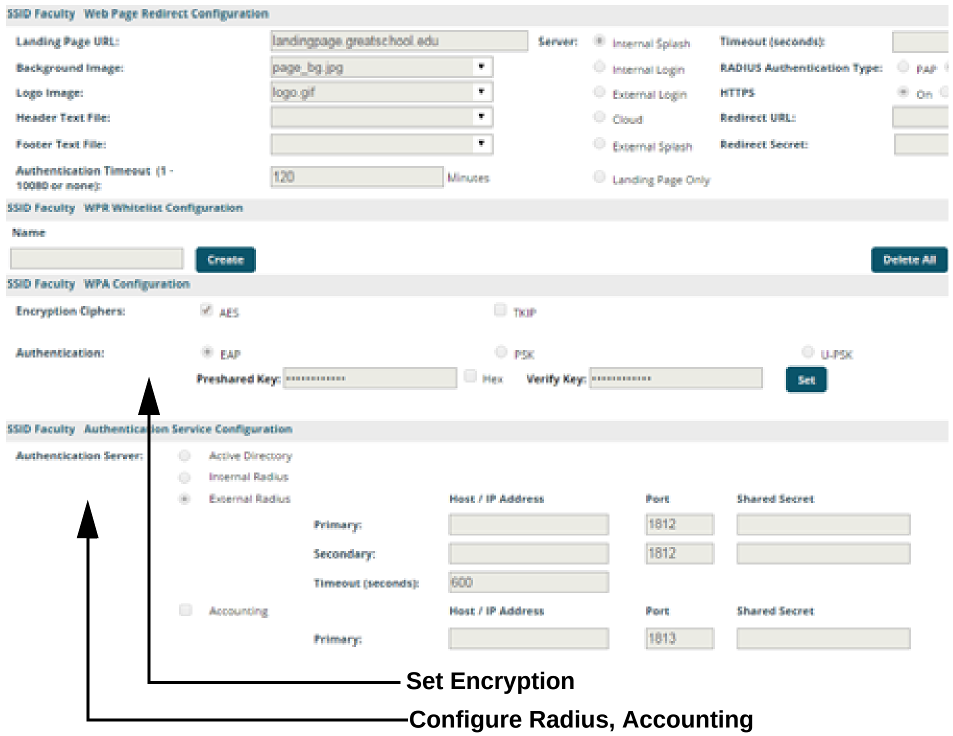
    If this SSID is on a VLAN, the VLAN must have management turned on in order to pass CHAP authentication challenges from the client station to the RADIUS server.

    - **802.1x:** Authenticates stations onto the wireless network via a RADIUS server using 802.1x with EAP. The RADIUS server can be internal (provided by the WAP) or external.

12. **Encryption**: Choose the encryption that will be required—specific to this SSID—either **None**, **WEP**, **WPA**, **WPA2** or **WPA-Both**. The None option provides no security and is not recommended; WPA2 provides the best Wi-Fi security.

    Each SSID supports only one encryption type at a time (except that WPA and WPA2 are both supported on an SSID if you select WPA-Both). If you need to support other encryption types, you must define additional SSIDs. The encryption used with WPA or WPA2 is selected in "Global Settings" on page 229. For an overview of the security options, see "Security Planning" on page 42 and "Understanding Security" on page 205.

13. **Global**: Check this box if you want this SSID to use the security settings established at the global level (see "Global Settings" on page 229). Clear this box if you want the settings established here to take precedence.



SSID Faculty Web Page Redirect Configuration

Landing Page URL: landingpage.greatschool.edu
Background Image: page_bg.jpg
Logo Image: logo.gif
Header Text File:
Footer Text File:
Authentication Timeout (1 - 10080 or none): 120 Minutes

Server: ● Internal Splash ○ Internal Login ○ External Login ○ Cloud ○ External Splash ○ Landing Page Only

Timeout (seconds):
RADIUS Authentication Type: ○ PAP
HTTPS ● On
Redirect URL:
Redirect Secret:

SSID Faculty WPR Whitelist Configuration

Name

SSID Faculty WPA Configuration

Encryption Ciphers: ☑ AES □ TKIP

Authentication: ● EAP ○ PSK ○ U-PSK

Preshared Key: ************ □ Hex Verify Key: ************

SSID Faculty Authentication Service Configuration

Authentication Server: ○ Active Directory ○ Internal Radius ● External Radius

	Host / IP Address	Port	Shared Secret
Primary:		1812	
Secondary:		1812	
Timeout (seconds):	600		

□ Accounting

	Host / IP Address	Port	Shared Secret
Primary:		1813	

Set Encryption

Configure Radius, Accounting

Figure 133. SSID Management—Encryption, Authentication, Accounting

Additional sections will be displayed to allow you to configure encryption, authentication server, and RADIUS accounting settings.

- The **WPA Configuration** encryption settings have the same parameters as those described in “Procedure for Configuring Network Security” on page 229.

- To configure **Active Directory** settings, see “Active Directory” on page 238).

- The **External RADIUS** and **Accounting** settings are configured in the same way as for an external RADIUS server (see “Procedure for Configuring an External RADIUS Server” on page 233). Note that external RADIUS servers may be specified using IP addresses or domain names.

14. **Roaming**: For this SSID, select whether to enable fast roaming between radios or WAPs at **L2&L3** (Layer 2 and Layer 3), at **L2** (Layer 2 only), or disable roaming (**Off**). You may only select fast roaming at Layers 2 and 3 if this has been selected in Global Settings. See "Understanding Fast Roaming" on page 283.

15. **WPR (Web Page Redirect**, also called captive portal**)**: Check the checkbox to enable the Web Page Redirect functionality, or clear it to disable this option. If enabled, WPR configuration fields will be displayed under the SSID Limits section. This feature may be used to provide an alternate mode of authentication, or to simply display a splash screen when a user first associates to the wireless network. After that, it can (optionally) redirect the user to an alternate URL. For example, some wireless devices and users may not have a correctly configured 802.1x (RADIUS) supplicant. Utilizing WPR's Web-based login, users may be authenticated without using an 802.1x supplicant. See "Web Page Redirect (Captive Portal) Configuration" on page 263 for details of WPR usage and configuration.

    You may specify "Whitelist" entries—a list of web sites to which users have unrestricted access, without needing to be redirected to the WPR page first. See "Whitelist Configuration for Web Page Redirect" on page 267 for details.

*When using WPR, it is particularly important to adhere to the SSID naming restrictions detailed in **Step 1**.*

16. **Fallback**: Network Assurance checks network connectivity for the WAP. When Network Assurance detects a failure, perhaps due to a bad link or WDS failure, if Fallback is set to **Disable** the WAP will automatically disable this SSID. This will disassociate current clients, and prevent new clients from associating. Since the WAP's network connectivity has failed,

this gives clients a chance to connect to other, operational parts of the wireless network. No changes are made to WDS configuration. See Step a on page 222 for more information on Network Assurance.

17. **Mobile Device Management** (MDM): If you are an AirWatch customer and wish to have AirWatch manage mobile device access to the wireless network on this SSID, select **AirWatch** from the drop-down list. Before selecting this option, you must configure your AirWatch settings. See “AirWatch” on page 378.

Note that you cannot use MDM and WPR on the same SSID.

The lower part of the window contains a few sections of additional settings to configure for the currently selected SSID, depending on the values chosen for the settings described above.

- **“SSID Limits and Scheduling” on page 260**
- **“Web Page Redirect (Captive Portal) Configuration” on page 263**
- **“Whitelist Configuration for Web Page Redirect” on page 267**
- **“WPA Configuration” on page 268**
- **“Authentication Service Configuration” on page 268**

SSID Limits and Scheduling

See “Group Limits” on page 280 for a discussion of the interaction of SSID limits and group limits. To eliminate confusion, we recommend that you configure one set of limits or the other, but not both.

18. **Stations**: Enter the maximum number of stations allowed on this SSID. This step is optional. Note that the Radios - Global Settings window also has a station limit option—**Max Station Association per** Radio, and the windows for Global Settings .11an and Global Settings .11bgn also have **Max Stations** settings. If multiple station limits are set, all will be enforced. As soon as any limit is reached, no new stations can associate until some other station has terminated its association.

19. **Overall Traffic**: Choose **Unlimited** if you do not want to place a restriction on the traffic for this SSID, or enter a value in the **Packets/Sec** field to force a traffic restriction.

20. **Traffic per Station**: Choose **Unlimited** if you do not want to place a restriction on the traffic per station for this SSID, or enter a value in the **Packets/Sec** field or the **Kbps** field to force a traffic restriction. If you set both values, the WAP will enforce the limit it reaches first.

21. **Rename SSID**: Use this field if you wish to change the name of an SSID without changing any of its other settings. For example, a convention center might wish to change the SSID name based on the name of the current exhibition.

Scheduling

22. **Days Active**: Choose **Everyday** if you want this SSID to be active every day of the week, or select only the specific days that you want this SSID to be active. Days that are not checked are considered to be the inactive days.

23. **Time Active**: Choose **Always** if you want this SSID active without interruption, or enter values in the **Time On** and **Time Off** fields to limit the time that this SSID is active.

24. **Date on**: Use this and the following two fields for *SSID Scheduling*—this lets you set up an SSID in advance and specify a period of time for the SSID to be in service. For example, a convention center might wish to set up SSIDs ahead of time for exhibitions that are scheduled for the next six months, and have each SSID be used only for the specified period.

    The SSID must be **Enabled** (see Step 1 on page 255), or the scheduling settings will be ignored. Note that once the SSID has reached its scheduled time and is in service, it will then obey the settings for **Days Active** and **Time Active** above.

    Set **Date on** to **none** (the default) if you don't want this SSID to be delayed until later—that is, it will be put in service starting immediately. Select **Specific Date & Time** to have the SSID start become active at the specified date and time. Use the format YYYY-MM-DD [HH:MM], where time (hour and minute) is optional. For example, enter **2016:09:29 08:00**. Use **After Duration** to delay for the specified amount of time in days, hours, and minutes, before the SSID is in service (use the format DD HH:MM, including the hours and minutes). For example, to have the SSID become valid after one day, one hour and 30 minutes have passed, enter **1 01:30**.

25. Use **Date off** to specify a date to take the SSID out of service without deleting it. At the specified date, the AP will turn the **Enabled** flag off. Leave **Expiration** and **Date off** set to **none** (the default) if you want this SSID to remain in service indefinitely after its scheduled start. Use **Specific Date & Time** to take the SSID out of service at the specified date and time. Use the format YYYY-MM-DD [HH:MM], where time (hour and minute) is optional. For example, enter **2016:09:29 18:00**. Use **After Duration** to keep the SSID in service for the specified amount of time in days, hours, and minutes (use the format DD [HH:MM], where hours and minutes are optional).

26. Use **Expiration** to specify a date to *delete this SSID* when it is taken out of service at the specified date (i.e., this option cleans up after itself when it reaches the expiration time). Leave **Expiration** and **Date off** set to **none** (the default) if you want this SSID to remain in service indefinitely after its scheduled start. Use **Specific Date & Time** to delete the SSID at the specified date and time. Use the format YYYY-MM-DD [HH:MM], where time (hour and minute) is optional. For example, enter **2016:09:29 18:00**. Use **After Duration** to keep the SSID in service for the specified amount of time in days, hours, and minutes (use the format DD [HH:MM], where hours and minutes are optional).

27. **Web Page Redirect Configuration**: see “Web Page Redirect (Captive Portal) Configuration” on page 263.

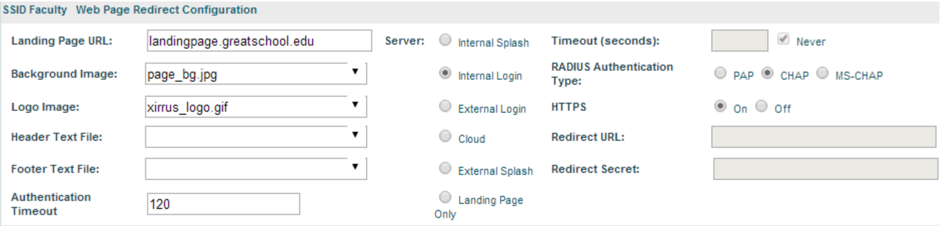
28. To delete an SSID, click its **Delete** button 🗑 .

29. Click the **Save** button 💾 if you wish to make your changes permanent.

Web Page Redirect (Captive Portal) Configuration

If you enable WPR, the SSID Management window displays additional fields that must be configured.

If enabled, WPR displays a splash or login page when a client associates to the wireless network and opens a browser to any URL (provided the URL does not point to a resource directly on the client's device). The user-requested URL is captured, the user's browser is redirected to the splash or login page, and then the browser is redirected either to your specified landing page, if any, or else back to the captured URL. The landing page may be specified for a user group as well. See "Group Management" on page 277. Note that if you change the management HTTPS port, WPR uses that port, too. See "HTTPS" on page 221.



SSID Faculty Web Page Redirect Configuration

Landing Page URL:	landingpage.greatschool.edu	Server:	○ Internal Splash	Timeout (seconds):	☑ Never
Background Image:	page_bg.jpg ▾		● Internal Login	RADIUS Authentication Type:	○ PAP ● CHAP ○ MS-CHAP
Logo Image:	xirrus_logo.gif ▾		○ External Login	HTTPS	● On ○ Off
Header Text File:	▾		○ Cloud	Redirect URL:	
Footer Text File:	▾		○ External Splash	Redirect Secret:	
Authentication Timeout	120		○ Landing Page Only		

Figure 134. WPR Internal Splash Page Fields (SSID Management)

Note that when clients roam between WAPs, their WPR Authentication will follow them so that re-authentication is not required.

You may select among several different modes for use of the Web Page Redirect feature, each displaying a different set of parameters that must be entered. For each of these modes, set **Authentication Timeout** to the length of time (in minutes) that an association using the captive portal will remain valid after a user is disconnected. If a user session is interrupted, say if a mobile device goes into power-save mode or a user closes a laptop lid, the user will not have to reauthenticate unless the length of the disconnection is longer than the timeout. The default is 120 minutes. The maximum timeout is 10080 minutes (seven days).

Web Page Redirect offers the following modes.

- **Internal Login** page

This option displays a login page (residing on the WAP) instead of the first user-requested URL. There is an upload function that allows you to replace the default login page, if you wish. Please see "Web Page Redirect (Captive Portal)" on page 394 for more information.

To set up internal login, set **Server** to **Internal Login**. Set **HTTPS** to **On** for a secure login, or select **Off** to use HTTP. You may also customize the login page with logo and background images and header and footer text. See "Customizing an Internal Login or Splash page" on page 266.

The user name and password are obtained by the login page. Authentication occurs according to your selection—**PAP**, **CHAP**, or **MS-CHAP**. Note that if you select CHAP, then you cannot select **Active Directory** in "Authentication Service Configuration" on page 268.

After authentication, the browser is redirected back to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

Both the Internal Login and External Login options of WPR perform authentication using your configured RADIUS servers.

- **Internal Splash** page

  This option displays a splash page instead of the first user-requested URL. The splash page files reside on the WAP. Note that there is an upload function that allows you to replace the default splash page, if you wish. Please see "Web Page Redirect (Captive Portal)" on page 394 for more information. You may also customize the splash page with logo and background images and header and footer text. See "Customizing an Internal Login or Splash page" on page 266.

  To use an internal splash page, set **Server** to **Internal Splash**. Enter a value in the **Timeout** field to define how many seconds the splash screen is displayed before timing out, or select **Never** to prevent the page from timing out automatically. After the splash page, the user is redirected to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

- **External Login** page

  This option redirects the user to a login page on an external web server for authentication, instead of the first user-requested URL. Login information (user name and password) must be obtained by that page, and returned to the WAP for authentication.

  Authentication occurs according to your configured RADIUS information. These parameters are configured as described in "Procedure for Configuring Network Security" on page 229, except that the **RADIUS Authentication Type** is selected here, as described below. After authentication, the browser is redirected back to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

  To set up external login page usage, set **Server** to **External Login**. Enter the URL of the external web server in **Redirect URL**, and enter that server's shared secret in **Redirect Secret**.

  Select the **RADIUS Authentication Type**. This is the protocol used for authentication of users, **CHAP** or **PAP** (the default).

  - Password Authentication Protocol (**PAP**), is a simple protocol. PAP transmits ASCII passwords over the network "in the clear" (unencrypted) and is therefore considered insecure.
  - Challenge-Handshake Authentication Protocol (**CHAP**) is a more secure Protocol. The login request is sent using a one-way hash function.

- **External Splash** page

  This option displays a splash page instead of the first user-requested URL. The splash page files reside on an external web server.

  To set up external splash page usage, set **Server** to **External Splash**. Enter the URL of the external web server in **Redirect URL**, and enter that server's shared secret in **Redirect Secret**.

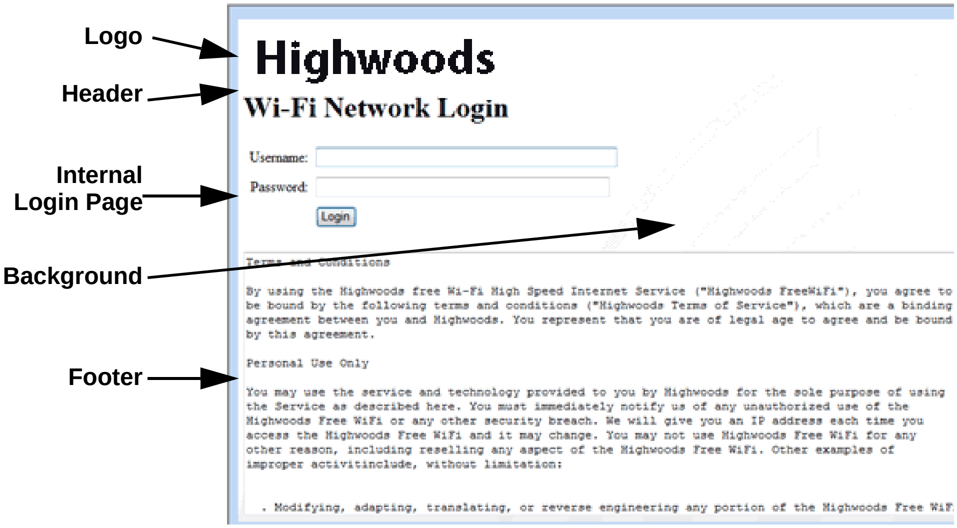
After the splash page, the user is redirected to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

- **Landing Page** Only

  This option redirects the user to a specific landing page. If you select this option, enter the desired address in **Landing Page URL**.

Customizing an Internal Login or Splash page

You may customize these pages with a logo and/or background image, and header and/or footer text, as shown below in Figure 135.



Terms and Conditions

By using the Highwoods free Wi-Fi High Speed Internet Service ("Highwoods FreeWiFi"), you agree to be bound by the following terms and conditions ("Highwoods Terms of Service"), which are a binding agreement between you and Highwoods. You represent that you are of legal age to agree and be bound by this agreement.

Personal Use Only

You may use the service and technology provided to you by Highwoods for the sole purpose of using the Service as described here. You must immediately notify us of any unauthorized use of the Highwoods Free WiFi or any other security breach. We will give you an IP address each time you access the Highwoods Free WiFi and it may change. You may not use Highwoods Free WiFi for any other reason, including reselling any aspect of the Highwoods Free WiFi. Other examples of improper activitinclude, without limitation:

. Modifying, adapting, translating, or reverse engineering any portion of the Highwoods Free WiF

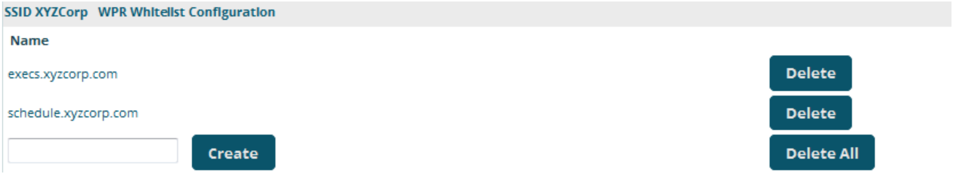
Figure 135. Customizing an Internal Login or Splash Page

- **Background Image**—specify an optional jpg, gif, or png file to display in the background of the page. Other customizations (logo, header, footer) will overlay the background, so that it will not be visible in those areas.
- **Logo Image**—specify an optional jpg, gif, or png file to display at the top of the page.

- **Header Text File**—specify an optional .txt file to display at the top of the page (beneath the logo, if any).
- **Footer Text File**—specify an optional .txt file to display at the bottom of the page.

Whitelist Configuration for Web Page Redirect

On a per-SSID basis, the whitelist allows you to specify Internet destinations that stations can access without first having to pass the WPR (captive portal) login/ splash page. Note that a whitelist may be specified for a user group as well. See "Group Management" on page 277.



SSID XYZCorp WPR Whitelist Configuration

Name	
execs.xyzcorp.com	Delete
schedule.xyzcorp.com	Delete

Figure 136. Whitelist Configuration for WPR

To add a web site to the whitelist for this SSID, enter it in the provided field, then click **Create**. You may enter an IP address or a domain name. Up to 32 entries may be created.

Example whitelist entries:

- Hostname: www.yahoo.com (but not www.yahoo.com/abc/def.html)
- Wildcards are supported: *.yahoo.com
- IP address: 121.122.123.124

Some typical applications for this feature are:

- to add allowed links to the WPR page
- to add a link to terms of use that may be hosted on another site
- to allow embedded video on WPR page

Note the following details of the operation of this feature:

- The list is configured on a per-SSID basis. You must have **WPR** enabled for the SSID to see this section of the SSID Management page.

- When a station that has not yet passed the WPR login/splash page attempts to access one of the white-listed addresses, it will be allowed access to that site as many times as requested.
- The station will still be required to pass through the configured WPR flow for all other Internet addresses.
- The whitelist will work against all traffic -- not just http or https
- Indirect access to other web sites is not permitted. For example, if you add www.yahoo.com to the whitelist, you can see that page, but not all the ads that it attempts to display.
- The whitelist feature does not cause traffic to be redirected to the whitelist addresses.

WPA Configuration

If you set **Encryption** for this SSID to one of the WPA selections (Step 12 on page 257) and you did not check the **Global** checkbox (Step 13), this section will be displayed. The **WPA Configuration** encryption settings have the same parameters as those described in "Procedure for Configuring Network Security" on page 229.

Authentication Service Configuration

The RADIUS settings section will be displayed if you set **Authentication** (Step 11 on page 257) to anything but **OPEN,** and you set **Encryption** (Step 12) to anything but **WEP**, and you did not check the **Global** checkbox (Step 13). This means that you wish to set up a RADIUS server or Active Directory server to be used for this particular SSID. If **Global** is checked, then the security settings (including the RADIUS server, if any) established at the global level are used instead (see "Global Settings" on page 229).

The RADIUS and accounting settings are configured in the same way as for an external RADIUS server (see "Procedure for Configuring an External RADIUS Server" on page 233). If you select **Active Directory**, then the settings are configured in "Active Directory" on page 238. Note that if you select **Active Directory**, then you cannot use CHAP authentication.

See Also

DHCP Server

External Radius

Global Settings

Internal Radius

Security Planning

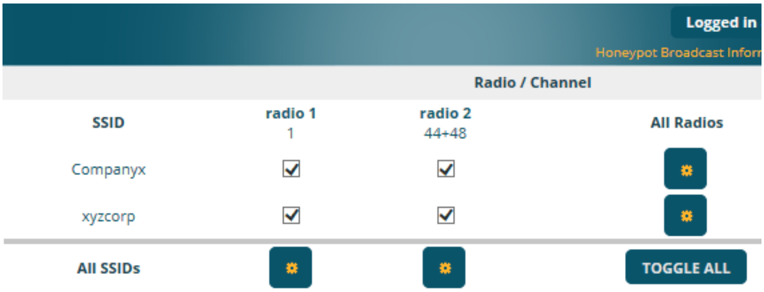
SSIDs

Understanding QoS Priority on the WAP

Active Radios

By default, when a new SSID is created, that SSID is active on all radios. This window allows you to specify which radios will offer that SSID. Put differently, you can specify which SSIDs are active on each radio.

This feature is useful in conjunction with WDS. You may use this window to configure the WDS link radios so that only the WDS link SSIDs are active on them.



	Radio / Channel		
SSID	radio 1 1	radio 2 44+48	All Radios
Companyx	☑	☑	✱
xyzcorp	☑	☑	✱
All SSIDs	✱	✱	TOGGLE ALL

Figure 137. Setting Active Radios per SSID

Procedure for Specifying Active Radios

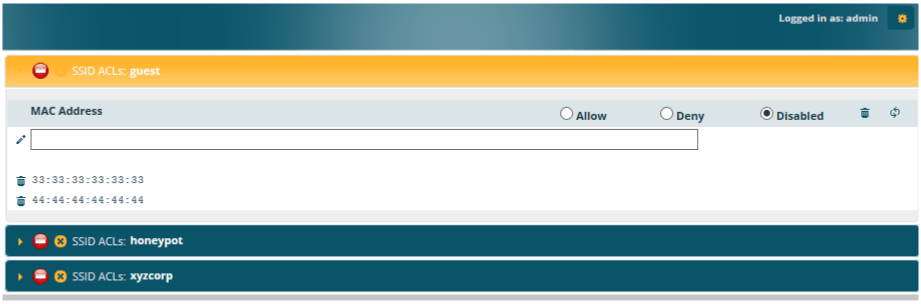
1. **SSID:** For a given SSID row, check the radios that should offer that SSID to clients. Uncheck any radios which should not offer that SSID.
2. **All Radios**: This button, in the last column, may be used to allow or deny this SSID on all radios, i.e., switch all radios between allow or deny.
3. **All SSIDs**: This button, in the bottom row, may be used to allow or deny all SSIDs on this radio.
4. **Toggle All**: This button, on the lower left, may be used to allow or deny all SSIDs on all radios.
5. Click the **Save** button 💾 if you wish to make your changes permanent.

Per-SSID Access Control List

This window allows you set up Access Control Lists (ACLs) on a per-SSID basis, to control whether a station with a particular MAC address may associate to a particular SSID. You may create access control list entries and delete existing entries, and control the type of list (allow or deny).

There is one ACL per SSID, and you may select whether its type is an **Allow** list or a **Deny** list, or whether use of this list is **Disabled**. You may create up to 1000 entries per SSID.

There is also a global ACL (see “Access Control List” on page 227). If the same MAC address is listed in both the global ACL and in an SSID’s ACL, and if either ACL would deny that station access to that SSID, then access will be denied.



Logged in as: admin

SSID ACLs: guest

MAC Address ○ Allow ○ Deny ● Disabled

33:33:33:33:33:33

44:44:44:44:44:44

SSID ACLs: honeypot

SSID ACLs: xyzcorp

Figure 138. Per-SSID Access Control List

Procedure for Configuring Access Control Lists

1. **SSID**: Select the line for the SSID whose ACL you wish to manage. Click the line to hide or expand (display) the list.
2. **Access Control List Type**: Select **Disabled** to disable use of the Access Control List for this SSID, or select the ACL type—either **Allow** or **Deny**.
    - **Allow**: Only allows the listed MAC addresses to associate to the WAP. All others are denied. The plus symbol ⊕ appears before the SSID name for an allow list.
    - **Deny List**: Denies the listed MAC addresses permission to associate to the WAP. All others are allowed. The minus symbol ⊖ appears before the SSID name for a deny list.
    - **Disabled**: A red dot 🔴 appears before the SSID name for a disabled list. A green dot 🟢 appears before the SSID name for an allow or deny list.

In addition to these lists, other authentication methods (for example, RADIUS) are still enforced for users.

3. **MAC Address**: If you want to add a MAC address to the ACL for the selected SSID, enter the new MAC address. You may use a wildcard (*) for one or more digits to match a range of addresses. **Delete**: You may delete selected MAC addresses from this list by clicking their **Delete** buttons 🗑 .

4. Click the **Save** button 💾 if you wish to make your changes permanent.

Honeypots

Use the honeypot feature carefully as it could interfere with legitimate SSIDs.

The honeypot SSID feature prevents the airwaves from being crowded with probes for named SSIDs. These probes are automatically generated by some popular wireless devices. When you create and enable a honeypot SSID on a WAP, it responds to any station probe looking for a named open SSID (unencrypted and unauthenticated) that is *not* configured on the WAP. For more details, see “High Density 2.4G Enhancement—Honeypot SSID” on page 253.

This page allows you to create a honeypot SSID, enter a whitelist of SSID names that are not to be honeypotted, and define alternate names for the SSID that will be broadcast instead of “honeypot”.

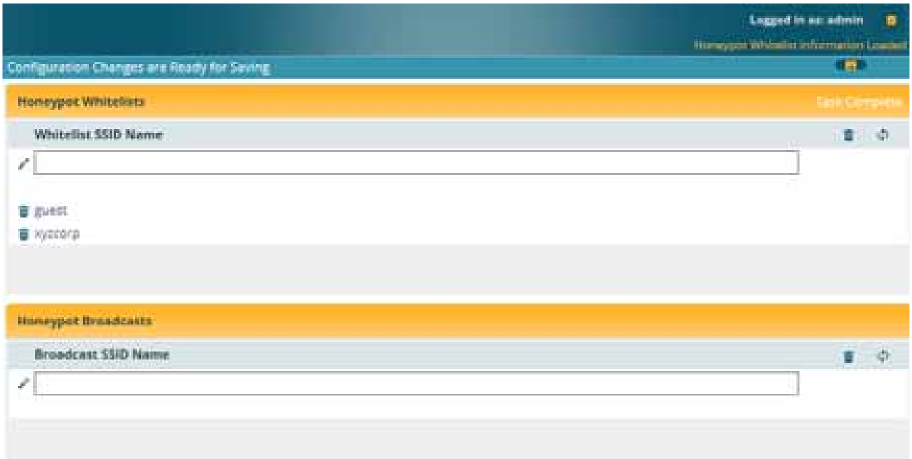


Figure 139. Honeypot Whitelist

Procedure for Configuring Honeypot Whitelists

1. **Create a honeypot:** If you have not already created an SSID named **honeypot**, you will be asked whether you wish to create one. Click **Yes**. You must have an SSID named honeypot to use this feature.

2. **Honeypot Whitelists**: This section only appears if you have created an SSID named honeypot. You may define a whitelist of allowed SSIDs which are not to be honeypotted, as described in "High Density 2.4G Enhancement—Honeypot SSID" on page 253. Type in each SSID name, and click **Create** to add it to the whitelist. Up to 50 SSIDs may be listed. The SSID names entered in this list are not case-sensitive.

   You may use the "*****" character as a wildcard to match any string at this position. For example, ava***** matches any string that starts with **AVA** or **ava**. You may use a **?** as a wildcard to match a single character by surrounding the SSID name in quotes. For example, "**avaya?**" will match any six-character long string that starts with **avaya** (again, the match is not case-sensitive). If you do not use a wildcard, then the SSID name entered must be matched exactly in order to be whitelisted (except that case is not considered).

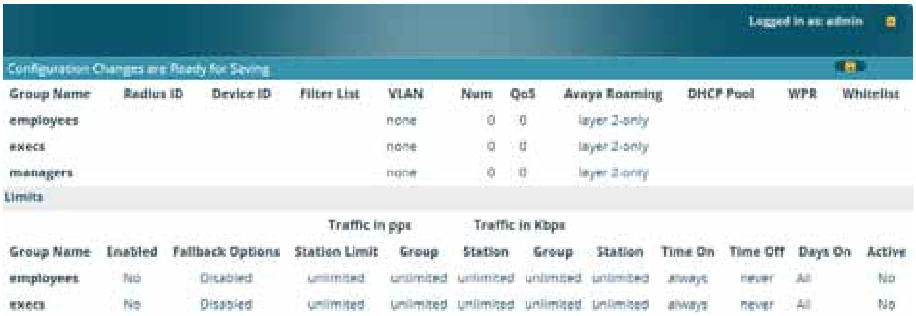
3. **Honeypot Broadcasts**: This section only appears if you have created an SSID named honeypot. You may define one or more alias names for this SSID. They will be broadcast *instead of* the name **honeypot**.

Groups

This is a status-only window that allows you to review user (i.e., wireless client) Group assignments. It includes the group name, Radius ID, Device ID, VLAN IDs and QoS parameters and roaming layer defined for each group, and DHCP pools and web page redirect information defined for the group. You may click on a group's name to jump to the edit page for the group. There are no configuration options available on this page, but if you are experiencing problems or reviewing group management parameters, you may want to print this page for your records.

The **Limits** section of this window shows any limitations configured for your defined groups. For example, this window shows the current state of a group (enabled or disabled), how much group and per-station traffic is allowed, time on and time off, and days on and off.

For information to help you understand groups, see Understanding Groups below.



Group Name	Radius ID	Device ID	Filter List	VLAN	Num	QoS	Avaya Roaming	DHCP Pool	WPR	Whitelist
employees				none	0	0	layer 2-only			
execs				none	0	0	layer 2-only			
managers				none	0	0	layer 2-only			

Limits

			Traffic in pps		Traffic in Kbps						
Group Name	Enabled	Fallback Options	Station Limit	Group	Station	Group	Station	Time On	Time Off	Days On	Active
employees	No	Disabled	unlimited	unlimited	unlimited	unlimited	unlimited	always	never	All	No
execs	No	Disabled	unlimited	unlimited	unlimited	unlimited	unlimited	always	never	All	No

Figure 140. Groups

Understanding Groups

User groups allow administrators to assign specific network parameters to users (wireless clients) through RADIUS privileges rather than having to map users to an SSID tailored for that set of privileges. Groups provide flexible control over user privileges without the need to create large numbers of SSIDs.

A group allows you to define a set of parameter values to be applied to selected users. For example, you might define the user group **Students**, and set its VLAN, security parameters, web page redirect (WPR), and traffic limits. When a new user is created, you can apply all of these settings just by making the user a member of the group. The group allows you to apply a uniform configuration to a set of users in one step.

In addition, you can restrict the group so that it only applies its settings to group members who are connecting using a specific device type, such as iPad or phone. Thus, you could define a group named **Student-Phone** with **Device ID** set to **Phone**, and set the group’s **VLAN Number** to 100. This group’s settings will only be applied to group members who connect using a phone, and they will all use VLAN 100. Note that settings for the group in the RADIUS server will override any settings on this WMI page.

Almost all of the parameters that can be set for a group are the same as SSID parameters. This allows you to configure features at the user group level, rather than for an entire SSID. If you set parameter values for an SSID, and then enter different values for the same parameters for a user group, the **user group values have priority** (i.e., group settings will override SSID settings).

Group names are case-sensitive and can contain up to 32 alphanumeric characters (do not include spaces when defining Groups).

Using Groups

User accounts are used to authenticate wireless clients that want to associate to the WAP. These accounts are established in one of two ways, using the **Security> Internal Radius** window or the **Security> External Radius** window. In either case, you may select a user group for the user, and that user group’s settings will apply to the user:

- Internal Radius—when you add or modify a user entry, select a user group to which the user will belong.
- External Radius—when you add or modify a user account, specify the **Radius ID** for the user group to which the user will belong. This must be the same Radius ID that was entered in the Group Management window. When the user is authenticated, the external Radius server will send the Radius ID to the WAP. This will allow the WAP to identify the group to which the user belongs.

See Also

External Radius

Internal Radius

SSIDs

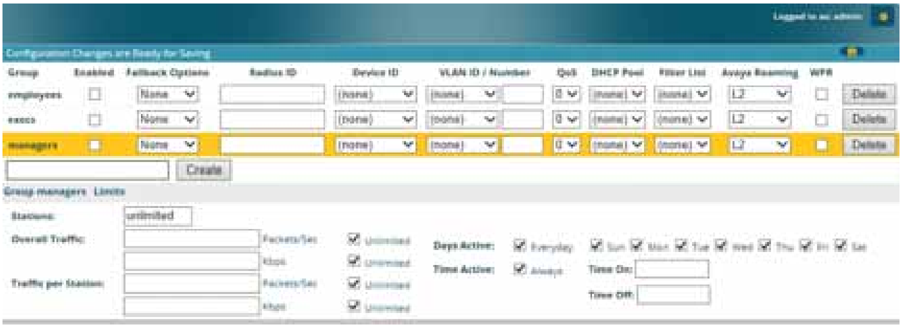
Understanding QoS Priority on the WAP

Web Page Redirect (Captive Portal) Configuration

Understanding Fast Roaming

Group Management

This window allows you to manage groups (create, edit and delete), assign usage limits and other parameters on a per group basis, and configure the Web Page Redirect (captive portal) functionality.



Logged in as: admin

Configuration Changes are Ready for Saving

Group	Enabled	Fallback Options	Radius ID	Device ID	VLAN ID / Number		QoS	DHCP Pool	Filter List	Avaya Roaming	WPR	
employees	□	None		(none)	(none)		0	(none)	(none)	L2	□	Delete
execs	□	None		(none)	(none)		0	(none)	(none)	L2	□	Delete
managers	□	None		(none)	(none)		0	(none)	(none)	L2	□	Delete

Create

Group managers Limits

Stations: unlimited

Overall Traffic: Packets/Sec ☑ Unlimited

Kbps ☑ Unlimited

Traffic per Station: Packets/Sec ☑ Unlimited

Kbps ☑ Unlimited

Days Active: ☑ Everyday ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time Active: ☑ Always Time On:

Time Off:

Figure 141. Group Management

Procedure for Managing Groups

1. **New Group Name:** To create a new group, enter a new group name next to the Create button, then click **Create**. You may create up to 16 groups.

   To configure and enable this group, proceed with the following steps.

2. **Group**: This column lists currently defined groups. When you create a new group, the group name appears in this list. Click on any group to select it, and then proceed to modify it as desired.

3. **Enabled**: Check this box to enable this group or leave it blank to disable it. When a group is disabled, users that are members of the group will behave as if the group did not exist. In other words, the options configured for the SSID will apply to the users, rather than the options configured for the group.

4. **Fallback**: Network Assurance checks network connectivity for the WAP. When Network Assurance detects a failure, perhaps due to a bad link or WDS failure, if Fallback is set to **Disable** the WAP will automatically disable users in this group. This will disassociate current clients, and prevent them from re-associating. Since the WAP's network connectivity has failed, this gives clients a chance to connect to other, operational parts of the wireless network. See Step a on page 222 for more information on Network Assurance.

5. **Radius ID**: Enter a unique Radius ID for the group, to be used on an external Radius server. When adding a user account to the external server, this Radius ID value should be entered for the user. When the user is authenticated, Radius sends this value to the WAP. This tells the WAP that the user is a member of the group having this Radius ID.

6. **Device ID**: You may select a device type from this drop-down list, for example, **Notebook**, **phone**, **iPhone**, or **Android**. This allows you to apply the group settings only if a station authenticates as a user that is a member of the group and the station's device type matches **Device ID. Select none** if you do not want to consider the device type. If you have a Radius ID you should not enter a Device ID.

7. **VLAN ID**: (Optional) From the pull-down list, select a VLAN or VLAN Pool for this user's traffic to use (see "VLANs" on page 191 and "VLAN Pools" on page 193). This user group's VLAN settings supersede Dynamic VLAN settings (which are passed to the WAP by the Radius server). To avoid confusion, we recommend that you avoid specifying the VLAN for a user in two places.

8. **QoS Priority**: (Optional) Select a value in this field for QoS (Quality of Service) priority filtering. The QoS value must be one of the following:

- 0—The lowest QoS priority setting, where QoS makes its best effort at filtering and prioritizing data, video and voice traffic without compromising the performance of the network. Use this setting in environments where traffic prioritization is not a concern.
- 1—Medium; QoS prioritization is aggregated across all traffic types.
- 2—High, normally used to give priority to video traffic.
- 3—The highest QoS priority setting, normally used to give priority to voice traffic.

The QoS setting you define here will prioritize wireless traffic for this group versus other traffic, as described in “Understanding QoS Priority on the WAP” on page 249. The default value for this field is 2.

9. **DHCP Pool**: (Optional) To associate an internal DHCP pool to this group, select it from the pull--down list. Only one pool may be assigned. An internal DHCP pool must be created before it can be assigned. To create a DHCP pool, go to “DHCP Server” on page 178.

10. **Filter List**: (Optional) If you wish to apply a set of filters to this user group’s traffic, select the desired Filter List. See “Filters” on page 363.

11. **Avaya Roaming**: (Optional) For this group, select roaming behavior. Select **L2&L3** to enable fast roaming between radios or WAPs at Layer 2 and Layer 3. If you select **L2**, then roaming uses Layer 2 only. You may only select fast roaming at Layers 2 and 3 if this has been selected in Global Settings. You may select **Off** to disable fast roaming. See “Understanding Fast Roaming” on page 283.

12. **Web Page Redirect (WPR)**: (Optional) Check this box if you wish to enable the Web Page Redirect (captive portal) functionality. This will open a **Web Page Redirect** details section in the window, where your WPR parameters may be entered. This feature may be used to display a splash screen when a user first associates to the wireless network. After that, it can (optionally) redirect the user to an alternate URL. See “Web Page Redirect (Captive Portal) Configuration” on page 263 for details of WPR configuration. Note that the Group Management window only allows you to set up an **Internal Splash** page and a **Landing Page URL**.

The authentication options that are offered on the SSID Management page are not offered here. Since the group membership of a user is provided to the WAP by a Radius server, this means the user has already been authenticated.

You may create a WPR Whitelist on a per-group basis if you wish. See "Whitelist Configuration for Web Page Redirect" on page 267 for details of WPR Whitelist usage and configuration.

Group Limits

The Limits section allows you to limit the traffic or connection times allowed for this user group. Note that the Radios—Global Settings window and the SSID management windows also have options to limit the number of stations, limit traffic, and/or limit connection times. If limits are set in more than one place, all limits will be enforced:

- As soon as any station limit is reached, no new stations can associate until some other station has terminated its association.
- As soon as any traffic limit is reached, it is enforced.
- If any connection date/time restriction applies, it is enforced.

You can picture this as a logical AND of all restrictions. For example, suppose that a station's SSID is available Monday - Friday between 8:00am and 5:00pm, and the User Group is available Monday, Tuesday, Wednesday between 6:00am and 8:00pm, then the station will be allowed on MWF between 8:00am and 5:00pm.

To eliminate confusion, we recommend that you configure one set of limits or the other, but not both.

13. **Stations**: Enter the maximum number of stations allowed on this group. The default is 1536.

14. **Overall Traffic**: Check the **Unlimited** checkbox if you do not want to place a restriction on the traffic for this group, or enter a value in the Packets/Sec field and make sure that the Unlimited box is unchecked to force a traffic restriction.

15. **Traffic per Station**: Check the **Unlimited** checkbox if you do not want to place a restriction on the traffic per station for this group, or enter a value in the **Packets/Sec** or **Kbps** field and make sure that the Unlimited box is unchecked to force a traffic restriction.

16. **Days Active**: Choose **Everyday** if you want this group to be active every day of the week, or select only the specific days that you want this group to be active. Days that are not checked are considered to be the inactive days.

17. **Time Active**: Choose **Always** if you want this group active without interruption, or enter values in the **Time On** and **Time Off** fields to limit the time that group members may associate.

18. To delete an entry, click its **Delete** button.

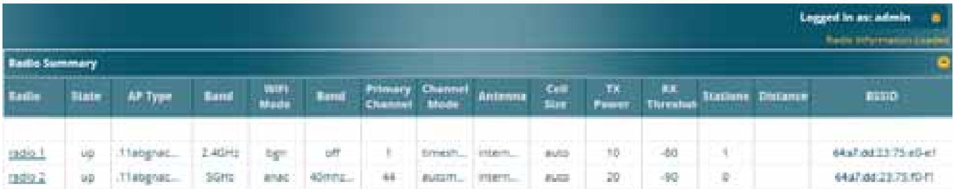
19. Click the **Save** button 💾 if you wish to make your changes permanent.

See Also

DHCP Server
External Radius
Internal Radius
Security Planning
SSIDs

Radios

This status-only window summarizes the status of the radios. For each radio, it shows whether it is up or down, the channel and wireless mode, the antenna that it is currently using, its cell size and transmit and receive power, how many users (stations) are currently associated to it, whether a WDS link distance has been set for it, and its BSSID (MAC address).



Logged in as: admin

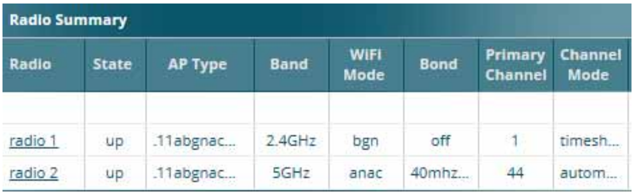
Radio information Loaded

Radio Summary

Radio	State	AP Type	Band	WiFi Mode	Bond	Primary Channel	Channel Mode	Antenna	Cell Size	TX Power	RX Threshold	Stations	Distance	BSSID
radio 1	up	.11abgnac...	2.4GHz	bgn	off	1	timesh...	intern...	auto	10	-60	1		64:a7:dd:23:75:e0-e1
radio 2	up	.11abgnac...	5GHz	anac	40mhz...	44	autom...	intern...	auto	20	-90	0		64:a7:dd:23:75:f0-f1

Figure 142. Radios

The **Channel Mode** column displays some status information that is not found elsewhere: the source of a channel setting. If you set a channel manually (via Radio Settings), it will be listed as **manual**. If an autochannel operation changed a channel, then it is labeled as **auto**. If the channel is set to the current factory default setting, the source will be **default**. This column also shows whether the channel selection is **locked**, or whether the radio was automatically switched to this channel because the WAP detected the signature of **radar** in operation on a conflicting channel (see also, Step 7 on page 292).



Radio Summary

Radio	State	AP Type	Band	WiFi Mode	Bond	Primary Channel	Channel Mode
radio 1	up	.11abgnac...	2.4GHz	bgn	off	1	timesh...
radio 2	up	.11abgnac...	5GHz	anac	40mhz...	44	autom...

Figure 143. Source of Channel Setting

There are no configuration options in this window, but if you are experiencing problems or simply reviewing the radio assignments, you may print this window for your records. Click any radio name to open the associated configuration page.

WAPs have a fast roaming feature, allowing them to maintain sessions for applications such as voice, even while users cross boundaries between WAPs. Fast roaming is set up in the Global Settings window and is discussed in:

- **"Understanding Fast Roaming" on page 283**

Radios are configured using the following windows:

- **"Radio Settings" on page 284**
- **"Global Settings" on page 290**
- **"Global Settings .11an" on page 306**
- **"Global Settings .11bgn" on page 311**
- **"Global Settings .11n" on page 318**
- **"Global Settings .11u" on page 323**
- **"Global Settings .11ac" on page 321**
- **"Advanced RF Settings" on page 329**
- **"Hotspot 2.0" on page 338**
- **"NAI Realms" on page 340**
- **"NAI EAP" on page 341**
- **"Intrusion Detection" on page 343**
- **"LED Settings" on page 350**
- **"DSCP Mappings" on page 352**

"Roaming Assist" on page 353***See Also***

Radio Statistics Summary

Understanding Fast Roaming

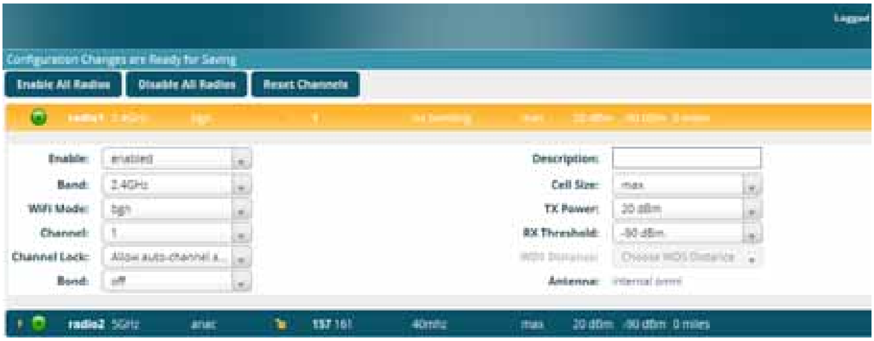
To maintain sessions for real-time data traffic, such as voice and video, users must be able to maintain the same IP address through the entire session. With traditional networks, if a user crosses VLAN or subnet boundaries (i.e., roaming between domains), a new IP address must be obtained.

Mobile wireless users are likely to cross multiple roaming domains during a single session (especially wireless users of VoIP phones). **Layer 3 roaming** allows a user to maintain the same IP address through an entire real-time data session. The user may be associated to any of the VLANs defined on the WAP. The Layer 3 session is maintained by establishing a tunnel back to the originating WAP. You should decide whether or not to use Layer 3 roaming based on your wired network design. Layer 3 roaming incurs extra overhead and may result in additional traffic delays. You may configure one SSID for Layer 3 fast roaming with up to 25 WAPs.

Fast Roaming is configured on two pages. To enable the fast roaming options that you want to make available on your WAP, see Step 30 to Step 32 in "Global Settings" on page 290. To choose which of the enabled options are used by an SSID or Group, see "Procedure for Managing SSIDs" on page 255 (Step 14) or "Procedure for Managing Groups" on page 277.

Radio Settings

This window allows you to enable/disable radios, define the wireless mode for each radio, specify the channel and bond width and the cell size for each radio, lock the channel selection, establish transmit/receive parameters, and reset channels. Buttons at the top of the list allow you to **Reset Channels**, **Enable All Radios,** or **Disable All Radios**. When finished, click the **Save** button if you wish to make your changes permanent.



radio1 2.4GHz bgn 1 no bonding max 20 dBm -90 dBm 0 miles

Enable: enabled
Band: 2.4GHz
WiFi Mode: bgn
Channel: 1
Channel Lock: Allow auto-channel a...
Bond: off
Description:
Cell Size: max
TX Power: 20 dBm
RX Threshold: -90 dBm
WDS Distance: Choose WDS Distance
Antenna: internal omni

radio2 5GHz anac 157 161 40mhz max 20 dBm -90 dBm 0 miles

Figure 144. Radio Settings

By default on the WAP 9100 Series, Radio 1 is set to 2.4GHz and higher radios are set to 5GHz.

Procedure for Auto Configuring Radios

You can auto-configure channel and cell size of radios by clicking on the **Auto Configure** buttons on the appropriate WMI page as shown below (auto configuration only applies to enabled radios):

- For all radios, go to "Advanced RF Settings" on page 329.
- For all 802.11a settings, go to "Global Settings .11an" on page 306.
- For all 802.11bg settings, go to "Global Settings .11bgn" on page 311.
- For all 802.11n settings, go to "Global Settings .11n" on page 318.
- For all 802.11ac settings, go to "Global Settings .11ac" on page 321.

Procedure for Manually Configuring Radios

1. The row for each radio summarizes its settings. Click to expand it and display the settings. Click again to collapse the entry.
2. In the **Enable** field select **enabled**, or select **disabled** if you want to turn off the radio. The state of the channel is displayed with a green dot 🟢 if enabled, and a red dot ⛔ if disabled.
3. In the **Band** field, select the wireless band for this radio from the choices available in the pull-down menu, either **2.4GHz** or **5 GHz**. Choosing the **5GHz** band will automatically select an adjacent channel for bonding. If the band displayed is **auto**, the **Band** is about to be changed based on a new **Channel** selection that you made that requires the change.

For WAO9122 Series WAPs only:
*—**radio1** may be set to either band or to monitor (also see the Timeshare option in "RF Monitor" on page 330).*
*—**radio2** is permanently set to 5 GHz.*

One of the radios must be set to **monitor** mode if you wish to support Spectrum Analyzer, Radio Assurance (loopback testing), and Intrusion Detection features. Monitoring has a **Timeshare** mode option, which is especially useful for WAPs with two radios allowing one radio to be shared between monitoring the airwaves for problems and providing services to stations. See **RF Monitor Mode** in “Advanced RF Settings” on page 329 to set this option.

4. In the **WiFi Mode** field, select the IEEE 802.11 wireless mode (or combination) that you want to allow on this radio. The drop-down list will only display the appropriate choices for the selected **Band**. For example, the 5 GHz band allows you to select **ac-only**, **anac**, **an**, **a-only**, or **n-only**, while 2.4GHz includes 802.11b and 802.11g choices. When you select a WiFi Mode for any radio, your selection in the **Channel** column will be checked to ensure that it is a valid choice for that WiFi Mode.

   By selecting appropriate WiFi Modes for the radios on your WAPs, you can greatly improve wireless network performance. For example, if you have 802.11n and 802.11ac stations using the same radio, throughput on that radio is reduced greatly for the 802.11ac stations. By supporting 802.11n stations only on selected radios in your network, the rest of your 802.11ac radios will have greatly improved performance. Take care to ensure that your network provides adequate coverage for the types of stations that you need to support.

5. In the **Channel** field, select the channel you want this radio to use from the channels available in the pull-down list. The list shows the channels available for the radio selected (depending on which band the radio is using). Channels that are shown in gray are unavailable. They are either already in use, or not offered for the selected Band.

   The channels that are available for assignment to radios will differ, depending on the country of operation. If **Country** is set to **United States** in the Global Settings window, then 21 channels are available to 802.11an radios.

As mandated by FCC/IC law, WAPs continually scan for signatures of radar. If such a signature is detected, the WAP will switch operation from conflicting channels to new ones. The WAP will switch back to the original channel after 30 minutes if the channel is clear. If a radio was turned off because there were no available channels not affected by radar, the WAP will now bring that radio back up after 30 minutes if that channel is clear. The 30 minute time frame complies with FCC/IC regulations.

6. Set **Channel Lock** to **Block auto-channel assignment** if you want to lock in your channel selection so that an autochannel operation (see Advanced RF Settings) can't change it. A locked padlock 🔒 will be displayed for the radio.

7. The **Bond** field works together with the **Channel** selected above. (For 802.11n radios, it also obeys the bonding options selected on the Global Settings .11n page.) Also see the discussion in "80 MHz and 160 MHz Channel Widths (Bonding)" on page 37. Bonding is available on all WAPs, including two-radio models. For 802.11n, two 20MHz channels may be bonded to create one 40 MHz channel with double the data rate. 802.11ac offers an additional option to bond four 20MHz channels to create one 80MHz channel with four times the data rate.

   - **Channel number**—If a channel number appears, then this channel is already bonded to the listed channel.
   - **Off**—Do not bond his channel to another channel.
   - **40 MHz**—Bond this channel to an adjacent channel. The bonded channel is selected automatically by the WAP based on the **Channel** (Step 5). The choice of banded channel is static—fixed once the selection is made.
   - **80 MHz**—Bond this channel to three adjacent channels. The bonded channels are selected automatically by the WAP based on the **Channel** (Step 5). The choice of bonded channels is static—fixed once the selection is made.

   The top line for the radio will show the channels that have been assigned based on the width of the bond.

8. In the **Cell Size** field, select **auto** to allow the optimal cell size to be automatically computed (see also, "RF Power and Sensitivity" on page 332). To set the cell size yourself, choose either **small**, **medium**, **large**, or **max** to use the desired pre-configured cell size. Alternatively, you can set the wireless cell size manually by specifying the transmit and receive power—in dB—in the **Tx Power** (transmit) and **Rx Threshold** (receive) fields. If you set manual values, the Cell Size field will display the value **manual** after the page is refreshed.

   The default for Cell Size is **max**. If you select a value other than **auto**, the cell size will not be affected by cell size auto configuration. Note that ultra low power **Tx dBm** settings are possible. Values from -15dB to 5dB are provided specifically to help in high density 2.4 GHz environments.

   When other WAPs are within listening range of this one, setting cell sizes to **Auto** allows the WAP to change cell sizes so that coverage between cells is maintained. Each cell size is optimized to limit interference between sectors of other WAPs on the same channel. This eliminates the need for a network administrator to manually tune the size of each cell when installing multiple WAPs. In the event that a WAP or a radio goes offline, an adjacent WAP can increase its cell size to help compensate.

   The number of users and their applications are major drivers of bandwidth requirements. The network architect must account for the number of users within the WAP's cell diameter. In a large office, or if multiple WAPs are in use, you may choose **Small** cells to achieve a higher data rate, since walls and other objects will not define the cells naturally.

   For additional information about cell sizes, go to "Coverage and Capacity Planning" on page 25.

9. If you are using WDS to provide backhaul over an extended distance, use **WDS Distance (Miles)** to prevent timeout problems associated with long transmission times. Set the approximate distance in miles between this radio and the connected WAP in this column. This increases the wait time for frame transmission accordingly.

10. The **Antenna** field displays the antenna that has automatically been selected for this radio.

11. If desired, enter a description for this radio in the **Description** field.

12. You may reset all of the enabled radios by clicking the **Reset Channels** button at the top of the list. A message will inform you that all enabled radios have been taken down and brought back up.

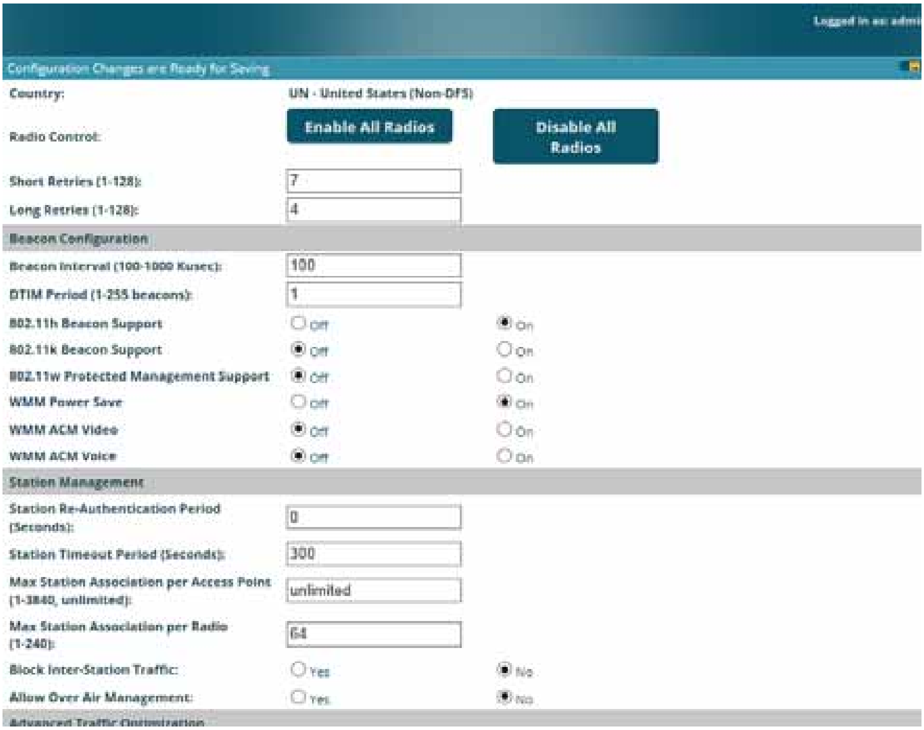
13. Buttons at the top of the list allow you to **Enable All Radios** or **Disable All Radios**.

14. Click the **Save** button 💾 if you wish to make your changes permanent.

See Also

Coverage and Capacity Planning
Global Settings
Global Settings .11an
Global Settings .11bgn
Global Settings .11n
Global Settings .11ac
Advanced RF Settings
Radios
Radio Statistics Summary
LED Settings

Global Settings



Logged in as: admi

Configuration Changes are Ready for Saving

Country:	UN - United States (Non-DFS)	
Radio Control:	Enable All Radios	Disable All Radios
Short Retries (1-128):	7	
Long Retries (1-128):	4	
Beacon Configuration		
Beacon Interval (100-1000 Kusec):	100	
DTIM Period (1-255 beacons):	1	
802.11h Beacon Support	○ Off	● On
802.11k Beacon Support	● Off	○ On
802.11w Protected Management Support	● Off	○ On
WMM Power Save	○ Off	● On
WMM ACM Video	● Off	○ On
WMM ACM Voice	● Off	○ On
Station Management		
Station Re-Authentication Period (Seconds):	0	
Station Timeout Period (Seconds):	300	
Max Station Association per Access Point (1-3840, unlimited):	unlimited	
Max Station Association per Radio (1-240):	64	
Block Inter-Station Traffic:	○ Yes	● No
Allow Over Air Management:	○ Yes	● No
Advanced Traffic Optimization		

Figure 145. Global Settings (Radios)

This window allows you to establish global radio settings. Global radio settings include enabling or disabling all radios (regardless of their operating mode), and changing settings for beacons, station management, and advanced traffic optimization—including multicast processing, load balancing, and roaming. Changes you make on this page are applied to all radios, without exception.

Procedure for Configuring Global Radio Settings

1. **Country**: This is a display-only value. Once a country has been set, it may not be changed.

   The channels that are available for assignment to radios will differ, depending on the country of operation. If **Country** is set to **United States**, then 21 channels are available for 802.11a / n.

   If no country is displayed, the channel set defaults to channels and power levels that are legal worldwide—this set only includes the lower eight 5 GHz channels.

2. **Radio Control**: Click on the **Enable All Radios** button to enable all radios for this WAP, or click on the **Disable All Radios** button to disable all radios.

3. **Short Retries**: This sets the maximum number of transmission attempts for a frame, the length of which is less than or equal to the RTS Threshold, before a failure condition is indicated. The default value is 7. Enter a new value (1 to 128) in the **Short Retry Limit** field if you want to increase or decrease this attribute.

4. **Long Retries**: This sets the maximum number of transmission attempts for a frame, the length of which is greater than the RTS Threshold, before a failure condition is indicated. The default value is 4. Enter a new value (1 to 128) in the **Long Retry Limit** field if you want to increase or decrease this attribute.

Beacon Configuration

5. **Beacon Interval**: When the WAP sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. Enter the desired value in the **Beacon Interval** field, between 20 and 1000 Kusecs. A Kusec is 1000 microseconds = 1 millisecond. The value you enter here is applied to all radios.

6. **DTIM Period**: A Delivery Traffic Indication Message (DTIM) is a signal sent as part of a beacon by the WAP to a client device in sleep mode, alerting the device to broadcast traffic awaiting delivery. The **DTIM**

Period is a multiple of the **Beacon Interval**, and it determines how often DTIMs are sent out. By default, the DTIM period is 1, which means that it is the same as the beacon interval. Enter the desired multiple, between 1 and 255. The value you enter here is applied to all radios.

7. **802.11h Beacon Support**: This option enables beacons on all of the WAP's radios to conform to 802.11h requirements, supporting dynamic frequency selection (DFS) and transmit power control (TPC) to satisfy regulatory requirements for operation in Europe.

8. **802.11k Beacon Support**: 802.11k offers faster and more efficient roaming. When enabled, each beacon lists the channels that nearby APs offer. This supports improved channel scanning, resulting in faster roam times and increased battery life due to shorter scan times since the station knows where to look for nearby APs. The WAP will also respond to requests from stations for an 802.11K Neighbor Report with additional information about nearby APs. This setting is enabled by default.

9. **802.11w Protected Management Support**: This option protects the wireless network infrastructure against spoofing by outside APs. Authenticate, De-authenticate, Associate, and Dis-associate management frames are sent in a secured manner when this option is enabled.

10. **WMM Power Save**: Click **On** to enable Wireless Multimedia Power Save support, as defined in IEEE802.11e. This option saves power and increases battery life by allowing the client device to doze between packets to save power, while the WAP buffers downlink frames. The default setting is **On**.

11. **WMM ACM Video**: Click **On** to enable Wireless Multimedia Admission Control for video traffic. When admission control for video is enabled, the WAP evaluates a video request from a client device against the network load and channel conditions. If the network is not congested, it accepts the request and grants the client the medium time for its traffic stream. Otherwise, it rejects the request. This enables the WAP to maintain QoS when the WLAN becomes congested after a connection has already been established. Some clients contain sufficient intelligence to decide to either

delay the traffic stream, associate with a different AP, or establish a best-effort traffic stream outside the operation of WMM-Admission Control. The default setting is **Off**. Note that the QoS priority of traffic queues is voice, video, best effort, background—this gives the highest priority to voice transmissions.

12. **WMM ACM Voice**: Click **On** to enable Wireless Multimedia Admission Control for voice calls. As for **WMM ACM Video** above, when admission control for voice is enabled, the WAP evaluates a voice request from a client device against the network load and channel conditions. If the network is not congested, it accepts the request and grants the client the medium time for its call. Otherwise, it rejects the request. Some clients contain sufficient intelligence to decide to either delay the traffic stream, associate with a different AP, or establish a best-effort traffic stream outside the operation of WMM-Admission Control. The default setting is **Off**.

Station Management

13. **Station Re-Authentication Period**: This specifies an interval (in seconds) for station reauthentications. This is the minimum time period between station authentication attempts, enforced by the WAP. This feature is part of the Avaya Advanced RF Security Manager (RSM).

14. **Station Timeout Period**: Specify a time (in seconds) in this field to define the timeout period for station associations.

15. **Max Station Association per Access Point**: This option allows you to define how many station associations are allowed per WAP, or enter **unlimited**. Note that the **Max Station Association per Radio** limit (below) may not be exceeded, so entering **unlimited**, in practice, will stop at the per-radio limit.

16. **Max Station Association per Radio**: This defines how many station associations are allowed per radio. Note that the SSIDs > SSID Management window also has a station limit option—**Station Limit**, and the windows for Global Settings .11an and Global Settings .11bgn also have **Max Stations** settings. If multiple station limits are set, all will be

enforced. As soon as any limit is reached, no new stations can associate until some other station has terminated its association.

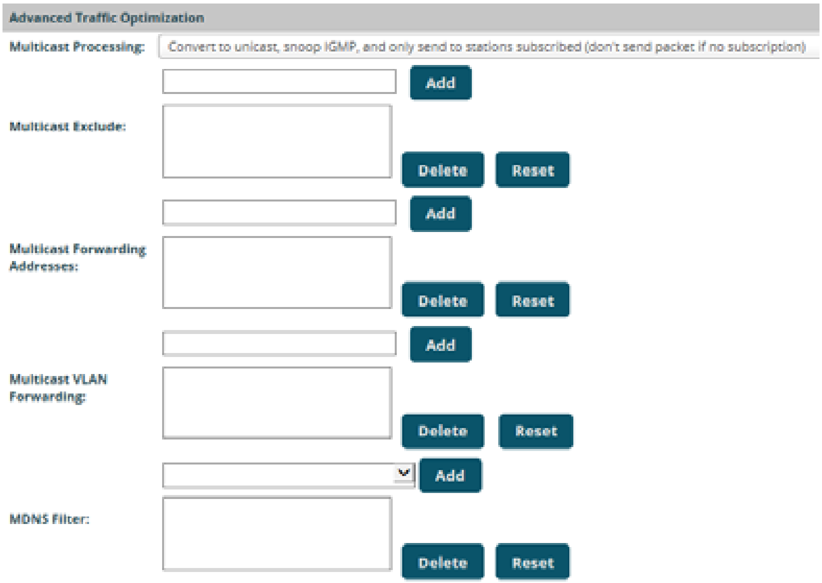
17. **Block Inter-Station Traffic:** This option allows you to block or allow traffic between wireless clients that are associated to the WAP. Choose either **Yes** (to block traffic) or **No** (to allow traffic).

18. **Allow Over Air Management**: Choose **Yes** to enable management of the WAP via the radios, or choose **No** (recommended) to disable this feature.

19. **Extract Station Info**: By default, **Hostname**, **IP Address**, **NetBIOS Name**, and **User Agent String** are all requested when the AP obtains information from a station that is associated to it. For your convenience, this information is shown in various places such as Station Status Windows and in station displays in WOS. If you don't need all of this information, you may disable the fetching of some or all of these items. Use **All** to enable or disable all items in one step.

20. **DHCP Period**: The time (in seconds) that the DHCP assigned IP address is treated as authoritative, as the AP extracts the IP address from DHCP packets only during this period. Once the DHCP Period has expired, or is set to a value of zero, the AP will extract the IP address from any packet.

Advanced Traffic Optimization



Advanced Traffic Optimization

Multicast Processing: Convert to unicast, snoop IGMP, and only send to stations subscribed (don't send packet if no subscription)

Multicast Exclude:

Multicast Forwarding Addresses:

Multicast VLAN Forwarding:

MDNS Filter:

Figure 146. Multicast Processing

*CLI commands offer additional handling options for multicast traffic to stations. These commands will pass specified multicast traffic even if you are using **Air Cleaner** filters. See "interface" on page 442.*

21. **Multicast Processing:** This sets how multicast traffic is handled. Multicast traffic can be received by a number of subscribing stations at the same time, thus saving a great deal of bandwidth. In some of the options below, the WAP uses IGMP snooping to determine the stations that are subscribed to the multicast traffic. IGMP (Internet Group Management Protocol) is used to establish and manage the membership of multicast groups.

    Multicast handling options are only applicable to traffic transmitted from the WAP to wireless stations. Select one of the following options:

- **Send multicasts unmodified**. This is useful when multicast is not needed because no video or audio streaming is required or when it is used only for discovering services in the network. Some situations where you might use this option are:
  - for compatibility with ordinary operation, i.e., there is no optimization or modification of multicast traffic.
  - if you have an application where many subscribers need to see the multicast—a large enough number that it would be less efficient to convert to unicast and better just to send out multicast even though it must be sent out at the speed of the slowest connected station.

  An example of a situation that might benefit from the use of this mode is ghosting all the laptops in a classroom using multicast. One multicast stream at, say, 6 Mbps is probably more efficient than thirty unicast streams.

The next three options convert multicast to unicast. Packets are sent directly to the stations at the best possible data rates. This approach significantly improves the quality of the voice and video multicast streams.

- **Convert to unicast and send unicast packets to all stations**. This may be useful in link-local multicast situations.
- **Convert to unicast, snoop IGMP, and only send to stations subscribed (send as multicast if no subscription)**. This option is useful when you need to stream voice or video multicast traffic to all stations, but some stations are capable of subscribing to multicast groups while other stations are not. The stations that do not subscribe will not benefit from conversion to unicast; their video or voice quality may be compromised.
- **Convert to unicast, snoop IGMP, and only send to stations subscribed (don't send packet if no subscription)**. This option is useful in well controlled environments when you need to stream voice or video multicast traffic only to stations that are capable of

subscribing to multicast groups and there is no need for the rest of the stations to receive the data stream.

22. **Multicast Exclude:** This is a list of multicast IP addresses that will not be subject to multicast-to-unicast conversion. This list is useful on networks where applications such as those using multicast Domain Name System (mDNS) are in use. For example, Apple Bonjour finds local network devices such as printers or other computers using mDNS. By default, the list contains the IPv4 multicast address for Apple Bonjour mDNS: 224.0.0.251.

    To add a new IP address to the list, type it in the top field and click the **Add** button to its right. You may only enter IP addresses—host names are not allowed. This is because mDNS is a link local multicast address, and does not require IGMP to the gateway.

    To remove an entry, select it in the list and click **Delete**. To remove *all* entries from the list, click **Reset**.

23. **Multicast Forwarding**

    Multicast Forwarding is an Avaya feature that forwards selected multicast traffic between wired VLANs and wireless SSIDs. For example, Apple devices use mDNS to advertise and find services, using local network multicasts that are not routed. This creates an issue when you are using Apple devices on the Wireless LAN, and have other devices that provide services connected on the wired infrastructure in a different VLAN, for example, printers and AppleTV devices. One way to address this issue is to set up multicast forwarding between the wireless SSID and the wired VLAN. This requires the wired VLAN to be trunked to the WAP. Once configured correctly, mDNS traffic will be forwarded from the specified wireless network(s) to the specified wired VLANs and vice-versa, subject to any mDNS service filtering defined (Step 25).

Use multicast forwarding together with multicast VLAN forwarding (Step 24) and mDNS filtering (Step 25) to make services available across VLANs as follows:

- In **Multicast Forwarding Addresses**, enter a list of multicast addresses that you want forwarded, for example, 224.0.0.251 (the multicast address for Bonjour).
- In **Multicast VLAN Forwarding**, enter a list of VLANs that participate in the multicast forwarding.
- In **MDNS Filter**, specify the mDNS service types that are allowed to be forwarded.
  - If you leave this field blank, then there is ***no*** filter, and *mDNS packets for all service types are passed.*
  - If you enter service types, then this acts as an allow filter, and *mDNS packets are passed **only** for the listed service types.*

  Note that mDNS filtering may be used to filter the mDNS packet types that are forwarded within the same VLAN. Also, in conjunction with multicast forwarding, it may be used to filter the mDNS packet types that are forwarded across configured VLANs.

After you have entered these settings, when multicast packets arrive from the wired network from one of the **Multicast Forwarding Addresses** on any VLAN specified in **Multicast VLAN Forwarding,** they are forwarded to the corresponding wireless SSID for that VLAN.

Multicast packets coming in from the wireless network on an SSID tied to one of the specified VLANs and matching one of the **Multicast Forwarding Addresses** are forwarded to the specified VLANs on the wired network.

No modifications are made to the forwarded packets – they are just forwarded between specified VLANs and associated SSIDs.

Avaya strongly recommends the use of MDNS Filters (Step 25) *when using multicast forwarding. Only allow required services to be forwarded.*

Carefully monitor results, as forwarding may flood your network with multicast traffic. Experience has shown Bonjour devices to be very chatty. Also note that since this is link local multicast traffic, it will be sent to every wired port in the VLAN, as IGMP snooping does not work with link local multicast addresses.

To specify **Multicast Forwarding Addresses:** enter each IP address in the top field and click the **Add** button to its right. You may only enter IPv4 multicast addresses - host names are not allowed. To remove an entry, select it in the list and click **Delete**. To remove *all* entries from the list, click **Reset**.

24. **Multicast VLAN Forwarding:** This is a list of VLANs that participate in the multicast forwarding. Please see the description of multicast forwarding in Step 23 above.

The VLANs you enter must be explicitly defined (see "VLANs" on page 191) in order to participate in multicast forwarding. In fact, the WAP discards packets from undefined VLANs.

Multicast VLAN Forwarding operates as follows:

- If you leave this field blank, then there is ***no*** filter, and *Multicast Forwarding traffic is passed across all VLANs.*
- If you enter VLANs, then this acts as an allow filter, and *Multicast Forwarding traffic is passed* ***only*** *to the listed VLANS.*

To add a new VLAN to the list, enter its number or name in the top field and click the **Add** button to its right. You may enter multiple VLANs at once, separated by a space. To remove an entry, select it in the list and click **Delete**. To remove *all* entries from the list, click **Reset**.

These VLANs must be trunked to the WAP from the LAN switch, and be defined on the WAP. See "VLAN Management" on page 194 and "SSID Management" on page 254.

Note that Multicast Forwarding and mDNS Filtering capabilities also work if both devices are wireless. For example, let's say that AppleTV is using wireless to connect to an SSID that is associated with VLAN 56, and the wireless client is on an SSID that is associated with VLAN 58. Normally the wireless client would not be able to use Bonjour to discover the AppleTV because they are on separate VLANs. But if you add 224.0.0.251 to the ***Multicast Forwarding Addresses****, then add VLANs 56 and 58 to the* ***Multicast VLAN Forwarding*** *list, then the wireless client will be able to discover the AppleTV. In this same scenario you could add AppleTV to the* ***MDNS Filter*** *list so that only MDNS packets for the AppleTV service type would be forwarded between VLANs 56 and 58.*

Note that all the VLANs that you add to this list do not have to be associated with SSIDs. As an example, say that AppleTV is on the wired network on VLAN 56, while the wireless device is connected to an SSID that is associated to VLAN 58. In this case, VLAN 56 and 58 need to be defined on the WAP but only VLAN 58 needs to be associated to a SSID.

25. **MDNS Filter:** There are many different types of services that may be specified in multicast query and response packets. The mDNS filters let you restrict forwarding, so that multicast packets are forwarded only for the services that you explicitly specify. This list may be used to restrict the amount of Apple Bonjour multicast traffic forwarding. For example, you may restrict forwarding to just AppleTV and printing services. Please see the description of multicast forwarding in Step 23 above.

    The **MDNS Filter** operates as follows:

    - If you leave this field blank, then there is ***no*** filter, and *mDNS packets for all service types are passed.*
    - If you enter service types, then this acts as an allow filter, and *mDNS packets are passed* ***only*** *for the listed service types.*

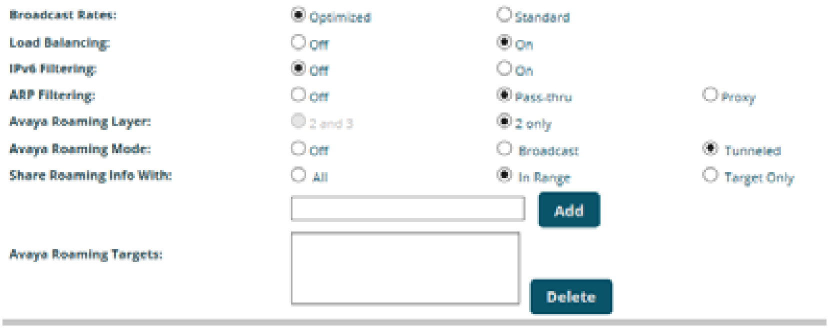
    To add an mDNS packet type to the list of packets that may be forwarded, select it from the drop-down list in the top field and click the **Add** button to its right. The drop-down list offers packet types such as **AirTunes**,

Apple-TV, **iChat**, **iPhoto**, **iTunes**, **iTunes-Home-Sharing**, **Internet-Printing**, **Mobile-Device-Sync**, and **Secure-Telnet**.

For example, to allow mirroring of an iPad on an Apple-TV, select **Apple-TV**.

You may define your own type if you do not see the service you want in the drop-down list. Simply enter the mDNS service name that you would like to allow through. Custom mDNS packet types must be prefixed with an underscore, e.g., **_airvideoserver**.

To remove an entry, select it in the list and click **Delete**. To remove *all* entries from the list, click **Reset**.



Broadcast Rates:	● Optimized	○ Standard	
Load Balancing:	○ Off	● On	
IPv6 Filtering:	● Off	○ On	
ARP Filtering:	○ Off	● Pass-thru	○ Proxy
Avaya Roaming Layer:	○ 2 and 3	● 2 only	
Avaya Roaming Mode:	○ Off	○ Broadcast	● Tunneled
Share Roaming Info With:	○ All	● In Range	○ Target Only
Avaya Roaming Targets:			

Figure 147. Additional Optimization Settings

26. **Broadcast Rates**: This changes the rates of broadcast traffic sent by the WAP (including beacons). When set to **Optimized**, each broadcast or multicast packet that is transmitted on each radio is sent at the lowest transmit rate used by any client associated to that radio at that time. This results in each radio broadcasting at the highest WAP TX data rate that can be heard by all associated stations, improving system performance. The rate is determined dynamically to ensure the best broadcast/ multicast performance possible. The benefit is dramatic. Consider a properly designed network (having -70db or better everywhere), where

virtually every client should have a 54Mbps connection. In this case, broadcasts and multicasts will all go out at 54Mbps vs. the standard rate. Thus, with broadcast rate optimization on, broadcasts and multicasts use between 2% and 10% of the bandwidth that they would in Standard mode.

When set to **Standard** (the default), broadcasts are sent out at the lowest basic rate only—6 Mbps for 5GHz clients, or 1 Mbps for 2.4GHz clients. The option you select here is applied to all radios.

27. **Load Balancing**: Wi-Fi is a shared medium and only one device can transmit data at any time. Faster devices supporting 802.11ac standards have to wait until the slower devices finish transmitting data. This brings down the overall throughput of the network. For example, an 802.11n client operates more than four times slower than an 802.11ac client, and thus will take four times more air time to communicate a given amount of data. This starves the available bandwidth from faster clients, reducing performance significantly. Avaya solves this issue with an innovative technique that automatically separates devices onto different radios by their speeds and capability.

    The technique identifies station capabilities based on fingerprinting and automatically groups devices by performance. It works on all modes (802.11a/b/g/n/ac) and bands (2.4GHz and 5GHz). This results in improved performance for every WLAN client and optimized use of wireless radio resources. Factors including wireless band, number of spatial streams, 802.11ac and 802.11n capability, and signal to noise ratio are considered.

    This feature also provides automatic load balancing designed to distribute wireless stations across multiple radios rather than having stations associate to the closest radios with the strongest signal strength, as they normally would. In wireless networks, the station selects the radio to which it will associate. The WAP cannot actually force load balancing, however it can “encourage” stations to associate in a more optimal fashion to underused radios of the most advantageous type. This option enables or disables active load balancing between the WAP radios.

If you select **On** and a radio is not the best choice for network performance, that radio will send an "AP Full" message in response to Probe, Association, or Authentication requests. This deters persistent clients from forcing their way onto overloaded radios.

Note that this type of load balancing is **not** used if:

- A station is re-associating—if it was already associated to this radio, it is allowed back on this radio immediately. This prevents the station from being bounced between different radios.
- The radio's **Band**, **WiFi Mode,** and **Channel** settings are not at their default values. For example, if the radio's WiFi mode is set to 11n-only, load balancing will not be used. See "Radio Settings" on page 284.
- If station counts (specified at the radio, SSID, or band level) are already exceeded.
- If a station has already been turned down a number of times when attempting to associate, i.e., the station will eventually be allowed onto the radio after a number of attempts have failed.

Choose **Off** to disable load balancing.

28. **ARP Filtering:** Address Resolution Protocol finds the MAC address of a device with a given IP address by sending out a broadcast message requesting this information. ARP filtering allows you to reduce the proliferation of ARP messages by restricting how they are forwarded across the network.

    You may select from the following options for handling ARP requests:

    - **Off**: ARP filtering is disabled. ARP requests are broadcast to radios that have stations associated to them.
    - **Pass-thru**: The WAP forwards the ARP request. It passes along only ARP messages that target the stations that are associated to it. This is the default value.
    - **Proxy**: The WAP replies on behalf of the stations that are associated to it. The ARP request is not broadcast to the stations.

Note that the WAP has a broadcast optimization feature that is always on (it is not configurable). Broadcast optimization restricts all broadcast packets (not just ARP broadcasts) to only those radios that need to forward them. For instance, if a broadcast comes in from VLAN 10, and there are no VLAN 10 users on a radio, then that radio will not send out that broadcast. This increases available air time for other traffic.

29. **IPv6 Filtering:** this setting allows blocking of IPv6 traffic which may be a concern for IT managers. The WAP currently bridges IPv6 traffic. Set IPv6 filtering **On** if you wish to prevent the forwarding of IPv6 packets through the WAP in both directions—wired network to wireless and wireless network to wired. The default is **Off**.

30. **Avaya Roaming Layer:** Roaming capabilities between radios or WAPs are available at Layer **2 only**.

31. **Avaya Roaming Mode:** This feature utilizes the Avaya Roaming Protocol (RP) ensuring fast and seamless roaming capabilities between radios or WAPs at Layer 2 (as specified in Step 32), while maintaining security. Fast roaming eliminates long delays for re-authentication, thus supporting time-sensitive applications such as Voice over Wi-Fi (see "Understanding Fast Roaming" on page 283 for a discussion of this feature). RP uses a discovery process to identify other WAPs as fast roaming targets. This process has two modes:

    - **Broadcast**—the WAP uses a broadcast technique to discover other WAPs that may be targets for fast roaming.
    - **Tunneled**—in this Layer 3 technique, fast roaming target WAPs must be explicitly specified.

    To enable fast roaming, choose **Broadcast** or **Tunneled**, and set additional fast roaming attributes (Step 32). To disable fast roaming, choose **Off**. If you enable Fast Roaming, the following ports **cannot** be blocked:

    - **Port 22610**—reserved for Layer 2 roaming using UDP to share PMK information between WAPs.
    - **Ports 15000 to 17999**—reserved for Layer 3 roaming (tunneling between subnets).

32. **Share Roaming Info With**: Three options allow your WAP to share roaming information with all WAPs; just with those that are within range; or with specifically targeted WAPs. Choose either **All**, **In Range** or **Target Only**, respectively.

    a. **Avaya Roaming Targets:** If you chose **Target Only**, use this option to add target MAC addresses. Enter the MAC address of each target WAP, then click on **Add** (add as many targets as you like). To find a target's MAC address, open the WAP **Info** window on the target WAP and look for radio **MAC Range**, then use the starting address of this range.

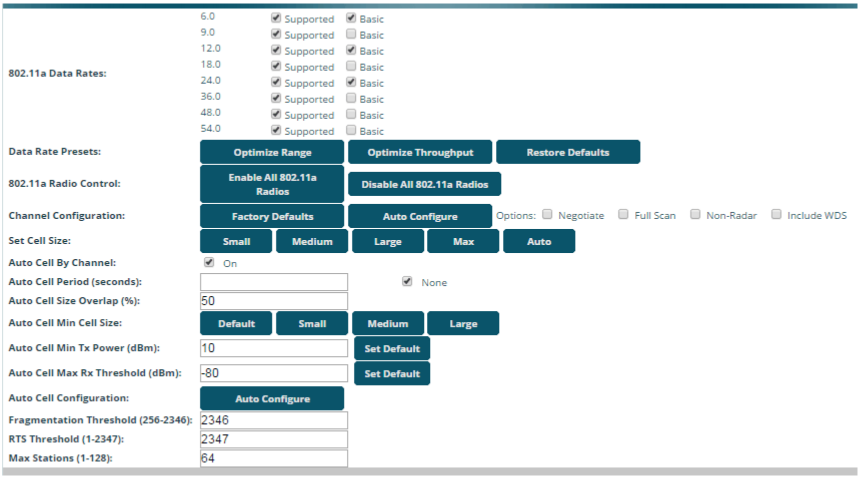
       To delete a target, select it from the list, then click **Delete**.

See Also

Coverage and Capacity Planning
Global Settings .11ac
Global Settings .11an
Global Settings .11bgn
Global Settings .11n
Advanced RF Settings
Radios
Radio Statistics Summary
LED Settings
Radio Settings

Global Settings .11an

This window allows you to establish global 802.11a radio settings. These settings include defining which 802.11a data rates are supported, enabling or disabling all 802.11an radios, auto-configuration of channel allocations for all 802.11an radios, and specifying the fragmentation and RTS thresholds for all 802.11an radios.



802.11a Data Rates:

6.0	☑ Supported	☑ Basic
9.0	☑ Supported	☐ Basic
12.0	☑ Supported	☑ Basic
18.0	☑ Supported	☐ Basic
24.0	☑ Supported	☑ Basic
36.0	☑ Supported	☐ Basic
48.0	☑ Supported	☐ Basic
54.0	☑ Supported	☐ Basic

Data Rate Presets: Optimize Range | Optimize Throughput | Restore Defaults

802.11a Radio Control: Enable All 802.11a Radios | Disable All 802.11a Radios

Channel Configuration: Factory Defaults | Auto Configure | Options: ☐ Negotiate ☐ Full Scan ☐ Non-Radar ☐ Include WDS

Set Cell Size: Small | Medium | Large | Max | Auto

Auto Cell By Channel: ☑ On

Auto Cell Period (seconds): ☑ None

Auto Cell Size Overlap (%): 50

Auto Cell Min Cell Size: Default | Small | Medium | Large

Auto Cell Min Tx Power (dBm): 10 | Set Default

Auto Cell Max Rx Threshold (dBm): -80 | Set Default

Auto Cell Configuration: Auto Configure

Fragmentation Threshold (256-2346): 2346

RTS Threshold (1-2347): 2347

Max Stations (1-128): 64

Figure 148. Global Settings .11an

Procedure for Configuring Global 802.11an Radio Settings

1. **802.11a Data Rates:** The WAP allows you to define which data rates are supported for all 802.11an radios. Select (or deselect) data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.

   - **Basic Rate**—a wireless station (client) must support this rate in order to associate.
   - **Supported Rate**—data rates that can be used to transmit to clients.

2. **Data Rate Presets**: The WAP can optimize your 802.11a data rates automatically, based on range or throughput. Click **Optimize Range** to optimize data rates based on range, or click **Optimize Throughput** to optimize data rates based on throughput. The **Restore Defaults** button will take you back to the factory default rate settings.

3. **802.11a Radio Control**: Click **Enable 802.11a Radios** to enable all 802.11an radios for this WAP, or click **Disable 802.11a Radios** to disable all 802.11an radios.

4. **Channel Configuration**: Click **Auto Configure** to instruct the WAP to determine the best channel allocation settings for each 802.11an radio and select the channel automatically, based on changes in the environment. This is the recommended method for 802.11a channel allocation (see "RF Spectrum Management" on page 333).

   Click **Factory Defaults** if you wish to instruct the WAP to return all radios to their factory preset channels. WAPs do not use the same factory preset values for channel assignments. Instead, if the WAP has been deployed for a while and already has data from the spectrum analyzer and Avaya Roaming Protocol about channel usage on neighboring WAPs, it performs a quick auto channel using that information (without doing a full RF scan) to make an intelligent choice of channel assignments. If the WAP has been rebooted and has no saved configuration or is just being deployed for the first time, it has no prior data about its RF environment. In this case, it will pick a set of compatible channel assignments at random.

   *On the 9120/9130 models, the **Factory Defaults** button will not restore radio1 to monitor mode. You will need to restore this setting manually. Also, you may need to set **Timeshare Mode** again - see "RF Monitor" on page 330.*

   The following options may be selected for auto configuration:

- **Non-Radar**: give preference to channels that are not required to use dynamic frequency selection (DFS) to avoid communicating in the same frequency range as some radar (also see Step 7 on page 292).
- **Negotiate**: negotiate air-time with other WAPs before performing a full scan.
- **Full Scan**: perform a full traffic scan on all channels on all radios to determine the best channel allocation.
- **Include WDS**: automatically assign 5GHz to WDS client links.

*To use the Auto Cell Size feature, any radios that will use Auto Cell must have **Cell Size** set to **auto**.*

*For Auto Cell by Channel, it is not necessary for RF Monitor Mode to be turned on, or for there to be a radio set to monitor mode. For Auto Cell by Band, RF Monitor Mode must be set to Dedicated or Timeshare mode, and there must be a radio set to monitor mode. See **"RF Monitor" on page 330.***

5. **Set Cell Size**: Cell Size may be set globally for all 802.11an radios to **Auto**, **Large, Medium, Small**, or **Max** using the buttons.

   For an overview of RF power and cell size settings, please see "RF Power and Sensitivity" on page 332, "Capacity and Cell Sizes" on page 26, and "Fine Tuning Cell Sizes" on page 27.

6. **Auto Cell By Channel**: By default, this feature is **On**, and auto cell will adjust the cell size for a radio when nearby WAPs have radios on the same channel within earshot of each other, so that the two radios minimize interference with each other. If this option is unchecked, then auto cell will adjust the cell size for a radio when nearby WAPs have radios on the same band, even if they are using different channels (called Auto Cell by Band, or Multichannel Auto Cell). This will result in smaller cell sizes. See "Fine Tuning Cell Sizes" on page 27.

7. **Auto Cell Period (seconds)**: You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will

run. If you select **None**, then auto-configuration of cell sizing will not be run periodically. You do not need to run Auto Cell often unless there are a lot of changes in the environment. If the RF environment is changing often, running Auto Cell every twenty-four hours (86400 seconds) should be sufficient). The default value is **None**.

8. **Auto Cell Size Overlap (%)**: Enter the percentage of cell overlap that will be allowed when the WAP is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring WAPs that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

9. **Auto Cell Min Cell Size**: Use this setting if you wish to set the minimum cell size that Auto Cell may assign. The values are **Default**, **Large, Medium,** or **Small**.

10. **Auto Cell Min Tx Power (dBm)**: Enter the minimum transmit power that the WAP can assign to a radio when adjusting automatic cell sizes. The default value is **10**.

11. **Auto Cell Max Rx Threshold (dBm)**: Enter the maximum receive threshold that the WAP can assign to a radio when adjusting automatic cell sizes. The default value is **-80**.

12. **Auto Cell Configuration**: Click this button to instruct the WAP to determine and set the best cell size for each 802.11an radio whose **Cell Size** is **auto** on the Radio Settings window, based on changes in the environment. This is the recommended method for setting cell size. You may look at the Tx and Rx values on the Radio Settings window to view the cell size settings that were applied.

13. **Fragmentation Threshold**: This is the maximum size for directed data packets transmitted over the 802.11an radio. Larger frames fragment into several packets, their maximum size defined by the value you enter here. Smaller fragmentation numbers can help to “squeeze” packets through in noisy environments. Enter the desired **Fragmentation Threshold** value in this field, between 256 and 2346.

14. **RTS Threshold**: The Request To Send (RTS) Threshold specifies the packet size. Packets larger than the RTS threshold will use CTS / RTS prior to transmitting the packet—useful for larger packets to help ensure the success of their transmission. Enter a value between 1 and 2347.

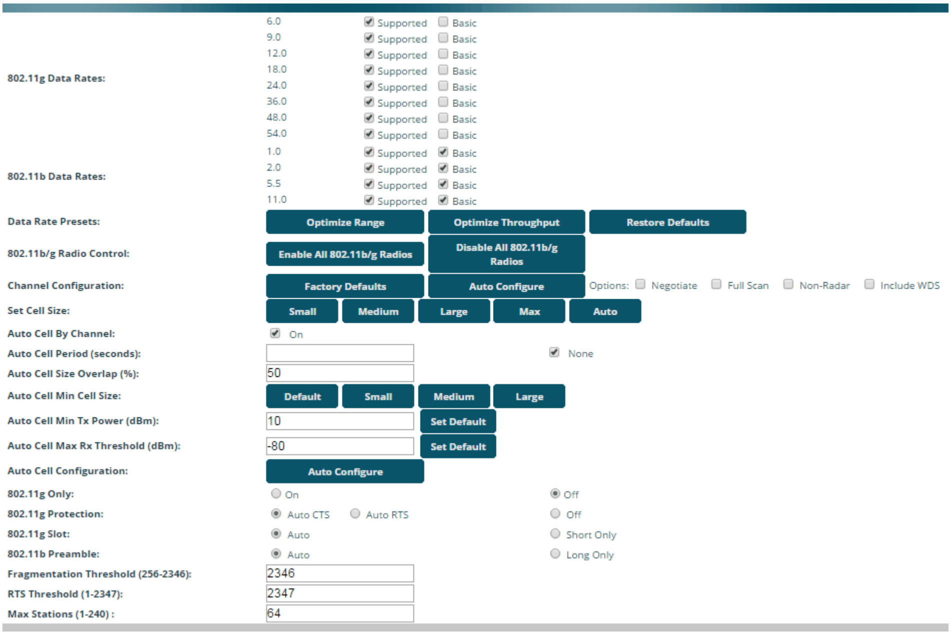
15. **Max Stations**: This defines how many station associations are allowed per 802.11an radio. Note that the Radios > Global Settings window and SSIDs—SSID Management window also have station limit settings— **Max Station Association per Radio** (page 293) and **Station Limit** (page 260), respectively. If multiple station limits are set, all will be enforced. As soon as any limit is reached, no new stations can associate until some other station has terminated its association.

See Also

Coverage and Capacity Planning
Global Settings
Global Settings .11bgn
Global Settings .11n
Radios
Radio Statistics Summary
Advanced RF Settings
Radio Settings

Global Settings .11bgn

This window allows you to establish global 802.11b/g radio settings. These settings include defining which 802.11b and 802.11g data rates are supported, enabling or disabling all 802.11b/g radios, auto-configuring 802.11b/g radio channel allocations, and specifying the fragmentation and RTS thresholds for all 802.11b/g radios.



802.11g Data Rates:	6.0	☑ Supported	☐ Basic			
	9.0	☑ Supported	☐ Basic			
	12.0	☑ Supported	☐ Basic			
	18.0	☑ Supported	☐ Basic			
	24.0	☑ Supported	☐ Basic			
	36.0	☑ Supported	☐ Basic			
	48.0	☑ Supported	☐ Basic			
	54.0	☑ Supported	☐ Basic			
802.11b Data Rates:	1.0	☑ Supported	☑ Basic			
	2.0	☑ Supported	☑ Basic			
	5.5	☑ Supported	☑ Basic			
	11.0	☑ Supported	☑ Basic			
Data Rate Presets:	Optimize Range	Optimize Throughput	Restore Defaults			
802.11b/g Radio Control:	Enable All 802.11b/g Radios	Disable All 802.11b/g Radios				
Channel Configuration:	Factory Defaults	Auto Configure	Options: ☐ Negotiate ☐ Full Scan ☐ Non-Radar ☐ Include WDS			
Set Cell Size:	Small	Medium	Large	Max	Auto	
Auto Cell By Channel:	☑ On					
Auto Cell Period (seconds):			☑ None			
Auto Cell Size Overlap (%):	50					
Auto Cell Min Cell Size:	Default	Small	Medium	Large		
Auto Cell Min Tx Power (dBm):	10	Set Default				
Auto Cell Max Rx Threshold (dBm):	-80	Set Default				
Auto Cell Configuration:	Auto Configure					
802.11g Only:	○ On		● Off			
802.11g Protection:	● Auto CTS	○ Auto RTS	○ Off			
802.11g Slot:	● Auto		○ Short Only			
802.11b Preamble:	● Auto		○ Long Only			
Fragmentation Threshold (256-2346):	2346					
RTS Threshold (1-2347):	2347					
Max Stations (1-240) :	64					

Figure 149. Global Settings .11bgn

Procedure for Configuring Global 802.11b/g Radio Settings

1. **802.11g Data Rates:** The WAP allows you to define which data rates are supported for all 802.11g radios. Select (or deselect) 11g data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.

   - **Basic Rate**—a wireless station (client) must support this rate in order to associate.
   - **Supported Rate**—data rates that can be used to transmit to clients.

2. **802.11b Data Rates**: This task is similar to Step 1, but these data rates apply only to 802.11b radios.

3. **Data Rate Presets**: The WAP can optimize your 802.11b/g data rates automatically, based on range or throughput. Click **Optimize Range** button to optimize data rates based on range, or click on the **Optimize Throughput** to optimize data rates based on throughput. **Restore Defaults** will take you back to the factory default rate settings.

4. **802.11b/g Radio Control**: Click **Enable All 802.11b/g Radios** to enable all 802.11b/g radios for this WAP, or click **Disable All 802.11b/g Radios** to disable them.

5. **Channel Configuration**: Click **Auto Configure** to instruct the WAP to determine the best channel allocation settings for each 802.11b/g radio and select the channel automatically, based on changes in the environment. This is the recommended method for channel allocation (see “RF Spectrum Management” on page 333).

   Click **Factory Defaults** if you wish to instruct the WAP to return all radios to their factory preset channels. WAPs do not use the same factory preset values for channel assignments. Instead, if the WAP has been deployed for a while and already has data from the spectrum analyzer and Avaya Roaming Protocol about channel usage on neighboring WAPs, it performs a quick auto channel using that information (without doing a full RF scan) to make an intelligent choice of channel assignments. If the WAP has been rebooted and has no saved configuration or is just being deployed for the first time, it has no prior data about its RF environment.

In this case, it will pick a set of compatible channel assignments at random.

*On the 9120/9130 Series, the **Factory Defaults** button will not restore radio1 to monitor mode. You will need to restore this setting manually. Also, you may need to set **Timeshare Mode** again - see "RF Monitor" on page 330.*

The following options may be selected for auto configuration:

- **Negotiate**: negotiate air-time with other WAPs before performing a full scan.
- **Full Scan**: perform a full traffic scan on all channels on all radios to determine the best channel allocation.
- **Non-Radar**: give preference to channels without radar-detect. See table in "Procedure for Configuring Global 802.11an Radio Settings" on page 306.
- **Include WDS**: automatically assign 5GHz to WDS client links.

6. **Set Cell Size/ Autoconfigure**: Cell Size may be set globally for all 802.11b/g radios to **auto**, **large, medium, small**, or **max** using the drop down menu.

   For an overview of RF power and cell size settings, please see "RF Power and Sensitivity" on page 332, "Capacity and Cell Sizes" on page 26, and "Fine Tuning Cell Sizes" on page 27.

7. **Auto Cell By Channel**: By default, this feature is **On**, and auto cell will adjust the cell size for a radio when nearby WAPs have radios on the same channel within earshot of each other, so that the two radios minimize interference with each other. If this option is unchecked, then auto cell will adjust the cell size for a radio when nearby WAPs have radios on the same band, even if they are using different channels (called Auto Cell by Band, or Multichannel Auto Cell). This will result in smaller cell sizes. See "Fine Tuning Cell Sizes" on page 27.

*To use the Auto Cell Size feature, any radios that will use Auto Cell must have **Cell Size** set to **auto**.*

*For **Auto Cell by Channel**, it is not necessary for RF Monitor Mode to be turned on, or for there to be a radio set to monitor mode. For **Auto Cell by Band**, RF Monitor Mode must be set to **Dedicated** or **Timeshare** mode, and there must be a radio set to monitor mode. See **"RF Monitor" on page 330.***

8. **Auto Cell Period (seconds)**: You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will run. If you select **None**, then auto-configuration of cell sizing will not be run periodically. You do not need to run Auto Cell often unless there are a lot of changes in the environment. If the RF environment is changing often, running Auto Cell every twenty-four hours (86400 seconds) should be sufficient). The default value is **None**.

9. **Auto Cell Size Overlap (%)**: Enter the percentage of cell overlap that will be allowed when the WAP is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring WAPs that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

10. **Auto Cell Min Cell Size**: Use this setting if you wish to set the minimum cell size that Auto Cell may assign. The values are **Default**, **Large, Medium,** or **Small**.

11. **Auto Cell Min Tx Power (dBm)**: Enter the minimum transmit power that the WAP can assign to a radio when adjusting automatic cell sizes. The default value is **10**.

12. **Auto Cell Max Rx Threshold (dBm)**: Enter the maximum receive threshold that the WAP can assign to a radio when adjusting automatic cell sizes. The default value is **-80**.

13. **Auto Cell Configuration**: Click **Auto Configure** to instruct the WAP to determine and set the best cell size for each enabled 802.11b/g radio whose **Cell Size** is **auto** on the Radio Settings window, based on changes in the environment. This is the recommended method for setting cell size. You may look at the Tx and Rx values on the Radio Settings window to view the cell size settings that were applied.

14. **802.11g Only**: Choose **On** to restrict use to 802.11g mode only. In this mode, no 802.11b rates are transmitted. Stations that only support 802.11b will not be able to associate.

15. **802.11g Protection**: You should select **Auto CTS** or **Auto RTS** to provide automatic protection for all 802.11g radios in mixed networks (802.11 b and g). You may select **Off** to disable this feature, but this is not recommended. Protection allows 802.11g stations to share the radio with older, slower 802.11b stations. Protection avoids collisions by preventing 802.11b and 802.11g stations from transmitting simultaneously. When **Auto CTS** or **Auto RTS** is enabled and any 802.11b station is associated to the radio, additional frames are sent to gain access to the wireless network.

    - Auto CTS requires 802.11g stations to send a slow Clear To Send frame that locks out other stations. Automatic protection reduces 802.11g throughput when 802.11b stations are present—Auto CTS adds less overhead than Auto RTS. The default value is Auto CTS.
    - With Auto RTS, 802.11g stations reserve the wireless media using a Request To Send/Clear To Send cycle. This mode is useful when you have dispersed nodes. It was originally used in 802.11b only networks to avoid collisions from “hidden nodes”—nodes that are so widely dispersed that they can hear the WAP, but not each other.

    When there are no 11b stations associated and an auto-protection mode is enabled, the WAP will not send the extra frames, thus avoiding unnecessary overhead.

16. **802.11g Slot**: Choose **Auto** to instruct the WAP to manage the 802.11g slot times automatically, or choose **Short Only**. Avaya recommends using **Auto** for this setting, especially if 802.11b devices are present.

17. **802.11b Preamble**: The preamble contains information that the WAP and client devices need when sending and receiving packets. All compliant 802.11b systems have to support the long preamble. A short preamble improves the efficiency of a network's throughput when transmitting special data, such as voice, VoIP (Voice-over IP) and streaming video. Select **Auto** to instruct the WAP to manage the preamble (long and short) automatically, or choose **Long Only**.

18. **Fragmentation Threshold**: This is the maximum size for directed data packets transmitted over the 802.11b/g radio. Larger frames fragment into several packets, their maximum size defined by the value you enter here. Enter the desired **Fragmentation Threshold** value, between 256 and 2346.

19. **RTS Threshold**: The RTS (Request To Send) Threshold specifies the packet size. Packets larger than the RTS threshold will use CTS/RTS prior to transmitting the packet—useful for larger packets to help ensure the success of their transmission. Enter a value between 1 and 2347.

20. **Max Stations**: This defines how many station associations are allowed per 802.11bgn radio. Note that the Radios > Global Settings window and SSIDs > SSID Management window also have station limit settings— **Max Station Association per Radio** (page 293) and **Station Limit** (page 260), respectively. If multiple station limits are set, all will be enforced. As soon as any limit is reached, no new stations can associate until some other station has terminated its association.

See Also

Coverage and Capacity Planning

Global Settings

Global Settings .11an

Global Settings .11n

Advanced RF Settings

LED Settings

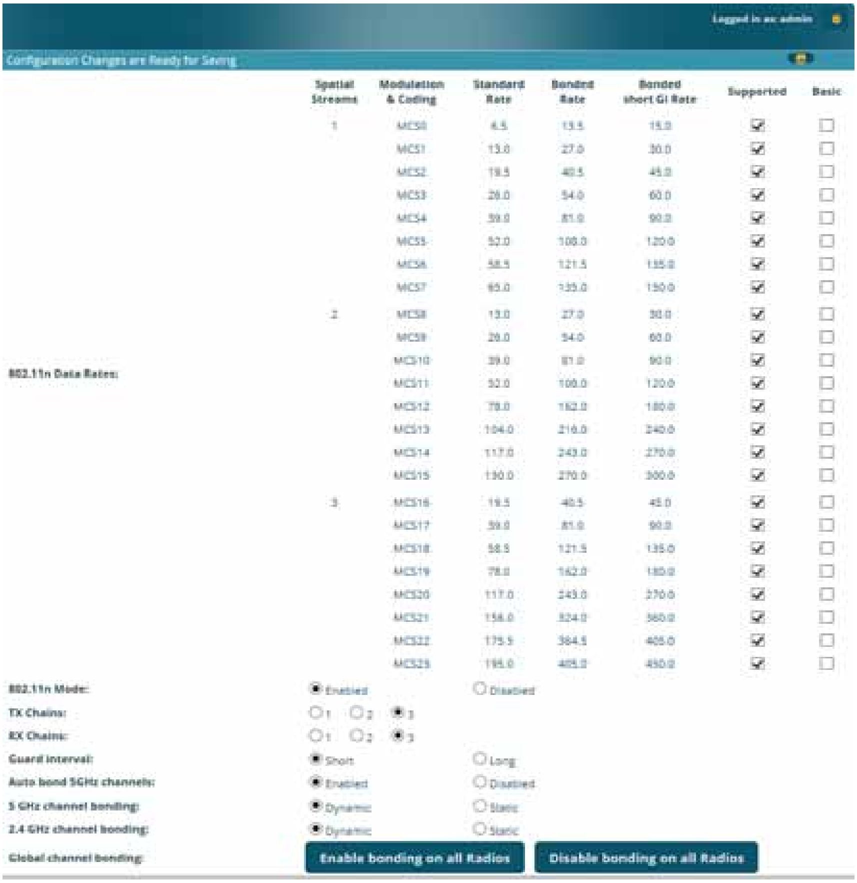
Radio Settings

Radio Statistics Summary

Global Settings .11n

This window allows you to establish global 802.11n radio settings. These settings include enabling or disabling 802.11n mode for the entire WAP, specifying the number of transmit and receive chains (data stream) used for spatial multiplexing, setting a short or standard guard interval, auto-configuring channel bonding, and specifying whether auto-configured channel bonding will be static or dynamic.

Before changing your settings for 802.11n, please read the discussion in “About IEEE 802.11ac” on page 31.



	Spatial Streams	Modulation & Coding	Standard Rate	Bonded Rate	Bonded short GI Rate	Supported	Basic
802.11n Data Rates:	1	MCS0	6.5	13.5	15.0	☑	□
		MCS1	13.0	27.0	30.0	☑	□
		MCS2	19.5	40.5	45.0	☑	□
		MCS3	26.0	54.0	60.0	☑	□
		MCS4	39.0	81.0	90.0	☑	□
		MCS5	52.0	108.0	120.0	☑	□
		MCS6	58.5	121.5	135.0	☑	□
		MCS7	65.0	135.0	150.0	☑	□
	2	MCS8	13.0	27.0	30.0	☑	□
		MCS9	26.0	54.0	60.0	☑	□
		MCS10	39.0	81.0	90.0	☑	□
		MCS11	52.0	108.0	120.0	☑	□
		MCS12	78.0	162.0	180.0	☑	□
		MCS13	104.0	216.0	240.0	☑	□
		MCS14	117.0	243.0	270.0	☑	□
		MCS15	130.0	270.0	300.0	☑	□
	3	MCS16	19.5	40.5	45.0	☑	□
		MCS17	39.0	81.0	90.0	☑	□
		MCS18	58.5	121.5	135.0	☑	□
		MCS19	78.0	162.0	180.0	☑	□
		MCS20	117.0	243.0	270.0	☑	□
		MCS21	156.0	324.0	360.0	☑	□
		MCS22	175.5	364.5	405.0	☑	□
		MCS23	195.0	405.0	450.0	☑	□

802.11n Mode: ● Enabled ○ Disabled

TX Chains: ○ 1 ○ 2 ● 3

RX Chains: ○ 1 ○ 2 ● 3

Guard interval: ● Short ○ Long

Auto bond 5GHz channels: ● Enabled ○ Disabled

5 GHz channel bonding: ● Dynamic ○ Static

2.4 GHz channel bonding: ● Dynamic ○ Static

Global channel bonding:

Figure 150. Global Settings .11n

Procedure for Configuring Global 802.11n Radio Settings

1. **802.11n Data Rates**: The WAP allows you to define which data rates are supported for all 802.11n radios. Select (or deselect) 11n data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.

   - **Basic Rate**—a wireless station (client) must support this rate in order to associate.
   - **Supported Rate**—data rates that can be used to transmit to clients.

2. **802.11n Mode**: Select **Enabled** to allow the WAP to operate in 802.11n mode.

   If you select **Disabled**, then 802.11n operation is disabled on the WAP.

3. **TX Chains**: Select the number of separate data streams transmitted by the antennas of each radio. The maximum number of chains is determined by whether the WAP has 2x2 or 3x3 radios. The default value is always the maximum supported by the radio type. See “Up to Eight Simultaneous Data Streams—Spatial Multiplexing” on page 33.

4. **RX Chains**: Select the number of separate data streams received by the antennas of each radio. This number should be greater than or equal to **TX Chains**. The maximum number of chains is determined by whether the WAP has 2x2 or 3x3 radios. The default value is always the maximum supported by the radio type. See “Up to Eight Simultaneous Data Streams—Spatial Multiplexing” on page 33.

5. **Guard interval**: Select **Short** to increase the data transmission rate by decreasing wait intervals in signal transmission. Select **Long** to use the standard interval. The default is Short.

6. **Auto bond 5 GHz channels**: Select **Enabled** to use Channel Bonding on 5 GHz channels and automatically select the best channels for bonding. The default is **Enabled**. See “80 MHz and 160 MHz Channel Widths (Bonding)” on page 37.

7. **5 GHz Channel Bonding**: Select **Dynamic** to have auto-configuration for bonded 5 GHz channels be automatically updated as conditions change. For example, if there are too many clients to be supported by a bonded channel, dynamic mode will automatically break the bonded channel into two channels. Select **Static** to have the bonded channels remain the same once they are selected. The Dynamic option is only available when **Auto bond 5 GHz channels** is enabled. The default is **Dynamic**. See “80 MHz and 160 MHz Channel Widths (Bonding)” on page 37.

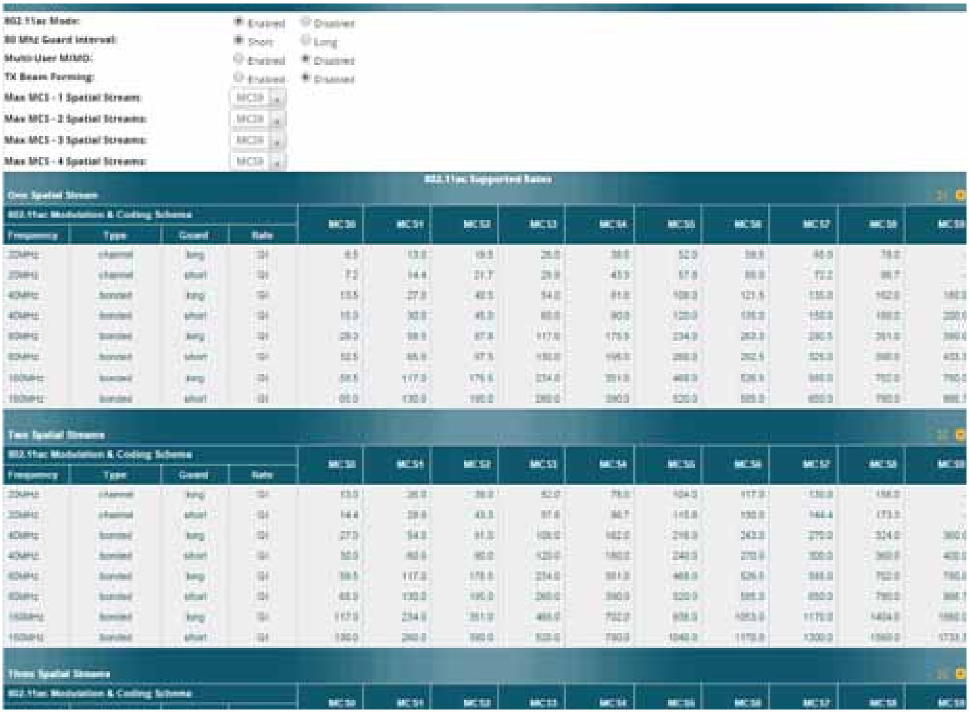
8. **2.4 GHz Channel Bonding**: Select **Dynamic** to have auto-configuration for bonded 2.4 GHz channels be automatically updated as conditions change. Select **Static** to have the bonded channels remain the same once they are selected. The default is **Dynamic**. See “80 MHz and 160 MHz Channel Widths (Bonding)” on page 37.

9. **Global channel bonding**: These buttons allow you to turn channel bonding on or off for all radios in one step. The effect of using one of these buttons will be shown if you go to the **Radio Settings** window and look at the **Bond** column. Clicking **Enable bonding on all Radios** causes all Radios to be bonded to their auto-bonding channel immediately, if appropriate. For example, the radio will not be bonded if it is set to monitor mode, and 2.4 GHz radios will not be bonded. Click **Disable bonding on all Radios** to turn off bonding on all radios immediately. See “80 MHz and 160 MHz Channel Widths (Bonding)” on page 37. Settings in Step 7 and Step 8 are independent of global channel bonding.

Global Settings .11ac

This window allows you to establish global 802.11ac radio settings. These settings include enabling or disabling 802.11ac mode for the entire WAP, specifying the number of data streams used in spatial multiplexing, and setting a short or long guard interval.

Before changing your settings for 802.11ac, please read the discussion in "About IEEE 802.11ac" on page 31.



802.11ac Mode:	● Enabled	○ Disabled
80 MHz Guard Interval:	● Short	○ Long
Multi-User MIMO:	○ Enabled	● Disabled
TX Beam Forming:	○ Enabled	● Disabled
Max MCS - 1 Spatial Stream:	MCS9	
Max MCS - 2 Spatial Streams:	MCS9	
Max MCS - 3 Spatial Streams:	MCS9	
Max MCS - 4 Spatial Streams:	MCS9	

802.11ac Supported Rates

One Spatial Stream

802.11ac Modulation & Coding Scheme				MCS0	MCS1	MCS2	MCS3	MCS4	MCS5	MCS6	MCS7	MCS8	MCS9
Frequency	Type	Guard	Rate										
20MHz	channel	long	GI	6.5	13.0	19.5	26.0	39.0	52.0	58.5	65.0	78.0	-
20MHz	channel	short	GI	7.2	14.4	21.7	28.9	43.3	57.8	65.0	72.2	86.7	-
40MHz	bonded	long	GI	13.5	27.0	40.5	54.0	81.0	108.0	121.5	135.0	162.0	180.0
40MHz	bonded	short	GI	15.0	30.0	45.0	60.0	90.0	120.0	135.0	150.0	180.0	200.0
80MHz	bonded	long	GI	29.3	58.5	87.8	117.0	175.5	234.0	263.3	292.5	351.0	390.0
80MHz	bonded	short	GI	32.5	65.0	97.5	130.0	195.0	260.0	292.5	325.0	390.0	433.3
160MHz	bonded	long	GI	58.5	117.0	175.5	234.0	351.0	468.0	526.5	585.0	702.0	780.0
160MHz	bonded	short	GI	65.0	130.0	195.0	260.0	390.0	520.0	585.0	650.0	780.0	866.7

Two Spatial Streams

802.11ac Modulation & Coding Scheme				MCS0	MCS1	MCS2	MCS3	MCS4	MCS5	MCS6	MCS7	MCS8	MCS9
Frequency	Type	Guard	Rate										
20MHz	channel	long	GI	13.0	26.0	39.0	52.0	78.0	104.0	117.0	130.0	156.0	-
20MHz	channel	short	GI	14.4	28.9	43.3	57.8	86.7	115.6	130.0	144.4	173.3	-
40MHz	bonded	long	GI	27.0	54.0	81.0	108.0	162.0	216.0	243.0	270.0	324.0	360.0
40MHz	bonded	short	GI	30.0	60.0	90.0	120.0	180.0	240.0	270.0	300.0	360.0	400.0
80MHz	bonded	long	GI	58.5	117.0	175.5	234.0	351.0	468.0	526.5	585.0	702.0	780.0
80MHz	bonded	short	GI	65.0	130.0	195.0	260.0	390.0	520.0	585.0	650.0	780.0	866.7
160MHz	bonded	long	GI	117.0	234.0	351.0	468.0	702.0	936.0	1053.0	1170.0	1404.0	1560.0
160MHz	bonded	short	GI	130.0	260.0	390.0	520.0	780.0	1040.0	1170.0	1300.0	1560.0	1733.3

Three Spatial Streams

802.11ac Modulation & Coding Scheme	MCS0	MCS1	MCS2	MCS3	MCS4	MCS5	MCS6	MCS7	MCS8	MCS9

Figure 151. Global Settings .11ac

Procedure for Configuring Global 802.11ac Radio Settings

1. **802.11ac Mode**: Select **Enabled** to allow the WAP to operate in 802.11ac mode. **If you select Disabled, then 802.11ac operation is disabled on the WAP.**

2. **80 MHz Guard interval**: This is the length of the interval between transmission of symbols (the smallest unit of data transfer) when you are using 80MHz bonded channels. (See "80 MHz and 160 MHz Channel Widths (Bonding)" on page 37.) Select **Short** to increase the data transmission rate by decreasing wait intervals in signal transmission. Select **Long** to use the standard interval. The default is Short.

3. **MU-MIMO**: This stands for the Multiple-User form of Multiple-Input Multiple-Output wireless communication, which is available on Wave 2 802.11ac APs. This can help the AP be more efficient with MU-MIMO enabled clients. For example, the WAP9144's Wave 2 radios have 4 antennas each. The mix of client devices connecting to the AP is likely to average fewer antennas. If MU-MIMO is enabled, then the AP radio could, for example, communicate concurrently with two clients that each have 2-antenna radios with MU-MIMO capability.

4. **Beamforming**: Beamforming is used for directional signal transmission or reception. This method results in an increased range for devices supporting beamforming. Avaya Wave 2 products support beamforming only for 802.11ac beamforming capable clients.

5. **Max MCS**: Select the highest Modulation and Coding Scheme level that may be used with **1** or **2 Spatial Streams**. For models with 3x3 radios, there is a setting for **3 Spatial Streams**, and for models with 4x4 radios, there is a setting for **4 Spatial Streams**. These settings may be used to limit the highest level of modulation to 64-QAM, or allow 256-QAM with its higher data rate. It also determines the coding scheme used for error correction. Higher MCS levels allocate fewer bits to error correction, and thus a higher proportion is used for data transfer. The default **Max MCS** value is **MCS9**.

The higher the MCS values, the higher the data rate, as shown in **802.11ac Supported Rates**, below. Higher MCS levels require higher signal-to-noise ratios (i.e., a less noisy environment) and shorter transmission distances. See "Higher Precision in the Physical Layer" on page 36.

The maximum number of separate data streams that may be transmitted by the antennas of each radio is determined by whether the WAP has 2x2, 3x3, or 4x4 radios. For a device that has 2x2 radios, such as the WAP9122 / 9132, the settings for three or more spatial streams are not shown. See "Up to Eight Simultaneous Data Streams—Spatial Multiplexing" on page 33.

6. **802.11ac Supported Rates**: This list shows the optimum data rates that can be expected, based on the number of spatial streams that a station can handle, and on your settings for Max MCS, Guard Interval, and the use of bonded channels, up to 80MHz wide.

Global Settings .11u

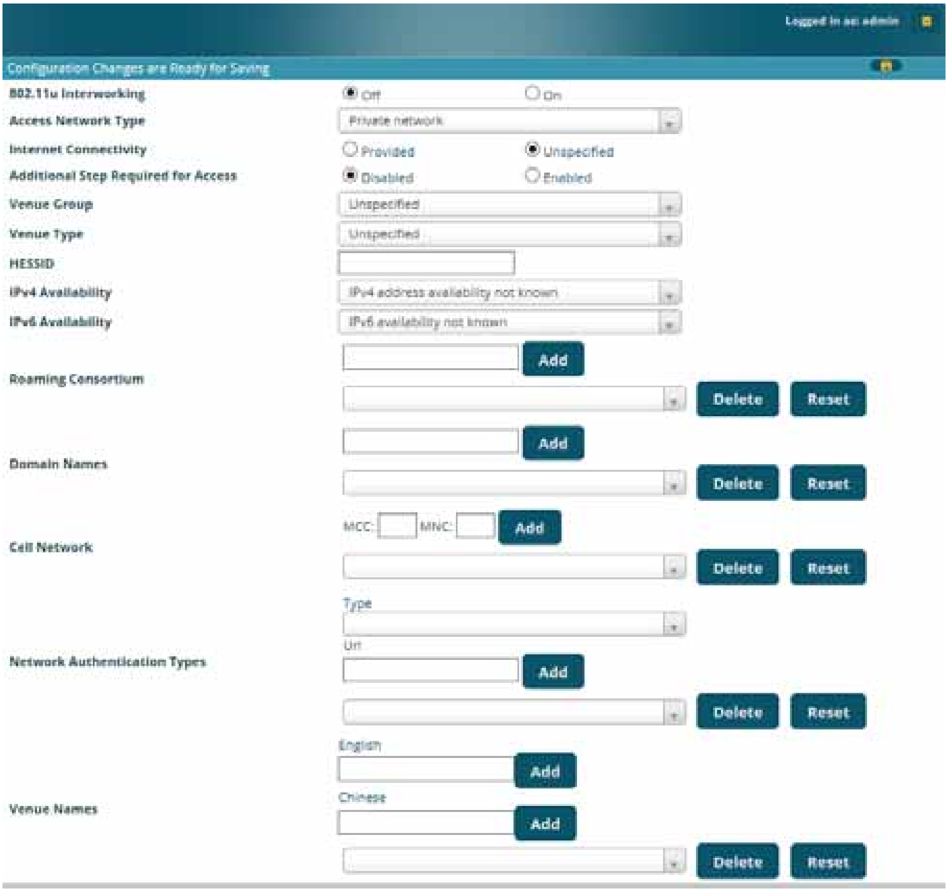
Understanding 802.11u

As the number of access points available in public venues increases, mobile devices users have a harder time distinguishing usable SSIDs from the tens, if not hundreds of access points visible. Using the 802.11u protocol, access points may broadcast information about the services and access that they offer and to respond to queries for additional information related to the facilities that the downstream service network provides.

The type of information broadcast or available from 802.11u-compliant access points includes:

- **Access Network Type**. Indicates the type of network available. For example: public or private, free or charged, etc.
- **Internet Connectivity**. Indicates whether the network provides Internet connectivity.
- **Authentication**. Indicates whether additional authentication steps will be required to use the network as well as the network authentication types that are in use.

- **Venue Information**. The type and name of the location where the access point is found.
- **Identification**. A globally unique identification for the access point.
- **IPv4/IPv6 Addressing.** Indicate the type of IP addressing (IPv4 and/or IPv6) and NATing that is performed by the network.
- **Roaming Consortium.** The service network may be connected to one or more roaming providers, called consortia, that allow access points from multiple service providers to be used transparently through a single paid service. The access point may advertise multiple consortia to mobile devices.
- **Domain Names.** A list of domain names to which the mobile user may end up belonging based on authentication credentials used.
- **Cellular Networks.** The service network may have arrangements with one or more cellular service providers who can transparently provide wireless and Internet connectivity.



Logged in as: admin

Configuration Changes are Ready for Saving

802.11u Interworking: ● Off ○ On

Access Network Type: Private network

Internet Connectivity: ○ Provided ● Unspecified

Additional Step Required for Access: ● Disabled ○ Enabled

Venue Group: Unspecified

Venue Type: Unspecified

HESSID:

IPv4 Availability: IPv4 address availability not known

IPv6 Availability: IPv6 availability not known

Roaming Consortium

Domain Names

Cell Network: MCC: MNC:

Network Authentication Types: Type, Url

Venue Names: English, Chinese

Figure 152. 802.11u Global Settings

Procedure for Configuring 802.11u Settings

Use this window to establish the 802.11u configuration.

1. **802.11u Internetworking.** Click **On** to enable 802.11u protocol operation.
2. **Access Network Type**: This indicates the type of network supported by the access point. The choices are:
   a. **Chargeable public network**

b. **Emergency services only network**

c. **Free public network**

d. **Personal device network**

e. **Private network with guest access**

f. **Test or experimental network**

g. **Wildcard**—all of the networks above are supported.

3. **Internet Connectivity.** Click **Provided** if Internet connectivity is available through the access point from the back end provider to which the mobile user ends up belonging. Click **Unspecified** otherwise—for example, depending on the SLAs (service level agreements) of the mobile user, Internet access may or may not be provided.

4. **Additional Step Required for Access.** Click **Disabled** if no additional authentication steps will be required to complete the connection and **Enabled** otherwise. The available authentication techniques are described in the **Network Authentication Types** field (Step 13).

5. **Venue Group.** Select the general type of venue that the access point is located in. Various choices are available, including **Business, Residential,** and **Outdoor.** For each **Venue Group**, a further set of sub-choices are available in the **Venue Type** field below. The particular name of the venue is specified in the **Venue Names** field (Step 14).

6. **Venue Type**. For each of the **Venue Group** choices, a further set of sub-choices are available. For example, if you set **Venue Group** to **Assembly**, the choices include **Amphitheater, Area, Library,** and **Theatre.**

7. **HESSID**. Enter the globally unique homogeneous ESS ID. This SSID is marked as being HotSpot 2.0 capable. This SSID attribute is global—if 802.11u is enabled and HotSpot 2.0 is enabled, then all SSIDs will have HotSpot 2.0 capability.

8. **IPv4 Availability.** Select the type of IPv4 addressing that will be assigned by the network upon connection. NATed addresses are IP addresses that have been changed by mapping the IP address and port number to IP

addresses and new port numbers routable by other networks. **Double NATed** addresses go through two levels of NATing. **Port restricted IPv4 addresses** refer to specific UDP and TCP port numbers associated with standard Internet services; for example, port 80 for web pages. The choices for this field are:

a. **Double NATed private IPv4 address available**

b. **IPv4 address not available**

c. **IPv4 address availability not known**

d. **Port-restricted IPv4 address available**

e. **Port-restricted IPv4 address and double NATed IPv4 address available**

f. **Port-restricted IPv4 address and single NATed IPv4 address available**

g. **Public IPv4 address available**

h. **Single NATed private IPv4 address available**

9. **IPv6 Availability.** Select the type of IPv6 addressing that is available from the network upon connection.

   a. **IPv6 address not available**

   b. **IPv6 address availability not known**

   c. **IPv6 address available**

10. **Roaming Consortium.** Each of the roaming consortia has an organizational identifier (OI) obtained from IEEE that unique identifies the organization. This is similar to the OUI part of a MAC address. Use this control to build up a list of OIs for the consortia available. Enter the OI as a hexadecimal string of between 6 and 30 characters in the **Add** field and click **Add**. The OI will appear in the list. An OI may be deleted by selecting it in the list and clicking **Delete**. All OIs may be deleted by clicking **Reset**.

11. **Domain Names.** Use this control to build up a list of domain names. Enter the name in the **Add** field and click **Add**, and it will appear in the list. A name may be deleted by selecting it in the list and clicking **Delete**. All names may be deleted by clicking **Reset**.

12. **Cell Network.** Each of the cell networks is identified by a mobile country code (MCC) and mobile network code (MNC). Use this control to build up a list of cell networks. Enter the MCC as a three digit number and the MNC as a two or three digit number and click **Add**. The cell network will appear in the list. A cell network may be deleted by selecting it in the list and clicking **Delete**. All networks may be deleted by clicking **Reset**.

13. **Network Authentication Types.** Each network authentication that is in use on the network should be specified in this list. The choices are:

    a. **Acceptance of terms and conditions.** This choice displays a web page asking for the user's acceptance of terms and conditions of use. The URL should be specified in the URL field before clicking **Add.**

    b. **DNS redirection.** Rather than use the DNS server on the network, the redirection points to a different server.

    c. **HTTP/HTTPS redirection.** This choice causes the user's first web page reference to be redirected to a different URL for login or other information. The URL should be specified in the URL field before clicking **Add.**

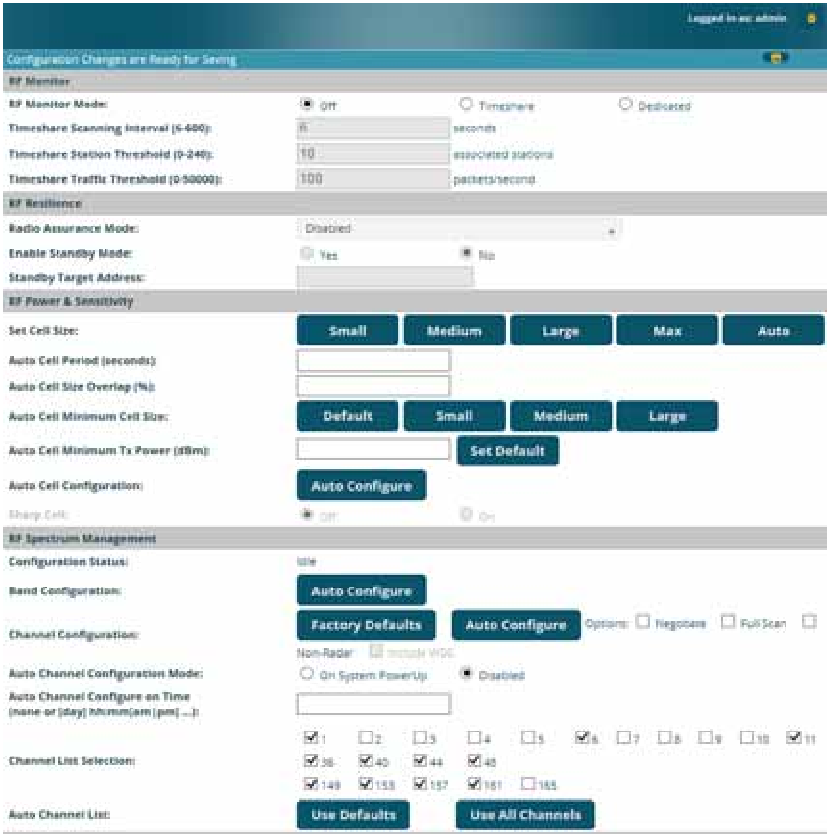
    d. **On-line enrollment supported.** This choice indicates that the user may sign up for network access as part of the authentication process.

    When **Add** is clicked the authentication type and optional URL will appear in the list. An authentication type may be deleted by selecting it in the list and clicking **Delete**. All authentication types may be deleted by clicking **Reset**.

14. **Venue Names.** The list of names associated with the venue are specified here. A venue name may be added to the list in English or Chinese. Enter the name in the appropriate field and click **Add.** The name will appear in the list. A name may be deleted by selecting it in the list and clicking **Delete**. All names may be deleted by clicking **Reset**.

Advanced RF Settings

This window allows you to establish RF settings, including automatically configuring channel allocation and cell size, and configuring radio assurance and standby modes. Changes you make on this page are applied to all radios, without exception.



Configuration Changes are Ready for Saving

RF Monitor

RF Monitor Mode: ● Off ○ Timeshare ○ Dedicated

Timeshare Scanning Interval (6-600): 6 seconds

Timeshare Station Threshold (0-240): 10 associated stations

Timeshare Traffic Threshold (0-50000): 100 packets/second

RF Resilience

Radio Assurance Mode: Disabled

Enable Standby Mode: ○ Yes ● No

Standby Target Address:

RF Power & Sensitivity

Set Cell Size: Small | Medium | Large | Max | Auto

Auto Cell Period (seconds):

Auto Cell Size Overlap (%):

Auto Cell Minimum Cell Size: Default | Small | Medium | Large

Auto Cell Minimum Tx Power (dBm): Set Default

Auto Cell Configuration: Auto Configure

Sharp Cell: ● Off ○ On

RF Spectrum Management

Configuration Status: Idle

Band Configuration: Auto Configure

Channel Configuration: Factory Defaults | Auto Configure Options: □ Negotiate □ Full Scan □ Non-Radar □ Include WDC

Auto Channel Configuration Mode: ○ On System PowerUp ● Disabled

Auto Channel Configure on Time (none or [day] hh:mm[am|pm] ...):

Channel List Selection:
☑ 1 □ 2 □ 3 □ 4 □ 5 ☑ 6 □ 7 □ 8 □ 9 □ 10 ☑ 11
☑ 36 ☑ 40 ☑ 44 ☑ 48
☑ 149 ☑ 153 ☑ 157 ☑ 161 □ 165

Auto Channel List: Use Defaults | Use All Channels

Figure 153. Advanced RF Settings

About Standby Mode

Standby Mode supports the WAP-to-WAP fail-over capability. When you enable Standby Mode, the WAP functions as a backup unit, and it enables its radios if it detects that its designated target WAP has failed. The use of redundant WAPs to provide this fail-over capability allows WAPs to be used in mission-critical applications. In Standby Mode, a WAP monitors beacons from the target WAP. When the target has not been heard from for 40 seconds, the standby WAP enables its radios until it detects that the target WAP has come back online. Standby Mode is off by default. Note that you must ensure that the configuration of the standby WAP is correct. This window allows you to enable or disable Standby Mode and specify the primary WAP that is the target of the backup unit.

Procedure for Configuring Advanced RF Settings

RF Monitor

1. **RF Monitor Mode:** RF monitoring permits the operation of features like intrusion detection. The monitor may operate in **Dedicated** mode, or in **Timeshare** mode which allows the radio to divide its time between monitoring and acting as a standard radio that allows stations to associate to it. **Timeshare** mode is especially useful for small WAPs with two radios, such as the 9120/9130 Series, allowing one radio to be shared between monitoring the airwaves for problems and providing services to stations. Settings allow you to give priority to monitoring or wireless services, depending on your needs. The default Monitor Mode for the WAP 9100 Series is **Timeshare** mode on the 2.4 GHz radio.

   If **Timeshare** mode is selected, you may adjust the following settings:

   - **Timeshare Scanning Interval (6-600)**: number of seconds between monitor (off-channel) scans.
   - **Timeshare Station Threshold (0-240)**: when the number of stations associated to the monitor radio exceeds this threshold, scanning is halted.
   - **Timeshare Traffic Threshold (0-50000)**: when the number of packets per second handled by the monitor radio exceeds this threshold, scanning is halted.

RF Resilience

2. **Radio Assurance Mode**: When this mode is enabled, the monitor radio performs loopback tests on the WAP. This mode requires RF Monitor Mode to be enabled (**Dedicated** or **Timeshare** mode, see Step 1) to support self-monitoring functions. It also requires a radio to be set to monitoring mode (see “Enabling Monitoring on the WAP” on page 497).

   Operation of Radio Assurance mode is described in detail in “WAP Monitor and Radio Assurance Capabilities” on page 497.

   The Radio Assurance mode scans and sends out probe requests on each channel, in turn. It listens for all probe responses and beacons. These tests are performed continuously (24/7). If no beacons or probe responses are observed from a radio for a predetermined period, Radio Assurance mode will take action according to the preference that you have specified:

   - **Failure alerts only**—The WAP will issue alerts in the Syslog, but will not initiate repairs or reboots.
   - **Failure alerts & repairs, but no reboots**—The WAP will issue alerts and perform resets of one or all of the radios if needed.
   - **Failure alerts & repairs & reboots if needed**—The WAP will issue alerts, perform resets, and schedule reboots if needed.
   - **Disabled**—Disable radio assurance tests (no self-monitoring occurs). Loopback tests are disabled by default.

3. **Enable Standby Mode**: Choose **Yes** to enable this WAP to function as a backup unit for the target WAP, or choose **No** to disable this feature. See “About Standby Mode” on page 330.

4. **Standby Target Address**: If you enabled the Standby Mode, enter the MAC address of the target WAP (i.e., the address of the primary WAP that is being monitored and backed up by this WAP). To find this MAC address, open the WAP Info window on the target WAP, and use the Gigabit1 MAC Address.

RF Power and Sensitivity

For an overview of RF power and cell size settings, please see "Capacity and Cell Sizes" on page 26 and "Fine Tuning Cell Sizes" on page 27.

To use the Auto Cell Size feature, the following additional settings are required: all radios that will use Auto Cell must have ***Cell Size*** *set to* ***auto****. See* ***"Procedure for Manually Configuring Radios" on page 285****.*

It is not necessary for RF Monitor Mode to be turned on, and you don't need to have any radio set to monitor mode. See ***"RF Monitor" on page 330.***

5. **Set Cell Size**: Cell Size may be set globally for all enabled radios to **Auto**, **Large, Medium, Small**, or **Max** using the buttons.

6. **Auto Cell Period (seconds)**: You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will run. If you select **None**, then auto-configuration of cell sizing will not be run periodically. You do not need to run Auto Cell often unless there are a lot of changes in the environment. If the RF environment is changing often, running Auto Cell every twenty-four hours (86400 seconds) should be sufficient). The default value is **None**.

7. **Auto Cell Size Overlap (%)**: Enter the percentage of cell overlap that will be allowed when the WAP is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring WAPs that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

8. **Auto Cell Min Cell Size**: Use this setting if you wish to set the minimum cell size that Auto Cell may assign. The values are **Default**, **Large, Medium,** or **Small**.

9. **Auto Cell Min Tx Power (dBm)**: Enter the minimum transmit power that the WAP can assign to a radio when adjusting automatic cell sizes. The default value is **10**.

10. **Auto Cell Configuration**: Click this button to instruct the WAP to determine and set the best cell size for each enabled radio whose **Cell Size** is **auto** on the Radio Settings window, based on changes in the environment. This is the recommended method for setting cell size. You may look at the Tx and Rx values on the Radio Settings window to view the cell size settings that were applied.

11. **Sharp Cell:** This feature reduces interference between neighboring WAPs or other Access Points by limiting to a defined boundary (cell size) the trailing edge bleed of RF energy. Choose **On** to enable the Sharp Cell functionality, or choose **Off** to disable this feature. See also, "Fine Tuning Cell Sizes" on page 27. This feature is available on 802.11n radios on WAPs, but not on 802.11ac radios.

    The Sharp Cell feature only works when the cell size is Small, Medium, or Large (or Auto)—but not Max. If radio cell size is set to Max, the Sharp Cell feature will be disabled for that radio.

RF Spectrum Management

12. **Configuration Status**: Shows the status of auto channel configuration. If an operation is in progress, the approximate time remaining until completion is displayed; otherwise **Idle** is displayed.

13. **Band Configuration**: Automatic band configuration is the recommended method for assigning bands to the abgn radios. It runs only on command, assigning radios to the 2.4GHz or 5GHz band when you click the **Auto Configure** button. The WAP uses its radios to listen for other APs on the same channel, and it assigns bands based on where it finds the least interference.

    Auto band assigns as many radios to the 5 GHz band as possible when there are other WAPs within earshot. It does this by determining how many WAPs are in range and then picking the number of radios to place in the 2.4 GHz band. Note that for another WAP to be considered to be in range, the other WAP must be visible via both the wireless and wired networks—the WAP must be listed in the Network Map table, its entry must have **In Range** set to **Yes**, and it must have at least one active radio with an SSID that has broadcast enabled.

Auto band runs separately from auto channel configuration. If a radio's band is changed, associated stations will be disconnected and will then reconnect.

14. **Channel Configuration**: Automatic channel configuration is a method for channel allocation. When the WAP performs auto channel configuration, you may optionally instruct it to first negotiate with any other nearby WAPs that have been detected, to determine whether to stagger the start time for the procedure slightly. Thus, nearby WAPs will not run auto channel at the same time. This prevents WAPs from interfering with each other's channel assignments.

*Note that Auto Channel normally assigns individual channels. However, if you select **Auto bond 5GHz channels** on the **Global Settings .11n** page, and have 40MHz channels set up prior to running Auto Channel, those bonds will be preserved. 80MHz bonds will not be preserved.*

The **Configuration Status** field displays whether an Auto Configure cycle is currently running on this WAP or not.

Click **Auto Configure** to instruct the WAP to determine the best channel allocation settings for each enabled radio and select the channel automatically, based on changes in the environment. This is the recommended method for channel allocation (see "RF Spectrum Management" on page 333). The following options may be selected for auto configuration:

- **Negotiate**: negotiate air-time with other WAPs before performing a full scan. Negotiating is slower, but if multiple WAPs are configuring channels at the same time the Negotiate option ensures that multiple WAPs don't select the same channels. Turning off the Negotiate option allows the **Auto Configure** button to manually perform auto channel without waiting, and may be used when you know that no other nearby WAPs are configuring their channels.

- **Full Scan**: perform a full traffic scan on all channels on all radios to determine the best channel allocation.
- **Non-Radar**: give preference to channels without radar-detect. See table in "Procedure for Configuring Global 802.11an Radio Settings" on page 306.
- **Include WDS**: automatically assign 5GHz to WDS client links.

Click **Factory Defaults** if you wish to instruct the WAP to return all radios to their factory preset channels. WAPs do not use the same factory preset values for channel assignments. Instead, if the WAP has been deployed for a while and already has data from the spectrum analyzer and Avaya Roaming Protocol about channel usage on neighboring WAPs, it performs a quick auto channel using that information (without doing a full RF scan) to make an intelligent choice of channel assignments. If the WAP has been rebooted and has no saved configuration or is just being deployed for the first time, it has no prior data about its RF environment. In this case, it will pick a set of compatible channel assignments at random.

*On 9120/9130 models, the **Factory Defaults** button will not restore radio1 to monitor mode. You will need to restore this setting manually. Also, you may need to set **RF Monitor Mode** to **Timeshare Mode** again - see "RF Monitor" on page 330.*

15. **Auto Channel Configuration Mode**: This option allows you to instruct the WAP to auto-configure channel selection for each enabled radio when the WAP is powered up. Choose **On WAP PowerUp** to enable this feature, or choose **Disabled** to disable this feature.

16. **Auto Channel Configure on Time**: This option allows you to instruct the WAP to auto-configure channel selection for each enabled radio at a time you specify here. Leave this field blank unless you want to specify a time at which the auto-configuration utility is initiated. Time is specified in hours and minutes, using the format: **[day]hh:mm [am|pm]**. If you omit the optional **day** specification, channel configuration will run daily at the

specified time. If you do not specify am or pm, time is interpreted in 24-hour military time. For example, Sat 11:00 pm and Saturday 23:00 are both acceptable and specify the same time.

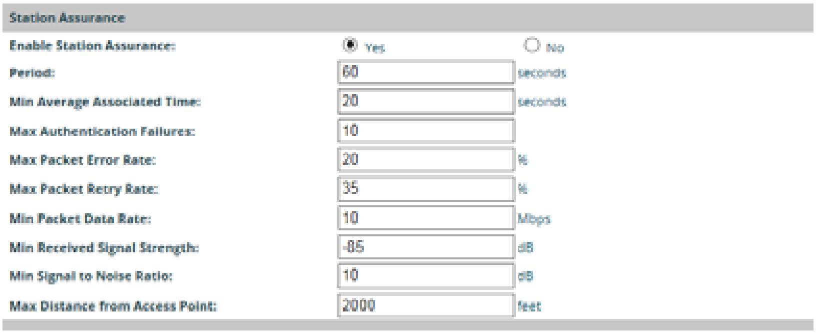
17. **Channel List Selection**: This list selects which channels are available to the auto channel algorithm. Channels that are not checked are left out of the auto channel selection process. Note that channels that have been locked by the user are also not available to the auto channel algorithm.

18. **Auto Channel List**: **Use All Channels** selects all available channels (this does not include locked channels). **Use Defaults** sets the auto channel list back to the defaults. This omits newer channels (100-140)—many wireless NICs don't support these channels.

Station Assurance

Station assurance monitors the quality of the connections that users are experiencing on the wireless network. You can quickly detect stations that are having problems and take steps to correct them. Use these settings to establish threshold values for errors and other problems. Station assurance is enabled by default, with a set of useful default thresholds that you may adjust as desired.

When a connection is experiencing problems and reaches one of these thresholds in the specified period of time, the WAP responds with several actions: an event is triggered, a trap is generated, and a Syslog message is logged. For example, if a client falls below the threshold for **Min Average Associated Time**, this "bouncing" behavior might indicate roaming problems with the network's RF design, causing the client to bounce between multiple WAPs and not stay connected longer than the time to re-associate and then jump again. This can be corrected with RF adjustments. Station assurance alerts you to the fact that this station is encountering problems.



Station Assurance		
Enable Station Assurance:	● Yes	○ No
Period:	60	seconds
Min Average Associated Time:	20	seconds
Max Authentication Failures:	10	
Max Packet Error Rate:	20	%
Max Packet Retry Rate:	35	%
Min Packet Data Rate:	10	Mbps
Min Received Signal Strength:	-85	dB
Min Signal to Noise Ratio:	10	dB
Max Distance from Access Point:	2000	feet

Figure 154. Station Assurance (Advanced RF Settings)

19. **Enable Station Assurance**: This is enabled by default. Click No if you wish to disable it, and click Yes to re-enable it. When station assurance is enabled, the WAP will monitor connection quality indicators listed below and will display associated information on the Station Assurance Status page. When a threshold is reached, an event is triggered, a trap is generated, and a Syslog message is logged.

20. **Period**: In seconds, the period of time for a threshold to be reached. For example, the WAP will check whether Max Authentication Failures has been reached in this number of seconds.

21. **Min Average Associated Time**: (seconds) Station assurance detects whether the average length of station associations falls below this threshold during a period.

22. **Max Authentication Failures**: Station assurance detects whether the number of failed login attempts reaches this threshold during a period.

23. **Max Packet Error Rate**: (%) Station assurance detects whether the packet error rate percentage reaches this threshold during a period.

24. **Max Packet Retry Rate**: (%) Station assurance detects whether the packet retry rate percentage reaches this threshold during a period.

25. **Min Packet Data Rate**: (Mbps) Station assurance detects whether the packet data rate falls below this threshold during a period.

26. **Min Received Signal Strength**: (dB) Station assurance detects whether the strength of the signal received from the station falls below this threshold during a period.

27. **Min Signal to Noise Ratio**: (dB) Station assurance detects whether the ratio of signal to noise received from the station falls below this threshold during a period.

28. **Max Distance from WAP**: **Min Received Signal Strength**: (feet) Station assurance detects whether the distance of the station from the WAP reaches this threshold during a period.

See Also

Coverage and Capacity Planning
Global Settings .11an
Global Settings .11bgn
Global Settings .11n
Radios
Radio Settings
Radio Assurance

Hotspot 2.0

Understanding Hotspot 2.0

Hotspot 2.0 is a part of the Wi-Fi Alliance’s Passpoint certification program. It specifies additional information above and beyond that found in 802.11u, which allows mobile clients to automatically discover, select, and connect to networks based on preferences and network optimization. Mobile clients that support Hotspot 2.0 are informed of an access point’s support via its beacon message.

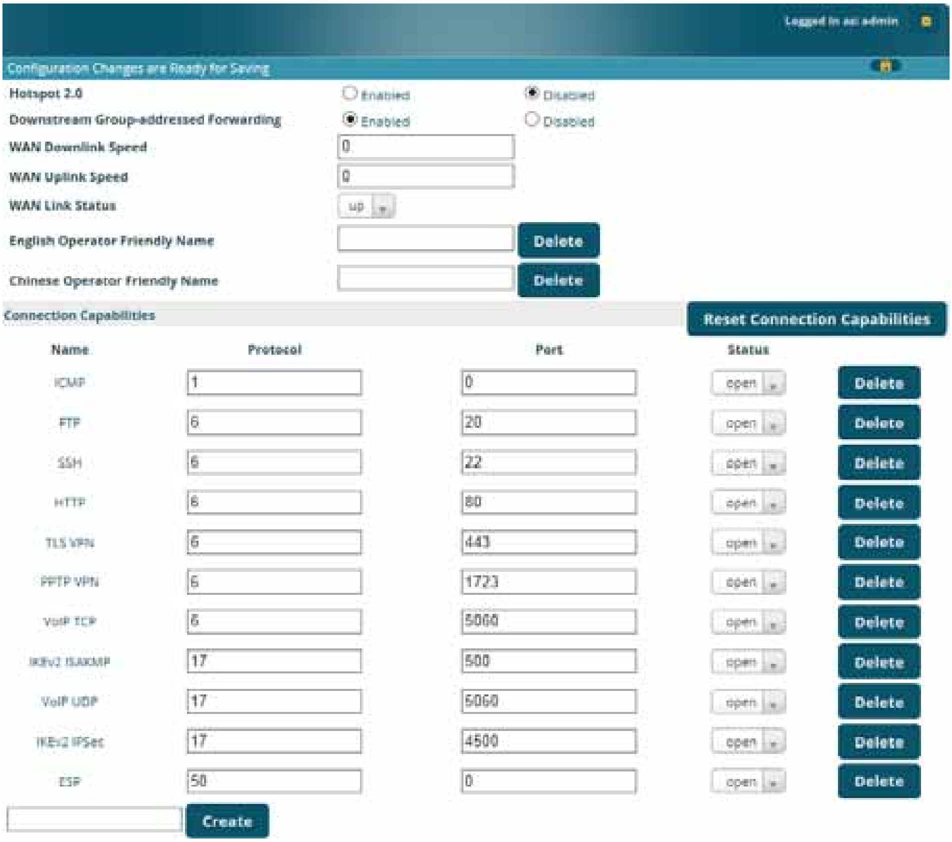
Hotspot 2.0 messages forward several types of information to clients, including:

- **Uplink and Downlink Speeds**
- **Link Status**
- **Friendly Name**
- **Connection Capabilities** The access point will restrict the protocols that can be used by a specification of protocol and port numbers.

Procedure for Hotspot 2.0 Settings

Use this window to establish the Hotspot 2.0 configuration.

1. **Hotspot 2.0.** Click **Enabled to** enable Hotspot 2.0 operation**.**
2. **Downstream Group-addressed Forwarding.** Click **Enabled** to allow the access point to forward group-addressed traffic (broadcast and multicast) to all connected devices. Click **Disabled** to cause the access point to convert group-addressed traffic to unicast messages.


Logged in as: admin
Configuration Changes are Ready for Saving

Hotspot 2.0	○ Enabled	● Disabled
Downstream Group-addressed Forwarding	● Enabled	○ Disabled
WAN Downlink Speed	0	
WAN Uplink Speed	0	
WAN Link Status	up	
English Operator Friendly Name		Delete
Chinese Operator Friendly Name		Delete

Connection Capabilities

Reset Connection Capabilities

Name	Protocol	Port	Status	
ICMP	1	0	open	Delete
FTP	6	20	open	Delete
SSH	6	22	open	Delete
HTTP	6	80	open	Delete
TLS VPN	6	443	open	Delete
PPTP VPN	6	1723	open	Delete
VoIP TCP	6	5060	open	Delete
IKEv2 ISAKMP	17	500	open	Delete
VoIP UDP	17	5060	open	Delete
IKEv2 IPSec	17	4500	open	Delete
ESP	50	0	open	Delete

Figure 155. Hotspot 2.0 Settings

3. **WAN Downlink Speed.** Enter the WAN downlink speed in kbps into the field.

4. **WAN Uplink Speed.** Enter the WAN uplink speed in kbps into the field.

5. **English/Chinese Operator Friendly Name.** Enter an English or Chinese name into one of the fields. An incorrectly entered name can be deleted by clicking the corresponding **Delete.**

6. **Connection Capabilities.** A Hotspot 2.0 access point limits the particular protocols that clients may use. The set of default protocols is shown initially. This table specifies the protocols in terms of:

   a. A common **Name**, such as FTP or HTTP.

   b. A **Protocol** number. For example 1 for ICMP, 6 for TCP, 17 for UDP, and 50 for Encapsulated Security Protocol in IPsec VPN connections.

   c. **Port** number for UDP / TCP connection.

   d. **Status**: one of **open, closed** or **unknown.**

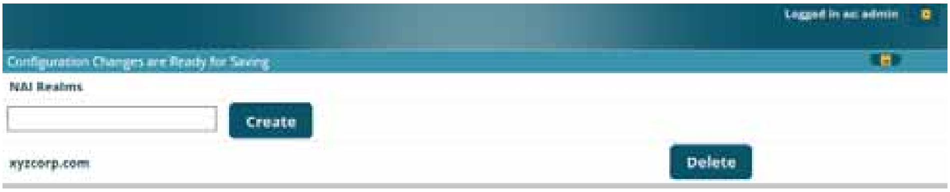
   Any of the entries may be deleted by clicking the corresponding **Delete** button. New entries may be created by entering the name of the protocol in the box beside the **Create** button, and then clicking **Create.** The new protocol will be added to the list with zeros in the protocol fields and **unknown** for the status. Enter the appropriate **Protocol** and **Port** values before setting the **Status** field to **open.**

NAI Realms

Understanding NAI Realm Authentication

A network access identifier (NAI) is a specification of a particular user. A NAI takes the general form of an e-mail address. Examples of NAIs are:

```
joe@example.com
fred@foo-9.example.com
jack@3rd.depts.example.com
fred.smith@example.com
```



Configuration Changes are Ready for Saving

xyzcorp.com

Figure 156. NAI Realms

The **NAI Realm** is the part of the NAI following the @ sign. For example, you might enter: **example.com**, **3rd.depts.example.com**, and **foo-9.example.com**. Use the **NAI Realms** page, in conjunction with the **NAI EAP** page, to specify the authentication techniques to be used to access that realm with appropriate parameters.

Procedure for NAI Realms Settings

Use this window to establish the names of the supported realms.

1. **Enter the realm name.** Enter the name of a realm in the box to the left of the **Create** button and click **Create**. The realm will be added to the **NAI Realms** list. Any of the realms may be deleted by clicking the corresponding **Delete** button**.**
2. **Enter Authentication Information.** The NAI EAP page is used to specify authentication for a realm. Click on the name of a realm to go to the NAI EAP page for that realm. See "NAI EAP" on page 341.

NAI EAP

This window allows specification of the authentication techniques for a realm.

Procedure for NAI Realms Settings

1. Select the realm to be configured in the **NAI Realm** drop down.
2. Select **EAP Methods**. Each realm may support up to five EAP authentication methods. Beside each of the five numbers (1, 2, 3, 4, 5) select the method from the drop down. The choices are:
   - **EAP-AKA**

- **EAP-AKA' (EAP-AKA prime)**
- **EAP-FAST**
- **EAP-MSCHAP-V2**
- **EAP-SIM**
- **EAP-TLS**
- **EAP-TTLS**
- **GTC**
- **MD5-Challenge**
- **None**
- **PEAP**

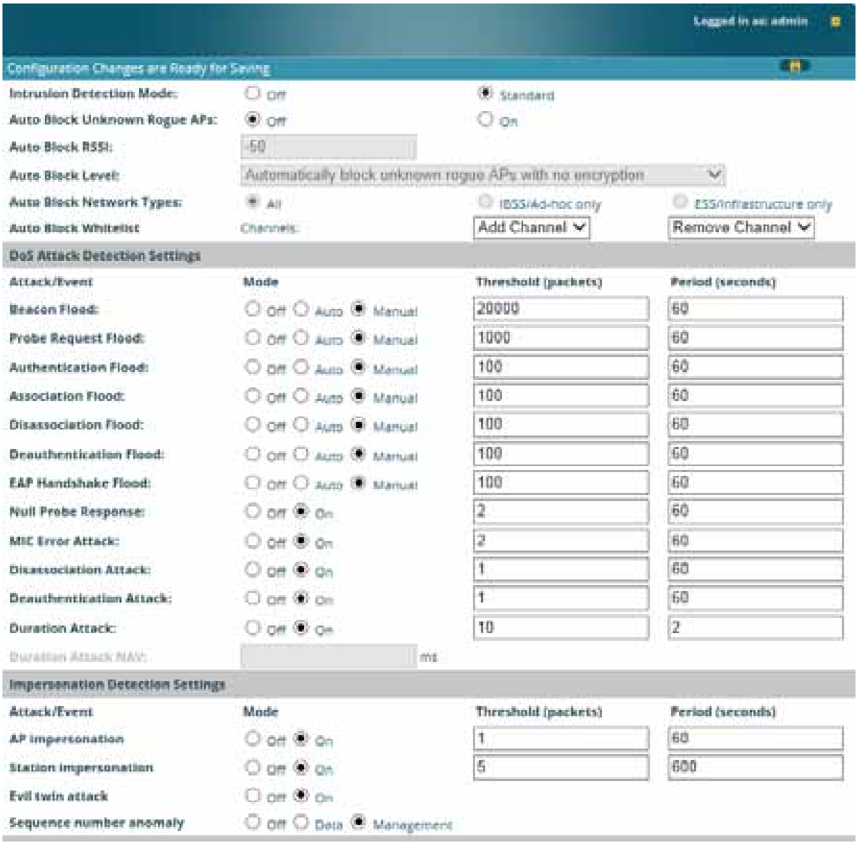
3. **Specify Authentication Parameters.** Each of the authentication methods may specify up to five authentication parameters. To specify the parameters click on the number corresponding to the authentication method; i.e. **1, 2, 3, 4,** or **5.** This displays the **EAP n Auth Parameter Configuration** below the list of **EAP Methods**. For up to five of the parameters, select the **Type** and **Value or Vendor ID / Type.** The choices for the **Type** are:

   - **Credential Type**
   - **Expanded EAP Method**
   - **Expanded Inner EAP Method**
   - **Inner Authentication EAP Method Type**
   - **Non-EAP Inner Authentication Type**
   - **None**
   - **Tunneled EAP Method Credential Type**

   For each type, a value or a vendor ID and type must be specified, as applicable.

Intrusion Detection

The WAP employs a number of IDS/IPS (Intrusion Detection System/ Intrusion Prevention System) strategies to detect and prevent malicious attacks on the wireless network. Use this window to adjust intrusion detection settings.



Configuration Changes are Ready for Saving

Intrusion Detection Mode:	○ Off	● Standard	
Auto Block Unknown Rogue APs:	● Off	○ On	
Auto Block RSSI:	-50		
Auto Block Level:	Automatically block unknown rogue APs with no encryption		
Auto Block Network Types:	● All	○ IBSS/Ad-hoc only	○ ESS/Infrastructure only
Auto Block Whitelist	Channels:	Add Channel	Remove Channel

DoS Attack Detection Settings

Attack/Event	Mode	Threshold (packets)	Period (seconds)
Beacon Flood:	○ Off ○ Auto ● Manual	20000	60
Probe Request Flood:	○ Off ○ Auto ● Manual	1000	60
Authentication Flood:	○ Off ○ Auto ● Manual	100	60
Association Flood:	○ Off ○ Auto ● Manual	100	60
Disassociation Flood:	○ Off ○ Auto ● Manual	100	60
Deauthentication Flood:	○ Off ○ Auto ● Manual	100	60
EAP Handshake Flood:	○ Off ○ Auto ● Manual	100	60
Null Probe Response:	○ Off ● On	2	60
MIC Error Attack:	○ Off ● On	2	60
Disassociation Attack:	○ Off ● On	1	60
Deauthentication Attack:	○ Off ● On	1	60
Duration Attack:	○ Off ● On	10	2
Duration Attack NAV:	ms		

Impersonation Detection Settings

Attack/Event	Mode	Threshold (packets)	Period (seconds)
AP impersonation	○ Off ● On	1	60
Station impersonation	○ Off ● On	5	600
Evil twin attack	○ Off ● On		
Sequence number anomaly	○ Off ○ Data ● Management		

Figure 157. Intrusion Detection Settings

The WAP provides a suite of intrusion detection and prevention options to improve network security. You can separately enable detection of the following types of problems:

- **Rogue Access Point Detection and Blocking**

  Unknown APs are detected, and may be automatically blocked based on a number of criteria. See "About Blocking Rogue APs" on page 346.

- **Denial of Service (DoS) or Availability Attack Detection**

  A DoS attack attempts to flood a WAP with communications requests so that it cannot respond to legitimate traffic, or responds so slowly that it becomes effectively unavailable. The WAP can detect a number of types of DoS attacks, as described in the table below. When an attack is detected, the WAP logs a Syslog message at the Alert level.

- **Impersonation Detection**

  These malicious attacks use various techniques to impersonate a legitimate AP or station, often in order to eavesdrop on wireless communications. The WAP detects a number of types of impersonation attacks, as described in the table below. When an attack is detected, the WAP logs a Syslog message at the Alert level.

Type of Attack	Description
DoS Attacks	
Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it hard for stations to find a legitimate AP.
Probe Request Flood	Generating thousands of counterfeit 802.11 probe requests to overburden the WAP.
Authentication Flood	Sending forged Authenticates from random MAC addresses to fill the WAP's association table.
Association Flood	Sending forged Associates from random MAC addresses to fill the WAP's association table.

Type of Attack	Description
Disassociation Flood	Flooding the WAP with forged Disassociation packets.
Deauthentication Flood	Flooding the WAP with forged Deauthenticates.
EAP Handshake Flood	Flooding an AP with EAP-Start messages to consume resources or crash the target.
Null Probe Response	Answering a station probe-request frame with a null SSID. Many types of popular NIC cards cannot handle this situation, and will freeze up.
MIC Error Attack	Generating invalid TKIP data to exceed the WAP's MIC error threshold, suspending WLAN service.
Disassociation Attack (Omerta)	Sending forged disassociation frames to all stations on a channel in response to data frames.
Deauthentication Attack	Sending forged deauthentication frames to all stations on a channel in response to data frames.
Duration Attack (Duration Field Spoofing)	Injecting packets into the WLAN with huge duration values. This forces the other nodes in the WLAN to keep quiet, since they cannot send any packet until this value counts down to zero. If the attacker sends such frames continuously it silences other nodes in the WLAN for long periods, thereby disrupting the entire wireless service.
Impersonation Attacks	
AP impersonation	Reconfiguring an attacker's MAC address to pose as an authorized AP. Administrators should take immediate steps to prevent the attacker from entering the WLAN.
Station impersonation	Reconfiguring an attacker's MAC address to pose as an authorized station. Administrators should take immediate steps to prevent the attacker from entering the WLAN.
Evil twin attack	Masquerading as an authorized AP by beaconing the WLAN's service set identifier (SSID) to lure users.

Type of Attack	Description
Sequence number anomaly	A sender may use an Add Block Address request (ADDBA - part of the Block ACK mechanism) to specify a sequence number range for packets that the receiver can accept. An attacker spoofs an ADDBA request, asking the receiver to reset its sequence number window to a new range. This causes the receiver to drop legitimate frames, since their sequence numbers will not fall in that range.

Some types of intrusion detection are turned off by default. These options affect AP performance more than other the other types of detection offered by the AP, thus they are disabled by default.

- Null probe response
- Deauthentication Attack
- Disassociation Attack
- AP Impersonation
- Station Impersonation
- Sequence Number Anomaly

About Blocking Rogue APs

If you classify a rogue AP as **blocked** (see “Rogue Control List” on page 242), then the WAP will take measures to prevent stations from staying associated to the rogue. When the monitor radio is scanning, any time it hears a beacon from a blocked rogue it sends out a broadcast “deauth” signal using the rogue's BSSID and source address. This has the effect of disconnecting all of a rogue AP’s clients approximately every 5 to 10 seconds, which is enough to make the rogue unusable.

The Intrusion Detection window allows you to set up **Auto Block** parameters so that unknown APs get the same treatment as explicitly blocked APs. This may result in many APs being blocked so use caution with auto block, and be sure to abide by applicable regulations. ***See the Caution on page 348.*** By default, auto blocking is turned off. Auto blocking provides two parameters for qualifying blocking so that APs must meet certain criteria before being blocked. This keeps the WAP from blocking every AP that it detects. You may:

- Set a minimum RSSI value for the AP—for example, if an AP has an RSSI value of -90, it is probably a harmless AP belonging to a neighbor and not in your building.
- Block based on encryption level.
- Block based on whether the AP is part of an ad hoc network or infrastructure network.
- Specify channels to be whitelisted. Rogues discovered on these channels are excluded from auto blocking. This allows specified channels to be freely used by customer or guests for their APs.

RF Intrusion Detection and Auto Block Mode

Procedure for Configuring Intrusion Detection

1. **Intrusion Detection Mode:** This option allows you to choose the **Standard** intrusion detection method, or you can choose **Off** to disable this feature. See "WAP Monitor and Radio Assurance Capabilities" on page 497 for more information.
   - **Standard**—enables the monitor radio to collect Rogue AP information.
   - **Off**—intrusion detection is disabled.
2. **Auto Block Unknown Rogue APs:** Enable or disable auto blocking (see "About Blocking Rogue APs" on page 346). You will be shown a Caution statement (below) and the WMI will ask whether you wish to proceed.

! *CAUTION: Selecting and engaging Auto Block may result in many APs being blocked. User caution in configuring and operating any form of Auto Block is highly recommended, as auto-blocking may be subject to significant statutory and U.S. Federal Communications Commission (FCC) regulatory controls, restrictions, enforcement actions and penalties.*

User is solely responsible for making sure that all uses of any auto-blocking feature(s) of this product are fully compliant with all applicable statutes, regulations, FCC enforcement actions and rules, etc. regarding Wi-Fi blocking. See for example FCC Enforcement Advisory No. 2015-01 dated January 27, 2015.

All uses of any auto-blocking feature(s) in this product are solely at User's discretion and individual choice. User assumes all liability and responsibility for all such uses. Avaya assumes no liability or responsibility for any discretionary decision by User to configure, engage and to use any auto-blocking feature(s) of this product.

Note that in order to set Auto Block RSSI and Auto Block Level, you must set Auto Block Unknown Rogue APs to **On**. Then the remaining Auto Block fields will be active.

3. **Auto Block RSSI**: Set the minimum RSSI for rogue APs to be blocked. APs with lower RSSI values will not be blocked. They are assumed to be farther away, and probably belonging to neighbors and posing a minimal threat.

4. **Auto Block Level:** Select rogue APs to block based on the level of encryption that they are using. The choices are:

   - Automatically block unknown rogue APs regardless of encryption.
   - Automatically block unknown rogue APs with no encryption.
   - Automatically block unknown rogue APs with WEP or no encryption.

5. **Auto Block Network Types:** Select rogues to automatically block by applying the criteria above only to networks of the type specified below. The choices are:

   - **All**—the unknown rogues may be part of any wireless network.
   - **IBSS/AD Hoc only**—only consider auto blocking rogues if they belong to an ad hoc wireless network (a network of client devices without a controlling Access Point, also called an Independent Basic Service Set—IBSS).
   - **ESS/Infrastructure only**—only consider auto blocking rogue APs if they are in infrastructure mode rather than ad hoc mode.

6. **Auto Block Whitelist:** Use this list to specify channels to be excluded from automatic blocking. If you have enabled **Auto Block**, it will not be applied to rogues detected on the whitelisted channels. Use the **Add Channel** drop-down to add entries to the **Channels** list, one at a time. You can delete entries from the list by selecting them from the **Remove Channel** drop-down list.

DoS Attack Detection Settings

7. **Attack/Event**: The types of DoS attack that you may detect are described in the Type of Attack Table page 344. Detection of each attack type may be separately enabled or disabled. For each attack, a default **Threshold** and **Period (seconds)** are specified. If the number of occurrences of the type of packet being detected exceeds the threshold in the specified number of seconds, then the WAP declares that an attack has been detected. You may modify the **Threshold** and **Period**.

   For the Flood attack settings, you also have a choice of **Auto** or **Manual**.

   - **Manual** mode—threshold and period settings are used to detect a flood. Packets received are simply counted for the specified time period and compared against the flood threshold. The default for all of the floods is **Manual** mode.
   - **Auto** mode—the WAP analyzes current traffic for packets of a given type versus traffic over the past hour to determine whether a packet

flood should be detected. In this mode, threshold and period settings are ignored. This mode is useful for floods like beacon or probe floods, where the numbers of such packets detected in the air can vary greatly from installation to installation.

8. **Duration Attack NAV (ms)**: For the duration attack, you may also modify the default duration value that is used to determine whether a packet may be part of an attack. If the number of packets having at least this duration value exceeds the **Threshold** number in the specified **Period**, an attack is detected.

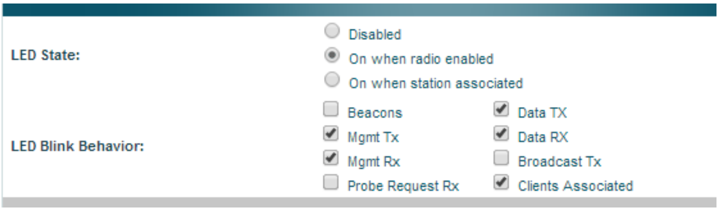
Impersonation Detection Settings

9. **Attack/Event**: The types of impersonation attack that you may detect are described in Impersonation Attacks page 345. Detection of each attack type may be turned **On** or **Off** separately. For **AP** or **Station Impersonation** attacks, a default **Threshold** and **Period (seconds)** are specified. If the number of occurrences of the type of packet being detected exceeds the threshold in the specified number of seconds, then the WAP declares that an attack has been detected. You may modify the **Threshold** and **Period**.

10. **Sequence number anomaly**: You may specify whether to detect this type of attack in **Data** traffic or in **Management** traffic, or turn **Off** this type of detection.

LED Settings

This window assigns behavior preferences for the WAP's radio LEDs.



LED State:
○ Disabled
● On when radio enabled
○ On when station associated

LED Blink Behavior:

□ Beacons	☑ Data TX
☑ Mgmt Tx	☑ Data RX
☑ Mgmt Rx	□ Broadcast Tx
□ Probe Request Rx	☑ Clients Associated

Figure 158. LED Settings

Procedure for Configuring the Radio LEDs

1. **LED State:** This option determines which event triggers the LEDs, either when the radio is enabled or when a station associates with the radio. Choose **On Radio Enabled** or **On First Association**, as desired. You may also choose Disabled to keep the LEDs from being lit. The LEDs will still light during the boot sequence, then turn off.

2. **LED Blink Behavior**: This option allows you to select when the radio LEDs blink, based on the activities you check here. From the choices available, select one or more activities to trigger when the LEDs blink. For default behavior, see "WAP LED Operating Sequences" on page 56.

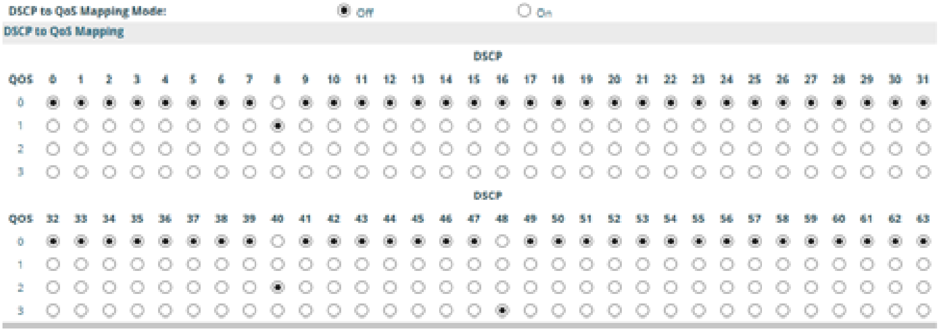
3. Click the **Save** button 💾 if you wish to make your changes permanent.

See Also

Global Settings
Global Settings .11an
Global Settings .11bgn
Radios
LED Boot Sequence

DSCP Mappings

DSCP is the 6-bit Differentiated Services Code Point (DiffServ) field in the IPv4 or IPv6 packet header, defined in RFC2474 and RFC2475. The DSCP value classifies the packet to determine the Quality of Service (QoS) required. DSCP replaces the outdated Type of Service (TOS) field.



DSCP to QoS Mapping Mode: ● Off ○ On

DSCP to QoS Mapping

DSCP

QOS	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	●	●	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

DSCP

QOS	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
0	●	●	●	●	●	●	●	●	○	●	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
2	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Figure 159. DSCP Mappings

The DSCP Mappings page shows the default mapping of each of the 64 DSCP values to one of the WAP's four QoS levels, and allows you to change these mappings.

For a detailed discussion of the operation of QoS and DSCP mappings on the WAP, please see "Understanding QoS Priority on the WAP" on page 249.

Procedure for Configuring DSCP Mappings

1. **DSCP to QoS Mapping Mode:** Use the **On** and **Off** buttons to enable or disable the use of the DSCP mapping table to determine the QoS level applied to each packet.
2. **DSCP to QoS Mapping**: The radio buttons in this table show all DSCP values (0 to 63), and the QoS level to which each is mapped. To change the QoS level applied to a DSCP value, click the desired QoS level (0 to 3) underneath it.

Roaming Assist

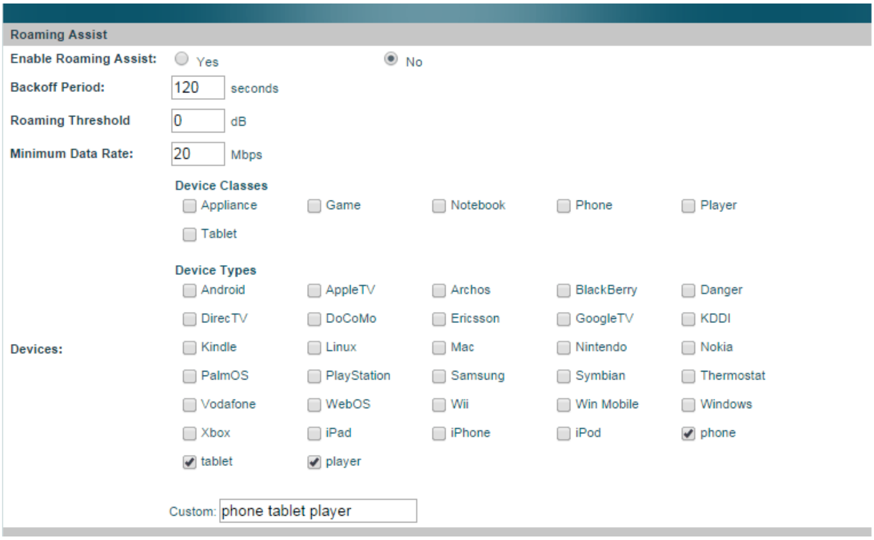
Roaming assist is an Avaya feature that helps clients roam to WAPs that will give them high quality connections. Some smart phones and tablets will stay connected to a radio with poor signal quality, even when there's a radio with better signal strength within range. When roaming assist is triggered, the WAP "assists" the device by deauthenticating it when certain parameters are met. This encourages a client with a high roaming threshold (i.e., a device that may not roam until signal quality has seriously dropped) to move to a WAP that gives it a better signal. The deauthentication is meant to cause the client to choose a different radio. You can specify the device types that will be assisted in roaming.

The roaming threshold is the difference in signal strength between radios that will trigger a deauthentication. If the client's signal is lower than the sum of the threshold and the stronger neighbor radio's RSSI, then we "assist" the client. For example:

Threshold = -5
RSSI of neighbor WAP = -65
RSSI of client = -75
-75 < (-5 + -65) : Therefore client will roam

Another example:

Threshold = -15
RSSI of neighbor WAP = -60
RSSI of station = -70
-70 > (-15 + -60) : Client will not roam



Roaming Assist

Enable Roaming Assist: ○ Yes ● No

Backoff Period: 120 seconds

Roaming Threshold: 0 dB

Minimum Data Rate: 20 Mbps

Devices:

Device Classes

□ Appliance □ Game □ Notebook □ Phone □ Player
□ Tablet

Device Types

□ Android □ AppleTV □ Archos □ BlackBerry □ Danger
□ DirecTV □ DoCoMo □ Ericsson □ GoogleTV □ KDDI
□ Kindle □ Linux □ Mac □ Nintendo □ Nokia
□ PalmOS □ PlayStation □ Samsung □ Symbian □ Thermostat
□ Vodafone □ WebOS □ Wii □ Win Mobile □ Windows
□ Xbox □ iPad □ iPhone □ iPod ☑ phone
☑ tablet ☑ player

Custom: phone tablet player

Figure 160. Roaming Assist

Procedure for Configuring Roaming Assist

1. **Enable Roaming Assist:** Use the **Yes** and **No** buttons to enable or disable this feature.

2. **Backoff Period**: After deauthenticating a station, it may re-associate to the same radio. To prevent the WAP from repeatedly deauthenticating the station when it comes back, there is a backoff period. This is the number of seconds the station is allowed to stay connected before another deauthentication.

3. **Roaming Threshold**: This is the difference in signal strength between radios that will trigger a deauthentication, as described in the discussion above. In most cases, this will be a negative number. Triggering occurs regardless of whether the data rate falls below the Minimum Data Rate.

4. **Minimum Data Rate**: Roaming assist will be triggered if the station’s packet data rate is below this value (1-99 Mbps), regardless of whether the Roaming Threshold has been reached.

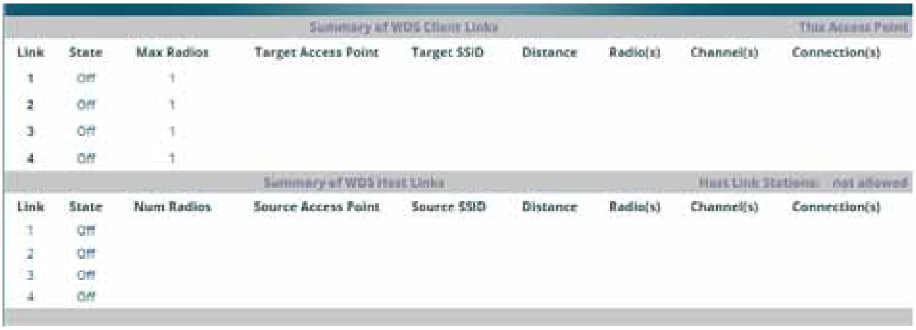
5. **Device Classes**: If you select any classes of device, such as **Phone** and **Notebook**, then roaming assist will *only* be applied to those kinds of stations. Many small, embedded devices (such as phones, tablets, and music players) are sticky—they have high roaming thresholds that tend to keep them attached to the same radio despite the presence of radios with better signal strength. You may check off one or more entries, but use care since roaming assist may cause poor results in some cases.

   If no Device Classes or Device Types are selected, then all devices are included in roaming assist. If you select entries in both Device Classes and Device Types, then stations matching any of your selected types/ classes will be assisted when the Roaming Threshold or Minimum Data Rate trigger is satisfied.

6. **Device Types**: If you select any types of device, such as **iPhone** and **Samsung**, then roaming assist will *only* be applied to those types of stations and to your selected Device Types as well, when the Roaming Threshold or Minimum Data Rate trigger is satisfied. If no Device Classes or Device Types are selected, then all devices are considered for roaming assist.

WDS

This is a status-only window that provides an overview of all WDS links that have been defined. Wireless Distribution System (WDS) is a system that enables the interconnection of access points wirelessly, allowing your wireless network to be expanded using multiple access points without the need for a wired backbone to link them. The **Summary of WDS Client Links** shows the WDS links that you have defined on this WAP and identifies the target WAP for each by its base MAC address. The **Summary of WDS Host Links** shows the WDS links that have been established on this WAP as a result of client WAPs associating to this WAP (i.e., the client WAPs have this WAP as their target). The summary identifies the source (client) WAP for each link. Both summaries identify the radios that are part of the link and whether the connection for each is up or down. See “WDS Planning” on page 49 for an overview.



Summary of WDS Client Links — This Access Point

Link	State	Max Radios	Target Access Point	Target SSID	Distance	Radio(s)	Channel(s)	Connection(s)
1	Off	1						
2	Off	1						
3	Off	1						
4	Off	1						

Summary of WDS Host Links — Host Link Stations: not allowed

Link	State	Num Radios	Source Access Point	Source SSID	Distance	Radio(s)	Channel(s)	Connection(s)
1	Off							
2	Off							
3	Off							
4	Off							

Figure 161. WDS

About Configuring WDS Links

A WDS link connects a client WAP and a host WAP. The host must be the WAP that has a wired connection to the LAN. Client links from one or more WAPs may be connected to the host, and the host may also have client links. See “WDS Planning” on page 49 for more illustrations.

The configuration for WDS is performed on the client WAP only, as described in “WDS Client Links” on page 359. No WDS configuration is performed on the host WAP. First you will set up a client link, defining the target (host) WAP and SSID, and the maximum number of radios in the link. Then you will select the radios to be used in the link. When the client link is created, each member radio will associate to a radio on the host WAP.

You may wish to consider configuring the WDS link radios so that only the WDS link SSIDs are active on them. See “Active Radios” on page 269.

It is VERY important to use the WDS Lock command in CLI if you are using WDS and your network is being managed by any version of WOS, *because WOS does not manage WDS. When WOS applies configuration changes, it resets the AP’s configuration before applying the new configuration, and this can sever WDS links. To prevent this, the following CLI command must be used:*

```
interface iap wds lock on
```

When WDS Lock is enabled, the AP will not make changes that can break the WDS link. Any attempt to make such changes via CLI, WMI, or SNMP will return an error. WOS-Cloud will not receive an error, but the changes will be refused. All methods of updating any part of the configuration associated with WDS are blocked when WDS Lock is enabled:

- Radio settings for radios involved with a link
- SSID settings for SSIDs involved with a link
- VLAN settings for VLANs associated with SSIDs involved with a link
- WDS settings for any active link
- Global WDS settings
- Reset preserveip will also preserve WDS settings

Once some radio has been selected to act as a WDS client link, you will not be allowed to use auto-configured cell sizing on that radio (since the cell must extend all the way to the other WAP).

When configuring WDS, if you use WPA-PSK (Pre-Shared Key) as a security mechanism, ensure that EAP is disabled. Communication between two WAPs in WDS mode will not succeed if the client WAP has both PSK and EAP enabled on the SSID used by WDS. See ***SSID Management****.*

TKIP encryption does not support high throughput rates, per IEEE 802.11n. TKIP should ***never*** *be used for WDS links on WAPs.*

WDS is available on most WAPs, including models with two radios (WDS will operate on either of the radios). If WDS is not available, the settings are grayed out or not shown.

Long Distance Links

If you are using WDS to provide backhaul over an extended distance, use the **WDS Dist. (Miles)** setting to prevent timeout problems associated with long transmission times. (See "Radio Settings" on page 284) Set the approximate distance in miles between this radio and the connected WAP in the **WDS Dist. (Miles)** column. This will increase the wait time for frame transmission accordingly.

See Also

SSID Management

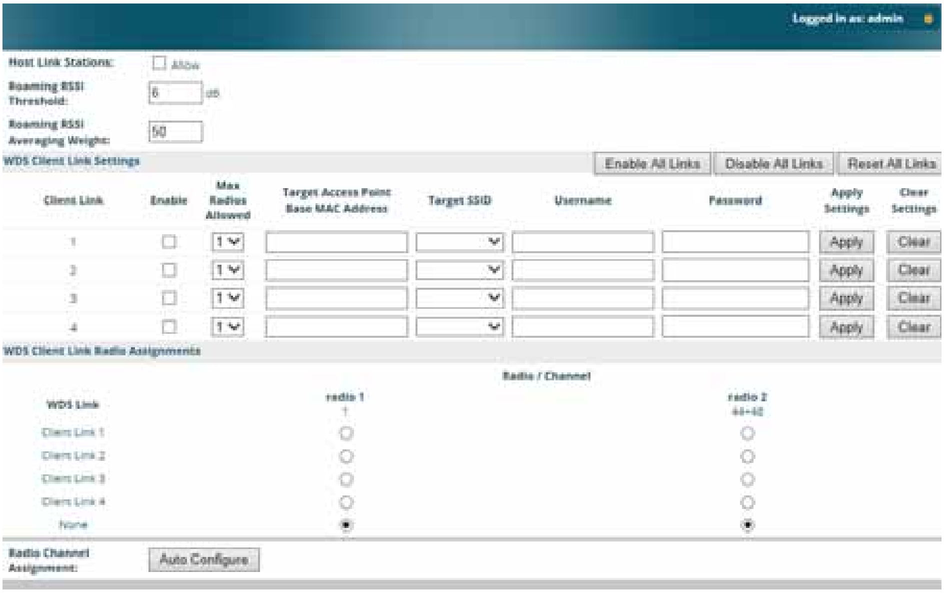
Active Radios

WDS Client Links

WDS Statistics

WDS Client Links

This window allows you to set up a maximum of four WDS client links.



Host Link Stations: □ Allow

Roaming RSSI Threshold: 6 dB

Roaming RSSI Averaging Weight: 50

WDS Client Link Settings

Client Link	Enable	Max Radios Allowed	Target Access Point Base MAC Address	Target SSID	Username	Password	Apply Settings	Clear Settings
1	□	1					Apply	Clear
2	□	1					Apply	Clear
3	□	1					Apply	Clear
4	□	1					Apply	Clear

WDS Client Link Radio Assignments

	Radio / Channel	
WDS Link	radio 1 1	radio 2 44+48
Client Link 1	○	○
Client Link 2	○	○
Client Link 3	○	○
Client Link 4	○	○
None	●	●

Radio Channel Assignment:

Figure 162. WDS Client Links

Procedure for Setting Up WDS Client Links

1. **Host Link Stations**: Check the **Allow** checkbox to instruct the WAP to allow stations to associate to radios on a host WAP that participates in a WDS link. The WDS host radio will send beacons announcing its availability to wireless clients. This is disabled by default.

Once some radio has been selected to act as a WDS client link, no other association will be allowed on that radio. However, wireless associations will be allowed on the WDS host side of the WDS session.

In situations like the one in the next step, where WDS is used by a WAP mounted on a high speed train, STP can add significant delay (often on the order of 30 to 60 seconds) while initially analyzing network topology. In such a situation, it may be desirable to disable STP. See "Management Control" on page 217.

Caution: If Spanning Tree Protocol ("Management Control" on page 217) is disabled and a network connection is made on the WDS Client WAP's Gigabit link that can reach the WDS Host WAP, broadcast and multicast packets will not be blocked. A broadcast storm may cause a network outage.

2. **Roaming RSSI Threshold**: If a WAP is deployed on a mobile site (on a train, for example), you can use WDS to implement a wireless backhaul that will roam between WAPs at fixed locations. When another candidate WAP for WDS host target is found, the client link will roam to the new WAP if its RSSI is stronger than the RSSI of the current host connection by at least the **Roaming RSSI Threshold.** The default is 6 dB.

3. **Roaming RSSI Averaging Weight**: This weight changes how much the latest RSSI reading influences the cumulative weighted RSSI value utilized in checking the threshold (above) to make a roaming decision. The higher the weight, the lower the influence of a new RSSI reading. This is not exactly a percentage, but a factor in the formula for computing the current RSSI value based on new readings:

   StoredRSSI = (StoredRSSI * RoamingAvgWeight
   + NewRSSIReading * (100 - RoamingAvgWeight)) / 100

   This prevents erroneous or out-of-line RSSI readings from causing the WDS link to jump to a new WAP. Such readings can result from temporary obstructions, external interference, etc.

4. Click the **Save** button 💾 after you are finished making changes on this page if you wish to make your changes permanent.

WDS Client Link Setting:

5. **Enable/Disable/Reset All Links**: Click the appropriate button to:

- **Enable All Links**—this command activates all WDS links configured on the WAP.
- **Disable All Links**—this command deactivates all WDS links configured on the WAP. It leaves all your settings unchanged, ready to re-enable.
- **Reset All Links**—this command tears down all links configured on the WAP and sets them back to their factory defaults, effective immediately.

6. **Client Link**: Shows the ID (1 to 4) of each of the four possible WDS links.

7. **Enabled**: Check this box if you want to enable this WDS link, or uncheck the box to disable the link.

8. **Max Radios Allowed (1-3)**: Enter the maximum number of radios for this link, between 1 and 3.

9. **Target WAP Base MAC Address**: Enter the base MAC address of the target WAP (the host WAP at the other side of this link). To find this MAC address, open the **WDS** window on the ***target*** WAP, and use **This WAP Address** located on the right under the Summary of WDS Host Links. To allow any Avaya WAP to be accepted as a WDS target, enter the Avaya OUI: **64:a7:dd:00:00:00** (this is useful for roaming in a mobile deployment, as described in Step 2 on page 360).

10. **Target SSID**: Enter the SSID that the target WAP is using.

11. **Username**: Enter a username for this WDS link. A username and password is required if the SSID is using PEAP for WDS authentication from the internal RADIUS server.

12. **Password**: Enter a password for this WDS link.

13. **Clear Settings**: Click on the **Clear** button to reset all of the fields on this line.

WDS Client Link Radio Assignments:

14. For each desired client link, select the radios that are part of that link. The radio channel assignments are shown in the column headers.

15. **Radio Channel Assignment**: Click **Auto Configure** to instruct the WAP to automatically determine the best channel allocation settings for each radio that participates in a WDS link, based on changes in the environment. These changes are executed immediately, and are automatically applied.

See Also

SSID Management

WDS Planning

WDS

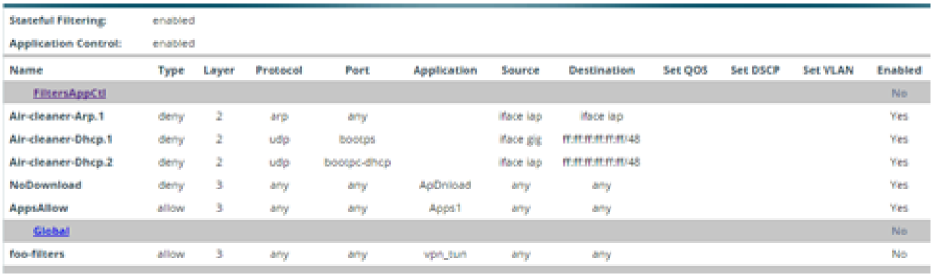
WDS Statistics

Filters

The WAP's integrated firewall uses stateful inspection to speed the decision of whether to allow or deny traffic. Filters are used to define the rules used for blocking or passing traffic. Filters can also set the VLAN and QoS level for selected traffic.

The air cleaner feature offers a number of predetermined filter rules that eliminate a great deal of unnecessary wireless traffic. See "Air Cleaner" on page 438.

Filters may be used based on your experience with Application Control Windows to eliminate or cap the amount of traffic allowed for less desirable applications.



Stateful Filtering: enabled
Application Control: enabled

Name	Type	Layer	Protocol	Port	Application	Source	Destination	Set QOS	Set DSCP	Set VLAN	Enabled
FiltersAppCtl											No
Air-cleaner-Arp.1	deny	2	arp	any		iface iap	iface iap				Yes
Air-cleaner-Dhcp.1	deny	2	udp	bootps		iface gig	ff:ff:ff:ff:ff:ff/48				Yes
Air-cleaner-Dhcp.2	deny	2	udp	bootpc-dhcp		iface iap	ff:ff:ff:ff:ff:ff/48				Yes
NoDownload	deny	3	any	any	ApDnload	any	any				Yes
AppsAllow	allow	3	any	any	Apps1	any	any				Yes
Global											No
foo-filters	allow	3	any	any	vpn_tun	any	any				No

Figure 163. Filters

User connections managed by the firewall are maintained statefully—once a user flow is established through the WAP, it is recognized and passed through without application of all defined filtering rules. Stateful inspection runs automatically on the WAP. The rest of this section describes how to view and manage filters.

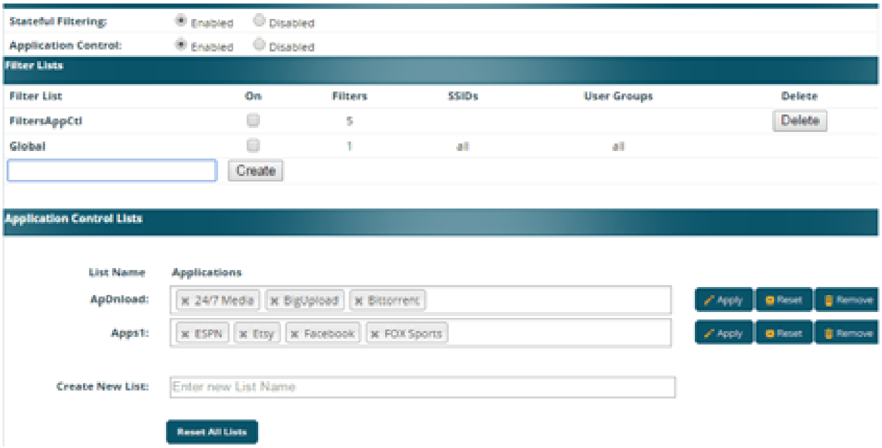
Filters are organized in groups, called Filter Lists. A filter list allows you to apply a uniform set of filters to SSIDs or Groups very easily. Similarly, you can use a custom Application Control list to create a set of applications that are handled as a group for convenience when creating filters.

The read-only Filters window provides you with an overview of all filter lists and Application Control lists that have been defined for this WAP, and the filters that have been created in each list. Filters are listed in the left side column by name under the filter list to which they belong. Each filter entry is a link that takes you to its Filter Management entry, and the list includes information about the type of filter, the protocol it is filtering, which port it applies to, source and destination addresses, and QoS and VLAN assignments.

Filter Lists

This window allows you to create filter lists and custom Application Control lists. These lists offer you ease of management of groups of filters and applications. The WAP comes with one predefined filter list, named **Global**, which cannot be deleted. Filter lists (including Global) may be applied to SSIDs or to Groups. Only one filter list at a time may be applied to a group or SSID (although the filter list may contain a number of filters). All filters are created within filter lists.

Use a custom Application Control list to create a set of applications that may then be handled as a group when creating filters. Thus, one filter can apply to an entire group of applications. This keeps the number of filters down and makes them much easier to manage. For example, you can include BitTorrent, Netflix, and Fox Sports in an Application Control list, and then create a single filter to block all three during business hours.



Stateful Filtering: ● Enabled ○ Disabled

Application Control: ● Enabled ○ Disabled

Filter Lists

Filter List	On	Filters	SSIDs	User Groups	Delete
FiltersAppCtl	□	5			Delete
Global	□	1	all	all	

Application Control Lists

List Name	Applications
ApDnload:	24/7 Media, BigUpload, Bittorrent
Apps1:	ESPN, Etsy, Facebook, FOX Sports

Figure 164. Filter Lists

Procedure for Managing Filter Lists

1. **Stateful Filtering:** Stateful operation of the integrated firewall can be **Enabled** or **Disabled**. If you have a large number of filters and you don't want to apply them in a stateful manner, you may use this option to turn the firewall off.

2. **Application Control:** Operation of the Application Control feature may be **Enabled** or **Disabled**. See "Application Control Windows" on page 130.

*The Application Control feature is only available if the WAP license includes **Application Control**. If a setting is unavailable (grayed out), then your license does not support the feature. See "Licensing" on page 61.*

Filter Lists

3. **New Filter List Name**: Enter a name for the new filter list in this field, then click on the Create button to create the list. All new filters are disabled when they are created. The new filter list is added to the Filter List table in the window. Click on the filter list name, and you will be taken to the Filter Management window for that filter list. You may create up to 16 filter lists.

4. **On**: Check this box to enable this filter list, or leave it blank to disable the list. If the list is disabled, you may still add filters to it or modify it, but none of the filters will be applied to data traffic.

5. **Filters**: This read-only field displays the number of filters that belong to this filter list.

6. **SSIDs**: This read-only field lists the SSIDs that use this filter list.

7. **User Groups**: This read-only field lists the Groups that use this filter list.

8. **Delete**: Click this button to delete this filter list. The **Global** filter list may not be deleted.

Custom Application Control List

9. **Create New List**: Enter a name for the new Application Control list in this field, followed by the ENTER key. The new list is added to the Application Control Lists table, and this list may be used to create filters. You may create up to 15 lists (on the WAO9122, the limits are reduced to 8 lists and 125 applications per list).

   Click in the field for the new Application Control list to display a list of applications. Add the desired applications to this list, one at a time. Up to 250 applications may be added. This field also provides a search feature—type in a string, and the list will display only the choices whose names contain that string in any position. Click the **Apply** button on the right when done adding applications to this list.

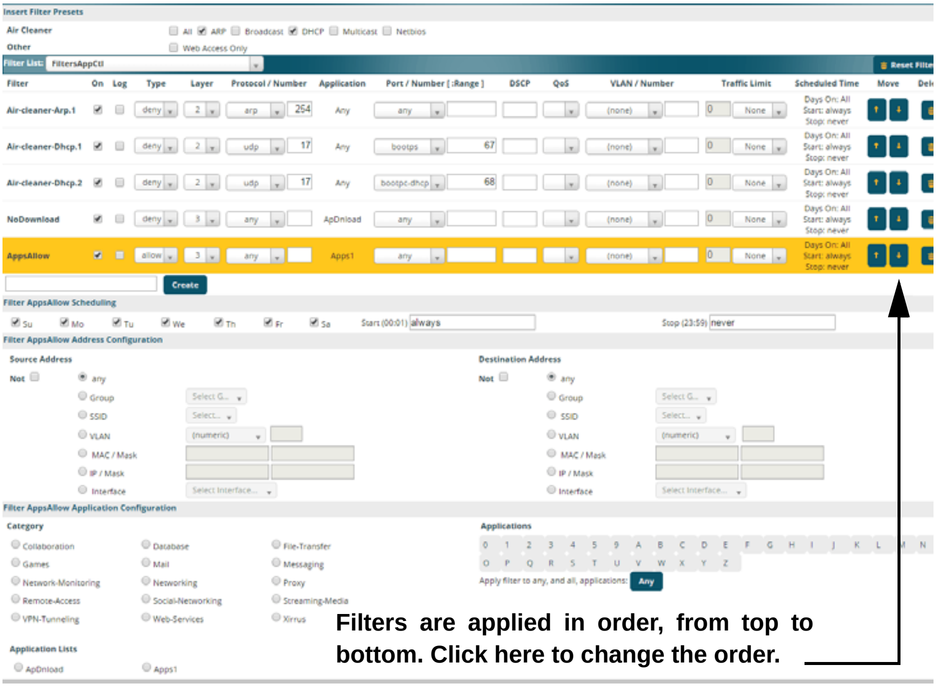
   Click **Reset** if you want to remove all of the entries from this field, i.e., to empty it. Click **Remove** to delete this Application Control list. You may use **Reset All Lists** on the bottom to delete all lists.

10. Click the **Save** button 💾 if you wish to make your changes permanent.

11. Click a filter list to go to the Filter Management window to create and manage the filters that belong to this list.

Filter Management

This window allows you to create and manage filters that belong to a selected filter list, based on the filter criteria you specify. Filters are an especially powerful feature when combined with the intelligence provided by the “Application Control Windows” on page 130.



Insert Filter Presets

Air Cleaner □ All ☑ ARP □ Broadcast ☑ DHCP □ Multicast □ Netbios

Other □ Web Access Only

Filter List: FiltersAppCtl

Reset Filte

Filter	On	Log	Type	Layer	Protocol / Number		Application	Port / Number [:Range]		DSCP	QoS	VLAN / Number		Traffic Limit		Scheduled Time	Move	Del
Air-cleaner-Arp.1	☑	□	deny	2	arp	254	Any	any				(none)		0	None	Days On: All Start: always Stop: never	↑ ↓	
Air-cleaner-Dhcp.1	☑	□	deny	2	udp	17	Any	bootps	67			(none)		0	None	Days On: All Start: always Stop: never	↑ ↓	
Air-cleaner-Dhcp.2	☑	□	deny	2	udp	17	Any	bootpc-dhcp	68			(none)		0	None	Days On: All Start: always Stop: never	↑ ↓	
NoDownload	☑	□	deny	3	any		ApDnload	any				(none)		0	None	Days On: All Start: always Stop: never	↑ ↓	
AppsAllow	☑	□	allow	3	any		Apps1	any				(none)		0	None	Days On: All Start: always Stop: never	↑ ↓	

Create

Filter AppsAllow Scheduling

☑ Su ☑ Mo ☑ Tu ☑ We ☑ Th ☑ Fr ☑ Sa Start (00:01) always Stop (23:59) never

Filter AppsAllow Address Configuration

Source Address

Not □

● any
○ Group Select G...
○ SSID Select...
○ VLAN (numeric)
○ MAC / Mask
○ IP / Mask
○ Interface Select Interface...

Destination Address

Not □

● any
○ Group Select G...
○ SSID Select...
○ VLAN (numeric)
○ MAC / Mask
○ IP / Mask
○ Interface Select Interface...

Filter AppsAllow Application Configuration

Category

○ Collaboration ○ Database ○ File-Transfer
○ Games ○ Mail ○ Messaging
○ Network-Monitoring ○ Networking ○ Proxy
○ Remote-Access ○ Social-Networking ○ Streaming-Media
○ VPN-Tunneling ○ Web-Services ○ Xirrus

Application Lists

○ ApDnload ○ Apps1

Applications

Apply filter to any, and all, applications: Any

Filters are applied in order, from top to bottom. Click here to change the order.

Figure 165. Filter Management

Based on Application Control’s analysis of your wireless traffic, you can create filters to enhance wireless usage for your business needs:

- Usage of non-productive and risky applications like BitTorrent can be restricted.
- Traffic for mission-critical applications like VoIP and Scopia may be given higher priority (QoS).

- Non- critical traffic from applications like YouTube may be given lower priority (QoS) or bandwidth allowed may be capped per station or for all stations.
- Traffic flows for specific applications may be controlled by sending them into VLANs that are designated for that type of traffic.
- Filters may be applied at specified times—for example, no games allowed from 8 AM to 6 PM.

Note that filtering is secondary to the stateful inspection performed by the integrated firewall. Traffic for established connections is passed through without the application of these filtering rules.

Procedure for Managing Filters

1. **Insert Filter Presets:** A number of predefined “Air Cleaner” filters are available using these buttons. You can use these rules to eliminate a great deal of unnecessary wireless traffic, resulting in improved performance. **Web Access Only** may be selected to allow only web access protocols to be used. For more information, please see “Air Cleaner” on page 438. When you select one of the filter presets, the appropriate filters will be added to the list, so that you can see exactly what settings have been used.

2. **Filter List**: Select the filter list to display and manage on this window. All of the filters already defined for this list are shown, and you may create additional filters for this list. You may create up to 50 filters per list.

3. **Add a New Filter**: To add a new filter, enter its name in the field next to the **Create** button at the bottom of the filter list, then click **Create**. All new filters are added to the table of filters in the window. The filter name must be unique within the list, but it may have the same name as a filter in a different filter list. Two filters with the same name in different filter lists will be completely unrelated to each other—they may be defined with different parameter values.

Viewing or modifying existing filter entries:

4. **Filter**: Select a filter entry if you wish to modify it. Source and destination details are displayed below the bottom of the list.

5. **On**: Use this field to enable or disable this filter.

6. **Log**: Log usage of this filter to Syslog.

7. **Type**: Choose whether this filter will be an **Allow** filter or a **Deny** filter. If you define the filter as an Allow filter, then any traffic that meets the filter criteria will be allowed. If you define the filter as a Deny filter, any traffic that meets the filter criteria will be denied.

8. **Layer**: Select network layer **2** or **3** for operation of this filter.

9. **Protocol/Number**: Choose a specific filter protocol from the pull-down list, or choose **numeric** and enter a **Number**, or choose **any** to instruct the WAP to use the best filter. This is a match criterion.

10. **Application**: Shows an application to filter, based on settings from Step 22 and Step 23. If an application has been selected, you should not enter **Protocol** or **Port**—application filters have intelligence built into them, and perform filtering that you cannot accomplish with just port and protocol. See "Application Control Windows" on page 130.

11. **Port/Number**: This is a match criterion. From the pull-down list, choose the target port type for this filter. Choose **any** to instruct the WAP to apply the filter to any port, or choose **1-65534** and enter a **Number**.

    To enter a **Range** of port numbers, separate the start and end numbers with a colon as shown: **Start # : End #**.

12. **DSCP**: Differentiated Services Code Point or DiffServ (DSCP) —Optional. Set packets ingressing from the wireless network that match the filter criteria to this DSCP level (0 to 63) before sending them out on the wired network. Select the level from the pull-down list. Level 0 has the lowest priority; level 63 has the highest priority. By default, this field is blank and the filter does not modify DSCP level. See "Understanding QoS Priority on the WAP" on page 249.

13. **QoS**: (Optional) Set packets ingressing from the wired network that match the filter criteria to this QoS level (0 to 3) before sending them out on the wireless network. Select the level from the pull-down list. Level 0 has the lowest priority; level 3 has the highest priority. By default, this field is blank and the filter does not modify QoS level. See "Understanding QoS Priority on the WAP" on page 249.

14. **VLAN/Number**: (Optional) Set packets that match the filter criteria to this VLAN. Select a VLAN from the pull-down list, or select **numeric** and enter the number of a previously defined VLAN (see "VLANs" on page 191).

15. **Traffic Limit**: Instead of simply allowing the specified traffic type, you may cap the amount of traffic allowed that matches this filter. First choose the units for the limit: kbps for all stations in total or per station, or packets per second (pps) for all stations in total or per station. Then enter the numeric limit in the field to the left.

16. **Scheduled Time**: shows the times at which this filter is active, if you have established a schedule in Step 19.

17. **Move Up/Down**: The filters are applied in the order in which they are displayed in the list, with filters on the top applied first. To change an entry's position in the list, just click its **Up** or **Down** button.

18. To delete a filter, click its **Delete** button.

Select an existing filter entry in the list to view or modify **Scheduling** or **Address Configuration,** shown below the list of filters:

19. **Scheduling**: Use these fields if you wish to specify a scheduled time for this filter to be active. Check the checkboxes for the days that the filter is to be active. By default, the filter is active all day on each selected day. You may also specify a time of day for the filter to be active by entering a **Start** and **Stop** time in 24:00 hour format (i.e., 6:30 PM is 18:30). To use this feature, you must enter both a Start and a Stop time.

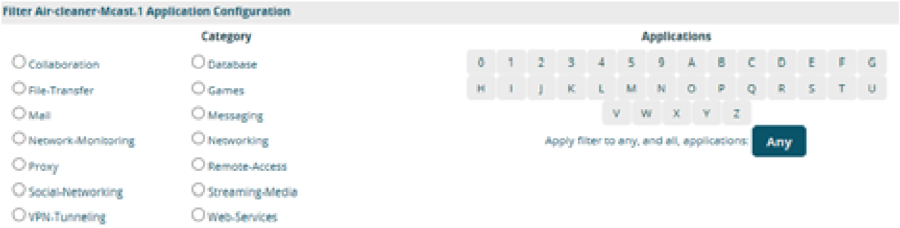
    You cannot apply one filter for two or more scheduled periods, but you can create two filters to achieve that. For example, one filter could deny the category Games from 9:00 to 12:00, and another could deny them from 13:00 to 18:00. Similarly, you might create two rules for different days—one to deny Games Mon-Fri 8:00 to 18:00, and another to deny them on Sat. from 8:00 to 12:00.

20. **Source Address**: Define a source address to match as a filter criterion. Click the radio button for the desired type of address (or other attribute) to match. Then specify the value to match in the field to the right of the button. Choose **Any** to use any source address. Check **Not** to match any address except for the specified address.

21. **Destination Address**: Define a destination address to match as a filter criterion. Click the radio button for the desired type of address (or other attribute) to match. Then specify the value to match in the field to the right of the button. Choose **any** to use any destination address. Check **Not** to match any address except for the specified address.

Below the Source and Destination Addresses, you may enter a **Category** or an **Application** or an **Application List** to be matched by the filter:

22. **Category**: If you wish this filter to apply to a particular category of application, such as **File-Transfer** or **Database**, select it from the listed options.



Filter Air-cleaner-Mcast.1 Application Configuration

Category

○ Collaboration ○ Database
○ File-Transfer ○ Games
○ Mail ○ Messaging
○ Network-Monitoring ○ Networking
○ Proxy ○ Remote-Access
○ Social-Networking ○ Streaming-Media
○ VPN-Tunneling ○ Web-Services

Applications

Apply filter to any, and all, applications: Any

Figure 166. Filter Category or Application

23. **Applications**: If you wish this filter to apply to a specific application, such as **Scopia**, click the letter or number that it starts with. Then select the desired application. You may select a **Category** or an **Application**, but not both.

24. **Application Lists**: If you wish this filter to apply to a previously configured Custom Application Control List, select the desired list. You may not select a **Category** or an **Application** in addition to the list.

25. Click the **Save** button 💾 if you wish to make your changes permanent.

See Also

Filters

Filter Statistics

Understanding QoS Priority on the WAP

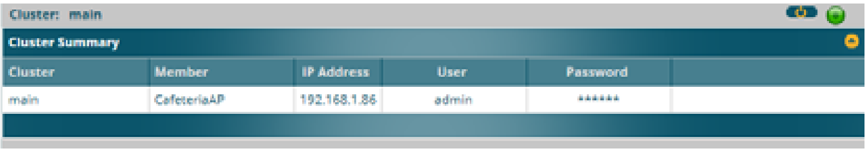
VLANs

Clusters

A WAO9122 cannot act as the Cluster controller. It will operate correctly as a member of a cluster.

Clusters allow you to configure multiple WAPs at the same time. Using WMI (or CLI), you may define a set of WAPs that are members of the cluster. Then you may enter Cluster mode for a selected cluster, which sends all successive configuration commands issued via CLI or WMI to all of the member WAPs. When you exit cluster mode, configuration commands revert to applying only to the WAP to which you are connected.

The Clusters window displays a summary of defined clusters and members.



Cluster: main

Cluster Summary

Cluster	Member	IP Address	User	Password
main	CafeteriaAP	192.168.1.86	admin	******

Figure 167. Clusters

Clusters are discussed in the following topics:

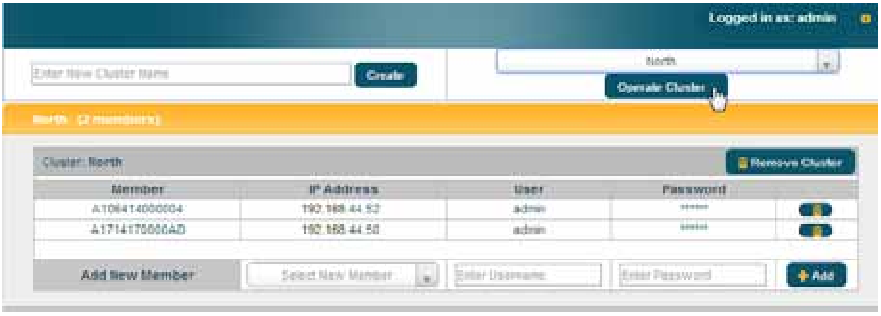
- **Cluster Management**

Cluster Management

A WAO9122 cannot act as the Cluster controller. It will operate correctly as a member of a cluster.

Clusters are displayed and managed in the single Cluster Management window. This window allows new clusters to be created and WAPs to be added or removed from clusters.

The Clusters window provides you with an overview of all clusters that have been defined for this WAP, and the WAPs that have been added to each. Clusters are listed and cluster members may be displayed by expanding a cluster entry. Each WAP entry displays its IP Address, Username, and Password. All existing clusters are shown, along with the number of WAPs currently in each. Up to 16 clusters may be created, with up to 50 WAPs in each.



Member	IP Address	User	Password
A106414000004	192.168.44.52	admin	******
A1714170006AD	192.168.44.50	admin	******

Figure 168. Cluster Management

Procedure for Managing Cluster Definition

1. **New Cluster Name:** Enter a name for the new cluster in the field to the left of the **Create** button, then click **Create** to add this entry. The new cluster is added to the list in the window.

2. **Delete**: To delete a cluster, expand the entry for the cluster and click its **Remove Cluster** button.

3. Click the **Save** button 💾 if you wish to make your changes permanent.

4. Expand the entry for a cluster to add or remove WAPs in the cluster.

Note that the WAP on which you are currently running WMI is not automatically a member of the cluster. If you would like it to be a member, you must add it explicitly.

Procedure for Managing Clusters

1. **Edit Cluster:** Expand the entry for the cluster to be managed. All of the WAPs already defined for this cluster are shown, and you may add additional WAPs to this list.
2. **Add New Member**: Select a new cluster member from the **Select New Member** drop-down list. This list shows APs that are accessible to this WAP for management purposes.
3. **User/Password**: In these columns, enter the administrator name and password for access to the WAP.
4. Click the **+Add** button to enter the WAP.
5. To delete a WAP, click its 🗑 button.
6. Click the **Save** button 💾 if you wish to make your changes permanent.

In Cluster Mode, all configuration operations that you execute in WMI or CLI are performed on the members of the cluster. They are **not** performed on the WAP where you are running WMI, unless it is a member of the cluster.

You must use the **Save** button 💾 at the top of configuration windows to permanently save your changes in Cluster Mode, just as you would in normal operation. When you are done configuring WAPs in the cluster, return to this window and click the ⏻ button to leave Cluster Mode.

Procedure for Operating in Cluster Mode

1. **Operate:** Select a defined cluster from the menu to the left of the **Operate Cluster** button and then click on the **Operate Cluster** button.
2. Select a WMI page for settings that you wish to configure for the cluster, and proceed to make the desired changes.
3. Proceed to any additional pages where you wish to make changes.

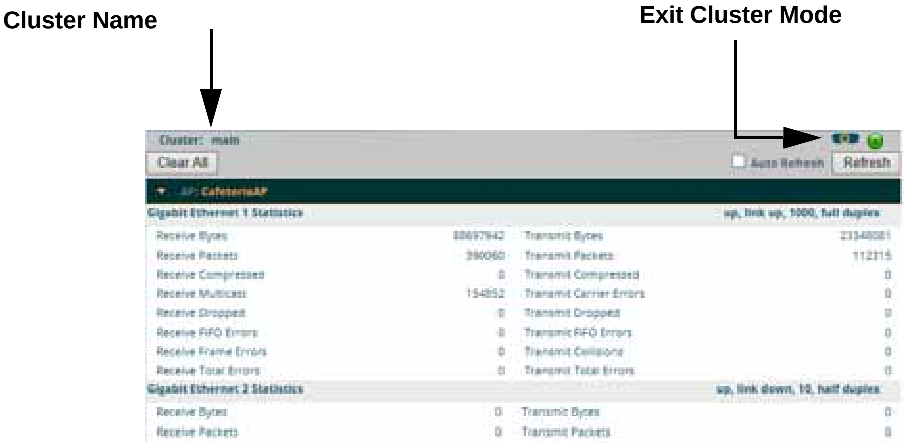
4. Some Status and Statistics windows will present information for all WAPs in the cluster.

5. Click the **Save** button when done if you wish to save changes on the cluster member WAPs.

6. **Exit:** Click the button to the right of the operating cluster to terminate Cluster Mode. The WMI returns to normal operation—managing only the WAP to which it is connected.

Status and Statistics Windows in Cluster Mode

In Cluster Mode, many of the Status and Statistics windows will display information for all of the members of the cluster. You can tell whether a window displays cluster information—if so, it will display the Cluster Name near the top, as shown in Figure 169.



Cluster: main

▼ AP: CafeteriaAP

Gigabit Ethernet 1 Statistics			**up, link up, 1000, full duplex**
Receive Bytes	88697942	Transmit Bytes	23348081
Receive Packets	390060	Transmit Packets	112315
Receive Compressed	0	Transmit Compressed	0
Receive Multicast	154852	Transmit Carrier Errors	0
Receive Dropped	0	Transmit Dropped	0
Receive FIFO Errors	0	Transmit FIFO Errors	0
Receive Frame Errors	0	Transmit Collisions	0
Receive Total Errors	0	Transmit Total Errors	0
Gigabit Ethernet 2 Statistics			**up, link down, 10, half duplex**
Receive Bytes	0	Transmit Bytes	0
Receive Packets	0	Transmit Packets	0

Figure 169. Viewing Statistics in Cluster Mode

You have the option to show aggregate information for the cluster members, or click the **Group by WAP** check box to separate it out for each WAP.

You may terminate cluster mode operation by clicking the ⏻ button to the right of the row.

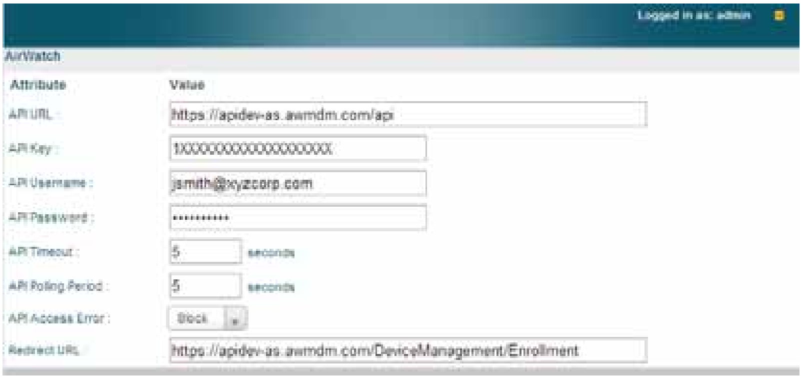
Mobile

Mobile Device Management (MDM) servers enable you to manage large-scale deployments of mobile devices. They may include capabilities to handle tasks such as enrolling devices in your environment, configuring and updating device settings over-the-air, enforcing security policies and compliance, securing mobile access to your resources, and remotely locking and wiping managed devices.

Avaya APs support the AirWatch MDM, using an AirWatch API call to determine the status of a user’s device and allow access to the wireless network only if the device is enrolled and compliant with the policies of the service.

AirWatch

Individual SSIDs may be configured to require AirWatch enrollment and compliance before a mobile device such as a smartphone or tablet is admitted to the wireless network. The WAP uses the AirWatch API with the settings below to request that AirWatch check whether the mobile device is enrolled and compliant with your wireless policies.



AirWatch

Attribute	Value
API URL :	https://apidev-as.awmdm.com/api
API Key :	1XXXXXXXXXXXXXXXXXXX
API Username :	jsmith@xyzcorp.com
API Password :	•••••••••••
API Timeout :	5 seconds
API Polling Period :	5 seconds
API Access Error :	Block
Redirect URL	https://apidev-as.awmdm.com/DeviceManagement/Enrollment

Figure 170. AirWatch Settings

Before configuring AirWatch settings on the WAP, you must have an AirWatch account, already set up with your organization’s compliance policies and other configuration as required by AirWatch.

The WAP settings entered on this page are mostly taken from AirWatch. Once you have entered these settings, your users will be constrained to follow a set of steps to access the wireless network, as described in "User Procedure for Wireless Access" on page 380.

Procedure for Managing AirWatch

If you have configured the **Mobile Device Management** setting on one or more SSIDs to use **AirWatch**, then the API specified below will be used to determine the admissibility of a mobile device requesting a connection to the wireless network.

1. **API URL**: Obtain this from your AirWatch server's **System / Advanced / Site URLs** page. Copy the **REST API URL** string into this field. This specifies the AirWatch API that the WAP will call to determine the enrollment and compliance status of a mobile device attempting to connect to the WAP. The steps that the user will need to take are described in "User Procedure for Wireless Access" on page 380.

2. **API Key**: Obtain this from your AirWatch server. Go to the **System / Advanced / API / REST** page, **General** tab, and copy the **API Key** string into this field. The key is required for access to the API.

3. **API Username**: Enter the user name for your account on the AirWatch server.

4. **API Password**: Enter the password for your account on the AirWatch server.

5. **API Timeout**: (seconds) If AirWatch does not respond within this many seconds, the request fails.

6. **API Polling Period**: (seconds) Mobile device enrollment and compliance status will be checked via polling at this interval. Note that there may thus be a delay before the mobile device will be admitted.

7. **API Access Error**: Specify whether or not to allow access if AirWatch fails to respond. The default is to **Block** access.

8. **Redirect URL**: Obtain this from your AirWatch server. Go to the **System / Advanced / Site URLs** page, and copy the **Enrollment URL** string into this field. When a mobile device that is not currently enrolled with AirWatch attempts to connect to the WAP, the device displays a page directing the user to install the AirWatch agent and go to the AirWatch enrollment page. Note that Android devices will need another form of network access (i.e. cellular) to download the agent, since un-enrolled devices will not have access to download it via the WAP. See "User Procedure for Wireless Access" on page 380 for more details.

9. You must configure the **Mobile Device Management** setting on one or more SSIDs to use **AirWatch**, as described in Procedure for Managing SSIDs (see Step 17 on page 260).

User Procedure for Wireless Access

1. A user attempts to connect a mobile device to an SSID that uses AirWatch.

2. The device will authenticate according to the SSID's authentication settings (Open, Radius MAC, 802.1x).

3. The user browses to any destination on the Internet.

   The WAP asks the user to wait while it checks device enrollment and compliance status by querying the AirWatch API with the device MAC address.

Device enrollment and compliance status will be checked via polling so there may be a delay before the device will be allowed in. That delay will depend on the API Polling Period setting.

4. If AirWatch responds that the device is enrolled and compliant, the device will be allowed into the network. The device will be considered compliant if AirWatch finds that the device does not violate any applicable policies for that device. (If no policies are assigned to the device in AirWatch, then the device is compliant by default.)

5. If the device is not enrolled, all user traffic will be blocked, except that HTTP traffic is redirected to an intermediate page on the WAP that tells the user to download and install the AirWatch agent. The page displays a link to the AirWatch-provided device enrollment URL. This link is a pass-though that allows the user to go through the enrollment process. The user will need to enter your organization's AirWatch Group ID and individual account credentials when requested.

   Once the agent is installed, the user must start again at Step 1.

   Android devices must go to the PlayStore to install the agent BEFORE they can go through the enrollment process. This means un-enrolled devices need another form of network access (i.e., cellular or an unrestricted SSID) to download this agent, as they are not permitted access to the PlayStore.

   Once the agent is installed, the user must start again at Step 1.

6. If the device is enrolled with AirWatch but not compliant with applicable policies, all traffic will be blocked as in Step 5 above, and the HTTP traffic will be redirected to an intermediate page on the WAP that tells the user which policies are out of compliance.

   This page contains a button for the user to click when the compliance issues have been corrected. This button causes AirWatch to again check device compliance. The user's browser is redirected to a “wait” page until the WAP has confirmed compliance with AirWatch. The user's browser is then redirected to a page announcing that the device is now allowed network access.

If the WAP is unable to access AirWatch to obtain enrollment and compliance status (for example, due to bad credentials, timeout, etc.), device access to the network will be granted according to the **API Access Error** setting (**Allow** or **Block**). If this field is set to **Block**, traffic will be blocked as in Step 5 above and HTTP traffic will be redirected to an informational page that informs the user that AirWatch cannot be contacted at this time and advises the user to contact the network administrator. If this field is set to **Allow**, then the device will be allowed network access.

Using Tools on the WAP

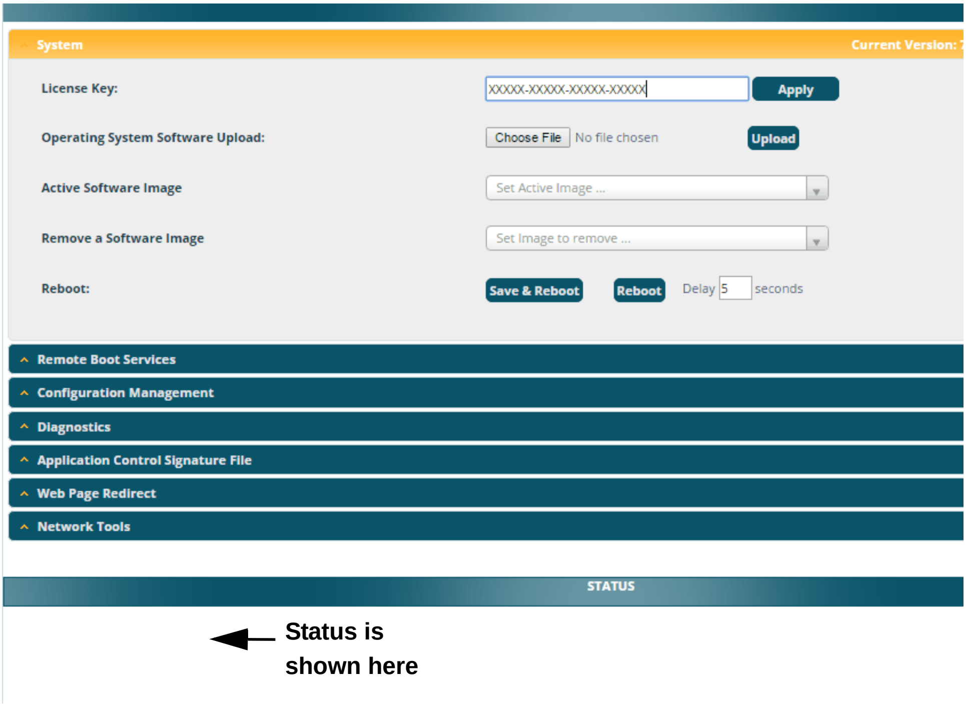
These WMI windows allow you to perform administrative tasks on your WAP, such as upgrading software, rebooting, uploading and downloading configuration files, and other utility tasks. Tools are described in the following sections:

- **“System Tools” on page 384**
- **“CLI” on page 398**
- **“API Documentation” on page 400**
- **“Options” on page 405**
- **“Logout” on page 406**

This section does not discuss using status or configuration windows. For information on those windows, please see:

- **“Viewing Status on the WAP” on page 77**
- **“Configuring the WAP” on page 141**

System Tools



License Key: XXXXX-XXXXX-XXXXX-XXXXX

Operating System Software Upload:

Active Software Image

Remove a Software Image

Reboot: Delay 5 seconds

Status is shown here

Figure 171. System Tools

This window allows you to manage files for software images, configuration, and Web Page Redirect (WPR), manage the system's configuration parameters, reboot the system, and use diagnostic tools. The page contains a number of sections that you may expand.

About Licensing and Upgrades

If you are a customer using WOS, when you upgrade a WAP using WOS, your license will automatically be updated for you first.

The WAP's license determines some of the features that are available on the WAP. For example, the Application Control feature is an option that must be separately licensed. To check the features supported by your license, see "Access Point

Information" on page 83. If you need a new license for a new feature, refer to "Licensing" on page 61 to obtain the extended license.

"Configuration Management" on page 389. *Procedure for Configuring System Tools*

These tools are broken down into the following sections:

- **System**
- **Remote Boot Services**
- **Configuration Management**
- **Diagnostics**
- **Application Control Signature File Management**
- **Web Page Redirect (Captive Portal)**
- **Network Tools**
- **Progress Bar and Status Frame**

System

Note that the top line of this section shows the current software version running on the WAP. See Figure 171.

1. **License Key**

   If you need an updated license (for example, if you are upgrading an AP to a new major release—say, from 7.0 to 7.1, and you are not using WOS to perform network-wide updates), you may obtain one through **Auto-provisioning**. See "Configuration Management" on page 389.

   If you need to enter a new license key manually, use the **License Key** field to enter it, then click the **Apply** button to the right.

   A valid license is required for WAP operation, and it controls the features available on the WAP. If you upgrade your WAP for additional features, you will be provided with a license key to activate those capabilities.

   A license update will automatically save a copy of the current configuration of the WAP. See Step 3 on page 389.

If you attempt to enter an invalid key, you will receive an error message and the current key will not be replaced.

2. **Operating System Software Upload**: This feature upgrades the Avaya OS to a newer version provided by Avaya. Avaya WAP models come with factory installed licenses and do not require a license upgrade to do a software upgrade. See "Licensing" on page 61.

9170 Series WAPs must run AvayaOS Release 7.2 or above. Do not attempt to downgrade them to an earlier release.

Click the **Choose File** button to locate the software upgrade file, then click on the **Upload** button to upload the new file to the WAP. Progress of the operation will be displayed in a progress bar. Completion status of the operation is shown in the **Status** section.

This operation does not run the new software or change any configured values. The existing software continues to run on the WAP until you reboot, at which time the uploaded software will be used. An upgrade will, however, automatically save a copy of the current configuration of the WAP. See Step 3 on page 389.

*If you have difficulty upgrading the WAP using the WMI, see **"Upgrading the WAP Using the Boot Loader" on page 506** for a lower-level procedure you may use.*

*Software Upgrade always uploads the file in binary mode. If you transfer any image file to your computer to have it available for the Software Upgrade command, it is **critical** to remember to transfer it (ftp, tftp) in **binary** mode!*

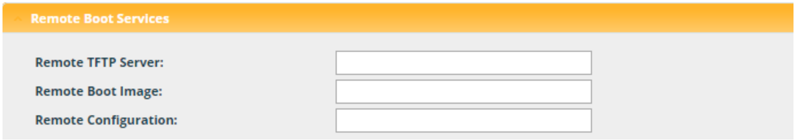
3. **Active Software Image**: Use the **Set Active Image** drop-down list to display all of the software versions that are on your WAP. Select the version from the list that you would like to become the active version the next time that you reboot.

4. **Remove a Software Image**: Use the **Set Image to remove** drop-down list to display all of the software versions that are on your WAP. Select a version from the list to remove it. *Note that there is no Apply button for this—the image is removed with no further action on your part.*

5. **Save & Reboot** or **Reboot**: Use **Save & Reboot** to save the current configuration and then reboot the WAP. The WAP will reboot using the software version that you have selected in **Active Software Image**, above. The LEDs on the WAP indicate the progress of the reboot, as described in "Powering Up the WAP" on page 55. Alternatively, use the **Reboot** button to discard any configuration changes which have not been saved since the last reboot. You may specify an optional **Delay** period in seconds to wait before the reboot starts.

Remote Boot Services

(Automatic updates from remote image or configuration file)



Remote TFTP Server:

Remote Boot Image:

Remote Configuration:

Figure 172. Remote Boot Services

The WAP software image or configuration file can be downloaded from an external server. In large deployments, all WAPs can be pointed to one TFTP server instead of explicitly initiating software image uploads to all WAPs. When the WAP boots, the WAP will download the software image from the specified TFTP server. Similarly, if you decide to change a setting in the WAPs, you can simply modify a single configuration file. After the WAPs are rebooted, they will automatically download the new configuration file from a single location on the specified TFTP server.

1. **Remote TFTP Server**: This field defines the path to a TFTP server to be used for automated remote update of software image and configuration files when rebooting. You may specify the server using an IP address or host name.

2. **Remote Boot Image**: When the WAP boots up, it fetches the software image file specified here from the TFTP server defined above, and upgrades to this image before booting. This must be a WAP image file with a **.bin** extension.

   Make sure to place the file on the TFTP server. If you disable the remote boot image (by blanking out this field) or if the image can't be transferred, the WAP will fall back to booting whatever image is on the compact flash.

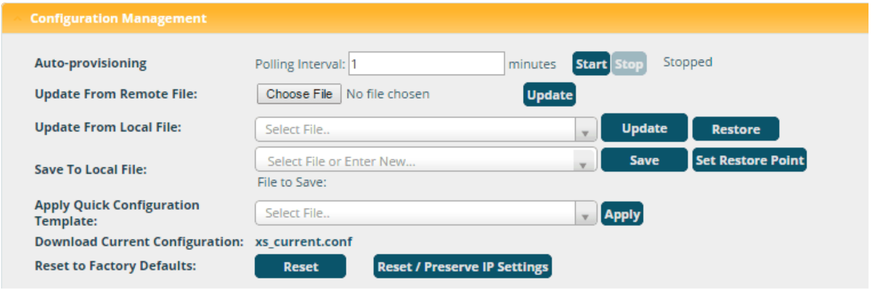
   The Remote Boot Image or Remote Configuration update happens every time that the WAP reboots. If you only want to fetch the remote image or configuration file one time, be sure to turn off the remote option (blank out the field on the System Tools page) after the initial download. When a remote boot image is used, the image is transferred directly into memory and is never written to the compact flash.

3. **Remote Configuration:** When the WAP boots up, it fetches the specified configuration file from the TFTP server defined above, and applies this configuration **after** the local configuration is applied. The remote configuration must be a WAP configuration file with a **.conf** extension. Make sure to place the file on the TFTP server.

   A partial configuration file may be used. For instance, if you wish to use a single configuration file for all of your WAPs but don't want to have the same IP address for each WAP, you may remove the **ipaddr** line from the file. You can then load the file on each WAP and the local IP addresses will not change.

   A remote configuration is never saved to the compact flash unless you issue a Save command.

Configuration Management



Auto-provisioning: Polling Interval: 1 minutes Stopped

Update From Remote File: No file chosen

Update From Local File: Select File..

Save To Local File: Select File or Enter New... File to Save:

Apply Quick Configuration Template: Select File..

Download Current Configuration: xs_current.conf

Reset to Factory Defaults:

Figure 173. Configuration Management

1. If you need an updated license, you may obtain one through **Auto-provisioning**. Click the **Start** button, and the WAP will contact the Avaya server with its serial number and MAC address to obtain and install its latest license. If the WAP is unable to access the activation server, it will continue to attempt to contact the server at intervals specified by the **Polling Interval** (the default value is one minute). Click the **Stop** button if you wish to stop contacting the server.

2. **Update from Remote File**: This field allows you to define the path to a configuration file (one that you previously saved—see Step 4 and Step 6 below). Click on the **Browse** button if you need to browse for the location of the file, then click **Update** to update your configuration settings.

3. **Update from Local File**: This field updates WAP settings from a local configuration file on the WAP. Select one of the following files from the drop-down list:

   - **factory.conf**: The factory default settings.
   - **lastboot.conf**: The setting values from just before the last reboot.
   - **saved.conf**: The last settings that were explicitly saved using the **Save** button at the top of each window.
   - **history/saved-yyyymmdd-pre-update.conf**: **history/saved-yyyymmdd-post-update.conf**:

Two files are automatically saved for a software upgrade or for a license change (including the setting values from just before the upgrade/change was performed, and the initial values afterward. The filename includes the date.

- **history/saved-yyyymmdd-auto.conf**: Each time you use the **Save** button, an “auto” file is saved with the settings current at that time.
- **history/saved-yyyymmdd-pre-reset.conf**:
  history/saved-yyyymmdd-post-reset.conf:

  Each time you use one of the **Reset to Factory Default** buttons, two files are saved: the setting values from just before the reset, and the initial values afterward. The filename includes the reset date.
- **history/saved-yyyymmdd-hhmm.conf**: The setting values that were explicitly saved using the **Set Restore Point** button (see Step 4 below).

Click **Update** to update your configuration settings by appending to the current WAP configuration. Click **Restore** to replace the WAP configuration with the configuration file selected.

Note that the History folder allows a maximum of 16 files. The oldest file is automatically deleted to make room for each new file.

4. **Save to Local File**: There are a few options for explicitly requesting the WAP to save your current configuration to a file on the WAP:

   - To view the list of configuration files currently on the WAP, click the down arrow to the right of this field. If you wish to replace one of these files (i.e., save the current configuration under an existing file name), select the file, then click **Save**. Note that you cannot save to the file names f**actory.conf**, **lastboot.conf**, and **saved.conf -** these files are write-protected.
   - You may enter the desired file name, then click **Save**.
   - Click **Set Restore Point** to save a copy of the current configuration, basing the file name on the current date and time. For example:

     history/saved-20100318-1842.conf

Note that the configuration is automatically saved to a file in a few situations, as described in Step 3 above.

✍ ***Important!*** *When you have initially configured your WAP, or have made significant changes to its configuration, we strongly recommend that you save the configuration to a file in order to have a safe backup of your working configuration.*

5. **Apply Quick Configuration Template:** This offers predefined configuration options such as **Classroom** and **High-Density** that capture best practices from years of field experience. If one of the options in the drop-down list is appropriate to your deployment, select it and click **Apply**. For example, the **High-Density** option uses best practices to configure the WAP for high density settings such as lecture halls, convention centers, stadiums, etc.

6. **Download Current Configuration:** Click on the link titled **current.conf** to download the WAP's current configuration settings to a file (that you can upload back to the WAP at a later date). The system will prompt you for a destination for the file. The file will contain the WAP's current configuration values.

7. **Reset to Factory Defaults**: Click on the **Reset/Preserve IP Settings** button to reset the system's current configuration settings to the factory default values, *except for the WAP's management IP address which is left unchanged.* This function allows you to maintain management connectivity to the WAP even after the reset. This will retain the Gigabit Ethernet port's IP address (see "Interfaces" on page 150), or if you have configured management over a VLAN it will maintain the management VLAN's IP address (see "VLAN Management" on page 194). *All other previous configuration settings will be lost.*

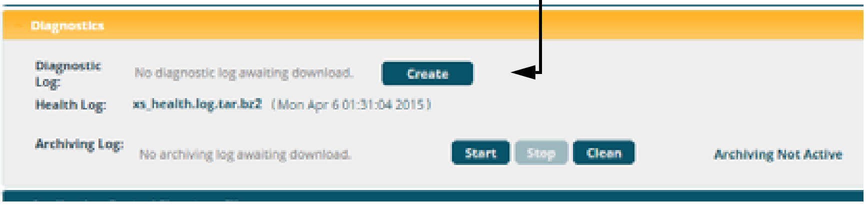
   Click **Reset** to reset all of the system's current configuration settings to the factory default values, including the management IP address—*all previous configuration settings will be lost*. The WAP's Gigabit Ethernet ports default to using DHCP to obtain an IP address.

If the IP settings change, the connection to the WMI may be lost.

Diagnostics

8. **Diagnostic Log**: Click the **Create** button to update the WAP information for use by Avaya Customer Support personnel. The name of the log file ends with `diagnostic.log`, and may have an additional prefix. (Figure 174)

Click Create to update log



Diagnostics

Diagnostic Log: No diagnostic log awaiting download.

Health Log: xs_health.log.tar.bz2 (Mon Apr 6 01:31:04 2015)

Archiving Log: No archiving log awaiting download.

Archiving Not Active

Figure 174. Saving the Diagnostic Log

This feature is only used at the request of Customer Support. It saves all of the information regarding your WAP, including status, configuration, statistics, log files, and recently performed actions.

The diagnostic log is always saved on your `C:\` drive, so you should immediately rename the file to save it. This way, it will not be lost the next time you save a diagnostic log. Often, Customer Support will instruct you to save two diagnostic logs about ten minutes apart so that they can examine the difference in statistics between the two snapshots (for example, to see traffic and error statistics for the interval). Thus, you must rename the first diagnostic log file.

All passwords are stored on the WAP in an encrypted form and will not be exposed in the diagnostic log.

9. **Health Log**: This file is created automatically when the WAP encounters an unexpected situation, although often, the problem (if any) is minor. Typically, this file will not exist. The Diagnostic Log **Update** button has no effect on this file whatsoever. When a health log exists, the filename **health.log.bz2** is displayed in blue and provides a link to the log file. This file is normally only used at the request of Customer Support.

10. **Archiving Log**: This log saves internal status information that may be needed by Avaya Customer Support personnel. Click the **Start** button to start accumulating this information. The size of the file is self-limiting so that you do not need to be concerned about it consuming too much storage space. Click the **Stop** button to stop accumulating data and make it available in a tar file, named `engineeringlogs_<hostname>.tar`. A link to this tar file appears. Click it to download the file. If you wish to click the **Start** button again to accumulate data for a later time interval, you should first download and rename the current file before it gets overwritten.

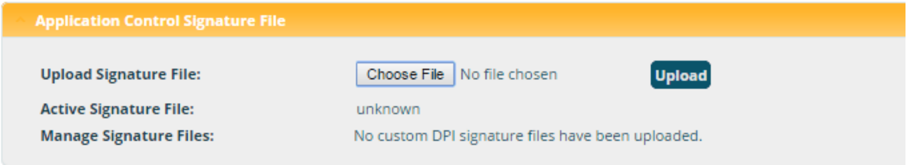
    You may use the **Clear** button to remove the tar file and all temporary data from the WAP's memory.

    This feature should only used at the request of Customer Support.

Application Control Signature File Management

Application Control recognizes applications using a file containing the signatures of hundreds of applications. This file may be updated regularly to keep up as Internet usage evolves over time. The latest signature file is available from the same location that you use to download the latest Avaya OS release. Note that new Avaya OS releases will automatically contain the latest signature file available at the time of the build.

See "Application Control Windows" on page 130 for more information about using Application Control.



Application Control Signature File

Upload Signature File: Choose File No file chosen Upload

Active Signature File: unknown

Manage Signature Files: No custom DPI signature files have been uploaded.

Figure 175. Managing Application Control Signature files

11. **Upload Signature File**: First, download the latest signature file from the Avaya Customer Support site to your file system. Click the **Browse** button, then browse to locate the new signature file. Click the **Upload** button when it appears. The new file will be uploaded to the WAP and will be used for identifying applications. **You must turn Application Control off and back on again** on the Filter Lists page to make the new signature file take effect. See "Filter Lists" on page 364. No reboot is required.

    Active Signature File shows which file is currently being used by Application Control. If you have installed any custom DPI signature files, you may use **Manage Signature Files**.

Web Page Redirect (Captive Portal)

The WAP uses a Perl script and a cascading style sheet to define the default splash/login Web page that the WAP delivers for WPR. You may replace these files with files for one or more custom pages of your own. See Step 14 below to view the default files. See Step 15 page 259 for more information about WPR and how the splash/login page is used.

Each SSID that has WPR enabled may have its own page. Custom files for a specific SSID **must** be named based on the SSID name. For example, if the SSID is named **Public**, the default `wpr.pl` and `hs.css` files should be modified as desired and renamed to `wpr-Public.pl` and `hs-Public.css` before uploading to the WAP. If you modify and upload files named `wpr.pl` and `hs.css`, they will replace the factory default files and will be used for any SSID that does not have its own custom files, per the naming convention just described. Be careful not to replace the default files unintentionally.

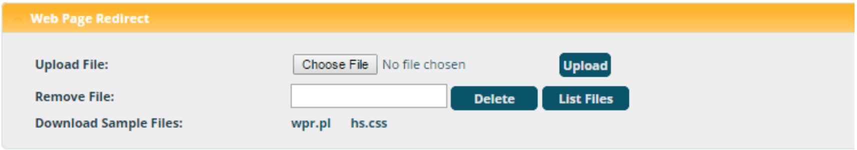


Figure 176. Managing WPR Splash / Login page files

12. **Upload File**: Use this to install files for your own custom WPR splash / login page (as described above) on the WAP. Note that uploaded files are not immediately used - you must reboot the WAP first. At that time, the WAP looks for and uses these files, if found.

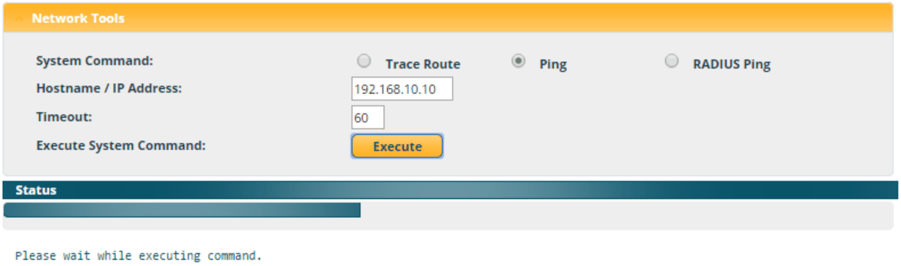
    Click **Choose File** to locate the splash / login page files, then click on the **Upload** button to upload the new files to the WAP. You must reboot to make your changes take effect.

13. **Remove File**: Enter the name of the WPR file you want to remove, then click on the **Delete** button. You can use the **List Files** button to show you a list of files that have been saved on the WAP for WPR. The list is displayed in the **Status** section at the bottom of the WMI window. You must reboot to make your changes take effect.

14. **Download Sample Files**: Click on a link to access the corresponding sample WPR files:

    - **wpr.pl**—a sample Perl script.
    - **hs.css**—a sample cascading style sheet.

Network Tools



Network Tools

System Command: ○ Trace Route ● Ping ○ RADIUS Ping

Hostname / IP Address: 192.168.10.10

Timeout: 60

Execute System Command: Execute

Status

```
Please wait while executing command.
```

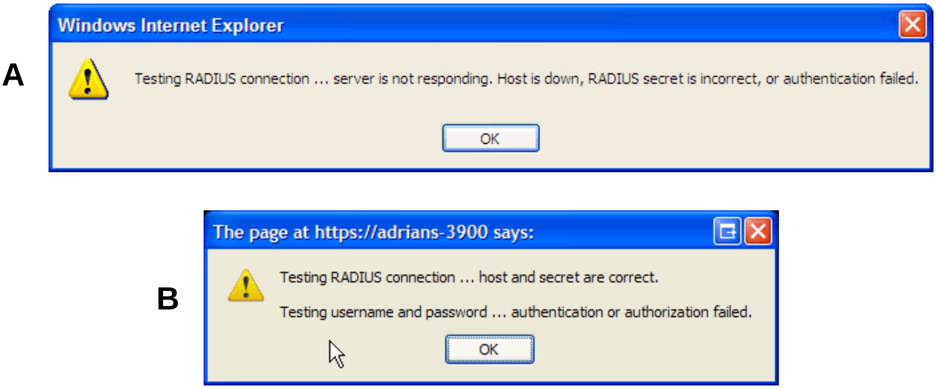
Figure 177. System Command (Ping)

15. **System Command**: Choose **Trace Route**, **Ping**., or **RADIUS Ping**. For Trace Route and Ping, fill in **IP Address** and **Timeout**. Then click the **Execute** button to run the command.

    The RADIUS Ping command is a simple utility that tests connectivity to a RADIUS server by attempting to log in with the specified Username and Password. When using a RADIUS server, this command allows you to verify that the server configuration is correct and whether a particular Username and Password are set up properly. If a client is having trouble accessing the network, you can quickly determine if there is a basic RADIUS problem by using the RADIUS Ping tool. For example, in Figure 178 (A), RADIUS Ping is unable to contact the server. In Figure 178 (B), RADIUS Ping verifies that the host information and secret for a RADIUS server are correct, but that the user account information is not.

    Select RADIUS allows you to select a RADIUS server that you have already configured. When you make a choice in this field, additional fields will be displayed. Set **Select RADIUS** to External Radius, Internal Radius, or a server specified for a particular SSID, or select **Other Server** to specify another server by entering its **Host** name or IP address, **Port**, and shared **Secret**.

    Enter the **RADIUS Credentials**: **Username** and **Password**. Select the **Authentication Type**, **PAP** or **CHAP**. Click the **Execute** button to run the command. The message **Testing RADIUS connection** appears. Click **OK** to proceed.


A
Windows Internet Explorer
OK
B
The page at https://adrians-3900 says:
OK

Testing RADIUS connection ... server is not responding. Host is down, RADIUS secret is incorrect, or authentication failed.

Testing RADIUS connection ... host and secret are correct.

Testing username and password ... authentication or authorization failed.

Figure 178. Radius Ping Output

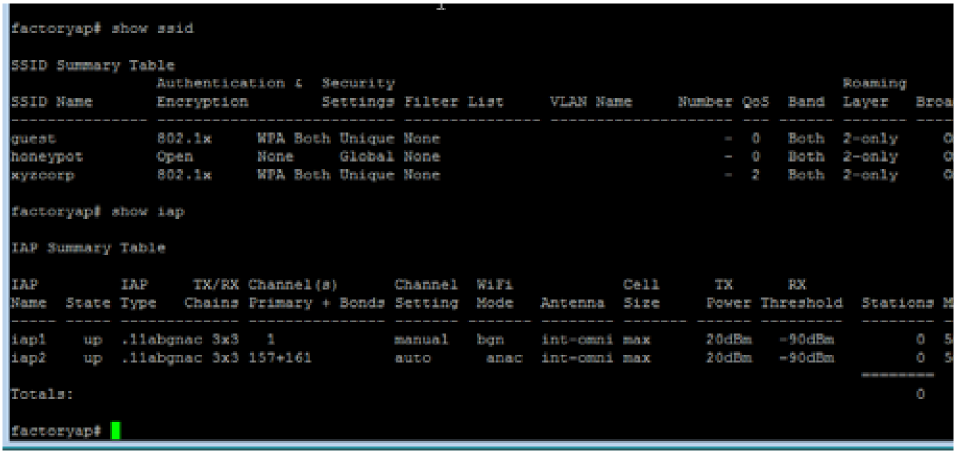
16. **IP Address**: For Ping or Trace Route, enter the IP address of the target device.
17. **Timeout**: For Ping or Trace Route, enter a value (in seconds) before the action times out.
18. **Execute System Command**: Click **Execute** to start the specified command. Progress of command execution is displayed in the **Progress** frame. Results are displayed in the **Status** frame.

Progress Bar and Status Frame

The **Progress** bar is displayed for commands such as Software Upgrade and Ping. The **Status** frame presents the output from system commands (Ping and Trace Route), as well as other information, such as the results of software upgrade.

CLI

The WMI provides this window to allow you to use the WAP's Command Line Interface (CLI). You can enter commands to configure the WAP, or display information using show commands. You will not need to log in - you already logged in to the WAP when you started the WMI.



```
factoryap# show ssid

SSID Summary Table
                Authentication &  Security                                                   Roaming
SSID Name       Encryption        Settings Filter List     VLAN Name         Number QoS  Band  Layer    Broa
--------------- ----------------------------- --------------- -------------------- --- ------ ------- ----
guest           802.1x     WPA Both Unique None                                   -  0    Both  2-only     O
honeypot        Open       None     Global None                                   -  0    Both  2-only     O
xyzcorp         802.1x     WPA Both Unique None                                   -  2    Both  2-only     O

factoryap# show iap

IAP Summary Table

IAP         IAP     TX/RX Channel(s)       Channel  WiFi               Cell        TX      RX
Name  State Type    Chains Primary + Bonds Setting  Mode    Antenna    Size       Power Threshold  Stations M
----- ----- --------------- ---------------- -------- ------- -------- -------- ------ ---------  -------- -
iap1    up  .11abgnac 3x3   1              manual   bgn     int-omni max        20dBm   -90dBm          0  5
iap2    up  .11abgnac 3x3 157+161          auto       anac  int-omni max        20dBm   -90dBm          0  5
                                                                                                  --------
Totals:                                                                                                 0

factoryap# 
```

Figure 179. CLI Window

To enter a command, simply type it in. The command is echoed and output is shown in the normal way—that is, the same way it would be if you were using the CLI directly. You may use the extra scroll bar inside the right edge of the window to scroll through your output. If output runs past the right edge of the screen, there is also a horizontal scroll bar at the bottom of the page.

This window has some minor differences, compared to direct use of the CLI via the console or an SSH connection:

- The CLI starts in **config** mode. All configuration and show commands are available in this mode. You can "drill down" the mode further in the usual way. For example, you can type **interface radio** to change the mode to **config-radio**. The prompt will indicate the current command mode, for example:

```
My-WAP(config-radio) #
```

- You can abbreviate a command and it will be executed if you have typed enough of the command to be unambiguous. The command will not auto-complete, however. Only the abbreviated command that you actually typed will be shown. You can type a partial command and press Tab to have the command auto-complete. If the partial command is ambiguous a list of legal endings is displayed.
- Entering **quit** will return you to the previously viewed WMI page.
- Most, but not all, CLI commands can be run in this window. Specifically the **run-test** menu of commands is **not** available in this window. To use the run-test command, please connect using SSH and use CLI directly, or use the System Tools described in this chapter, such as Trace Route, Ping, and RADIUS Ping.

Help commands (the **?** character) are available, either at the prompt or after you have typed part of a command.

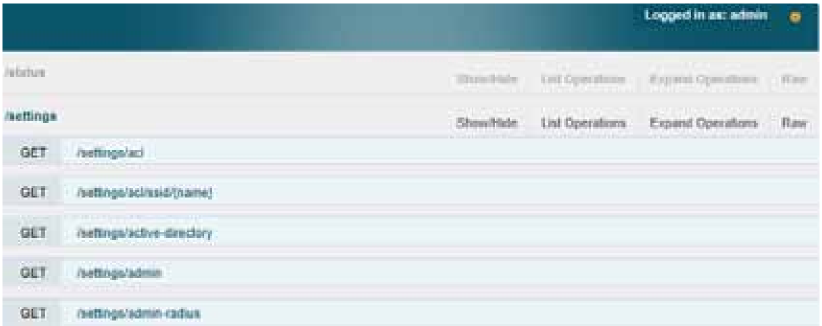
API Documentation

WAPs provide an API interface conforming to the RESTful API model. Developers may use this read-only API to read status, statistics, and settings from the WAP. The interactive API Documentation page provides documentation for the API.

You may use the WAP's API for purposes such as integrating with third party applications or creating your own applications for network monitoring and analysis. Using the RESTful API eliminates the need to use CLI scripting, or to use SNMP which can be cumbersome for polling large amounts of data. Results are returned in JavaScript Object Notation (JSON) format, a text-based open standard designed for human-readable data interchange. The API documentation is tightly integrated with the server code. The API Documentation page allows you to interact with the API in a sandbox UI that gives clear insight into how the API responds to parameters and options.

Security for the API is provided with OAuth, as described in "OAuth 2.0 Management" on page 244. Once registration is complete and a permanent token for this WAP has been obtained, your application may access the RESTful API using the **client_id** and the **token** at the following URL:

```
https://[WAP hostname or IP address]/api/v3/[api-name]
```



GET /settings/acl
GET /settings/acl/ssid/{name}
GET /settings/active-directory
GET /settings/admin
GET /settings/admin-radius

Figure 180. API Documentation

The API Documentation page lists all of the APIs that are available, lists their calling parameters, if any, and allows you to perform sample calls and view sample output.

Status/Settings

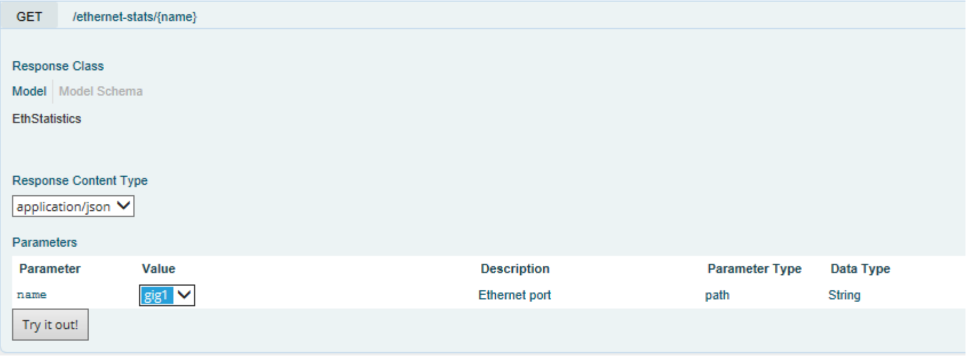
The RESTful API on the WAP is broken into these two main headings: **status** and **settings**. Each is a node that may be clicked to expand or collapse the list of corresponding API requests available on the WAP. Since this is a read-only API, the list consists exclusively of GET operations.

The figure below shows part of the list displayed by clicking **/settings**. Click again to collapse (hide) the list.

Status requests include **GET** requests for many of the status and statistics items described in the chapter titled, “Viewing Status on the WAP” on page 77. **Settings** requests include **GET** requests for many of the settings described in the chapter titled, “Configuring the WAP” on page 141

GET Requests

Each request name in the list is a link. Click it to see more information and to try the API and see its output.



EthStatistics

application/json

Parameter	Value	Description	Parameter Type	Data Type
name	gig1	Ethernet port	path	String

Figure 181. API — GET Request Details

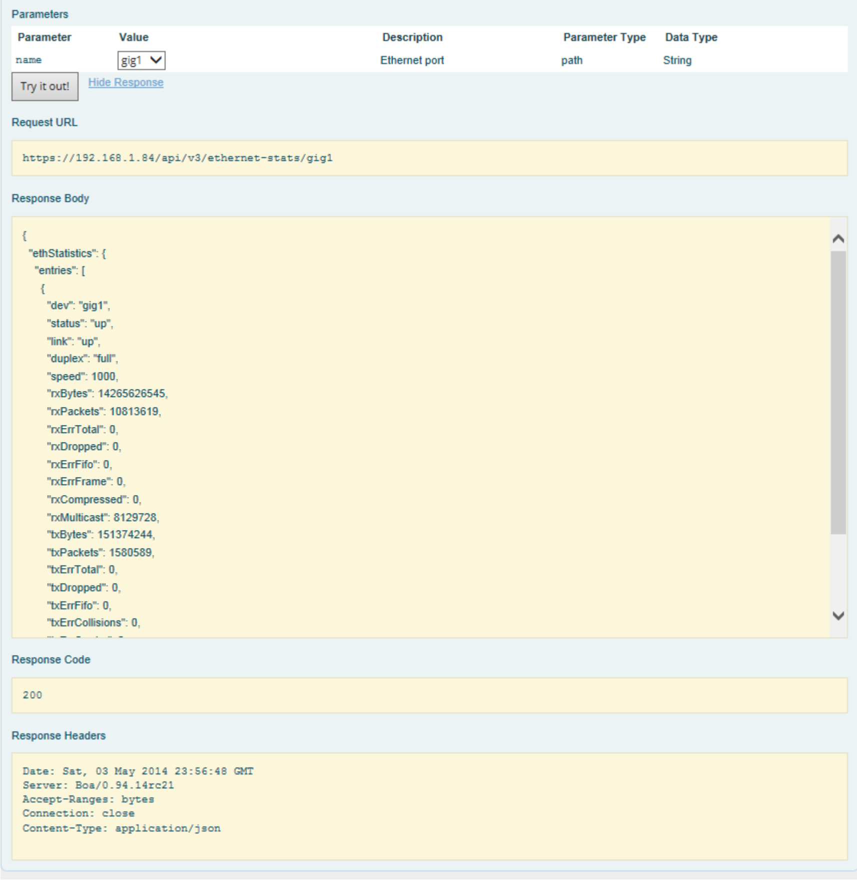
The figure above shows the GET request for **ethernet-stats{name}**. Click again to collapse (hide) the API details.

High-level details are shown, including the **Response Class** name and the **Response Content Type** (limited to JSON at this time).

Trying a GET Request

The **Try it out!** button allows you to send the GET request to the WAP API and see its response. Developers can use this feature to design and implement applications that use this response.

Enter any necessary **Parameters** and click the **Try it out!** button. Most GET requests do not use any parameters. If they are required, their names will be listed and there will be a field or a drop-down list to specify each one. An example is shown in Figure 181. In some cases, there may be two versions of a request, with and without parameters. For example, **GET /ethernet-stats/{name}** returns status and statistics for a particular Ethernet port, while **GET /ethernet-stats/** returns information for all Ethernet ports.



Parameters

Parameter	Value	Description	Parameter Type	Data Type
name	gig1	Ethernet port	path	String

Request URL

```
https://192.168.1.84/api/v3/ethernet-stats/gig1
```

Response Body

```
{
 "ethStatistics": {
  "entries": [
   {
    "dev": "gig1",
    "status": "up",
    "link": "up",
    "duplex": "full",
    "speed": 1000,
    "rxBytes": 14265626545,
    "rxPackets": 10813619,
    "rxErrTotal": 0,
    "rxDropped": 0,
    "rxErrFifo": 0,
    "rxErrFrame": 0,
    "rxCompressed": 0,
    "rxMulticast": 8129728,
    "txBytes": 151374244,
    "txPackets": 1580589,
    "txErrTotal": 0,
    "txDropped": 0,
    "txErrFifo": 0,
    "txErrCollisions": 0,
```

Response Code

```
200
```

Response Headers

```
Date: Sat, 03 May 2014 23:56:48 GMT
Server: Boa/0.94.14rc21
Accept-Ranges: bytes
Connection: close
Content-Type: application/json
```

Figure 182. API — GET Request Response

The figure above shows the response for **ethernet-stats{name}**. The response is produced in the human-readable JSON format. The status and statistics data shown are as described in “Viewing Status on the WAP” on page 77. Click **Hide Response** if you wish to hide the output.

The **Response Code** and the **Response Header** are standard for HTTP(S).

API Documentation Toolbar

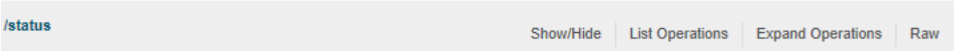


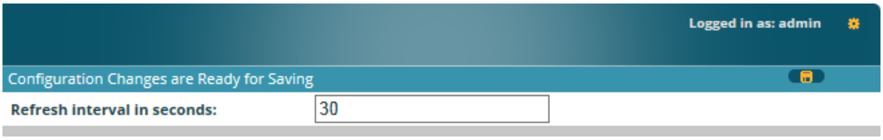
Figure 183. API Documentation Toolbar

The Status and Settings sections each have a toolbar as shown above, offering the following options.

- **Show/Hide**—expands or collapses this list of GET requests. Hiding and then showing again displays the requests as they were before, i.e., expanded GET requests will still be expanded when displayed again.
- **List Operations**—expands this list of GET requests. Each individual entry is collapsed.
- **Expand Operations**—shows all of the GET requests in this list. Each individual entry is expanded.
- **Raw**—shows the source XML code for this list of GET requests. Click the link for the API Documentation page again to return to the normal display.

Options

This window allows you to customize the behavior of the WMI.



Configuration Changes are Ready for Saving

Refresh interval in seconds: 30

Figure 184. WMI Display Options

Procedure for Configuring Options

1. **Refresh Interval in Seconds**: Many of the windows in the Status section of the WMI have an Auto Refresh option. You may use this setting to change how often a status or statistics window is refreshed, if its auto refresh option is enabled. Enter the desired number of seconds between refreshes. The default refresh interval is 30 seconds.

Logout

Click on the Logout button to terminate your session. When the session is terminated, you are presented with the login window.

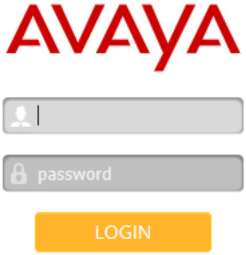


Figure 185. Login Window

The Command Line Interface

This section covers the commands and the command structure used by the WAP's Command Line Interface (CLI), and provides a procedure for establishing an SSH connection to the WAP. Topics discussed include:

Some commands are only available if the WAP's license includes appropriate features or if the WAP model supports it. If a command is unavailable, an error message will notify you. See "Licensing" on page 61.

See Also

Ongoing Management

Network Map

System Tools

Establishing a Secure Shell (SSH) Connection

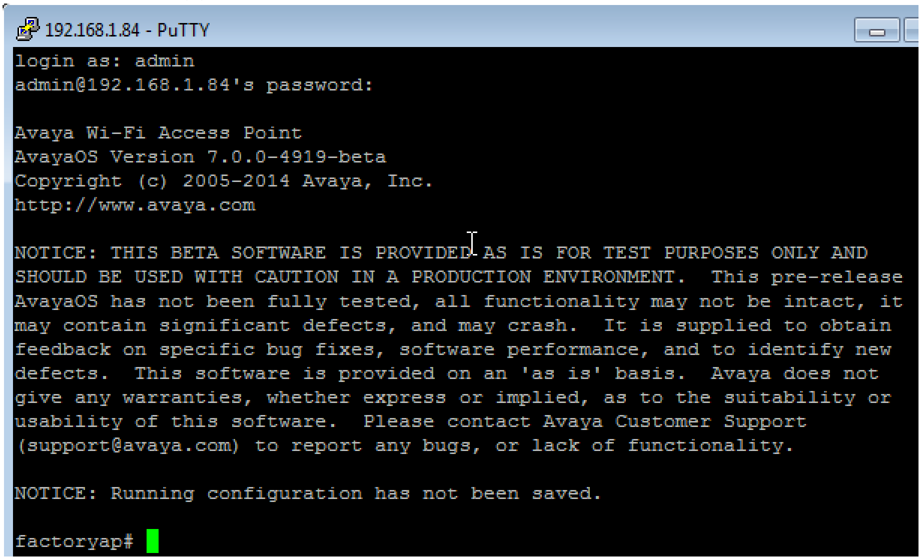
Use this procedure to initialize the system and log in to the Command Line Interface (CLI) via a Secure Shell (SSH) utility, such as PuTTY. When connecting to the unit's Command Line Interface over a network connection, you must use a Secure SHell version 2 (SSH-2) utility. Make sure that your SSH utility is set up to use SSH-2.

1. Start your SSH session and communicate with the WAP via its IP address.

   - If the WAP is connected to a network that uses DHCP, use the address assigned by DHCP. We recommend that you have the network administrator assign a reserved address to the WAP for ease of access in the future.

- If the network does not use DHCP, use the factory default address 192.168.1.3 to access either the Gigabit 1 or Gigabit 2 Ethernet port. You may need to change the IP address of the port on your computer that is connected to the WAP—change that port's IP address so that it is on the same 192.168.1.xx subnet as the WAP port.

2. At the login prompt, enter your user name and password (the default for both is **admin**). Login names and passwords are case-sensitive. You are now logged in to the WAP's Command Line Interface.



```
login as: admin
admin@192.168.1.84's password:

Avaya Wi-Fi Access Point
AvayaOS Version 7.0.0-4919-beta
Copyright (c) 2005-2014 Avaya, Inc.
http://www.avaya.com

NOTICE: THIS BETA SOFTWARE IS PROVIDED AS IS FOR TEST PURPOSES ONLY AND
SHOULD BE USED WITH CAUTION IN A PRODUCTION ENVIRONMENT.  This pre-release
AvayaOS has not been fully tested, all functionality may not be intact, it
may contain significant defects, and may crash.  It is supplied to obtain
feedback on specific bug fixes, software performance, and to identify new
defects.  This software is provided on an 'as is' basis.  Avaya does not
give any warranties, whether express or implied, as to the suitability or
usability of this software.  Please contact Avaya Customer Support
(support@avaya.com) to report any bugs, or lack of functionality.

NOTICE: Running configuration has not been saved.

factoryap#
```

Figure 186. Logging In

Getting Started with the CLI

The root command prompt (**Root Command Prompt**) is the first prompt you see after logging in to the CLI. If you are at a level other than the root command prompt you can return to this prompt at any time by using the **exit** command to step back through each command prompt level. The root command prompt you see in the CLI window is determined by the host name you assigned to your WAP. The prompt **factoryap** is displayed throughout this document simply as a sample host name assigned to the WAP. To terminate your session at any time, use the **quit** command.

Entering Commands

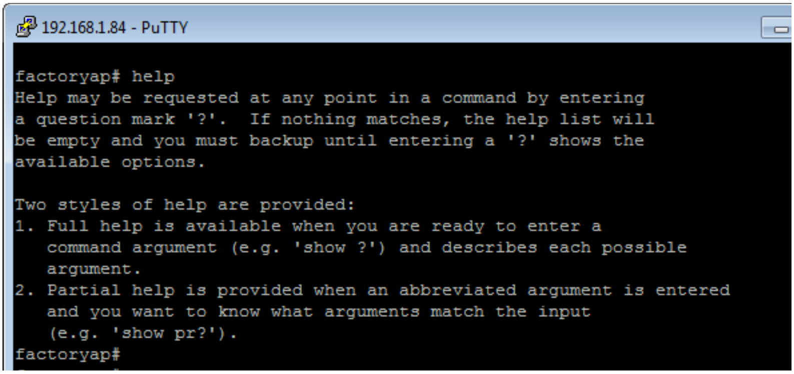
When typing commands, you need only type enough characters to uniquely specify the command. For example, you can type the abbreviated term **config** to access the configure prompt, or even simply type **c**, since no other top level command starts with “c”.

Getting Help

The CLI offers the following two levels of assistance:

- help Command

The **help** command is only available at the root command prompt. Initiating this command generates a window that provides information about the types of help that are available with the CLI.

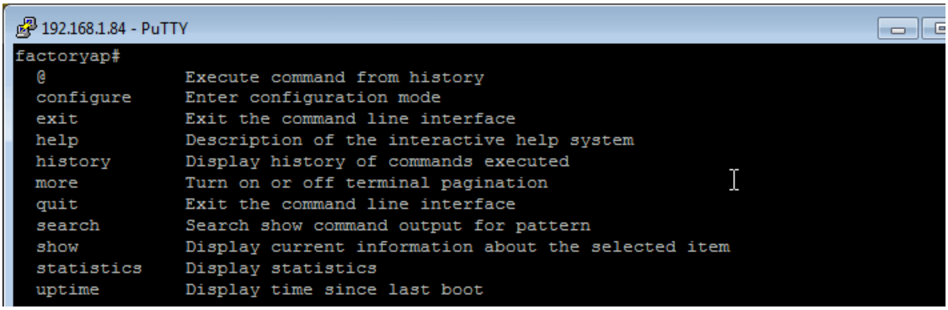


```
factoryap# help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.

Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?').
factoryap#
```

Figure 187. Help Window

- ? Command

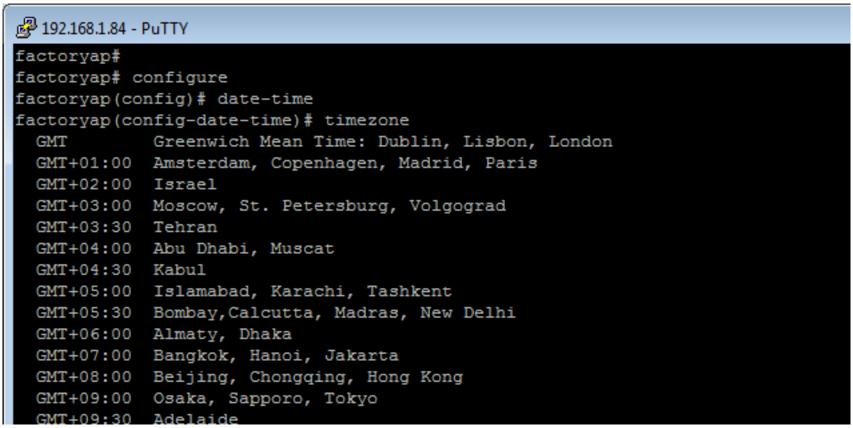
This command is available at any prompt and provides either FULL or PARTIAL help. Using the **?** (question mark) command when you are ready to enter an argument will display all the possible arguments (full help). Partial help is provided when you enter an abbreviated argument and you want to know what arguments will match your input.



```
factoryap#
  @              Execute command from history
  configure      Enter configuration mode
  exit           Exit the command line interface
  help           Description of the interactive help system
  history        Display history of commands executed
  more           Turn on or off terminal pagination
  quit           Exit the command line interface
  search         Search show command output for pattern
  show           Display current information about the selected item
  statistics     Display statistics
  uptime         Display time since last boot
```

Figure 188. Full Help

Figure 189 shows an example of how the Help system can provide the argument and format when specifying the time zone under the **date-time** command.



192.168.1.84 - PuTTY

```
factoryap#
factoryap# configure
factoryap(config)# date-time
factoryap(config-date-time)# timezone
  GMT         Greenwich Mean Time: Dublin, Lisbon, London
  GMT+01:00   Amsterdam, Copenhagen, Madrid, Paris
  GMT+02:00   Israel
  GMT+03:00   Moscow, St. Petersburg, Volgograd
  GMT+03:30   Tehran
  GMT+04:00   Abu Dhabi, Muscat
  GMT+04:30   Kabul
  GMT+05:00   Islamabad, Karachi, Tashkent
  GMT+05:30   Bombay,Calcutta, Madras, New Delhi
  GMT+06:00   Almaty, Dhaka
  GMT+07:00   Bangkok, Hanoi, Jakarta
  GMT+08:00   Beijing, Chongqing, Hong Kong
  GMT+09:00   Osaka, Sapporo, Tokyo
  GMT+09:30   Adelaide
```

Figure 189. Partial Help

Top Level Commands

This section offers an at-a-glance view of all top level commands—organized alphabetically. Top level commands are defined here as commands that are directly accessible from the root command prompt that consists of the name of the WAP followed by a “#” sign (e.g. **MyAP#**). When inputting commands, be aware that all commands are **case-sensitive**.

All other commands are considered second level configuration commands—these are the commands you use to configure specific elements of the WAP’s features and functionality. For a listing of these commands with examples of command formats and structure, go to “Configuration Commands” on page 423.

Root Command Prompt

The following table shows the top level commands that are available from the root command prompt [**MyAP**].

Command	Description
@	Type **@n** to execute command n (as shown by the history command).
configure	Enter the configuration mode. See “Configuration Commands” on page 423.
exit	Exit the CLI and terminate your session—if this command is used at any level other than the root command prompt you will simply exit the current level (step back) and return to the previous level.
help	Show a description of the interactive help system. See also, “Getting Help” on page 409.
history	List history of commands that have been executed.
more	Turn terminal pagination ON or OFF.
quit	Exit the Command Line Interface (from any level).
search	Search for pattern in show command output.

Command	Description
show	Display information about the selected item. See “show Commands” on page 417.
statistics	Display statistical data about the WAP. See “statistics Commands” on page 421.
uptime	Display the elapsed time since the last boot.
wos-override	Override WOS managed mode and allow local configuration changes according to your user privileges. See “Managing WAPs Locally or Using WOS” on page 67.

configure Commands

The following table shows the second level commands that are available with the top level **configure** command [**MyAP(config)#**].

Command	Description
@	Type **@n** to execute command n (as shown by the history command).
acl	Configure the Access Control List.
activation	Start or stop activation server polling
admin	Define administrator access parameters.
auth	Configure Oauth tokens.
authentication-server	Configure authentication server parameters
boot-env	Display or modify boot loader environment variables.
clear	Remove / clear the requested elements.
contact-info	Contact information for assistance on this WAP.

Command	Description
date-time	Configure date and time settings.
dhcp-server	Configure the DHCP Server.
dns	Configure the DNS settings.
end	Exit the configuration mode.
exit	Go UP one mode level.
file	Manage the file system.
filter	Define protocol filter parameters.
group	Define user groups with parameter settings
help	Description of the interactive Help system.
history	List history of commands that have been executed.
hostname	Host name for this WAP.
interface	Select the interface to configure.
lldp	Configure LLDP settings
load	Load running configuration from flash
location	Location name for this WAP.
location-reporting	Configure location server settings.
management	Configure WAP management parameters
more	Turn ON or OFF terminal pagination.
netflow	Configure NetFlow data collector.
no	Disable (if enabled) or set to default value.
proxy-fwd	Configure Proxy Forwarding settings.

Command	Description
quick-config	Apply configuration template for typical deployment scenario.
quit	Exit the Command Line Interface.
reboot	Reboot the WAP.
reset	Reset all settings to their factory default values and reboot.
restore	Reset all settings to their factory default values and reboot.
revert	Revert to saved configuration after specified delay in seconds if configuration not saved.
roaming-assist	Set parameters for roaming assistance.
run-tests	Run selective tests.
save	Save the running configuration to FLASH.
search	Search for pattern in show command output.
security	Set the security parameters for the WAP.
show	Display current information about the selected item.
snmp	Enable, disable or configure SNMP.
ssid	Configure the SSID parameters.
station-assurance	Location name for this WAP.
statistics	Display statistics.
syslog	Enable, disable or configure the Syslog Server.
tunnel	Configure tunnels.
uptime	Display time since the last boot.

Command	Description
vlan	Configure VLAN parameters.
wifi-tag	Configure VLAN parameters.
wos-override	Override WOS managed mode and allow local configuration changes according to your user privileges. See "Managing WAPs Locally or Using WOS" on page 67.

show Commands

The following table shows the second level commands that are available with the top level **show** command [**MyAP# show**].

Command	Description
acl	Display the Access Control List.
active-directory	Show Active Directory information.
admin	Display the administrator list or login information.
applications	Application statistics.
arp	ARP table information.
associated-stations	Display stations that have associated to the WAP.
auth	Show Open Authentication tokens.
authentication-server	Authentication server settings summary.
bond	Bond information
boot-env	Display Boot loader environment variables.
capabilities	Display detailed station capabilities.
channel-list	Display list of WAP’s 802.11an and bgn channels.
cluster	Display Cluster summary.
conntrack	Display the Connection Tracking table.
contact-info	Display contact information.
country-list	Display countries that the WAP can be set to support.
date-time	Display date and time settings summary.

Command	Description
dhcp-leases	Display IP addresses (leases) assigned to stations by the DHCP server.
dhcp-pool	Display internal DHCP server settings summary information.
diff	Display the difference between configurations.
dns	Display DNS summary information.
env-ctrl	Display the environmental controller status for the outdoor enclosure.
error-numbers	Display the detailed error number in error messages.
ethernet	Display Ethernet interface summary information.
external-radius	Display summary information for the external RADIUS server settings.
factory-config	Display the WAP factory configuration information.
filter	Display filter information.
filter-list	Filter list information.
group	User Group summary.
radio	Display radio configuration information.
ids-event-log	IDS event log.
ids-stats	IDS statistics
internal-radius	Display the users defined for the embedded RADIUS server.
intrude-detect	Intrusion detection information.
lastboot-config	Display WAP configuration at the time of the last boot-up.

Command	Description
lldp	Link Layer Discovery Protocol information.
location-reporting	Location server reporting information.
mac-table	MAC address bridging table
management	Display settings for managing the WAP, plus Standby and other information.
netflow	NetFlow information
network-assurance	Network Assurance status
network-map	Display network map information.
proxy-fwd	Display Proxy Forwarding summary.
radio-assurance	Radio Assurance status.
realtime-monitor	Display realtime statistics for all radios.
roaming-assist	Roaming assist settings
roaming-stations	Roaming station information
rogue-ap	Display rogue AP information.
route	Display the routing table.
rssi-map	Display RSSI map by radio for station.
running-config	Display configuration information for the WAP currently running.
saved-config	Display the last saved WAP configuration.
security	Display security settings summary information.
self-test	Display self test results.
snmp	Display SNMP summary information.

Command	Description
spanning-tree	Display spanning tree information.
spectrum-analyzer	Display spectrum analyzer measurements.
ssid	Display SSID summary information.
station-assurance	Station assurance information.
stations	Display station information.
statistics	Display statistics.
syslog	Display the system log.
syslog-settings	Display the system log (Syslog) settings.
system-info	System information
temperature	Display the current board temperatures.
tunnel	Tunnel information
unassociated-stations	Display unassociated station information.
undefined-vlan	Undefined VLANs detected
uptime	Display time since last boot.
vlan	Display VLAN information.
wds	Display WDS information.
wifi-tag	Display WiFi tag summary.
wpr-whitelist	Show WPR whitelist
<cr>	Display configuration or status information.
IAP-NAME **iap1, iap2**	IAP interface information

statistics Commands

The following table shows the second level commands that are available with the top level **statistics** command [**MyAP# statistics**].

Command	Description
ethernet	Display statistical data for all Ethernet interfaces.
filter	Display statistics for defined filters (if any). FORMAT: **statistics filter [detail]**
filter-list	Display statistics for defined filter list (if any). FORMAT: **statistics filter <filter-list>**
radio	Display statistical data for the defined radio. FORMAT: **statistics radio radio2**
station	Display statistical data about associated stations. FORMAT: **statistics station billw**
vlan	Display statistical data for the defined VLAN. You must use the VLAN number (not its name) when defining a VLAN. FORMAT: **statistics vlan 1**
wds	Display statistical data for the defined active WDS (Wireless Distribution System) links. FORMAT: **statistics wds 1**
<cr>	Display configuration or status information.

Command	Description
Ethernet Name **eth0**, **gig1**, **gig2**	Display statistical data for the defined Ethernet interface (either eth0, gig1 or gig2). FORMAT: **statistics gig1**
IAP-NAME **iap1, iap2**	IAP interface information

Configuration Commands

All configuration commands are accessed by using the **configure** command at the root command prompt (**MyAP#**). This section provides a brief description of each command and presents sample formats where deemed necessary. The commands are organized alphabetically. When inputting commands, be aware that all commands are **case-sensitive**.

To see examples of some of the key configuration tasks and their associated commands, go to “Sample Configuration Tasks” on page 468.

acl

The **acl** command [**MyAP(config)# acl**] is used to configure the Access Control List.

Command	Description
add	Add a MAC address to the list. FORMAT: **acl add AA:BB:CC:DD:EE:FF**
del	Delete a MAC address from the list. FORMAT: **acl del AA:BB:CC:DD:EE:FF**
disable	Disable the Access Control List FORMAT: **acl disable**
enable	Enable the Access Control List FORMAT: **acl enable**
reset	Delete all MAC addresses from the list. FORMAT: **acl reset**

admin

The **admin** command [**MyAP(config-admin)#**] is used to configure the Administrator List.

Command	Description
add	Add a user to the Administrator List. FORMAT: **admin add [userID]**
del	Delete a user to the Administrator List. FORMAT: **admin del [userID]**
edit	Modify user in the Administrator List. FORMAT: **admin edit [userID]**
privilege-name	Define administrator privilege level names
privilege-section	Define administrator privilege level required by config section.
radius	Define a RADIUS server to be used for authenticating administrators. FORMAT: **admin radius [disable | enable | off | on | timeout <seconds> | auth-type [PAP | CHAP]]** **admin radius [primary |secondary] port <portid> server [<ip-addr> | <host>] secret <shared-secret>**
reset	Delete all users and restore the default user. FORMAT: **admin reset**

auth

The **auth** command [**MyAP(config)# auth**] is used to configure Oauth tokens.

Command	Description
del	Delete an Oauth token. FORMAT: **auth del <Oauth token>**
reset	Delete all Oauth tokens. FORMAT: **auth reset**

See also, "OAuth 2.0 Management" on page 244.

clear

The **clear** command [**MyAP(config)# clear**] is used to clear requested elements.

Command	Description
arp	Clear the arp table entry for a requested IP address, or clear all entries if no IP address is entered. FORMAT: **clear arp [ipaddress]**
authentication	Deauthenticate a station (specified by MAC address, hostname, or IP address). If you specify the permanent option, then the station is deauthenticated and put on the access control list. FORMAT: **clear authentication [permanent] [authenticated station]**
history	Clear the history of CLI commands executed. FORMAT: **clear history**
screen	Clear the screen where you're viewing CLI output. FORMAT: **clear screen**
station-assurance	Clear all station assurance data, but continue to collect new data. FORMAT: **clear station-assurance**
statistics	Clear the statistics for thee change, but it won't show up requested element. FORMAT: **clear statistics [ethname | all-eth | applications | filters |radio | station | vlan | wds]**

Command	Description
syslog	Clear all Syslog messages, but continue to log new messages. FORMAT: **clear syslog**
undefined-vlan	Clear undefined VLAN information. FORMAT: **clear undefined-vlan**

cluster

The **cluster** command [MYAP**(config)# cluster**] is used to create and operate clusters. Clusters allow you to configure multiple WAPs at the same time. Using CLI (or WMI), you may define a set of WAPs that are members of the cluster. Then you may switch the WAP to Cluster operating mode for a selected cluster, which sends all successive configuration commands issued via CLI or WMI to all of the member WAPs. When you exit cluster mode, configuration commands revert to applying only to the WAP to which you are connected.

For more information, see "Clusters" on page 373.

Command	Description
add	Create a new WAP cluster. Enters edit mode for that cluster to allow you to specify the WAPs that belong to the cluster. FORMAT: **cluster add [cluster-name]**
del	Delete a WAP cluster. Type **del?** to list the existing clusters. FORMAT: **cluster del [cluster-name]**
edit	Enter edit mode for selected cluster to add or delete WAPs that belong to the cluster. FORMAT: **cluster edit [cluster-name]**
operate	Enter Cluster operation mode. All configuration commands are applied to all of the selected cluster's member WAPs until you give the **end** command (see above). FORMAT: **cluster operate [cluster-name]**
reset	Delete all clusters. FORMAT: **cluster reset**

contact-info

The **contact-info** command [**MyAP(config)# contact-info**] is used for managing administrator contact information.

Command	Description
email	Add an email address for the contact (must be in quotation marks). FORMAT: **contact-info email [“contact@mail.com”]**
name	Add a contact name (must be in quotation marks). FORMAT: **contact-info name [“Contact Name”]**
phone	Add a telephone number for the contact (must be in quotation marks). FORMAT: **contact-info phone [“8185550101”]**

date-time

The **date-time** command [**MyAP(config-date-time)#**] is used to configure the date and time parameters. Your WAP supports the Network Time Protocol (NTP) in order to ensure that the WAP's internal time is accurate. NTP is set to UTC time by default; however, you can set the time zone so that your WAP will display local time. This is done by defining an offset from the UTC value. For example, Pacific Standard Time is 8 hours behind UTC time, so the offset from UTC time would be -8.

Command	Description
dst_adjust	Enable adjustment for daylight savings. FORMAT: **date-time dst_adjust**
no	Disable daylight savings adjustment. FORMAT: **date-time no dst_adjust**
ntp	Enable the NTP server. FORMAT: **date-time ntp on** (or **off** to disable)
offset	Set an offset from Greenwich Mean Time. FORMAT: **date-time no dst_adjust**
set	Set the date and time for the WAP. FORMAT: **date-time set [10:24 10/23/2007]**
timezone	Configure the time zone. FORMAT: **date-time timezone [-8]**

dhcp-server

The **dhcp-server** command [**MyAP(config-dhcp-server**)#] is used to add, delete and modify DHCP pools.

Command	Description
add	Add a DHCP pool. FORMAT: **dhcp-server add [dhcp pool]**
del	Delete a DHCP pool. FORMAT: **dhcp-server del [dhcp pool]**
edit	Edit a DHCP pool FORMAT: **dhcp-server edit [dhcp pool]**
reset	Delete all DHCP pools. FORMAT: **dhcp-server reset**

dns

The **dns** command [**MyAP(config-dns)#**] is used to configure your DNS parameters.

Command	Description
domain	Enter your domain name. FORMAT: **dns domain [www.mydomain.com]**
server1	Enter the IP address of the primary DNS server. FORMAT: **dns server1 [1.2.3.4]**
server2	Enter the IP address of the secondary DNS server. FORMAT: **dns server1 [2.3.4.5]**
server3	Enter the IP address of the tertiary DNS server. FORMAT: **dns server1 [3.4.5.6]**
use-dhcp	Enable or disable updates to DNS settings via DHCP. FORMAT: **dns use-dhcp [off | on]**

file

The **file** command [**MyAP(config-file)#**] is used to manage files.

Command	Description
active-image	Validate and commit a new WAP software image.
backup-image	Validate and commit a new backup software image.
cat	List file contents.
check-image	Validate a new WAP software image.
chkdsk	Check flash file system.
copy **cp**	Copy a file to another file. FORMAT: **file copy [sourcefile destinationfile]**
create-text	Create a text file on the flash file system, <EOF> to finish.
dir	List the contents of a directory. FORMAT: **file dir [directory]**
erase	Delete a file from the FLASH file system. FORMAT: **file erase [filename]**
format	Format flash file system.
ftp	Open an FTP connection with a remote server. Files will be transferred in binary mode. FORMAT: **file ftp host {<hostname> | <ip>} [port <port_#>] [user {anonymous | <username> password <passwd> }] { put <source_file> [<dest_file>] | get <source_file> [<dest_file>] }** **Note:** Any time you transfer any kind of software image file for the WAP, it **must** be transferred in binary mode, or the file may be corrupted.

Command	Description
http-get	Perform an HTTP file download. FORMAT: **http-get [no-cert-check] <url> [<local_file>]** **no-cert-check** causes the WAP to download the file even if the SSL certificate is invalid, expired, or not signed by a recognized CA **<url>** is a standard HTTP URL, e.g. https://file.example.com:8080/mydir/myfile.ext. ● **http://** or **https://** may be omitted, in which case HTTP is assumed **<local_file>** is an optional parameter that describes the path and name where the file should be saved ● if no local_file is specified, the file will be saved in the root of the flash storage ● the local_file does support specifying a directory, which will be created if it doesn't already exist
list	List the contents of a file. FORMAT: **file list [filename]**
mkdir	Create a directory on the flash file system.
mv	Rename a file on the flash file system.

Command	Description
remote-config	When the WAP boots up, it fetches the specified configuration file from the TFTP server defined in the **file remote-server** command, and uses this configuration. This must be a WAP configuration file with a **.conf** extension. A partial configuration file may be used. For instance, if you wish to use a single configuration file for all of your WAPs but don't want to have the same IP address for each WAP, you may remove the **ipaddr** line from the file. You can then load the file on each WAP and the local IP addresses will not change. FORMAT: **file remote-config <config-file.conf>** **Note:** If you enter **file remote-config ?**, the help response suggests possibilities by listing all of the configuration files that are currently in the WAP's flash.
remote-image	When the WAP boots up, it fetches the named image file from the TFTP server defined in the **file remote-server** command, and upgrades to this file before booting. This must be a WAP image file with a **.bin** extension. FORMAT: **file remote-image <image-file.bin>** **Note**: This will happen every time that the WAP reboots. If you only want to fetch the remote-image one time be sure to turn off the remote image option after the initial download.
remote-server	Sets up a TFTP server to be used for automated remote update of software image and configuration files when rebooting. FORMAT: **file remote-server A.B.C.D**
rename	Rename a file.
rm	Delete a file from the flash file system.

Command	Description
rmdir	Delete a directory on the flash file system.
scp	Copy a file to or from a remote system. You may specify the port to use.
tftp	Open a TFTP connection with a remote server. FORMAT: **file tftp host {<hostname> |<ip>} [port <port_#>] [user {anonymous | <username> password <passwd> }] { put <source_file> [<dest_file>] | get <source_file> [<dest_file>] }** **Note:** Any time you transfer any kind of software image file for the WAP, it **must** be transferred in binary mode, or the file may be corrupted.

filter

The **filter** command [**MyAP(config-filter)#**] is used to manage protocol filters and filter lists.

Command	Description
add	Add a filter. Details about the air cleaner feature are after the end of this table. FORMAT: **filter add [air-cleaner | name]**
add-list	Add a filter list. FORMAT: **filter add-list [name]**
del	Delete a filter. FORMAT: **filter del [name]**
del-list	Delete a filter list. FORMAT: **filter del-list [name]**
edit	Edit a filter. FORMAT: **filter edit [name type]**
edit-list	Edit a filter list FORMAT: **filter edit-list [name type]**
enable	Enable a filter list. FORMAT: **filter enable**
move	Change a filter priority. FORMAT: **filter move [name priority]**

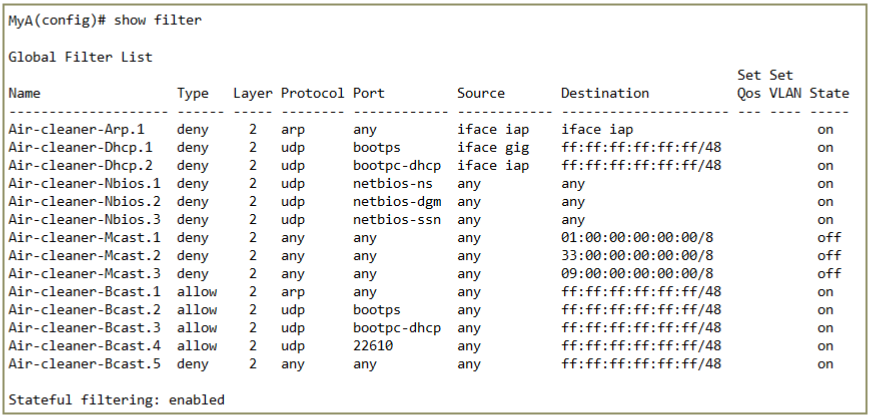
Command	Description
off	Disable a filter list. FORMAT: **filter off**
on	Enable a filter list. FORMAT: **filter on**
reset	Delete all protocol filters and filter lists. FORMAT: **filter reset**
stateful	Enable or disable stateful filtering (firewall). FORMAT: **Stateful [enable | disable | on |off]**
track-apps	Enable or disable application tracking. FORMAT: **filter track-apps [enable | disable | on |off]**

Air Cleaner

The air cleaner feature offers a number of predetermined filter rules that eliminate a great deal of unnecessary wireless traffic, resulting in improved performance. You may select **all** of the air cleaner rules for the greatest effect, or only specific rules, such as **broadcast** or **multicast**, to eliminate only a particular source of traffic. The following options are offered:

```
MyAP(config)# filter add air-cleaner
  all        All air cleaner filters
  arp        Eliminate station to station ARPs over the air
  broadcast  Eliminate broadcast traffic from the air
  dhcp       Eliminate stations serving DHCP addresses from the air
  multicast  Eliminate chatty multicast traffic from the air
  netbios    Eliminate NetBIOS traffic from the air
```

If you select all, the rules shown in Figure 190 are added to the predefined filter list named **Global**. These rules assume that you have station-to-station blocking enabled, that a DHCP server is on the WAP's wired connection, and that you want to block most all multicast and all broadcast traffic not vital to normal operation. If you find that there is a particular type of multicast or broadcast traffic that you want to allow, just add a specific allow filter for it before the deny filter in this list that would normally block it. Add or delete any of the Multicast rules as necessary for a specific site. Remember that the order of the rules is important.



```
MyA(config)# show filter

Global Filter List
                                                                                          Set Set
Name                 Type   Layer Protocol Port         Source       Destination          Qos VLAN State
-------------------- ------ ----- -------- ------------ ------------ -------------------- --- ---- -----
Air-cleaner-Arp.1    deny     2   arp      any          iface iap    iface iap                      on
Air-cleaner-Dhcp.1   deny     2   udp      bootps       iface gig    ff:ff:ff:ff:ff:ff/48           on
Air-cleaner-Dhcp.2   deny     2   udp      bootpc-dhcp  iface iap    ff:ff:ff:ff:ff:ff/48           on
Air-cleaner-Nbios.1  deny     2   udp      netbios-ns   any          any                            on
Air-cleaner-Nbios.2  deny     2   udp      netbios-dgm  any          any                            on
Air-cleaner-Nbios.3  deny     2   udp      netbios-ssn  any          any                            on
Air-cleaner-Mcast.1  deny     2   any      any          any          01:00:00:00:00:00/8            off
Air-cleaner-Mcast.2  deny     2   any      any          any          33:00:00:00:00:00/8            off
Air-cleaner-Mcast.3  deny     2   any      any          any          09:00:00:00:00:00/8            off
Air-cleaner-Bcast.1  allow    2   arp      any          any          ff:ff:ff:ff:ff:ff/48           on
Air-cleaner-Bcast.2  allow    2   udp      bootps       any          ff:ff:ff:ff:ff:ff/48           on
Air-cleaner-Bcast.3  allow    2   udp      bootpc-dhcp  any          ff:ff:ff:ff:ff:ff/48           on
Air-cleaner-Bcast.4  allow    2   udp      22610        any          ff:ff:ff:ff:ff:ff/48           on
Air-cleaner-Bcast.5  deny     2   any      any          any          ff:ff:ff:ff:ff:ff/48           on

Stateful filtering: enabled
```

Figure 190. Air Cleaner Filter Rules

Explanations of some sample rules are below.

- **Air-cleaner-Arp.1** blocks ARPs from one client from being transmitted to clients via all of the radios. The station to station block setting doesn't block this traffic, so this filter eliminates this unnecessary traffic.
- **Air-cleaner-Dhcp.1** drops all DHCP client traffic coming in from the Gigabit interface. This traffic doesn't need to be transmitted by the radios since there shouldn't be any DHCP server associated to the radios and offering DHCP addresses. For large subnets the DHCP discover/request broadcast traffic can be significant.

- **Air-cleaner-Dhcp.2** drops all DHCP server traffic coming in from the radio interfaces. There should not be any DHCP server associated to the radios. These rogue DHCP servers are blocked from doing any damage with this filter. There have been quite a few cases in public venues like schools and conventions where such traffic is seen.
- **Air-cleaner-Mcast.1** drops all multicast traffic with a destination MAC address starting with 01. This filters out a lot of IP multicast traffic that starts with 224.
- **Air-cleaner-Mcast.2** drops all multicast traffic with a destination MAC address starting with 33. A lot of IPv6 traffic and other multicast traffic is blocked by this filter.
- **Air-cleaner-Mcast.3** drops all multicast traffic with a destination MAC address starting with 09. A lot of Appletalk traffic and other multicast traffic is blocked by this filter. Note that for OSX 10.6.* Snow Leopard no longer supports Appletalk.
- **Air-cleaner-Bcast.1** allows all ARP traffic (other than the traffic that was denied by **Air-cleaner-Arp.1**). This is needed because **Air-cleaner-Bcast.5** would drop this valid traffic.
- **Air-cleaner-Bcast.4** allows all roaming protocol traffic from WAPs to be received from the wire. This is needed because **Air-cleaner-Bcast.5** would drop this valid traffic.
- **Air-cleaner-Bcast.5** drops all other broadcast traffic that hasn't previously been explicitly allowed. This filter will catch all UDP broadcast traffic as well as all other known and unknown protocol broadcast traffic.

group

The **group** command [**MyAP(config)# group**] is used to create and configure user groups. User groups allow administrators to assign specific network parameters to users through RADIUS privileges rather than having to map users to a specific SSID. Groups provide flexible control over user privileges without the need to create large numbers of SSIDs. For more information, see "Groups" on page 275.

Command	Description
add	Create a new user group. FORMAT: **group add [group-name]**
del	Delete a user group. FORMAT: **group del [group-name]**
edit	Set parameters values for a group. FORMAT: **group edit [group-name]**
reset	Reset the group. FORMAT: **group reset**

hostname

The **hostname** command [**MyAP(config)# hostname**] is used to change the hostname used by the WAP.

Command	Description
hostname	Change the hostname of the WAP. FORMAT: **hostname [name]**

interface

The **interface** command [**MyAP(config)# interface**] is used to select the interface that you want to configure. To see a listing of the commands that are available for each interface, use the **?** command at the selected interface prompt. For example, using the **?** command at the **MyAP(config-gig1}#** prompt displays a listing of all commands for the **gig1** interface.

Command	Description
bond1	Bond 1.
bond2	Bond 2.
console	Select the console interface. The console interface is used for management purposes only. FORMAT: **interface console**
gig1	Select the Gigabit 1 interface. FORMAT: **interface gig1**
gig2	Select the Gigabit 2 interface. FORMAT: **interface gig2**
iap	Select a radio. FORMAT: **interface iap**
IAP-NAME **iap1, iap2**	IAP interface information

Multicast Traffic Isolation (supports Airplay and mDNS service)

In today’s deployments, we recommend filtering multicast traffic using Air Cleaner filters in any subnet network that has more than 500 clients. This makes technologies that rely on multicast unusable (e.g., Apple TV and printers, etc.) unless you add individual Access Control List entries per Access Point. To solve this problem, use multicast isolation. If you are using Air Cleaner filters, the multicast isolation commands will pass the desired multicasts along to the specified stations.

The Avaya OS multicast isolation feature provides control over which multicast frames are distributed in the network and how they are distributed. It supports devices that rely on multicast and at the same time minimizes the airtime impact. Multicast traffic is blocked based on the Layer 2 multicast MAC addresses.

There are two multicast isolation commands (they are in **interface iap** mode):

```
(config)# interface iap
(config-iap)# multicast isolate-by {none | { access-point | ap-neighbors | user-group
   | fixed-list } }
(config-iap)# multicast fixed-addr { reset | {add | del} <addr> [ group [<grp>] ] }
(config-iap)# exit
```

Where:

- **isolate-by access-point** only shares multicasts among stations connected to this AP.
- **isolate-by ap-neighbors** shares multicasts among stations connected to this AP and this AP's neighbors (those APs within range of each other—that can hear each other's beacons).
- **isolate-by user-groups** only shares multicasts among stations connected to the same User Group (see "Groups" on page 275).
- **isolate-by fixed-list** only shares multicasts originating from a fixed list of MAC addresses.

These options can be used alone, or in any combination. For example, isolating by access-point and user-group would only share multicasts between stations on the same AP and user-group. This could be used to provide access to certain services to one group of users (i.e., teachers) in a specific location without making them available to another group (i.e., students).

Specify the multicast fixed address list with the **multicast fixed-addr** command by adding or deleting MAC addresses from the list, optionally associating a user-group with each MAC address. This list can be unique to each AP, and provides a means to allow wired devices to advertise their services on specified APs.

load

The **load** command [**MyAP(config)# load**] loads a configuration file.

Command	Description
factory.conf	Load the factory settings configuration file. FORMAT: **load [factory.conf]**
lastboot.conf	Load the configuration file from the last boot-up. FORMAT: **load [lastboot.conf]**
[myfile].conf	If you have saved a configuration, enter its name to load it. FORMAT: **load [myfile.conf]**
saved.conf	Load the configuration file with the last saved settings. FORMAT: **load [saved.conf]**

location

The **location** command [**MyAP(config)# location**] is used to set the location descriptive string for the WAP.

Command	Description
<cr>	Set the location for the WAP. FORMAT: **location [newlocation]**

location-reporting

The **location-reporting** command [**MyAP(config)# location-reporting**] is used to configure Location Server settings. See also, “Location” on page 169.

Command	Description
cust-key	Set Location Server customer key. FORMAT: **location-reporting cust-key enc <loc-server-customer-key>**
disable **off**	Disable location-reporting. FORMAT: **location-reporting disable**
enable **on**	Enable location-reporting. FORMAT: **location-reporting enable**
period	Set Location Server reporting period (seconds). FORMAT: **location-reporting period <#-seconds>**
url	Set URL of Location Server. FORMAT: **location-reporting url <loc-server-URL>**

management

The **management** command [**MyAP(config)# management**] enters management mode, where you may configure management parameters.

Command	Description
<cr>	Enter management mode. FORMAT: **management <cr>**

The following types of settings may be configured in management mode:

Setting	Description
activation	Start or stop activation server polling.
avcon	Enable / disable Avaya Console access. See Avaya Console *User's Guide* for more information.
banner	Configure login banner messages.
clear	Remove / clear requested elements.
console	Configure console management parameters.
help	Description of the interactive help system.
history	Display history of commands executed.
https	Enable / disable HTTPS access.
license	Set access point software license key
load	Load running configuration from flash.
max-auth-attempts	Maximum number of authentication (login) attempts (0 means unlimited).
more	Turn on or off terminal pagination.
network-assurance	Enable / disable network assurance.

Setting	Description
pci-audit	Enable / disable PCI (Payment Card Industry) audit mode. See "Auditing PCI DSS" on page 509.
quick-config	Apply quick configuration template.
quit	Exit the command line interface.
reauth-period	Time between failed CLI login attempts.
restore	Restore to previous saved config.
revert	Revert to saved configuration after delay if configuration not saved.
save	Save running configuration to flash.
search	Search show command output for pattern.
show	Display current information about the selected item.
spanning-tree	Enable / disable Spanning Tree Protocol.
ssh	Enable / disable SSH access.
standby	Configure standby parameters.
statistics	Display statistics.
telnet	Enable / disable telnet access.
top	Return to top level of configuration mode.
uptime	Display time since last boot.
wos-override	Override WOS managed mode and allow local configuration changes according to your user privileges. See "Managing WAPs Locally or Using WOS" on page 67.

more

The **more** command [**MyAP(config)# more**] is used to turn terminal pagination ON or OFF.

Command	Description
disable **off**	Turn OFF terminal pagination. FORMAT: **more off**
enable **on**	Turn ON terminal pagination. FORMAT: **more on**

netflow

The **netflow** command [**MyAP(config-netflow)#**] is used to enable or disable, or configure sending IP flow information (traffic statistics) to the collector you specify.

Command	Description
collector	Set the Netflow collector IP address or fully qualified domain name (host.domain). Only one collector may be set. If port is not specified, the default is 2055. FORMAT: **netflow collector host {<ip-addr> | <domain>} [port <port#>]**
disable **off**	Disable netflow. FORMAT: **netflow disable**
ipfix	Enable NetFlow IPFIX probe.
off	Disable netflow. FORMAT: **netflow off**
v5	Enable NetFlow v5 probe.
v9	Enable Netflow v9 probe.

no

The **no** command [**MyAP(config)# no**] is used to disable a selected element or set the element to its default value.

Command	Description
2.4GHz	Disable all 2.4GHz Radios.
5GHz	Disable all 5GHz Radios.
acl	Disable the Access Control List. FORMAT: **no acl**
clear-text	Disable entry and display of passwords and secrets in the clear.
gig1	Disable gig1.
gig2	Disable gig2.
https	Disable https access. FORMAT: **no https**
intrude-detect	Disable intrusion detection. FORMAT: **no intrude-detect**
management	Disable management on all Ethernet interfaces. FORMAT: **no management**
more	Disable terminal pagination. FORMAT: **no more**
ntp	Disable the NTP server. FORMAT: **no ntp**

Command	Description
snmp	Disable SNMP features. FORMAT: **no snmp**
spanning-tree	Disable spanning tree.
ssh	Disable ssh access. FORMAT: **no ssh**
syslog	Disable the Syslog services. FORMAT: **no syslog**
telnet	Disable Telnet access. FORMAT: **no telnet**

quick-config

The **quick-config** command is used to apply configuration templates to the WAP for typical deployment scenarios.

Command	Description
Classroom	Configure WAP for classroom deployment. FORMAT: **quick-config Classroom** Configures the WAP for use in classroom settings (K-12 schools, Higher education, etc.)
High-density	Configure WAP for high density deployment. FORMAT: **quick-config High-density** Configures the WAP for use in high density settings (lecture halls, convention centers, stadiums, etc.)

quit

The **quit** command [**MyAP(config)# quit**] is used to exit the Command Line Interface.

Command	Description
<cr>	Exit the Command Line Interface. FORMAT: **quit** If you have made any configuration changes and your changes have not been saved, you are prompted to save your changes to Flash. At the prompt, answer **Yes** to save your changes, or answer **No** to discard your changes.

authentication-server

The **authentication-server** command [**MyAP(config-authserver)#**] is used to configure the external and internal RADIUS server parameters.

Command	Description
active-directory	Configure Active Directory parameters.
external-radius	Configure an external RADIUS server. FORMAT: **authentication-server external-radius** To configure a RADIUS server (primary, secondary, or accounting server, by IP address or host name), and the reporting interval use: **authentication-server external-radius accounting**
internal-radius	Configure the internal RADIUS server. FORMAT: **authentication-server internal-radius**

Command	Description
use	Choose the active RADIUS server (either external or internal). FORMAT: **authentication-server use external** (or internal)

reboot

The **reboot** command [**MyAP(config)# reboot**] is used to reboot the WAP. If you have unsaved changes, the command will notify you and give you a chance to cancel the reboot.

Command	Description
<cr>	Reboot the WAP. FORMAT: **reboot**
delay	Reboot the WAP after a delay of 1 to 60 seconds. FORMAT: **reboot delay [n]**

reset

The **reset** command [**MyAP(config)# reset**] is used to reset all settings to their default values then reboot the WAP.

Command	Description
<cr>	Reset all configuration parameters to their factory default values. FORMAT: **reset** The WAP is rebooted automatically.
preserve-ip-settings	Preserve all ethernet and VLAN settings and reset all other configuration parameters to their factory default values. FORMAT: **reset preserve-ip-settings** The WAP is rebooted automatically.

restore

The **restore** command [**MyAP(config)# restore**] is used to restore configuration to a version that was previously saved locally.

Command	Description
?	Use this to display the list of available config files. FORMAT: **restore ?**
<filename>	Enter the name of the locally saved configuration to restore. FORMAT: **restore <config-filename>**

roaming-assist

The **roaming-assist** command [**MyAP(config)# roaming-assist**] is used to configure roaming assistance settings. See also, "Roaming Assist" on page 353.

Command	Description
data-rate	Set minimum packet data rate before roaming, in Mbps. FORMAT: **roaming-assist data-rate <1-99>**
devices	Set device types or classes to assist. FORMAT: **roaming-assist devices all | unidentified | DEVICE-CLASS <ID-string> | DEVICE-TYPE <ID-string>**
disable **off**	Disable roaming assist. FORMAT: **roaming-assist disable**
enable **on**	Enable roaming assist. FORMAT: **roaming-assist enable**
period	Set roaming assist backoff period (seconds). FORMAT: **roaming-assist period <#-seconds>**
threshold	Set roaming RSSI threshold in db relative to RSSI of nearest WAP. FORMAT: **roaming-assist threshold <-50 to 50>**

run-tests

The **run-tests** command [**MyAP(run-tests)#**] is used to enter run-tests mode, which allows you to perform a range of tests on the WAP.

Command	Description
@	Execute command from history
ad-authenticate	Test domain user authentication.
ad-check-secret	Check machine trust secret.
ad-debug-info	Display detailed Active Directory information.
ad-list-groups	List all domain groups.
ad-status	Display Active Directory status.
capture	Execute a packet capture.
clear	Remove/clear requested elements.
diagnostic-log	Generate diagnostic log file.
end	Exit configuration mode.
help	Description of the interactive help system.
history	Display history of commands executed.
iperf	Execute iperf utility. FORMAT: **run-tests iperf**
led	LED test. FORMAT: **run-tests led [flash | rotate]**
memtest	Execute memory tests. FORMAT: **run-tests memtest**
more	Turn on or off terminal pagination.

Command	Description
ping	Execute ping utility. FORMAT: **run-tests ping [host-name | ip-addr]**
quick-config	Apply quick configuration template.
quit	Exit the command line interface.
radius-ping	Special ping utility to test the connection to a RADIUS server. FORMAT: **run-tests radius-ping [external | ssid <ssidnum>] [primary | secondary] user <raduser> password <radpasswd> auth-type [CHAP | PAP]** **run-tests radius-ping [internal | server <radserver> port <radport> secret <radsecret>] user <raduser> password <radpasswd> auth-type [CHAP | PAP]** You may select a RADIUS server that you have already configured (**ssid** or **external** or **internal**) or specify another **server**.
restore	Restore to previous saved configuration.
revert	Revert to saved configuration after delay if configuration is not saved.
save	Save running configuration to flash.
search	Search show command output for pattern.
show	Display current information about the selected item.
site-survey	Enable or disable site survey mode. FORMAT: **run-tests site-survey [on | off | enable | disable]**

Command	Description
ssh	Execute ssh utility. FORMAT: **run-tests ssh [hostname | ip-addr] [command-line-switches (optional)]**
tcpdump	Execute tcpdump utility to dump traffic for selected interface or VLAN. Supports 802.11 headers. FORMAT: **run-tests tcpdump**
telnet	Execute telnet utility. FORMAT: **run-tests telnet [hostname | ip-addr] [command-line-switches (optional)]**
traceroute	Execute traceroute utility. FORMAT: **run-tests traceroute [host-name | ip-addr]**
uptime	Display time since last boot.

security

The **security** command [**MyAP(config-security)#**] is used to establish the security parameters for the WAP.

Command	Description
wep	Set the WEP encryption parameters. FORMAT: **security wep**
wpa	Set the WEP encryption parameters. FORMAT: **security wpa**

snmp

The **snmp** command [**MyAP(config-snmp)#**] is used to enable, disable, or configure SNMP.

Command	Description
trap	Configure traps for SNMP. Up to four trap destinations may be configured, and you may specify whether to send traps for authentication failure. FORMAT: **snmp trap**
v2	Enable SNMP v2. FORMAT: **snmp v2**
v3	Enable SNMP v3. FORMAT: **snmp v3**

ssid

The **ssid** command [**MyAP(config-ssid)#**] is used to establish your SSID parameters.

Command	Description
add	Add an SSID. FORMAT: **ssid add [newssid]**
del	Delete an SSID. FORMAT: **ssid del [oldssid]**
edit	Edit an existing SSID. FORMAT: **ssid edit [existingssid]**
reset	Delete all SSIDs and restore the default SSID. FORMAT: **ssid reset**
stations	Set station limit for this SSID.
traffic	Set traffic limits for this SSID

syslog

The **syslog** command [**MyAP(config-syslog)#**] is used to enable, disable, or configure the Syslog server.

Command	Description
console	Enable or disable the display of Syslog messages on the console, and set the level to be displayed. All messages at this level and lower (i.e., more severe) will be displayed. FORMAT: **syslog console [on/off] level [0-7]**
disable **off**	Disable the Syslog server. FORMAT: **syslog disable**
email	Disable the Syslog server. FORMAT: **syslog email from [email-from-address]** **level [0-7]** **password [email-acct-password]** **server [email-server-IPaddr]** **test [test-msg-text]** **to-list [recipient-email-addresses]** **user [email-acct-username]**
enable **on**	Enable the Syslog server. FORMAT: **syslog enable**
local-file	Set the size and / or severity level (all messages at this level and lower will be logged). FORMAT: **syslog local-file size [1-500] level [0-7]**
no	Disable the selected feature. FORMAT: **syslog no [feature]**

Command	Description
primary	Set the IP address of the primary Syslog server and/or the severity level of messages to be logged. FORMAT: **syslog primary [1.2.3.4] level [0-7]**
secondary	Set the IP address of the secondary (backup) Syslog server and/or the severity level of messages to be logged. FORMAT: **syslog primary [1.2.3.4] level [0-7]**
sta-format	Select format of station information in Syslog messages.
sta-url-log	Enable or disable station URL logging.
tertiary	Set Tertiary Syslog Server parameters.
time-format	Select format of date/time information in Syslog messages.

tunnel

The **tunnel** command [**MyAP(config-tunnel)#**] is used to establish your tunnel parameters.

Command	Description
add	Add a tunnel. FORMAT: **tunnel add [newtunnel]**
delete	Delete a tunnel. FORMAT: **tunnel delete [oldtunnel]**

Command	Description
edit	Modify an existing tunnel. FORMAT: **tunnel edit [existingtunnel]**
reset	Delete all existing tunnels. FORMAT: **tunnel reset**

uptime

The **uptime** command [**MyAP(config)# uptime**] is used to display the elapsed time since you last rebooted the WAP.

Command	Description
continuous	Continuously update information.
<cr>	Display time since last reboot. FORMAT: **uptime**

vlan

The **vlan** command [**MyAP(config-vlan)#**] is used to establish your VLAN parameters.

Command	Description
add	Add a VLAN. FORMAT: **vlan add [newvlan]**

Command	Description
default-route	Assign a VLAN for the default route (for outbound management traffic). FORMAT: **vlan default-route [defaultroute]**
delete	Delete a VLAN. FORMAT: **vlan delete [oldvlan]**
edit	Modify an existing VLAN. FORMAT: **vlan edit [existingvlan]**
native-vlan	Assign a native VLAN (traffic is untagged). FORMAT: **vlan native-vlan [nativevlan]**
no	Disable the selected feature. FORMAT: **vlan no [feature]**
reset	Delete all existing VLANs. FORMAT: **vlan reset**

wifi-tag

The **wifi-tag** command [**MyAP(config-wifi-tag)#**] is used to enable or disable Wi-Fi tag capabilities. When enabled, the WAP listens for and collects information about Wi-Fi RFID tags sent on the designated channels. See also “Wi-Fi Tag” on page 168.

Command	Description
disable **off**	Disable wifi-tag. FORMAT: **wifi-tag disable**
enable **on**	Enable wifi-tag. FORMAT: **wifi-tag enable**
refresh	Disable and enable WiFi tag.
server	Set hostname or IP address of the tag server.
tag-channel-bg	Set an 802.11b or g channel for listening for tags. FORMAT: **wifi-tag tag-channel-bg <1-255>**
udp-port	Set the UDP port which a tagging server will use to query the WAP for tagging information. FORMAT: **wifi-tag udp-port <1025-65535>**

Sample Configuration Tasks

This section provides examples of some of the common configuration tasks used with the WAP, including:

- **"Configuring a Simple Open Global SSID" on page 469.**
- **"Configuring a Global SSID using WPA-PEAP" on page 470.**
- **"Configuring an SSID-Specific SSID using WPA-PEAP" on page 471.**
- **"Enabling Global Radios" on page 472.**
- **"Disabling Global Radios" on page 473.**
- **"Enabling a Specific Radio" on page 474.**
- **"Disabling a Specific Radio" on page 475.**
- **"Setting Cell Size Auto-Configuration for All Radios" on page 476**
- **"Setting the Cell Size for All Radios" on page 477.**
- **"Setting the Cell Size for a Specific Radio" on page 478.**

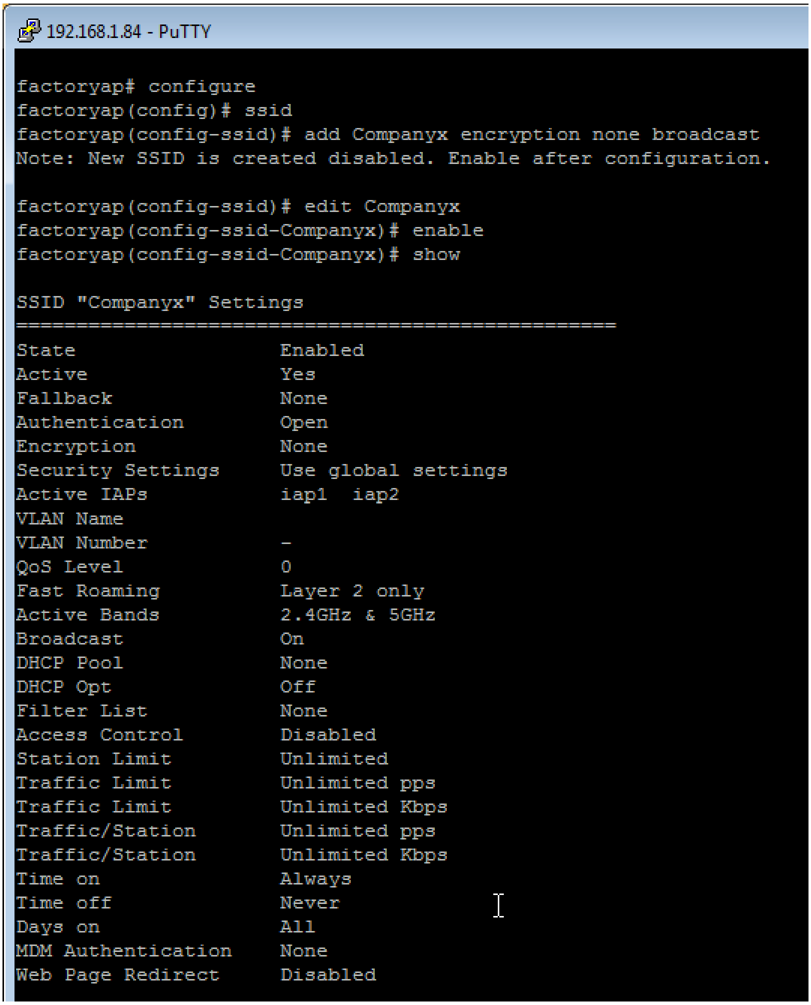
To facilitate the accurate and timely management of revisions to this section, the examples shown here are presented as screen images taken from a Secure Shell (SSH) session (in this case, PuTTY). Depending on the application you are using to access the Command Line Interface, and how your session is set up (for example, font and screen size), the images presented on your screen may be different than the images shown in this section. However, the data displayed will be the same.

Some of the screen images shown in this section have been modified for clarity. For example, the image may have been "elongated" to show all data without the need for additional images or scrolling. We recommend that you use the Adobe PDF version of this User's Guide when reviewing these examples—a hard copy document may be difficult to read.

As mentioned previously, the root command prompt is determined by the host name assigned to your WAP.

Configuring a Simple Open Global SSID

This example shows you how to configure a simple open global SSID.

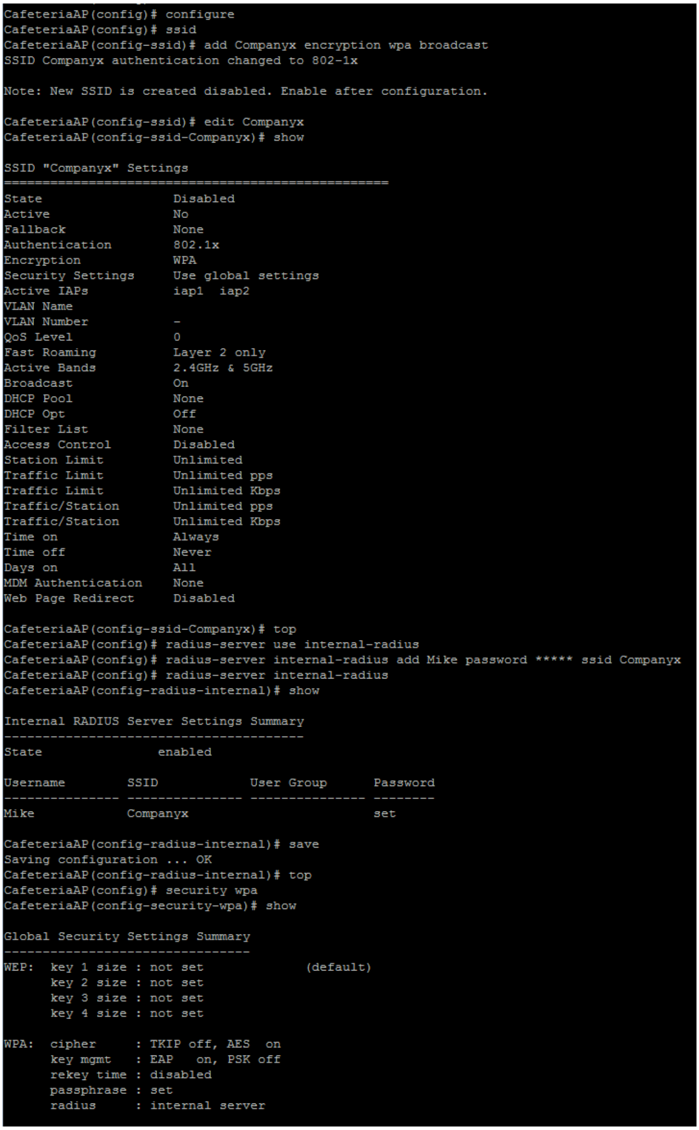


```
factoryap# configure
factoryap(config)# ssid
factoryap(config-ssid)# add Companyx encryption none broadcast
Note: New SSID is created disabled. Enable after configuration.

factoryap(config-ssid)# edit Companyx
factoryap(config-ssid-Companyx)# enable
factoryap(config-ssid-Companyx)# show

SSID "Companyx" Settings
==================================================
State                     Enabled
Active                    Yes
Fallback                  None
Authentication            Open
Encryption                None
Security Settings         Use global settings
Active IAPs               iap1  iap2
VLAN Name
VLAN Number               -
QoS Level                 0
Fast Roaming              Layer 2 only
Active Bands              2.4GHz & 5GHz
Broadcast                 On
DHCP Pool                 None
DHCP Opt                  Off
Filter List               None
Access Control            Disabled
Station Limit             Unlimited
Traffic Limit             Unlimited pps
Traffic Limit             Unlimited Kbps
Traffic/Station           Unlimited pps
Traffic/Station           Unlimited Kbps
Time on                   Always
Time off                  Never
Days on                   All
MDM Authentication        None
Web Page Redirect         Disabled
```

Figure 191. Configuring a Simple Open Global SSID

Configuring a Global SSID using WPA-PEAP

This example shows you how to configure a global SSID using WPA-PEAP encryption in conjunction with the WAP’s Internal RADIUS server.

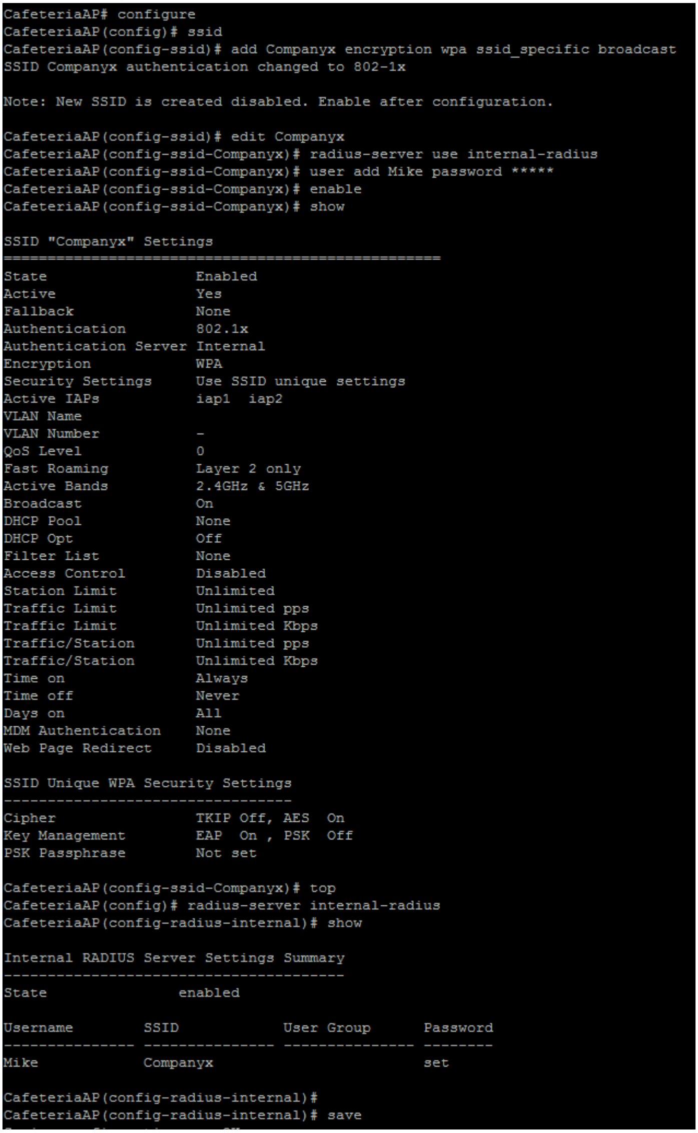


```
CafeteriaAP(config)# configure
CafeteriaAP(config)# ssid
CafeteriaAP(config-ssid)# add Companyx encryption wpa broadcast
SSID Companyx authentication changed to 802-1x

Note: New SSID is created disabled. Enable after configuration.

CafeteriaAP(config-ssid)# edit Companyx
CafeteriaAP(config-ssid-Companyx)# show

SSID "Companyx" Settings
==================================================
State                 Disabled
Active                No
Fallback              None
Authentication        802.1x
Encryption            WPA
Security Settings     Use global settings
Active IAPs           iap1  iap2
VLAN Name
VLAN Number           -
QoS Level             0
Fast Roaming          Layer 2 only
Active Bands          2.4GHz & 5GHz
Broadcast             On
DHCP Pool             None
DHCP Opt              Off
Filter List           None
Access Control        Disabled
Station Limit         Unlimited
Traffic Limit         Unlimited pps
Traffic Limit         Unlimited Kbps
Traffic/Station       Unlimited pps
Traffic/Station       Unlimited Kbps
Time on               Always
Time off              Never
Days on               All
MDM Authentication    None
Web Page Redirect     Disabled

CafeteriaAP(config-ssid-Companyx)# top
CafeteriaAP(config)# radius-server use internal-radius
CafeteriaAP(config)# radius-server internal-radius add Mike password ***** ssid Companyx
CafeteriaAP(config)# radius-server internal-radius
CafeteriaAP(config-radius-internal)# show

Internal RADIUS Server Settings Summary
---------------------------------------
State               enabled

Username        SSID            User Group      Password
--------------- --------------- --------------- --------
Mike            Companyx                        set

CafeteriaAP(config-radius-internal)# save
Saving configuration ... OK
CafeteriaAP(config-radius-internal)# top
CafeteriaAP(config)# security wpa
CafeteriaAP(config-security-wpa)# show

Global Security Settings Summary
--------------------------------
WEP:  key 1 size : not set             (default)
      key 2 size : not set
      key 3 size : not set
      key 4 size : not set

WPA:  cipher     : TKIP off, AES  on
      key mgmt   : EAP   on, PSK off
      rekey time : disabled
      passphrase : set
      radius     : internal server
```

Figure 192. Configuring a Global SSID using WPA-PEAP

Configuring an SSID-Specific SSID using WPA-PEAP

This example shows you how to configure an SSID-specific SSID using WPA-PEAP encryption in conjunction with the WAP’s Internal RADIUS server.

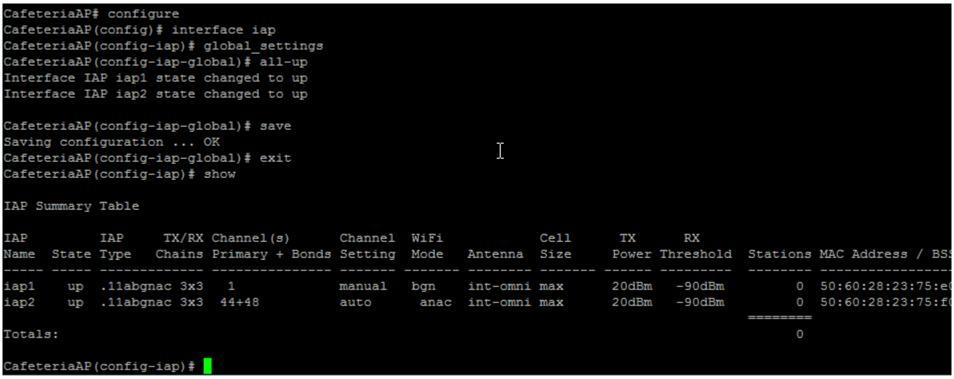


```
CafeteriaAP# configure
CafeteriaAP(config)# ssid
CafeteriaAP(config-ssid)# add Companyx encryption wpa ssid_specific broadcast
SSID Companyx authentication changed to 802-1x

Note: New SSID is created disabled. Enable after configuration.

CafeteriaAP(config-ssid)# edit Companyx
CafeteriaAP(config-ssid-Companyx)# radius-server use internal-radius
CafeteriaAP(config-ssid-Companyx)# user add Mike password *****
CafeteriaAP(config-ssid-Companyx)# enable
CafeteriaAP(config-ssid-Companyx)# show

SSID "Companyx" Settings
==================================================
State                 Enabled
Active                Yes
Fallback              None
Authentication        802.1x
Authentication Server Internal
Encryption            WPA
Security Settings     Use SSID unique settings
Active IAPs           iap1  iap2
VLAN Name
VLAN Number           -
QoS Level             0
Fast Roaming          Layer 2 only
Active Bands          2.4GHz & 5GHz
Broadcast             On
DHCP Pool             None
DHCP Opt              Off
Filter List           None
Access Control        Disabled
Station Limit         Unlimited
Traffic Limit         Unlimited pps
Traffic Limit         Unlimited Kbps
Traffic/Station       Unlimited pps
Traffic/Station       Unlimited Kbps
Time on               Always
Time off              Never
Days on               All
MDM Authentication    None
Web Page Redirect     Disabled

SSID Unique WPA Security Settings
---------------------------------
Cipher                TKIP Off, AES  On
Key Management        EAP  On , PSK  Off
PSK Passphrase        Not set

CafeteriaAP(config-ssid-Companyx)# top
CafeteriaAP(config)# radius-server internal-radius
CafeteriaAP(config-radius-internal)# show

Internal RADIUS Server Settings Summary
---------------------------------------
State               enabled

Username        SSID            User Group      Password
--------------- --------------- --------------- --------
Mike            Companyx                        set

CafeteriaAP(config-radius-internal)#
CafeteriaAP(config-radius-internal)# save
```

Figure 193. Configuring an SSID-Specific SSID using WPA-PEAP

Enabling Global Radios

This example shows you how to enable all radios (radios), regardless of the wireless technology they use.

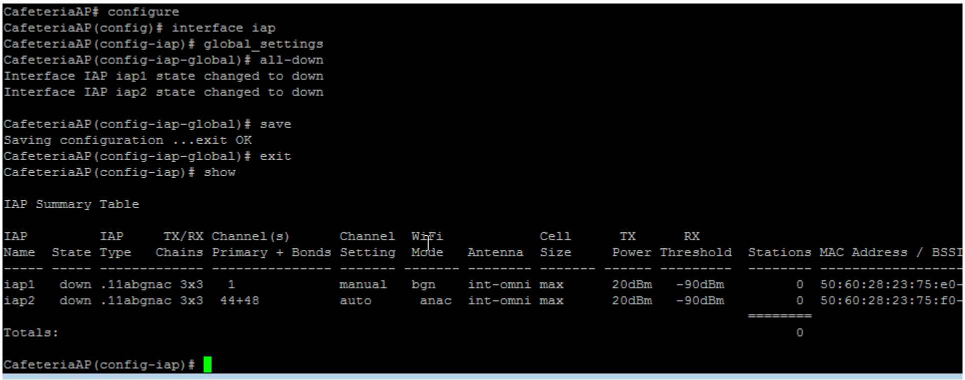


```
CafeteriaAP# configure
CafeteriaAP(config)# interface iap
CafeteriaAP(config-iap)# global_settings
CafeteriaAP(config-iap-global)# all-up
Interface IAP iap1 state changed to up
Interface IAP iap2 state changed to up

CafeteriaAP(config-iap-global)# save
Saving configuration ... OK
CafeteriaAP(config-iap-global)# exit
CafeteriaAP(config-iap)# show

IAP Summary Table

IAP         IAP     TX/RX Channel(s)      Channel  WiFi            Cell      TX      RX
Name  State Type   Chains Primary + Bonds Setting  Mode   Antenna  Cell      Power Threshold  Stations MAC Address / BS
----- ----- ------------- --------------- ------- ------- -------- ------- ------ ---------  -------- -----------------
iap1    up  .11abgnac 3x3   1             manual   bgn    int-omni max       20dBm   -90dBm          0  50:60:28:23:75:e
iap2    up  .11abgnac 3x3  44+48          auto      anac  int-omni max       20dBm   -90dBm          0  50:60:28:23:75:f
                                                                                             ========
Totals:                                                                                             0

CafeteriaAP(config-iap)# 
```

Figure 194. Enabling Global Radios

Disabling Global Radios

This example shows you how to disable all radios (radios), regardless of the wireless technology they use.

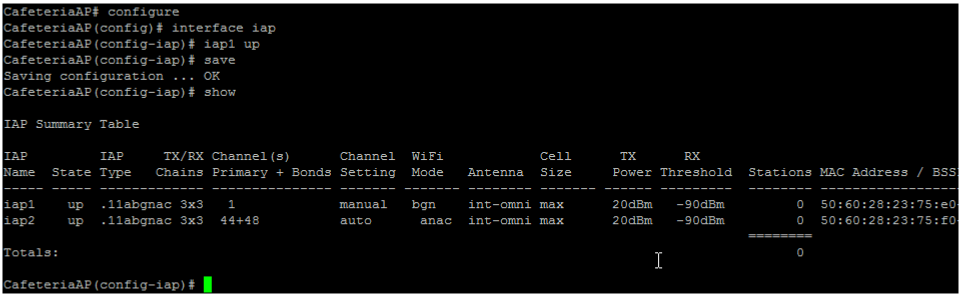


```
CafeteriaAP# configure
CafeteriaAP(config)# interface iap
CafeteriaAP(config-iap)# global_settings
CafeteriaAP(config-iap-global)# all-down
Interface IAP iap1 state changed to down
Interface IAP iap2 state changed to down

CafeteriaAP(config-iap-global)# save
Saving configuration ...exit OK
CafeteriaAP(config-iap-global)# exit
CafeteriaAP(config-iap)# show

IAP Summary Table

IAP         IAP     TX/RX Channel(s)      Channel  WiFi            Cell      TX      RX
Name  State Type   Chains Primary + Bonds Setting  Mode   Antenna  Size     Power Threshold  Stations MAC Address / BSSI
----- ----- ------------- --------------- ------- ------- -------- ------- ------ ---------  -------- ------------------
iap1   down .11abgnac 3x3   1             manual   bgn    int-omni max      20dBm   -90dBm          0 50:60:28:23:75:e0-
iap2   down .11abgnac 3x3  44+48          auto      anac  int-omni max      20dBm   -90dBm          0 50:60:28:23:75:f0-
                                                                                             ========
Totals:                                                                                             0

CafeteriaAP(config-iap)# 
```

Figure 195. Disabling Global Radios

Enabling a Specific Radio

This example shows you how to enable a specific radio (radio). In this example, the radio that is being enabled is **a1** (the first radio in the summary list).

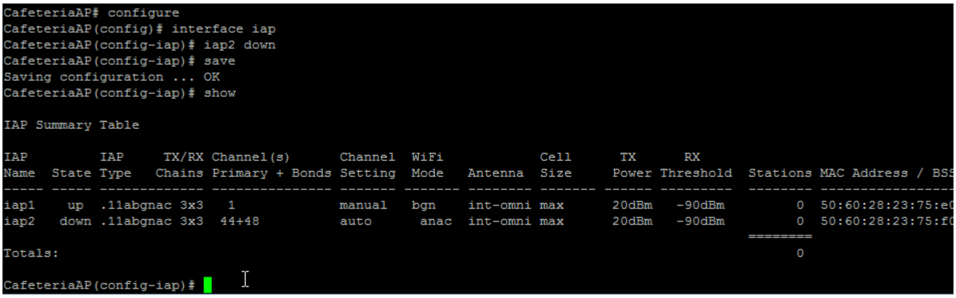


```
CafeteriaAP# configure
CafeteriaAP(config)# interface iap
CafeteriaAP(config-iap)# iap1 up
CafeteriaAP(config-iap)# save
Saving configuration ... OK
CafeteriaAP(config-iap)# show

IAP Summary Table

IAP         IAP     TX/RX Channel(s)      Channel  WiFi            Cell      TX      RX
Name  State Type   Chains Primary + Bonds Setting  Mode   Antenna  Size     Power Threshold  Stations MAC Address / BSS
----- ----- ------------- --------------- ------- ------- -------- ------- ------ ---------  -------- ------------------
iap1    up  .11abgnac 3x3   1             manual   bgn    int-omni max      20dBm   -90dBm          0  50:60:28:23:75:e0
iap2    up  .11abgnac 3x3  44+48          auto      anac  int-omni max      20dBm   -90dBm          0  50:60:28:23:75:f0
                                                                                             ========
Totals:                                                                                             0

CafeteriaAP(config-iap)# 
```

Figure 196. Enabling a Specific Radio

Disabling a Specific Radio

This example shows you how to disable a specific radio (radio). In this example, the radio that is being disabled is **a2** (the second radio in the summary list).



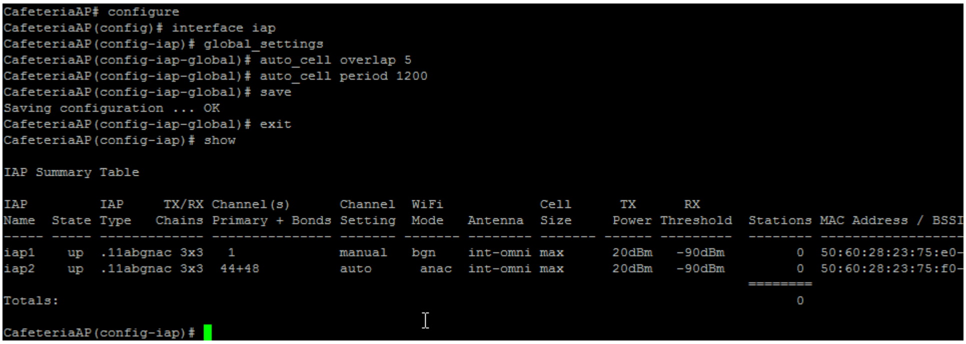
```
CafeteriaAP# configure
CafeteriaAP(config)# interface iap
CafeteriaAP(config-iap)# iap2 down
CafeteriaAP(config-iap)# save
Saving configuration ... OK
CafeteriaAP(config-iap)# show

IAP Summary Table

IAP         IAP     TX/RX Channel(s)      Channel  WiFi            Cell       TX      RX
Name  State Type   Chains Primary + Bonds Setting  Mode   Antenna  Size     Power Threshold   Stations MAC Address / BSS
----- ----- ------------- --------------- ------- ------- -------- ------- ------ ---------   -------- -----------------
iap1    up  .11abgnac 3x3   1             manual   bgn    int-omni max      20dBm   -90dBm          0 50:60:28:23:75:e0
iap2   down .11abgnac 3x3  44+48          auto      anac  int-omni max      20dBm   -90dBm          0 50:60:28:23:75:f0
                                                                                              ========
Totals:                                                                                              0

CafeteriaAP(config-iap)# 
```

Figure 197. Disabling a Specific Radio

Setting Cell Size Auto-Configuration for All Radios

This example shows how to set the cell size for all enabled radios to be auto-configured (**auto**). (See “Fine Tuning Cell Sizes” on page 27.) The **auto_cell** option may be used with **global_settings**, **global_a_settings**, or **global_bg_settings**. It sets the cell size of the specified radios to **auto**, and it launches an auto-configuration to adjust the sizes. Be aware that if the **intrude-detect** feature is enabled on the **monitor** radio**,** its cell size is unaffected by this command. Also, any radios used in WDS links are unaffected.

Auto-configuration may be set to run periodically at intervals specified by **auto_cell period** (in seconds) if **period** is non-zero. The percentage of overlap allowed between cells in the cell size computation is specified by **auto_cell overlap** (0 to 100). This example sets auto-configuration to run every 1200 seconds with an allowed overlap of 5%.



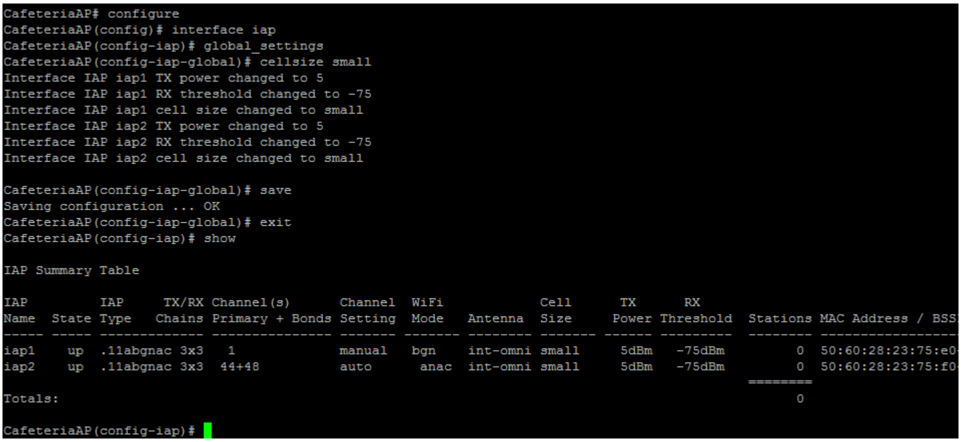
```
CafeteriaAP# configure
CafeteriaAP(config)# interface iap
CafeteriaAP(config-iap)# global_settings
CafeteriaAP(config-iap-global)# auto_cell overlap 5
CafeteriaAP(config-iap-global)# auto_cell period 1200
CafeteriaAP(config-iap-global)# save
Saving configuration ... OK
CafeteriaAP(config-iap-global)# exit
CafeteriaAP(config-iap)# show

IAP Summary Table

IAP         IAP     TX/RX Channel(s)      Channel  WiFi            Cell      TX      RX
Name  State Type   Chains Primary + Bonds Setting  Mode    Antenna  Cell      Power Threshold  Stations MAC Address / BSSI
----- ----- ------------- --------------- ------- ------- -------- ------- ------ ---------  -------- ------------------
iap1    up  .11abgnac 3x3   1             manual   bgn     int-omni max      20dBm   -90dBm          0  50:60:28:23:75:e0-
iap2    up  .11abgnac 3x3  44+48          auto      anac   int-omni max      20dBm   -90dBm          0  50:60:28:23:75:f0-
                                                                                             ========
Totals:                                                                                             0

CafeteriaAP(config-iap)#
```

Figure 198. Setting Cell Size Auto-Configuration for All Radios

Setting the Cell Size for All Radios

This example shows you how to establish the cell size for all radios (radios), regardless of the wireless technology they use. Be aware that if the **intrude-detect** feature is enabled on the monitor radio the cell size cannot be set globally—you must first disable the intrude-detect feature on the monitor radio.

In this example, the cell size is being set to **small** for all radios. You have the option of setting radio cell sizes to small, medium, large, or max. See also, "Fine Tuning Cell Sizes" on page 27.

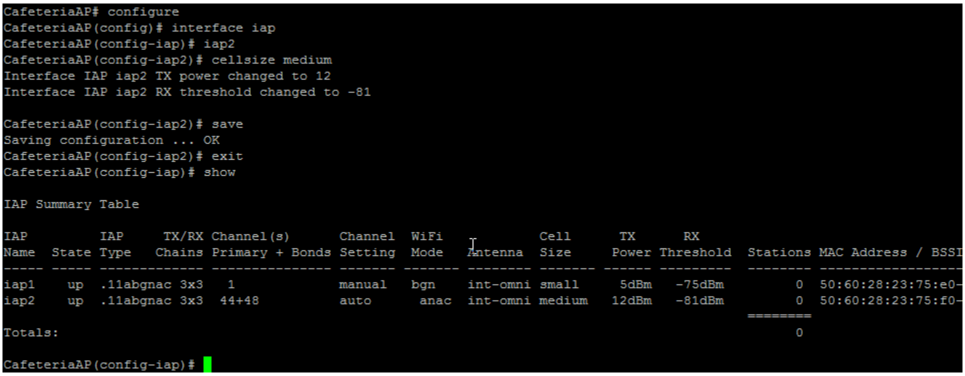


```
CafeteriaAP# configure
CafeteriaAP(config)# interface iap
CafeteriaAP(config-iap)# global_settings
CafeteriaAP(config-iap-global)# cellsize small
Interface IAP iap1 TX power changed to 5
Interface IAP iap1 RX threshold changed to -75
Interface IAP iap1 cell size changed to small
Interface IAP iap2 TX power changed to 5
Interface IAP iap2 RX threshold changed to -75
Interface IAP iap2 cell size changed to small

CafeteriaAP(config-iap-global)# save
Saving configuration ... OK
CafeteriaAP(config-iap-global)# exit
CafeteriaAP(config-iap)# show

IAP Summary Table

IAP         IAP     TX/RX Channel(s)      Channel  WiFi            Cell      TX      RX
Name  State Type   Chains Primary + Bonds Setting  Mode   Antenna  Size     Power Threshold  Stations MAC Address / BSS
----- ----- ------------- --------------- ------- ------- -------- ------- ------ ---------  -------- -----------------
iap1    up  .11abgnac 3x3   1             manual   bgn    int-omni small     5dBm   -75dBm          0 50:60:28:23:75:e0
iap2    up  .11abgnac 3x3  44+48          auto      anac  int-omni small     5dBm   -75dBm          0 50:60:28:23:75:f0
                                                                                             ========
Totals:                                                                                             0

CafeteriaAP(config-iap)#
```

Figure 199. Setting the Cell Size for All Radios

Setting the Cell Size for a Specific Radio

This example shows you how to establish the cell size for a specific radio (radio). In this example, the cell size for **a2** is being set to **medium**. You have the option of setting radio cell sizes to small, medium, large, or max (the default is max). See also, "Fine Tuning Cell Sizes" on page 27.



```
CafeteriaAP# configure
CafeteriaAP(config)# interface iap
CafeteriaAP(config-iap)# iap2
CafeteriaAP(config-iap2)# cellsize medium
Interface IAP iap2 TX power changed to 12
Interface IAP iap2 RX threshold changed to -81

CafeteriaAP(config-iap2)# save
Saving configuration ... OK
CafeteriaAP(config-iap2)# exit
CafeteriaAP(config-iap)# show

IAP Summary Table

IAP         IAP     TX/RX Channel(s)      Channel  WiFi            Cell      TX      RX
Name  State Type   Chains Primary + Bonds Setting  Mode   Antenna  Size     Power Threshold  Stations MAC Address / BSSI
----- ----- ------------- --------------- ------- ------- -------- ------- ------ ---------  -------- ------------------
iap1    up  .11abgnac 3x3   1             manual   bgn    int-omni small     5dBm   -75dBm          0  50:60:28:23:75:e0-
iap2    up  .11abgnac 3x3  44+48          auto      anac  int-omni medium   12dBm   -81dBm          0  50:60:28:23:75:f0-
                                                                                             ========
Totals:                                                                                            0

CafeteriaAP(config-iap)# 
```

Figure 200. Setting the Cell Size for a Specific Radio

Appendices

Page is intentionally blank

Appendix A: Quick Reference Guide

This section contains product reference information. Use this section to locate the information you need quickly and efficiently. Topics include:

- **"Factory Default Settings" on page 481**.
- **"Keyboard Shortcuts" on page 487**.

Factory Default Settings

The following tables show the WAP's factory default settings.

Host Name

Setting	Default Value
Host name	Serial Number (e.g., A1714170008D)

Network Interfaces

Serial

Setting	Default Value
Baud Rate	115200
Word Size	8 bits
Stop Bits	1
Parity	No parity
Time Out	10 seconds

Gigabit 1 and Gigabit 2

Setting	Default Value
Enabled	Yes
DHCP	Yes
Default IP Address	192.168.1.3
Default IP Mask	255.255.255.0
Default Gateway	None
Auto Negotiate	On
Duplex	Full
Speed	1000 Mbps
MTU Size	1500
Management Enabled	Yes

Server Settings

NTP

Setting	Default Value
Enabled	No
Primary	time.nist.gov
Secondary	pool.ntp.org

Syslog

Setting	Default Value
Enabled	Yes

Setting	Default Value
Local Syslog Level	Information
Maximum Internal Records	500
Primary Server	None
Primary Syslog Level	Information
Secondary Server	None
Secondary Syslog Level	Information

SNMP

Setting	Default Value
Enabled	Yes
Read-Only Community String (v2)	public
Read-Write Community String (v2)	private
Read-Only Community String (v3)	avaya-public
Read-Write Community String (v3)	avaya-private
Trap Host	null (no setting)
Trap Port	162
Authorization Fail Port	On

DHCP

Setting	Default Value
Enabled	No
Maximum Lease Time	300 minutes
Default Lease Time	300 minutes

Setting	Default Value
IP Start Range	192.168.1.4
IP End Range	192.168.1.254
NAT	Disabled
IP Gateway	None
DNS Domain	None
DNS Server (1 to 3)	None

Default SSID

Setting	Default Value
ID	**avaya**
VLAN	None
Encryption	Off
Encryption Type	None
QoS	2
Enabled	Yes
Broadcast	On

Security

Global Settings - Encryption

Setting	Default Value
Enabled	Yes
WEP Keys	null (all 4 keys)

Setting	Default Value
WEP Key Length	null (all 4 keys)
Default Key ID	1
WPA Enabled	No
TKIP Enabled	Yes
AES Enabled	Yes
EAP Enabled	Yes
PSK Enabled	No
Pass Phrase	null
Group Rekey	Disabled

External RADIUS (Global)

Setting	Default Value
Enabled	Yes
Primary Server	None
Primary Port	1812
Primary Secret	null (no secret)
Secondary Server	null (no IP address)
Secondary Port	1812
Secondary Secret	null (no secret)
Time Out (before primary server is retired)	600 seconds
Accounting	Disabled
Interval	300 seconds

Setting	Default Value
Primary Server	None
Primary Port	1813
Primary Secret	null (no secret)
Secondary Server	None
Secondary Port	1813
Secondary Secret	null (no secret)

Internal RADIUS

Setting	Default Value
Enabled	No
The user database is cleared upon reset to the factory defaults. For the Internal RADIUS Server you have a maximum of 1,000 entries.	

Administrator Account and Password

Setting	Default Value
ID	admin
Password	admin

Management

Setting	Default Value
SSH	On
SSH timeout	300 seconds

Setting	Default Value
Telnet	Off
Telnet timeout	300 seconds
Serial	On
Serial timeout	300 seconds
Management over Radios	Off
http timeout	300 seconds

Keyboard Shortcuts

The following table shows the most common keyboard shortcuts used by the Command Line Interface.

Action	Shortcut
Cut selected data and place it on the clipboard.	**Ctrl + X**
Copy selected data to the clipboard.	**Ctrl + C**
Paste data from the clipboard into a document (at the insertion point).	**Ctrl + V**
Go to top of screen.	**Ctrl + Z**
Copy the active window to the clipboard.	**Alt + Print Screen**
Copy the entire desktop image to the clipboard.	**Print Screen**
Abort an action at any time.	**Esc**
Go back to the previous screen.	**b**
Access the Help screen.	**?**

Appendix B: FAQ and Special Topics

This appendix provides valuable support information that can help you resolve technical difficulties. Before contacting Avaya, review all topics below and try to determine if your problem resides with the WAP or your network infrastructure. Topics include:

General Hints and Tips

This section provides some useful tips that will optimize the reliability and performance of your WAPs.

- The WAP requires careful handling. For best performance, units should be mounted in a dust-free and temperature-controlled environment.
- If using multiple WAPs in the same area, maintain a distance of at least 100 feet (30m) between WAPs if there is direct line-of-sight between the units, or at least 50 feet (15 m) if a wall or other barrier exists between the units.
- Keep the WAP away from electrical devices or appliances that generate RF noise. Because the WAP is generally mounted on ceilings, be aware of its position relative to lighting (especially fluorescent lighting).
- If you are deploying multiple units, the WAP should be oriented so that the monitor radio is oriented in the direction of the least required coverage, because when in monitor mode the radio does not function as an AP servicing stations.
- The WAP should only be used with Wi-Fi certified client devices.

See Also

Multiple SSIDs
Security
VLAN Support

Frequently Asked Questions

This section answers some of the most frequently asked questions, organized by functional area.

Multiple SSIDs

Q. What Are BSSIDs and SSIDs?

A. BSSID (Basic Service Set Identifier) refers to an individual access point radio and its associated clients. The identifier is the MAC address of the access point radio that forms the BSS.

A group of BSSs can be formed to allow stations in one BSS to communicate to stations in another BSS by way of a backbone that interconnects each access point.

The Extended Service Set (ESS) refers to the group of BSSIDs that are grouped together to form one ESS. The ESSID (often referred to as SSID or “wireless network name”) identifies the Extended Service Set. Clients must associate to a single ESS at any given time. Clients ignore traffic from other Extended Service Sets that do not have the same SSID.

Legacy access points typically support one SSID per access point. WAPs support the ability for multiple SSIDs to be defined and used simultaneously.

Q. What would I use SSIDs for?

A. The creation of different wireless network names allows system administrators to separate types of users with different requirements. The following policies can be tied to an SSID:

- Minimum security required to join this SSID.

- The wireless Quality of Service (QoS) desired for this SSID.
- The wired VLAN associated with this SSID.

As an example, one SSID named **accounting** might require the highest level of security, while another SSID named **guests** might have low security requirements.

Another example may define an SSID named **voice** that supports voice over Wireless LAN phones with the highest possible Quality of Service (QoS) definition. This type of SSID might also forward traffic to specific VLANs on the wired network.

Q. How do I set up SSIDs?

A. Use the following procedure as a guideline. For more detailed information, go to “SSIDs” on page 246.

1. From the Web Management Interface, go to the SSID Management page.
2. Select **Yes** to make the SSID visible to all clients on the network. Although the WAP will not broadcast SSIDs that are hidden, clients can still associate to a hidden SSID if they know the SSID name to connect to it.
3. Select the minimum security that will be required by users for this SSID.
4. If desired (optional), select a Quality of Service (QoS) setting for this SSID. The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID wireless traffic.
5. If desired (optional), select a VLAN that you want this traffic to be forwarded to on the wired network.
6. If desired (optional), you can select which radios this SSID will not be available on—the default is to make this SSID available on all radios.
7. Click on the **Save** button 💾 if you wish to make your changes permanent.

8. If you need to edit any of the SSID settings, you can do so from the SSID Management page.

See Also

General Hints and Tips
Security
SSIDs
SSID Management
VLAN Support

Security

Q. How do I configure the WAP for PCI DSS auditing?

A. A. To audit PCI DSS requirements, follow the instructions in "Auditing PCI DSS" on page 509.

Q. How do I know my management session is secure?

A. Follow these guidelines:

- Administrator passwords
  Always change the default administrator password (the default is **admin**), and choose a strong replacement password. When appropriate, issue **read only** administrator accounts.

- SSH versus Telnet
  Be aware that Telnet is not secure over network connections and should be used only with a direct serial port connection. When connecting to the unit's Command Line Interface over a network connection, you must use a Secure SHell (SSH) utility. The most commonly used freeware providing SSH tools is PuTTY. The WAP only allows SSH-2 connections, so your SSH utility must be set up to use SSH-2.

- Configuration auditing
  Do not change approved configuration settings. The optional WOS offers powerful management features for small or large WAP deployments, and can audit your configuration settings

automatically. In addition, using the WOS eliminates the need for an FTP server.

Q. Which wireless data encryption method should I use?

A. Wireless data encryption prevents eavesdropping on data being transmitted or received over the airwaves. The WAP allows you to establish the following data encryption configuration options:

- Open
  This option offers no data encryption and is **not recommended**, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTy.

- Wired Equivalent Privacy (WEP)
  This option provides minimal protection (though much better than using an open network). An early standard for wireless data encryption and supported by all Wi-Fi certified equipment, WEP is vulnerable to hacking and is therefore not recommended for use by Enterprise networks.

- Wi-Fi Protected Access (WPA)
  This is a much stronger encryption model than WEP and uses TKIP (Temporal Key Integrity Protocol) with AES (Advanced Encryption Standard) to prevent WEP cracks.

  TKIP solves security issues with WEP. It also allows you to establish encryption keys on a per-user-basis, with key rotation for added security. In addition, TKIP provides Message Integrity Check (MIC) functionality and prevents active attacks on the wireless network.

  AES is the strongest encryption standard and is used by government agencies; however, old legacy hardware may not be capable of supporting the AES mode (it probably won't work on older wireless clients). Because AES is the strongest encryption standard currently available, it is highly recommended for Enterprise networks.

Any of the above encryption modes can be used (and can be used at the same time).

TKIP encryption does not support high throughput rates, per the IEEE 802.11n.

Q. Which user authentication method should I use?

A. User authentication ensures that users are who they say they are. For example, the most obvious example of authentication is logging in with a user name and password. The WAP allows you to choose between the following user authentication methods:

- <u>Pre-Shared Key</u>
  Users must manually enter a key (pass phrase) on the client side of the wireless network that matches the key stored by the administrator in your WAPs.

- <u>RADIUS 802.1x with EAP</u>
  802.1x uses a RADIUS server to authenticate large numbers of clients, and can handle different EAP (Extensible Authentication Protocol) authentication methods, including EAP-TLS, EAP-TTLS and EAP-PEAP. The RADIUS server can be internal (provided by the WAP) or external. An external RADIUS server offers more functionality and is **recommended** for large Enterprise deployments.

  When using this method, user names and passwords must be entered into the RADIUS server for user authentication.

- <u>MAC Address ACLs (Access Control Lists)</u>
  MAC address ACLs provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network. Access Control Lists work well when there are a limited number of users—in this case, enter the MAC addresses of each user in the **Allow** list. In the event of a lost or stolen MAC adapter, enter the affected MAC address in the **Deny** list.

Q. Why do I need to authenticate my WAP units?

A. When deploying multiple WAPs, you may need to define which units are part of which wireless network (for example, if you are establishing more than one network). In this case you need to employ the WOS, which can authenticate your WAPs automatically and ensure that only authorized units are associated with the defined wireless network.

Q. What is rogue AP (Access Point) detection?

A. The WAP has integrated monitor capabilities, which can constantly scan the local wireless environment for rogue APs (non-Avaya devices that are not part of your wireless network), unencrypted transmissions, and other security issues. Administrators can then classify each rogue AP and ensure that these devices do not interrupt or interfere with the network.

See Also

General Hints and Tips

Multiple SSIDs

VLAN Support

VLAN Support

Q. What Are VLANs?

A. Virtual Local Area Networks (VLANs) are a logical grouping of network devices that share a common network broadcast domain. Members of a particular VLAN can be on any segment of the physical network but logically only members of a particular VLAN can see each other.

VLANs are defined and implemented using the wired network switches that are VLAN capable. Packets are tagged for transmission on a particular VLAN according to the IEEE 802.1Q standard, with VLAN switches processing packets according to the tag.

Q. What would I use VLANs for?

A. Logically separating different types of users, systems, applications, or other logical division aids in performance and management of different network devices. Different VLANs can also be assigned with different packet priorities to prioritize packets from one VLAN over packets from another VLAN.

VLANs are managed by software settings—instead of physically plugging in and moving network cables and users—which helps to ease network management tasks.

Q. What are Wireless VLANs?

A. Wireless VLANs allow similar functionality to the wired VLAN definitions and extend the operation of wired VLANs to the wireless side of the network.

Wireless VLANs can be mapped to wireless SSIDs so that traffic from wired VLANs can be sent to wireless users of a particular SSID. The reverse is also true, where wireless traffic originating from a particular SSID can be tagged for transmission on a particular wired VLAN.

Sixteen SSIDs can be defined on your WAP, allowing a total of sixteen VLANs to be accessed (one per SSID).

As an example, to provide guest user access an SSID of **guest** might be created. This SSID could be mapped to a wired VLAN that segregates unknown users from the rest of the wired network and restricts them to Internet access only. Wireless users could then associate to the wireless network via the **guest** SSID and obtain access to the Internet through the selected VLAN, but would be unable to access other privileged network resources.

See Also

General Hints and Tips

Multiple SSIDs

WAP Monitor and Radio Assurance Capabilities

All models of the WAP have integrated monitoring capabilities to check that the WAP's radios are functioning correctly, and act as a threat sensor to detect and prevent intrusion from rogue access points.

Enabling Monitoring on the WAP

Any radio may be set to monitor the WAP or to be a normal radio. In order to enable the functions required for intrusion detection and for monitoring the other WAP radios, you **must** configure one monitor radio on the Radio Settings window as follows:

- Check the **Enabled** checkbox.
- Set **Mode** to **Monitor**.
- Set **Channel** to **Monitor**.

The settings above will automatically set the **Antenna** selection to **Internal-Omni**., also required for monitoring. See the "Radio Settings" on page 284 for more details. The values above are the factory default settings for the WAP.

You must also enable **RF Monitor Mode** on the WAP (either **Timeshare** or **Dedicated**). See "Advanced RF Settings" on page 329.

How Monitoring Works

When the monitor radio has been configured as just described, it performs these steps continuously (24/7) to check the other radios on the WAP and detect possible intrusions:

1. The monitor radio scans all channels with a 200ms dwell time, hitting all channels about once every 10 seconds.
2. Each time it tunes to a new channel it sends out a probe request in an attempt to smoke out rogues.
3. It then listens for all probe responses and beacons to detect any rogues within earshot.
4. WAP radios respond to that probe request with a probe response.

Intrusion Detection is enabled or disabled separately from monitoring. See Step 1 in "Intrusion Detection" on page 343.

Radio Assurance

The WAP is capable of performing continuous, comprehensive tests on its radios to assure that they are operating properly. Testing is enabled using the **Radio Assurance Mode** setting (see "Advanced RF Settings" on page 329). When this mode is enabled, the monitor radio performs loopback tests on the WAP. Radio Assurance Mode requires **Intrusion Detection** to be set to **Standard** (See Step 1 in "Intrusion Detection" on page 343).

When **Radio Assurance Mode** is enabled:

1. The WAP keeps track of whether or not it hears beacons and probe responses from the WAP's radios.
2. After 10 minutes (roughly 60 passes on a particular channel by the monitor radio), if it has not heard beacons or probe responses from one of the WAP's radios it issues an alert in the Syslog. If repair is allowed (see "Radio Assurance Options" on page 499), the WAP will reset and reprogram that particular radio at the Physical Layer (PHY—Layer 1). This action takes under 100ms and stations are not deauthenticated, thus users should not be impacted.
3. After another 10 minutes (roughly another 60 passes), if the monitor still has not heard beacons or probe responses from the malfunctioning radio it will again issue an alert in the Syslog. If repair is allowed, the WAP will reset and reprogram the MAC (the lower sublayer of the Data Link Layer) and then all of the PHYs. This is a global action that affects all radios. This action takes roughly 300ms and stations are not deauthenticated, thus users should not be impacted.
4. After another 10 minutes, if the monitor still has not heard beacons or probe responses from that radio, it will again syslog the issue. If reboot is allowed (see "Radio Assurance Options" on page 499), the WAP will schedule a reboot. This reboot will occur at one of the following times, whichever occurs first:

- When no stations are associated to the WAP
- Midnight

Radio Assurance Options

If the monitor detects a problem with a WAP radio as described above, it will take action according to the preference that you have specified in the **Radio Assurance Mode** setting on the Advanced RF Settings window (see Step 2):

- **Failure alerts only**—The WAP will issue alerts in the Syslog, but will not initiate repairs or reboots.
- **Failure alerts & repairs, but no reboots**—The WAP will issue alerts and perform resets of the PHY and MAC as described above.
- **Failure alerts & repairs & reboots if needed**—The WAP will issue alerts, perform resets of the PHY and MAC, and schedule reboots as described above.
- **Disabled**—Disable loopback tests (no self-monitoring occurs). Loopback tests are disabled by default.

RADIUS Vendor Specific Attribute (VSA) for Avaya

Attribute Name	Attribute Value	Attribute Type	Attribute Specific Description	Attribute Specific Value
Avaya-Admin-Role	1	string	See note below	See note below
Avaya-User-VLAN	2	string		
Avaya-User-Qos-WiFi	3	integer	Best-Effort	0
			Background	1
			Video	2
			Voice	3
Avaya-User-Qos-L2	4	integer	Best-Effort	0
			Background	1
			Standard	2
			Excellent-Effort	3
			Controlled	4
			Video	5
			Voice	6
			Network-Control	7
Avaya-User-Qos-L3-TOS	5	integer	Routine	0
			Priority	1
			Immediate	2
			Flash	3
			Flash-Override	4
			Critical-ECP	5
			Internetwork-Control	6
			Network-Control	7
			Low-Delay	8

Attribute Name	Attribute Value	Attribute Type	Attribute Specific Description	Attribute Specific Value
			High-Throughput	16
			High-Reliability	32
Avaya-User-Qos-L3-DSCP	6	integer		
Avaya-User-Roaming-Layer	7	integer	L2-only	0
			L2-and-L3	1
			None	3
Avaya-User-Traffic-Limit	8	integer		
Avaya-User-DHCP-Pool	9	string		
Avaya-User-Filter-List	10	string		
Avaya-User-Group	11	string		
Avaya-User-Interface	12	string		
Avaya-User-Location	13	string		

A RADIUS VSA is defined for Avaya WAPs to control administrator privilege settings for user accounts. The RADIUS VSA is used by WAPs to define the following attribute for administrator accounts:

- **WAP administrators**—the **Avaya-Admin-Role** attribute sets the privilege level for this account. Set the value to the string defined in **Privilege Level Name** as described in "About Creating Admin Accounts on the RADIUS Server" on page 214.

VSA 100 Identifies WAPs

Attribute Name	Attribute Value	Attribute Type	Attribute Specific Description	Attribute Specific Value
Avaya-WLAN-Device-Id	100	string	See note below	See note below

This Attribute is sent by WAP 9100 Series Access Points with every authentication request. Thus the AP identifies itself as part of standard RADIUS Authentication messages.

This allows Avaya Identity Engines to identify an Authenticator device as a WAP 9100 Series AP, for applying pre-defined templates or policies.

Note that the VSA key (VENDOR value) for Avaya is 45:1.

Location Service Data Formats

Avaya WAPs are able to capture and upload visitor analytics data, acting as a sensor network in addition to providing wireless connectivity. This data is sent to the location server in different formats, based on the type of server. The **Location Server URL**, **Location Customer Key**, and **Location Period** for reporting data are configured under Location settings. See "Location" on page 169 for details. If a **Location Customer Key** has been entered, data is sent encrypted using AES with that key.

Euclid Location Server

If the **Location Server URL** contains the string **euclid**, then it specifies a Euclid server. Data is sent at the specified intervals, in the proprietary format expected by the Euclid location server.

Non-Euclid Location Server

If the **Location Server URL** doesn't contain the string "euclid", then data is sent as a JSON object at the specified intervals, with the following fields.

Field			Name	Description
ln			Location Name	WAP location string
ld			Location Data	Defined below
	vn		Version Number	Set to 1
	ma		MAC Address	Base Radio MAC Address
	mc		Message Count	Running message count (resets to 0 when WAP is rebooted)
	lt		Location Table	Table of Stations and APs heard during this window
		si	Station ID	Station MAC address (AES encrypted if cust-key is not blank)

Field			Name	Description
		bi	BSSID	BSSID that the station is on (AES encrypted if cust-key is not blank). Only stations that are associated to this AP will have a bi (BSSID) field, i.e., for unassociated stations the bi (BSSID) field will not be included.
		sm	Station OUI	OUI of Station manufacturer (the top 3 bytes of the MAC address that can be used to look up the manufacturer), unencrypted
		ap	AP Flag	1=AP, 0=Station
		dm	Device Mfg	Station manufacturer
		dt	Device Type	Type of device, such as iPhone or Android
		dc	Device Class	Category of device, such as phone or notebook
		px	Coordinate x	These location coordinates are sent to the AP by WOS. They appear only if the AP has been placed on an WOS map. *
		py	Coordinate y	
		pz	Coordinate z	
		cn	Count	Count of frames heard from device during this window
		ot	Origin Time	Timestamp of first frame in this window (Unix time in seconds)
		ct	Current Time	Timestamp of last frame in this window (Unix time in seconds)
		cf	Current Frequency	Frequency (MHz) last frame was heard on
		il	Interval Low	Minimum interval between frames (within 24 hr period)
		ih	Interval High	Maximum interval between frames (within 24 hr period)
		sl	Signal Low	Minimum signal strength (within 24 hr period)
		sh	Signal High	Maximum signal strength (within 24 hr period)
		so	Signal Origin	Signal strength of first frame heard

Field			Name	Description
		sc	Signal Current	Signal strength of last frame heard
		pr	Probe Request	For each radio hearing a probe request from a station: BSSID of receiving radio and the corresponding signal strength of last probe heard for the station on that radio **

* X, y, and z indicate the station location in terms of the number of pixels from the top left (x=0, y=0, z=0) on the WOS map, where x and y are the horizontal and vertical axes on the map, respectively, and z is typically the station's distance below the AP from the mounting site. The scale is the distance covered by a pixel in feet or meters based on the map's scale setting.

** Sample format with four radios receiving a station's probe request:

```
"pr":{"64:a7:dd:44:03:20":-69,"64:a7:dd:44:03:30":-68,"64:a7:dd:44:03:40":-70,
"64:a7:dd:44:03:60":-60}
```

Upgrading the WAP Using the Boot Loader

This procedure does not apply to Boot Loader versions 7000 or higher (these recent versions are supplied with Avaya OS 7.3 and above). See "Access Point Information" on page 83 to view the Boot Loader version on the WAP.

If you are experiencing difficulties communicating with the WAP using the Web Management Interface, the WAP provides lower-level facilities that may be used to accomplish an upgrade via the Boot Loader.

1. Log in to your Avaya customer support account and download the latest software update. The software update is provided as a zip file. Unzip the contents to a local temp directory. Take note of the extracted file name in case you need it later on—you may also need to copy this file elsewhere on the network depending on your situation.

2. Install a TFTP server software package if you don't have one running. It may be installed on any computer on your network, including your desktop or laptop. The Solar Winds version is freeware and works well.

   http://www.solarwinds.com

   The TFTP install process creates the **TFTP-Root** directory on your C: drive, which is the default target for sending and receiving files. This may be changed if desired. Place the extracted Avaya software update file(s) on this directory.

   You must make the following change to the default configuration of the Solar Winds TFTP server. In the **File** menu, select **Configure**, then select the **Security** tab. Click **Send files** and click **OK**.

3. Determine the IP address of the computer hosting the TFTP server. (To display the IP address, open a command prompt and type **ipconfig**)

4. Connect your WAP to the computer running TFTP: use Avaya Console to communicate with the WAP. Download Avaya Console and see the User's Guide here.

   Attach a network cable to the WAP's Gig1 port, if it is not already part of your network. Boot your WAP and watch the progress messages. When

Press space bar to exit to bootloader: is displayed, press the space bar. The rest of this procedure is performed using the bootloader.

The following steps assume that you are running DHCP on your local network.

5. Type **dhcp** and hit return. This instructs the WAP to obtain a DHCP address and use it during this boot in the bootloader environment.
6. Type **dir** and hit return to see what's currently in the compact flash.
7. Type **update server <TFTP-server-ip-addr> XS-7.x.x-xxxx.bin** (the actual file name will vary depending on WAP model and software version—use the file name from your software update) and hit return. The software update will be transferred to the WAP's memory and will be written to the compact flash card.
8. Type **dir** and hit return to verify that the new image is in the compact flash.
9. Type **env set bootfile_active XS-7.x.x-xxxx.bin** (the actual file name of the new image) and hit return. This sets the new image to be the current image—the image to load when the WAP reboots.
10. Type **env save** and hit return to save the change you just made.
11. Type **boot** and hit return. Your WAP will reboot, running your new version of software.

Appendix C: Auditing PCI DSS

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by major credit card companies to help those that process credit card transactions (or cardholder information) in order to secure cardholder information and protect it from unauthorized access, fraud and other security issues. The major contributors to the standard are VISA, MasterCard, American Express, JCB, and Discover. The standard also helps consolidate various individual standards that were developed by each of the listed card companies. Merchants or others who process credit card transactions are required to comply with the standard and to prove their compliance by way of an audit from a Qualified Security Assessor.

PCI DSS lays out a set of requirements that must be met in order to provide adequate security for sensitive data.

Payment Card Industry Data Security Standard Overview

The PCI Data Security Standard (PCI DSS) has 12 main requirements that are grouped into six *control objectives*. The following table lists each control objective and the specific requirements for each objective. For the latest updates to this list, check the PCI Security Standards Web site: www.pcisecuritystandards.org.

PCI DSS Control Objectives and Associated Requirements
Objective: Build and Maintain a Secure Network ● Requirement 1: Install and maintain a firewall configuration to protect cardholder data. ● Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
Objective: Protect Cardholder Data ● Requirement 3: Protect stored cardholder data. ● Requirement 4: Encrypt transmission of cardholder data across open, public networks.

PCI DSS Control Objectives and Associated Requirements
Objective: Maintain a Vulnerability Management Program ● Requirement 5: Use and regularly update anti-virus software. ● Requirement 6: Develop and maintain secure systems and applications.
Objective: Implement Strong Access Control Measures ● Requirement 7: Restrict access to cardholder data by business need-to-know. ● Requirement 8: Assign a unique ID to each person with computer access. ● Requirement 9: Restrict physical access to cardholder data.
Objective: Regularly Monitor and Test Networks ● Requirement 10: Track and monitor all access to network resources and cardholder data. ● Requirement 11: Regularly test security systems and processes.
Objective: Maintain an Information Security Policy ● Requirement 12: Maintain a policy that addresses information security.

PCI DSS and Wireless

The Avaya WAP provides numerous security features that allow it to be a component of a PCI DSS-compliant network. The following sections indicate the specific features that allow the WAP to operate in a PCI DSS mode.

The Avaya WAP PCI Compliance Configuration

The check list below is designed to help ensure that WAPs are configured in a manner that is supportive of PCI Data Security Standards. Detailed configuration steps for each item are found in the referenced section of the User's Guide.

✓	Avaya WAP Configuration for PCI DSS	See...
( ) ( )	Register at the Avaya Support Site to ensure notification and access to software updates. Confirm that the latest version of AOS is being used by checking the Avaya web site.	support.avaya.com
( )	Enable PCI Mode after configuring the WAP in a PCI compliant state to ensure configuration changes cannot be saved that would invalidate a PCI compliant configuration. This item is covered on the following pages.	The pci-audit Command, p. 512
( )	Allow only necessary protocols and networks to be accessed by configuring your corporate firewall or using the internal WAP firewall.	Filters, p. 363
( ) ( ) ( ) ( ) ( ) ( )	Change the default Admin account password. Remove any unnecessary admin or user accounts. Change the SNMP community string from the default password. Use WPA2 and 802.1x authentication. Change default SSID to a user-defined SSID. Disable SSID broadcast for all PCI compliant SSIDs.	Express Setup, p. 143 Admin Management, p. 210 SNMP, p. 175 SSIDs, p. 246 and Global Settings, p. 229 SSIDs, p. 246 SSIDs, p. 246
( ) ( ) ( )	Enable Secure Shell (ssh) for CLI (command line) access. Confirm telnet access is disabled (done by default). Confirm management over the wireless network is disabled.	Management Control, p. 217 Global Settings, p. 290

✓	Avaya WAP Configuration for PCI DSS	See...
( ) ( )	Check that external RADIUS servers have been configured for use with 802.1x and WPA / WPA2 wireless security. Ensure that WAP Administration Accounts are being validated by External RADIUS servers.	SSIDs, p. 246 and Global Settings, p. 229 Admin RADIUS, p. 214
( )	Ensure that each WAP is physically inaccessible such that console ports and management ports are not accessible.	See Indoor Enclosure
( ) ( )	Enable Syslog messaging and define a Syslog server on the wired network to receive Syslog messages. Enable NTP and define an NTP server (optional).	System Log, p. 171 Time Settings (NTP), p. 165
( )	Enable the RF Monitor radio in the WAP. Categorize known or approved devices as such. Respond to any alert of unknown or unapproved wireless devices discovered by the RF Monitor.	Radio Settings, p. 284 Rogue Control List, p. 242 Rogues, p. 101

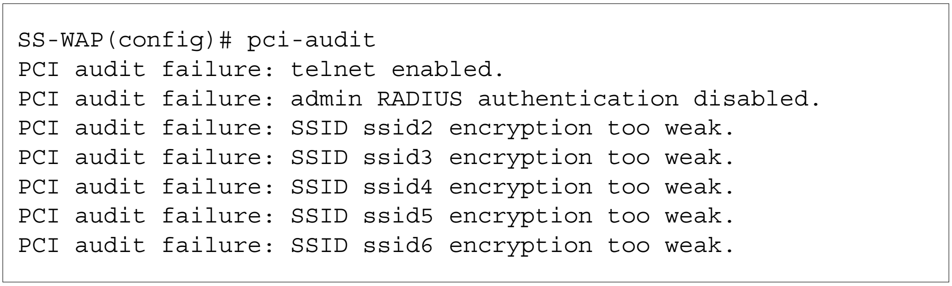
The pci-audit Command

The WAP provides a CLI command, pci-audit (part of the management command), that checks whether the WAP's configuration satisfies PCI DSS wireless requirements. This command does not change any parameters, but will inform you of any violations that exist. Furthermore, the command **pci-audit enable** will put the WAP in PCI Mode and monitor changes that you make to the WAP's configuration in CLI or the WMI. PCI Mode will warn you (and issue a Syslog message) if the change violates PCI DSS requirements. A warning is issued when a non-compliant change is first applied to the WAP, and also if you attempt to save a configuration that is non-compliant. Use this command in conjunction with The Avaya WAP PCI Compliance Configuration above to ensure that you are using the WAP in accordance with the PCI DSS requirements.

The pci-audit command checks items such as:

- Telnet is disabled.
- Admin RADIUS is enabled (admin login authentication is via RADIUS server).
- An external Syslog server is in use.
- All SSIDs must set encryption to WPA or better (which also enforces 802.1x authentication)

Sample output from this command is shown below.



```
SS-WAP(config)# pci-audit
PCI audit failure: telnet enabled.
PCI audit failure: admin RADIUS authentication disabled.
PCI audit failure: SSID ssid2 encryption too weak.
PCI audit failure: SSID ssid3 encryption too weak.
PCI audit failure: SSID ssid4 encryption too weak.
PCI audit failure: SSID ssid5 encryption too weak.
PCI audit failure: SSID ssid6 encryption too weak.
```

Figure 201. Sample output of pci-audit command

Additional Resources

- PCI Security Standards Web site: www.pcisecuritystandards.org
- List of Qualified PCI Security Assessors: www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

Glossary of Terms

802.11a

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 5 GHz and data rates of up to 54 Mbps.

802.11ac

A supplement to the IEEE 802.11 WLAN specification. Operates in the 5 GHz range, using a number of advanced techniques to achieve a maximum speed of 1.3 Gbps. These techniques include improvements on the methods used for 802.11n, below.

802.11b

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 11 Mbps.

802.11d

A supplement to the Media Access Control (MAC) layer in 802.11 to promote worldwide use of 802.11 WLANs. It allows Access Points to communicate information on the permissible radio channels with acceptable power levels for user devices. Because the 802.11 standards cannot legally operate in some countries, 802.11d adds features and restrictions to allow WLANs to operate within the rules of these countries.

802.11g

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 54 Mbps.

802.11n

A supplement to the IEEE 802.11 WLAN specification that describes enhancements to 802.11a/b/g to greatly enhance reach, speed, and capacity.

802.1Q

An IEEE standard for MAC layer frame tagging (also known as encapsulation). Frame tagging uniquely assigns a user-defined ID to each frame. It also enables a switch to communicate VLAN membership information across multiple (and multi-vendor) devices by frame tagging.

AES

(Advanced Encryption Standard) A data encryption scheme that uses three different key sizes (128-bit, 192-bit, and 256-bit). AES was adopted by the U.S. government in 2002 as the encryption standard for protecting sensitive but unclassified electronic data.

authentication

The process that a station, device, or user employs to announce its identify to the network which validates it. IEEE 802.11 specifies two forms of authentication, open system and shared key.

bandwidth

Specifies the amount of the frequency spectrum that is usable for data transfer. In other words, it identifies the maximum data rate a signal can attain on the medium without encountering significant attenuation (loss of power).

beacon interval

When a device in a wireless network sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. Network administrators can adjust the beacon interval—usually measured in milliseconds (ms) or its equivalent, kilo-microseconds (Kmsec).

bit rate

The transmission rate of binary symbols ('0' and '1'), equal to the total number of bits transmitted in one second.

BSS

(Basic Service Set) When a WLAN is operating in infrastructure mode, each access point and its connected devices are called the Basic Service Set.

BSSID

The unique identifier for an access point in a BSS network. See also, SSID.

cell

The basic geographical unit of a cellular communications system. Service coverage of a given area is based on an interlocking network of cells, each with a radio base station (transmitter/receiver) at its center. The size of each cell is determined by the terrain and forecasted number of users.

channel

A specific portion of the radio spectrum—the channels allotted to one of the wireless networking protocols. For example, 802.11ac and 802.11g use 14 channels in the 2.4 GHz band, only 3 of which don't overlap (1, 6, and 11).

CoS

(Class of Service) A category based on the type of user, type of application, or some other criteria that QoS systems can use to provide differentiated classes of service.

default gateway

The gateway in a network that a computer will use to access another network if a gateway is not specified for use. In a network using subnets, a default gateway is the router that forwards traffic to a destination outside of the subnet of the transmitting device.

DHCP

(Dynamic Host Configuration Protocol) A method for dynamically assigning IP addresses to devices on a network. DHCP issues IP addresses automatically within a specified range to client devices when they are first powered up.

DHCP lease

The DHCP lease is the amount of time that the DHCP server grants to the DHCP client for permission to use a particular IP address. A typical DHCP server allows its administrator to set the lease time.

DNS

(Domain Name System) A system that maps meaningful domain names with complex numeric IP addresses. DNS is actually a separate network—if one DNS server cannot translate a domain name, it will ask a second or third until a server is found with the correct IP address.

domain

The main name/Internet address of a user's Internet site as registered with the InterNIC organization, which handles domain registration on the Internet. For example, the "domain" address for Google is: http://www.google.com, broken down as follows:

- **http://** represents the Hyper Text Teleprocessing Protocol used by all Web pages.
- **www** is a reference to the World Wide Web.
- **google** refers to the company.
- **com** specifies that the domain belongs to a commercial enterprise.

DTIM

(Delivery Traffic Indication Message) A DTIM is a signal sent as part of a beacon by an access point to a client device in sleep mode, alerting the device to a packet awaiting delivery.

EAP

(Extensible Authentication Protocol) When you log on to the Internet, you're most likely establishing a PPP connection via a remote access server. The password, key, or other device you use to prove that you are authorized to do so is controlled via PPP's Link Control Protocol (LCP). However, LCP is somewhat inflexible because it has to specify an authentication device early in the process. EAP allows the system to gather more information from the user before deciding which authenticator to use. It is called extensible because it allows more authenticator types than LCP (for example, passwords and public keys).

EDCF

(Enhanced Distributed Coordinator Function) A QoS extension which uses the same contention-based access mechanism as current devices but adds "offset contention windows" that separate high priority packets from low priority packets (by assigning a larger random backoff window to lower priorities than to higher priorities). The result is "statistical priority," where high-priority packets usually are transmitted before low-priority packets.

encapsulation

A way of wrapping protocols such as TCP/IP, AppleTalk, and NetBEUI in Ethernet frames so they can traverse an Ethernet network and be unwrapped when they reach the destination computer.

encryption

Any procedure used in cryptography to translate data into a form that can be decrypted and read only by its intended receiver.

Fast Ethernet

A version of standard Ethernet that runs at 100 Mbps rather than 10 Mbps.

FCC

(Federal Communications Commission) US wireless regulatory authority. The FCC was established by the Communications Act of 1934 and is charged with regulating Interstate and International communications by radio, television, wire, satellite and cable.

FIPS

The Federal Information Processing Standard (FIPS) Publication 140-2 establishes a computer security standard used to accredit cryptographic modules. The standard is a joint effort by the U.S. and Canadian governments.

frame

A packet encapsulated to travel on a physical medium, like Ethernet or Wi-Fi. If a packet is like a shipping container, a frame is the boat on which the shipping container is loaded.

Gigabit Ethernet

A version of Ethernet with data transfer rates of 1 Gigabit (1,000 Mbps).

Group

A user group, created to define a set of attributes (such as VLAN, traffic limits, and Web Page Redirect) and privileges (such as fast roaming) that apply to all users that are members of the group. This allows a uniform configuration to be easily applied to multiple user accounts. The attributes that can be configured for user groups are almost identical to those that can be configured for SSIDs.

host name

The unique name that identifies a computer on a network. On the Internet, the host name is in the form **comp.xyz.net**. If there is only one Internet site the host name is the same as the domain name. One computer can have more than one host name if it hosts more than one Internet site (for example, **home.xyz.net** and **comp.xyz.net)**. In this case, **comp** and **home** are the host names and **xyz.net** is the domain name.

IPsec

A Layer 3 authentication and encryption protocol. Used to secure VPNs.

LLDP

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol used for advertising identities, capabilities, and neighbors on an IEEE 802 local area network

MAC address

(Media Access Control Address) A 6-byte hexadecimal address assigned by a manufacturer to a device.

Mbps

(Megabits per second) A standard measure for data transmission speeds (for example, the rate at which information travels over the Internet). 1 Mbps denotes one million bits per second.

MTU

(Maximum Transmission Unit) The largest physical packet size—measured in bytes—that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. Every network has a different MTU, which is set by the network administrator. Ideally, you want the MTU to be the same as the smallest MTU of all the networks between your machine and a message's final destination. Otherwise, if your messages are larger than one of the intervening MTUs, they will get broken up (fragmented), which slows down transmission speeds.

NTP

(Network Time Protocol) An Internet standard protocol (built on top of TCP/IP) that ensures the accurate synchronization (to the millisecond) of computer clock times in a network of computers. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock.

packet

Data sent over a network is broken down into many small pieces—packets—by the Transmission Control Protocol layer of TCP/IP. Each packet contains the address of its destination as well the data. Packets may be sent on any number of routes to their destination, where they are reassembled into the original data. This system is optimal for connectionless networks, such as the Internet, where there are no fixed connections between two locations.

PLCP

(Physical Layer Convergence Protocol) Defined by IEEE 802.6, a protocol specified within the Transmission Convergence layer that defines exactly how cells are formatted within a data stream for a particular type of transmission facility.

PoE

This refers to the Power over Gigabit Ethernet modules that provide DC power to WAPs. Power is supplied over the same Cat 5e or Cat 6 cable that supplies the data connection to your gigabit Ethernet switch, thus eliminating the need to run a power cable.

preamble

Preamble (sometimes called a header) is a section of data at the head of a packet that contains information that the access point and client devices need when sending and receiving packets. PLCP Has two structures, a long and a short preamble. All compliant 802.11b systems have to support the long preamble. The short preamble option is provided in the standard to improve the efficiency of a network's throughput when transmitting special data, such as voice, VoIP (Voice-over IP) and streaming video.

private key

In cryptography, one of a pair of keys (one public and one private) that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The private key is provided only to the requestor and never shared. The requestor uses the private key to decrypt text that has been encrypted with the public key by someone else.

PSK

(Pre-Shared Key) A TKIP passphrase used to protect your network traffic in WPA.

public key

In cryptography, one of a pair of keys (one public and one private) that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The public key is made publicly available for encryption and decryption.

QoS

(Quality of Service) QoS can be used to describe any number of ways in which a network provider prioritizes or guarantees a service's performance.

RADIUS

(Remote Authentication Dial-In User Service) A client-server security protocol, developed to authenticate, authorize, and account for dial-up users. The RADIUS server stores user profiles, which include passwords and authorization attributes.

RSSI

(Received Signal Strength Indicator) A measure of the energy observed by an antenna when receiving a signal.

SDMA

(Spatial Division Multiple Access) A wireless communications mode that optimizes the use of the radio spectrum and minimizes cost by taking advantage of the directional properties of antennas. The antennas are highly directional, allowing duplicate frequencies to be used for multiple zones.

SNMP

(Simple Network Management Protocol) A standard protocol that regulates network management over the Internet.

SNTP

(Simple Network Time Protocol) A simplified version of NTP. SNTP can be used when the ultimate performance of the full NTP implementation described in RFC 1305 is not needed or justified.

SSH

(Secure SHell) Developed by SSH Communications Security, Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. The WAP only allows SSH-2 connections. SSH-2 provides strong authentication and secure communications over insecure channels. SSH-2 protects a network from attacks, such as IP spoofing, IP source routing, and DNS spoofing. Attackers who has managed to take over a network can only force SSH to disconnect—they cannot "play back" the traffic or hijack the connection when encryption is enabled. When using SSH-2's slogin (instead of rlogin) the entire login session, including transmission of password, is encrypted making it almost impossible for an outsider to collect passwords. Be aware that your SSH utility must be set up to use SSH-2.

SSID

(Service Set IDentifier) Every wireless network or network subset (such as a BSS) has a unique identifier called an SSID. Every device connected to that part of the network uses the same SSID to identify itself as part of the family—when it wants to gain access to the network or verify the origin of a data packet it is sending over the network. In short, it is the unique name shared among all devices in a WLAN.

subnet mask

A mask used to determine what subnet an IP address belongs to. An IP address has two components: (1) the network address and (2) the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.

TKIP

(Temporal Key Integrity Protocol) Provides improved data encryption by scrambling the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the encryption keys haven't been tampered with.

transmit power

The amount of power used by a radio transceiver to send the signal out. Transmit power is generally measured in milliwatts, which you can convert to dBm.

User group

See Group.

VLAN

(Virtual LAN) A group of devices that communicate as a single network, even though they are physically located on different LAN segments. Because VLANs are based on logical rather than physical connections, they are extremely flexible. A device that is moved to another location can remain on the same VLAN without any hardware reconfiguration.

VLAN tagging

(Virtual LAN tagging) Static port-based VLANs were originally the only way to segment a network without using routing, but these port-based VLANs could only be implemented on a single switch (or switches) cabled together. Routing was required to transfer traffic between unconnected switches. As an alternative to routing, some vendors created proprietary schemes for sharing VLAN information across switches. These methods would only operate on that vendor's equipment and were not an acceptable way to implement VLANs. With the adoption of the 802.11n standard, traffic can be confined to VLANs that exist on multiple switches from different vendors. This interoperability and traffic containment across different switches is the result of a switch's ability to use and recognize 802.1Q tag headers—called VLAN tagging. Switches that implement 802.1Q tagging add this tag header to the frame directly after the destination and source MAC addresses. The tag header indicates:

1. That the packet has a tag.
2. Whether the packet should have priority over other packets.
3. Which VLAN it belongs to, so that the switch can forward or filter it correctly.

WDS (Wireless Distribution System)

WDS creates wireless backhauls between WAPs. These links between WAPs may be used rather than having to install data cabling to each WAP.

WEP

(Wired Equivalent Privacy) An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.

Wi-Fi Alliance

A nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability.

WAP

A high capacity wireless networking device consisting of multiple radios arranged in a circular WAP.

Wireless LAN Orchestration System (WOS)

An Avaya product used for managing large Wireless WAP deployments from a centralized Web-based interface.

WPA

(Wi-Fi Protected Access) A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP as an encryption method and 802.1x for authentication.

WPA2

(Wi-Fi Protected Access 2) WPA2 is the follow-on security method to WPA for wireless networks and provides stronger data protection and network access control. It offers Enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Like WPA, WPA2 is designed to secure all versions of 802.11 devices, including 802.11a, 802.11b, 802.11g, and 802.11n, multi-band and multi-mode.

Index