2-Port and 6-Port Wireless Access Controller

EWS4502
EWS4606

Software Release v1.3.0.47

Administrator's Guide

www.edge-core.com

Administrator's Guide

EWS4502 Wireless Access Controller
with 2 1000BASE-T (RJ-45) Ports

EWS4606 Wireless Access Controller
with 6 1000BASE-T (RJ-45) Ports

FW1.3.0.47
E082016/ST-R02
150200001196A

Table of Contents

List of Figures

List of Tables

About This Document

Purpose and Audience

This guide describes how to configure the ECW4502/ECW4606 software features by using the Web-based graphical user interface (GUI). The ECW4502/ECW4606 architecture accommodates a variety of software modules so that a platform running HAWK software can be a Layer 2 switch in a basic network or a Layer 3 router in a large, complex network.

The information in this guide is intended for any of the following individuals:

- System administrators who are responsible for configuring and operating a network using ECW4502/ECW4606 software
- Level 1 and/or Level 2 Support providers

To obtain the greatest benefit from this guide, you should have an understanding of the base software and should have read the specification for your networking device platform. You should also have basic knowledge of Ethernet and networking concepts.

Document Organization

This guide contains the following sections:

- Section 1: “Getting Started,” on page 33 contains information about performing the initial system configuration and accessing the user interfaces.
- Section 2: “Configuring System Information,” on page 41 describes how to configure administrative features such as SNMP, DHCP, and port information.
- Section 3: “Configuring Switching Information,” on page 117 describes how to manage and monitor the layer 2 switching features.
- Section 4: “Managing Device Security,” on page 131 contains information about configuring switch security information such as captive portal configuration, port access control, TACACS+, and RADIUS server settings.
- Section 5: “Configuring the Wireless Features,” on page 177 describes how to configure the switch so it can manage multiple access points on the network.

Document Conventions

The following conventions may be used in this document:

Convention	*Description*
Bold	User input and actions: for example, type **exit**, click **OK,** press **Alt+C**
`Monospace`	Code: `#include <iostream>` HTML: `<td rowspan = 3>` Command line commands and parameters: `wl [-l] <command>`
< >	Placeholders for *required* elements: enter your <username> or `wl <command>`

Convention	*Description*
[ ]	Indicates *optional* command-line parameters: `wl [-l]` Indicates bit and byte ranges (inclusive): [0:3] or [7:0]

Revision History

This section summarizes the changes in each revision of this guide.

Revision	*Date*	*Change Description*
DCSS Software v1.3.0.47	9/2016	**New** • "Displaying the Dashboard" on page 42 • "Setting the System Time" on page 44 • "Daylight Savings Time" on page 46 • "Select Authentication List" on page 61 • "Configuring System Information" on page 41 • "Configuring Switching Information" on page 117 • "GARP Configuration" on page 124"IP ACL Configuration" on page 220 • "WIFI Scheduler" on page 223 • "WIDS Security" on page 265 • "Remote Packet Capture" on page 288 • "WDS Configuration" on page 381 **Updated:** • Table 2: "Dashboard Fields," on page 42 • Table 10: "Network Connectivity Configuration for IPv4 Fields," on page 54 • Table 11: "DHCP Client Options Configuration Fields," on page 55 • Table 26: "Upload File to Switch Fields," on page 84 • Table 30: "HTTP File Upload Fields," on page 90 • Table 59: "Global Captive Portal Configuration," on page 133 • Table 60: "Captive Portal Summary," on page 134 • Table 61: "CP Configuration," on page 135 • Table 67: "Local User Summary Fields," on page 144 • Table 71: "Global Captive Portal Status Fields," on page 148 • Table 72: "CP Activation and Activity Status Fields," on page 149 • Table 73: "Interface Activation Status Fields," on page 150 • "Unified Access Point" on page 178 • Table 97: "Profile," on page 189 • "Radio Configuration" on page 190Table 98: "Radio Settings," on page 191 • Table 100: "Wireless Network Configuration," on page 197 • Table 104: "Valid Access Point Configuration," on page 206 • Table 107: "General Global Configurations," on page 213

Revision	*Date*	*Change Description (Cont.)*
		• **Updated (Cont.):** • "IP ACL Configuration" on page 220 • "WIFI Scheduler" on page 223 • Table 112: "WIFI Scheduler Configuration Fields," on page 224 • Table 113: "Rate Limit Configuration Fields," on page 226 • Table 115: "Known Client Summary Fields," on page 231 • Table 116: "Known Client Configuration," on page 233 • "AP Image Availability List" on page 233 • "Configuring Networks" on page 234 • Table 120: "Access Point Profile Global Configuration," on page 243 • Table 121: "Radio Settings," on page 247 • Table 124: "Local Access Point Database," on page 257 • Table 127: "Peer Switch Configuration Enable/Disable," on page 262 • "WIDS Security" on page 265 • Table 136: "Channel Plan History," on page 278 • Table 138: "Manual Power Adjustments," on page 281 • "License Management" on page 282 • Table 139: "License Management," on page 282 • Table 140: "Advanced AP Management," on page 284 • "Remote Packet Capture" on page 288 • Table 156: "Managed AP Radio Detail," on page 312 • Table 162: "Distributed Tunneling Status," on page 322 • Table 167: "Managed Access Point VAP Statistics," on page 329 • Table 168: "Managed Access Point Distributed Tunneling Statistics," on page 330 • Table 171: "Detailed Associated Client Status," on page 334 • "WDS Managed APs" on page 348 • Table 202: "Access Point Authentication Failure Status," on page 376` • "Access Point Authentication Failure Status" on page 374 • "WDS Configuration" on page 381 • "WDS Managed AP Configuration" on page 383 **Removed:** • "Access Point Software Download" • "Locating WLAN Devices" • "Switch Configuration" • "IP Address Conflict Detection" • "Serial Port" • "Authentication List Summary" • "Password Management Configuration" • "Configuring and Searching the Forwarding Database" • "AP Image Settings" • "Erase Startup Config File"

Revision	*Date*	*Change Description (Cont.)*
		Removed (cont.): • "AutoInstall"
DCSS Software v1.2.0.5	4/2015	**Updated:** • Table 115: "Known Client Summary Fields," on page 231 • "AP Image Availability List" on page 233 • "Configuring Networks" on page 234 • Table 120: "Access Point Profile Global Configuration," on page 244 • Table 121: "Radio Settings," on page 247 • "UWS and AP Discovery Methods" on page 179 • "IP Address of Switch Configured in the AP" on page 179 • "Discovery and Peer Switches" on page 182 • "Setup Wizard" on page 184 • "Wireless Global Configuration" on page 184 • "AP Image Settings" on page 187 • "Profile Configuration" on page 188 • "Radio Configuration" on page 190 • "Configuring the Default Network" on page 196 • "Using Static WEP" on page 200 • "Using WPA/WPA2 Personal or Enterprise" on page 201 • "Valid AP Configuration" on page 204 • "Adding a Valid Access Point" on page 204 • "Valid Access Point Configuration" on page 205 • "Network Connectivity Configuration" on page 210 • "Wireless Global Configuration" on page 212 • "Wireless SNMP Trap Configuration" on page 217 • "Wireless Network Summary" on page 234 • "Wireless Network Configuration" on page 236 • "Creating, Copying, and Deleting AP Profiles" on page 240 • "Applying an AP Profile" on page 241 • "Access Point Profile Global Configuration" on page 242 • "Access Point Profile Radio Configuration" on page 246 • "Configuring Basic Settings for a Wireless Network" on page 256 • "Local Access Point Database" on page 257 • "Adding a Valid Access Point" on page 257 • "Valid Access Point Configuration" on page 258 • "Peer Switch Configuration Enable/Disable" on page 262 • "RF Management" on page 275 • "Adjusting the Channel and Power" on page 286 • "AP Hardware Radio Capability" on page 303 • "Viewing Detected Client Pre-Authentication History" on page 368 • "Detected Client Pre-Authentication Summary" on page 371

Revision	*Date*	*Change Description (Cont.)*
		Updated (cont.): • "Detected Client Roam History Summary" on page 372 • "Access Point Authentication Failure Status" on page 374 **Removed:** • "Configuring Email Alerts" • "Configuring Time Ranges"
DCSS Software v1.0.7.1	6/2013	Initial release

Related Documents

The following documentation provides additional information about ECW4502/ECW4606 software:

- The *CLI Command Reference* describes the command-line interface (CLI) for managing, monitoring, and configuring the wireless controller.

About ECW4502/ECW4606 Software Modules

The ECW4502/ECW4606 software suite includes the following modules:

- Switching (Layer 2)
- Multicast
- Quality of Service
- WLAN Switching
- Management (CLI, Web UI, and SNMP)

Not all modules are available for all platforms or software releases.

ECW4502/ECW4606 software consists of flexible modules that can be applied in various combinations to develop advanced Layer 2/3/4+ products. The user-configurable features available on your switch depend on the installed modules.

Section 1: Getting Started

This section describes how to start the switch and access the user interface. It contains the following sections:

- Connecting the Switch to the Network
- Booting the Switch
- Understanding the User Interfaces

Connecting the Switch to the Network

To enable remote management of the wireless controller (switch) through telnet, a Web browser, or SNMP, you must connect the switch to the network. The switch has no IP address by default, and DHCP is disabled, so you must provide network information by connecting to the switch command-line interface (CLI) by using a local serial connection.

To access the switch over a network you must first configure it with network information (an IP address, subnet mask, and default gateway). You can configure the IP information using any of the following:

- BOOTP
- DHCP
- Terminal interface via the serial Console port

After you configure network information, such as the IP address and subnet mask, and the switch is physically and logically connected to the network, you can manage and monitor the switch remotely through SSH, telnet, a Web browser, or an SNMP-based network management system. You can also continue to manage the switch through the terminal interface via the Console port.

After you perform the physical hardware installation, you need to make a serial connection to the switch so that you can do one of the following:

- Manually configure network information for the management interface, or
- Enable the management interface as a DHCP or BOOTP client on your network (if not already enabled) and then view the network information after it is assigned by the DHCP server.

To connect to the switch and configure or view network information, use the following steps:

1. Using the included console cable, connect a VT100/ANSI terminal or a workstation to the Console (serial) port.

   If you attached a PC, Apple®, or UNIX® workstation, start a terminal-emulation program, such as HyperTerminal or TeraTerm.
2. Configure the terminal-emulation program to use the following settings:
   - Baud rate: 115200 bps
   - Data bits: 8
   - Parity: none
   - Stop bit: 1
   - Flow control: none

3. Power on the switch.

   For information about the boot process, including how to access the boot menu, see "Booting the Switch" on page 34.

4. Press the return key, and the `User:` prompt appears.

   Enter `admin` as the user name. There is no default password. Press ENTER at the password prompt if you did not change the default password.

   After a successful login, the screen shows the system prompt, for example `(EdgeCore Switching)>`.

5. At the `(EdgeCore Switching)>` prompt, enter `enable` to enter the Privileged EXEC command mode. There is no default password to enter Privileged EXEC mode. Press ENTER at the password prompt if you did not change the default password.

   The command prompt changes to `(EdgeCore Switching)#`.

6. Configure network information.
   - To use a DHCP server to obtain the IP address, subnet mask, and default gateway information, enter:
     ```
     network protocol dhcp.
     ```
   - To use a BOOTP server to obtain the IP address, subnet mask, and default gateway information, enter:
     ```
     network protocol bootp.
     ```
   - To manually configure the IPv4 address, subnet mask, and (optionally) default gateway, enter:
     ```
     network parms <ipaddress> <netmask> [<gateway>],
     ```
     For example:
     ```
     network parms 192.168.2.23 255.255.255.0 192.168.2.1
     ```
   - To manually configure the IPv6 address, subnet mask, and (optionally) default gateway, enter:
     ```
     network ipv6 address <address>/<prefix-length> [eui64]
     network ipv6 gateway <gateway>
     ```
   - To view the network information, enter `show network`.
   - To save these changes so they are retained during a switch reset, enter the following command:
     ```
     copy system:running-config nvram:startup-config
     ```

After the switch is connected to the network, you can use the IP address for remote access to the switch by using a Web browser or through Telnet or SSH.

Booting the Switch

When the power is turned on with the local terminal already connected, the switch goes through Power-On Self-Test (POST). POST runs every time the switch is initialized and checks hardware components to determine if the switch is fully operational before completely booting.

If a critical problem is detected, the program flow stops. If POST passes successfully, a valid executable image is loaded into RAM.

POST messages are displayed on the terminal and indicate test success or failure.

To boot the switch, perform the following steps:

1. Make sure that the serial cable is connected to the terminal.
2. Connect the power supply to the switch.

3. Power on the switch.

   As the switch boots, the bootup test first counts the switch memory availability and then continues to boot.

After the switch boots successfully, the User login prompt appears and you can use the local terminal to begin configuring the switch. However, before configuring the switch, make sure that the software version installed on the switch is the latest version. If it is not the latest version, download and install the latest version. See "Upload File To Switch (TFTP)" on page 82.

Understanding the User Interfaces

EWS4502/EWS4606 software includes a set of comprehensive management functions for configuring and monitoring the system by using one of the following three methods:

- Web User Interface
- Command-Line Interface (CLI)
- Simple Network Management Protocol (SNMP)

Each of the standards-based management methods allows you to configure and monitor the components of the EWS4502/EWS4606 software. The method you use to manage the system depends on your network size and requirements, and on your preference.

This guide describes how to use the Web-based interface to manage and monitor the system. For information about how to manage and monitor the system by using the CLI, see the *CLI Command Reference*.

Using the Web Interface

To access the switch by using a Web browser, the browser must meet the following software requirements:

- HTML version 4.0, or later
- HTTP version 1.1, or later
- JavaScript™ version 1.5, or later

Use the following procedures to log on to the Web Interface:

1. Open a Web browser and enter the IP address of the switch in the Web browser address field.
2. Type the user name and password into the fields on the login screen, and then click **Login**.

   The user name and password are the same as those you use to log on to the command-line interface. By default, the user name is ***admin***, and there is no password. Passwords are case sensitive.

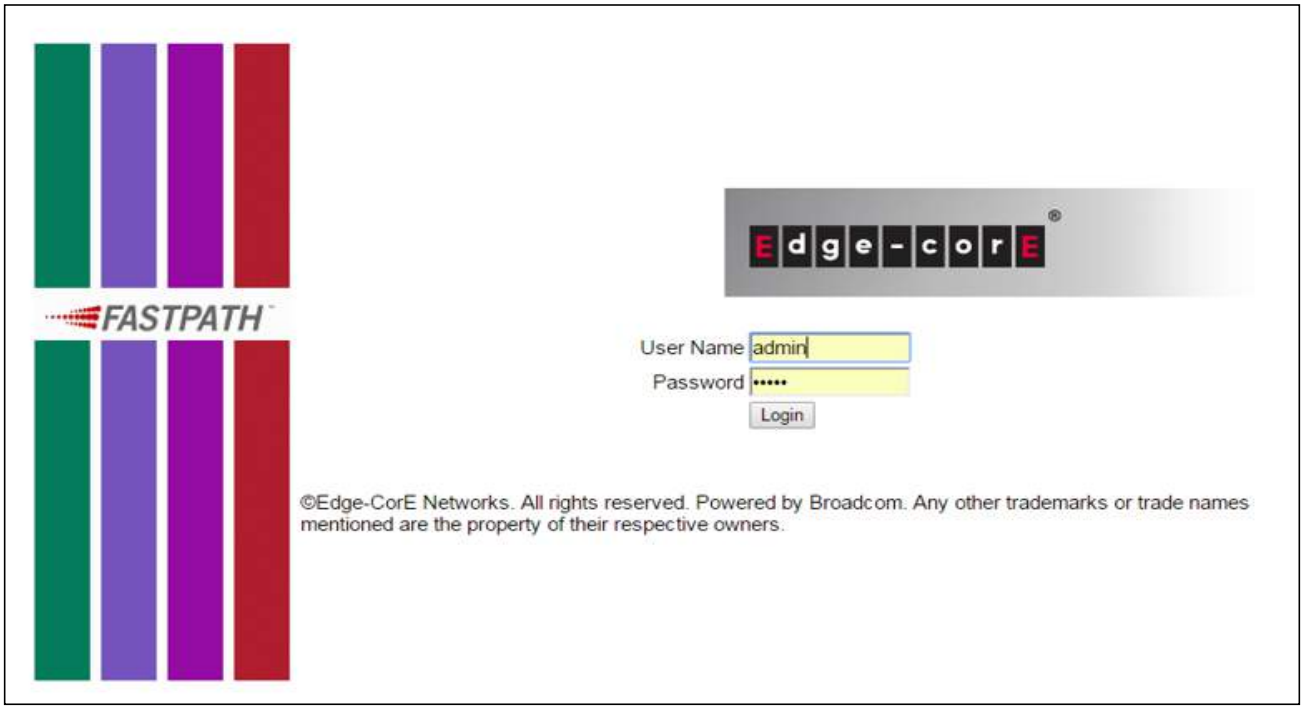


Figure 1: Login Page

3. After the system authenticates you, the Dashboard displays. For a description of the items listed on this page, refer to "Displaying the Dashboard" on page 42.

Navigation Tree View

The hierarchical-tree view is on the left side of the Web interface. The tree view contains a list of various device features. The branches in the navigation tree can be expanded to view all the components under a specific feature, or retracted to hide the feature's components.

The tree consists of a combination of folders, subfolders, and configuration and status HTML pages. Click the folder to view the options in that folder. Each folder contains either subfolders or HTML pages, or a combination of both. Figure 2 shows an example of a folder, subfolder, and HTML page in the navigation menu. When you click a folder or subfolder that is preceded by a plus sign (+), the folder expands to display the contents. If you click an HTML page, a new page displays in the main frame. A folder or subfolder has no corresponding HTML page.

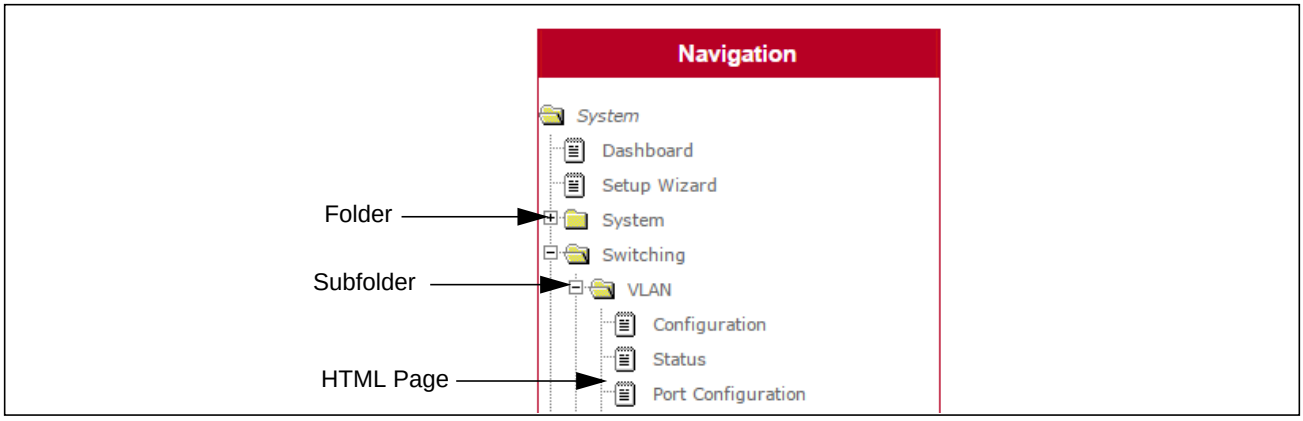


Figure 2: Navigation Tree View

Configuration and Monitoring Options

The panel directly under the graphic and to the right of the navigation menu displays the configuration information or status for the page you select. On pages that contain configuration options, you can input information into fields or select options from drop-down menus.

Each page contains access to the HTML-based help that explains the fields and configuration options for the page. Many pages also contain command buttons.

The following command buttons are used throughout the pages in the Web interface:

Table 1: Common Command Buttons

Button	*Function*
Submit	Clicking the **Submit** button sends the updated configuration to the switch. Configuration changes take effect immediately, but changes are not retained across a power cycle unless you save them to the system configuration file.
Refresh	Clicking the **Refresh** button refreshes the page with the latest information from the router.
Save	Clicking the **Save** button saves the current configuration to the system configuration file. When you click **Save**, changes that you have submitted are saved even when you reboot the system. To save the configuration to non-volatile memory, navigate to the **System > System Utilities > Save All Applied Changes** page and click **Save**.
Logout	Clicking the **Logout** button ends the session.

Caution! Submitting changes makes them effective during the current boot session only. You must save any changes if you want them to be retained across a power cycle (reboot).

Help Page Access

Every page contains a link to the online help, which contains information to assist in configuring and managing the switch. The online help pages are context sensitive. For example, if the IP Addressing page is open, the help topic for that page displays if you click Help. Figure 3 shows the link to click to access online help on each page.

Figure 3: Help Link

User-Defined Fields

User-defined fields can contain 1-159 characters, unless otherwise noted on the configuration Web page.

All characters may be used except for the following (unless specifically noted in for that feature):

\ <
/ >|
* |
?

Using the Command-Line Interface

The command-line interface (CLI) is a text-based way to manage and monitor the system. You can access the CLI by using a direct serial connection or by using a remote logical connection with telnet or SSH.

The CLI groups commands into modes according to the command function. Each of the command modes supports specific software commands. The commands in one mode are not available until you switch to that particular mode, with the exception of the User EXEC mode commands. You can execute the User EXEC mode commands in the Privileged EXEC mode.

To display the commands available in the current mode, enter a question mark (?) at the command prompt. To display the available command keywords or parameters, enter a question mark (?) after each word you type at the command prompt. If there are no additional command keywords or parameters, or if additional parameters are optional, the following message appears in the output:

```
<cr>                    Press Enter to execute the command
```

For more information about the CLI, see the *CLI Command Reference.*

The *CLI Command Reference* lists each command available from the CLI by the command name and provides a brief description of the command. Each command reference also contains the following information:

- The command keywords and the required and optional parameters.
- The command mode you must be in to access the command.

- The default value, if any, of a configurable setting on the device.

The `show` commands in the document also include a description of the information that the command shows.

Using SNMP

For EWS4502/EWS4606 software that includes the SNMP module, you can configure SNMP groups and users that can manage traps that the SNMP agent generates.

EWS4502/EWS4606 software uses both standard public MIBs for standard functionality and private MIBs that support additional switch functionality. All private MIBs begin with a "-" prefix. The main object for interface configuration is in -SWITCHING-MIB, which is a private MIB. Some interface configurations also involve objects in the public MIB, IF-MIB.

SNMP is enabled by default. The System Description Web page, which is the page that displays after a successful login, and the `show sysinfo` command displays the information you need to configure an SNMP manager to access the switch.

Any user can connect to the switch using the SNMPv3 protocol, but for authentication and encryption, you need to configure a new user profile. To configure a profile by using the CLI, see the SNMP section in the *CLI Command Reference*. To configure an SNMPv3 profile by using the Web interface, use the following steps:

1. Select **System > Configuration > User Accounts** from the hierarchical tree on the left side of the Web interface.
2. From the **User** menu, select **Create** to create a new user.
3. Enter a new user name in the **User Name** field.
4. Enter a new user password in the **Password** field and then retype it in the **Confirm Password** field.

   To use SNMPv3 Authentication for this user, set a password of eight or more alphanumeric characters.
5. To enable authentication, use the **Authentication Protocol** menu to select either MD5 or SHA for the authentication protocol.
6. To enable encryption, use the **Encryption Protocol** menu to select **DES** for the encryption scheme. Then, enter an encryption code of eight or more alphanumeric characters in the Encryption Key field.
7. Click **Submit**.

To access configuration information for SNMPv1 or SNMPv2, click and click the page that contains the information to configure.

Section 2: Configuring System Information

Use the features in the System navigation tree folder to define the switch's relationship to its environment. The **System** folder contains links to the following features:

- Displaying the Dashboard
- Setting the System Time
- Viewing ARP Cache
- Viewing Inventory Information
- Viewing the Dual Image Status
- Viewing System Resources
- Defining General Device Information
- Defining SNMP Parameters
- Viewing System Statistics
- Using System Utilities
- Managing SNMP Traps
- Configuring DNS
- Configuring SNTP Settings

Displaying the Dashboard

When your web browser connects with the switch's web agent, the Dashboard is displayed as shown below. The Dashboard displays the main menu on the left side of the screen. Basic switch Information is displayed on the right side. The main menu links are used to navigate to other menus, and display configuration parameters and statistics.

To display the Dashboard, click **System > Dashboard** in the navigation tree.

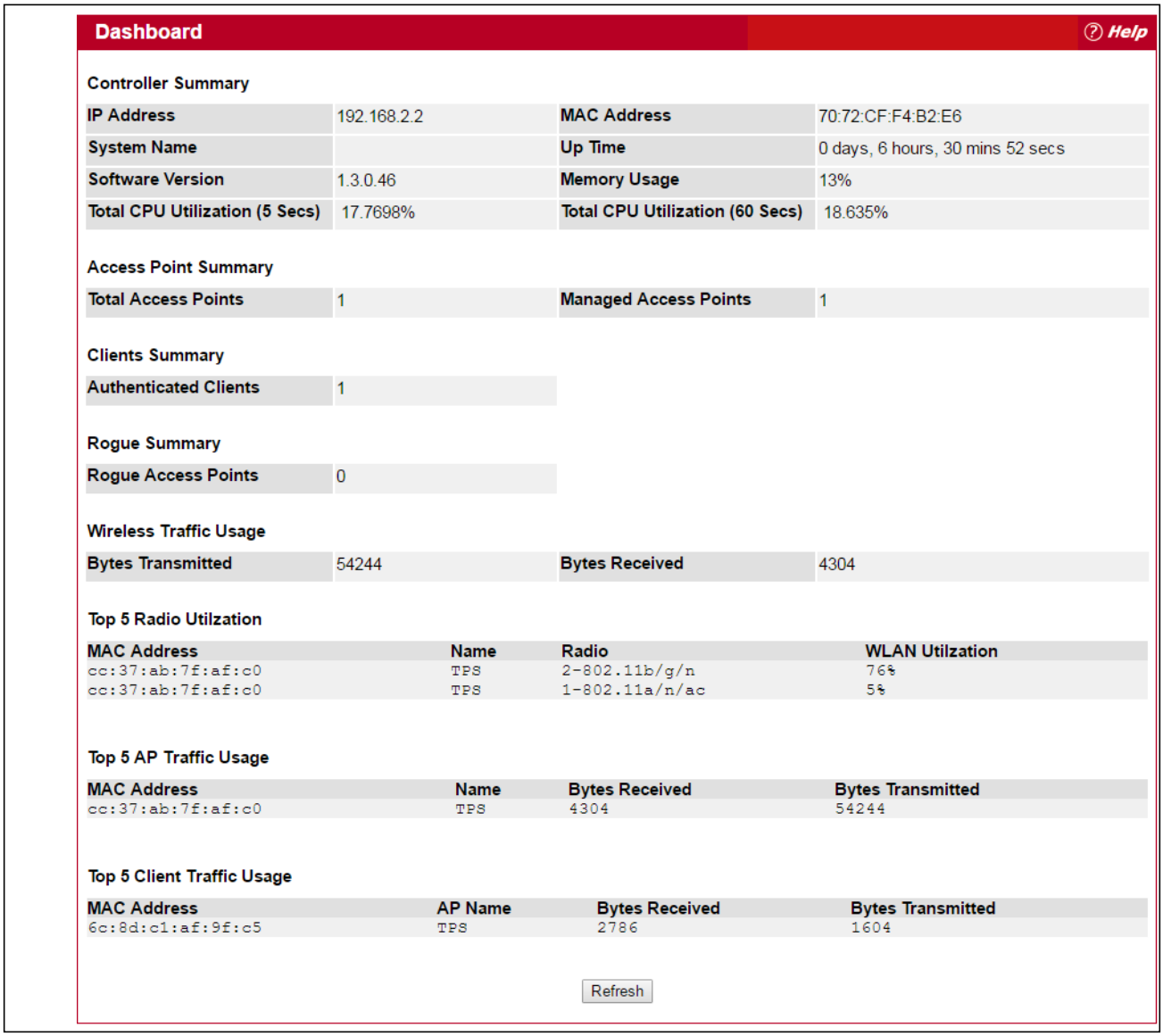


Figure 4: Dashboard

Table 2: Dashboard Fields

Field	*Description*
IP Address	Displays the IP address associated with the system's MAC address.

Table 2: Dashboard Fields (Cont.)

Field	*Description*
MAC Address	Displays the physical (MAC) address of the system.
System Name	The name used to identify this switch.
Up Time	The number of days, hours, minutes, and seconds since the last system restart.
Software Version	The release version.maintenance number of the code currently running on the switch. For example, if the release is 1, the version is 2 and the maintenance number is 4, the format is "1.2.4."
Memory Usage	The amount of memory allocated to active processes.
Total CPU Utilization (5 Secs)	Displays the total CPU utilization in the last five seconds.
Total CPU Utilization (60 Secs)	Displays the total CPU utilization in the last sixty seconds.
Access Point Summary	
Total Access Points	The number of access points known by the system.
Managed Access Points	The number of access points managed by the system.
Clients Summary	
Authenticated Clients	The number of authenticated clients registered by the system.
Rogue Summary	
Rogue Access Points	The number of APs classified as a threat by one of the threat detection algorithms.
Wireless Traffic Usage	
Bytes Transmitted	The number of WLAN bytes transmitted by the system.
Bytes Received	The number of WLAN bytes received by the system.
Top 5 Radio Utilzation	The top five clients in terms of radio utilization and WLAN utilization.
MAC Address	MAC address of the client.
Name	Configured name of the client.
Radio	Radio on which the utilization is reported.
WLAN Utilzation	WLAN utilization for the indicated client
Top 5 AP Traffic Usage	The top five access points in terms of traffic usage.
MAC Address	MAC address of the indicated access point.
Name	Configured name of the access point.
Bytes Received	The number of bytes received from each access point.
Bytes Transmitted	The number of bytes transmitted by each access point.
Top 5 Client Traffic Usage	The top five clients in terms of traffic usage.
MAC Address	MAC address of the indicated client.
AP Name	Configured name of the client.
Bytes Received	The number of bytes received from each client.
Bytes Transmitted	The number of bytes transmitted by each client.

Click **Refresh** to refresh the information on the dashboard.

Setting the System Time

The System Time folder in the System menu contains links to pages that allow you to display the system time, or configure the time zone and summer time parameters. The System Time folder contains links to the following features:

- Summer Time Status
- Time Zone
- Daylight Savings Time

Summer Time Status

The Summer Time Status page displays information on the system time. Use this page to view the system clock, time zone, and summer time settings.

To display the Summer Time Status page, click **System > System Time > Status** in the navigation tree.

Figure 5: System Time Status

Table 3: System Time Status Fields

Field	*Description*
System Time	Displays the system clock.
Time Zone	Displays the time zone for the system clock.
DST Status	Displays the status of Daylight Savings Time (DST). In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time. Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.

Time Zone

The Time Zone page sets the time zone for the switch's internal clock. Use this page to configure the local time zone relative to the Coordinated Universal Time (UTC), formerly Greenwich Mean Time or GMT).

The Time Zone page allows you to change the local time zone using the Web interface. To configure the settings on the Time Zone page, click **System > System Time> Time Zone** in the navigation tree.

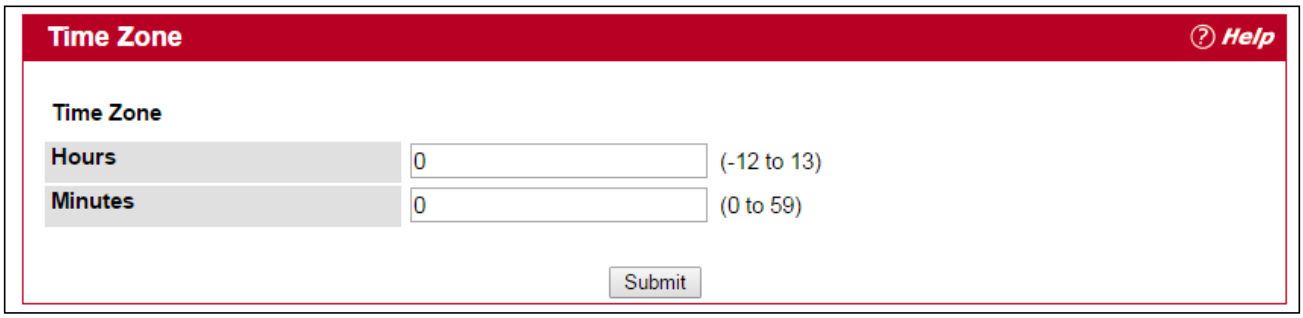


Figure 6: Time Zone

Table 4: Time Zone Fields

Field	*Description*
Hours	Number of hours before/after UTC. (Range: 0-12 hours before UTC, 0-13 hours after UTC)
Minutes	Number of minutes before/after UTC. (Range: 0-59 minutes)

This page sets the local time zone relative to the Coordinated Universal Time (UTC), formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To configure a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Defining The Time Zone

1. Open the **Time Zone** page.
2. Define the following fields: **Hours**, and **Minutes**.
3. Click **Submit**.

   The system parameters are applied, and the device is updated.

Daylight Savings Time

The Summer Time Support page configures Summer Time status.

To configure the status on the Summer Time Support page, click **System > System Time> Daylight Savings Time** in the navigation tree.

Figure 7: Summer Time Support

If you change the summer time status, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

Viewing ARP Cache

The ARP cache is a table maintained locally in each station on a network. ARP cache entries are learned by examining the source information in the ARP packet payload fields, regardless of whether it is an ARP request or response. Thus, when an ARP request is broadcast to all stations on a LAN segment or virtual LAN (VLAN), every recipient has the opportunity to store the sender's IP and MAC address in their respective ARP cache. The ARP response, being unicast, is normally seen only by the requestor, who stores the sender information in its ARP cache. Newer information always replaces existing content in the ARP cache.

The ARP cache can support 1024 entries, although this size is user-configurable to any value less than 1024. When multiple network interfaces are supported by a device, as is typical of a router, either a single ARP cache is used for all interfaces, or a separate cache is maintained per interface. While the latter approach is useful when network addressing is not unique per interface, this is not the case for Ethernet MAC address assignment so a single ARP cache is employed.

To display the system ARP cache, click **System** > **ARP Cache** page in the navigation tree.

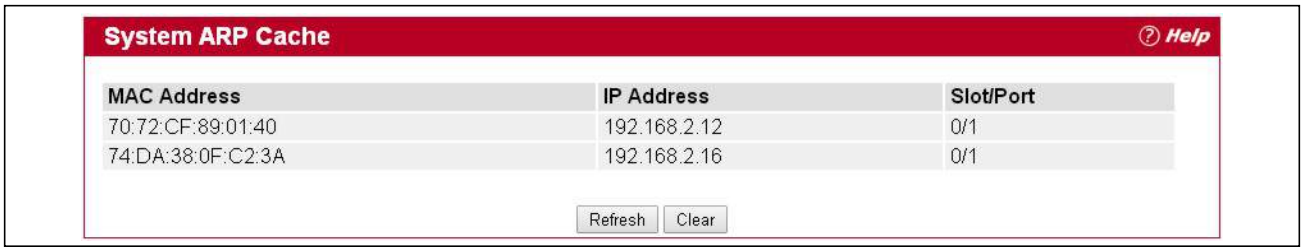


Figure 8: ARP Cache

Table 5: ARP Cache Fields

Field	*Description*
MAC Address	Displays the physical (MAC) address of the system in the ARP cache.
IP Address	Displays the IP address associated with the system's MAC address.
Slot/Port	Displays the unit, slot, and port number being used for the connection. For non-stacking systems, only the slot and port number is displayed. For units that have a service port, the service port will be listed as "Management" in this field.

Click **Refresh** to reload the page and refresh the ARP cache view.

Viewing Inventory Information

Use the Inventory Information page to display the switch's Vital Product Data, which is stored in non-volatile memory at the factory.

To display the inventory information, click **System** > **Inventory Information** page in the navigation tree.

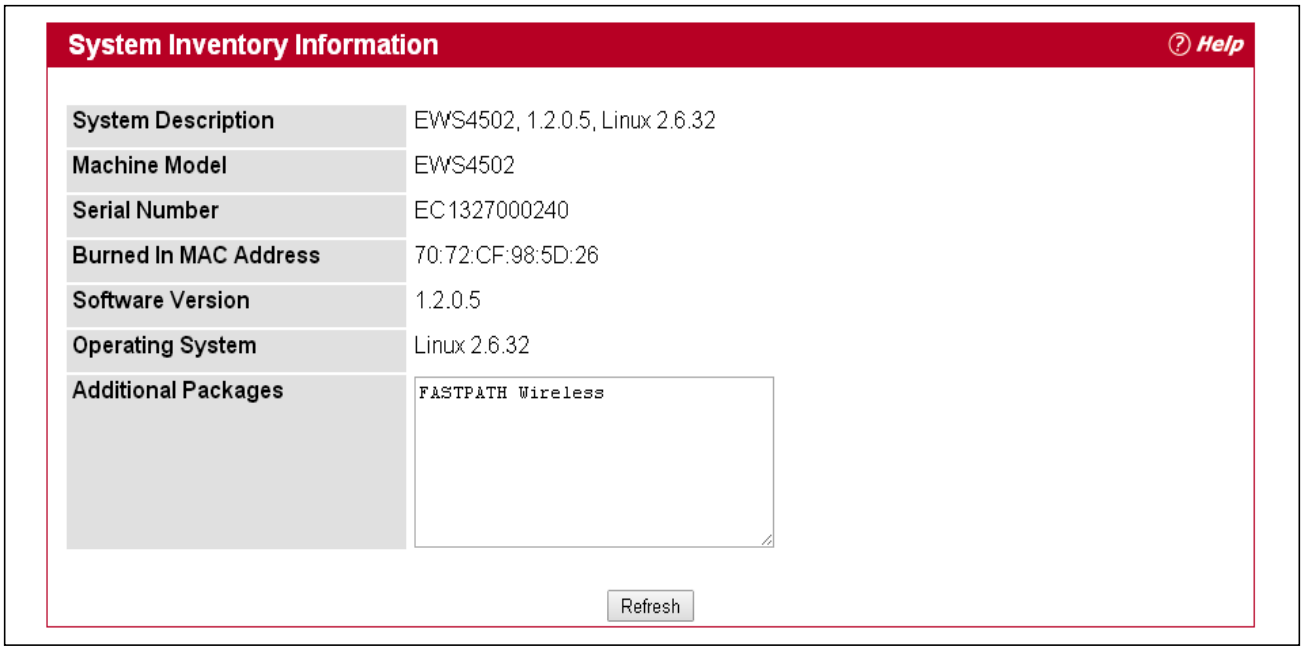


Figure 9: Inventory Information

Table 6: Inventory Information Fields

Field	*Description*
System Description	The product name of this switch.
Machine Model	The model within the machine type.
Serial Number	The unique serial number for this switch.
Burned in MAC Address	The burned-in universally administered MAC address of this switch.
Software Version	The release version.maintenance number of the code currently running on the switch. For example, if the release is 1, the version is 2 and the maintenance number is 4, the format is “1.2.4.”
Operating System	The operating system currently running on the switch.
Additional Packages	A list of the optional software packages installed on the switch, if any. For example, FASTPATH BGP-4, or FASTPATH Multicast.

Viewing the Dual Image Status

The Dual Image feature allows the switch to have two software images in the permanent storage. One image is the active image, and the second image is the backup. This feature reduces the system down-time during upgrades and downgrades. You can use the Dual Image Status page to view information about the system images on the device.

To display the Dual Image Status page, click **System** > **Dual Image Status** in the navigation menu.

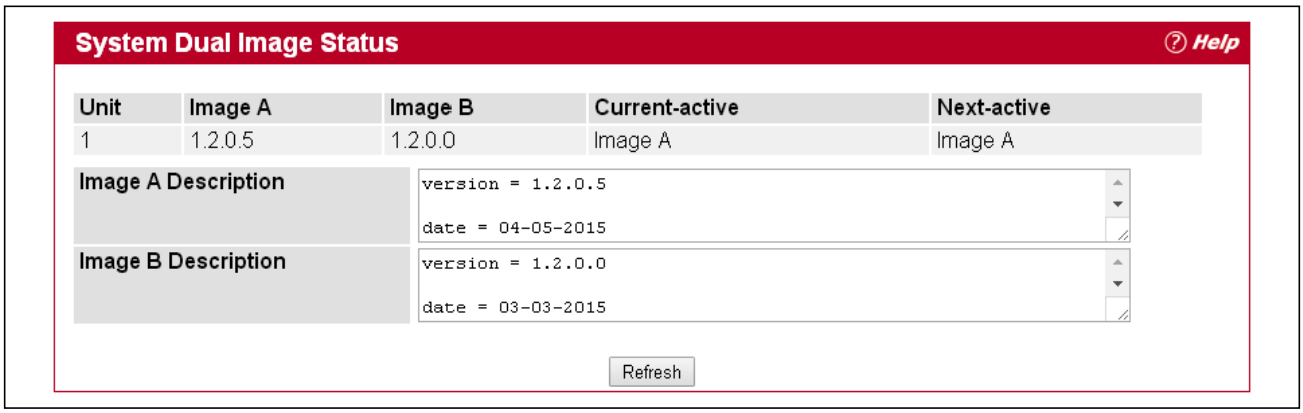


Figure 10: Dual Image Status

Table 7: Dual Image Status Fields

Field	*Description*
Unit	Displays the unit ID of the switch.
Image A	Displays the version of the Image A code file.
Image B	Displays the version of the Image B code file.
Current-active	Displays the currently active image on this unit.
Next-active	Displays the image to be used on the next restart of this unit.
Image A Description	Displays the description associated with the Image A code file.
Image B Description	Displays the description associated with the Image B code file.

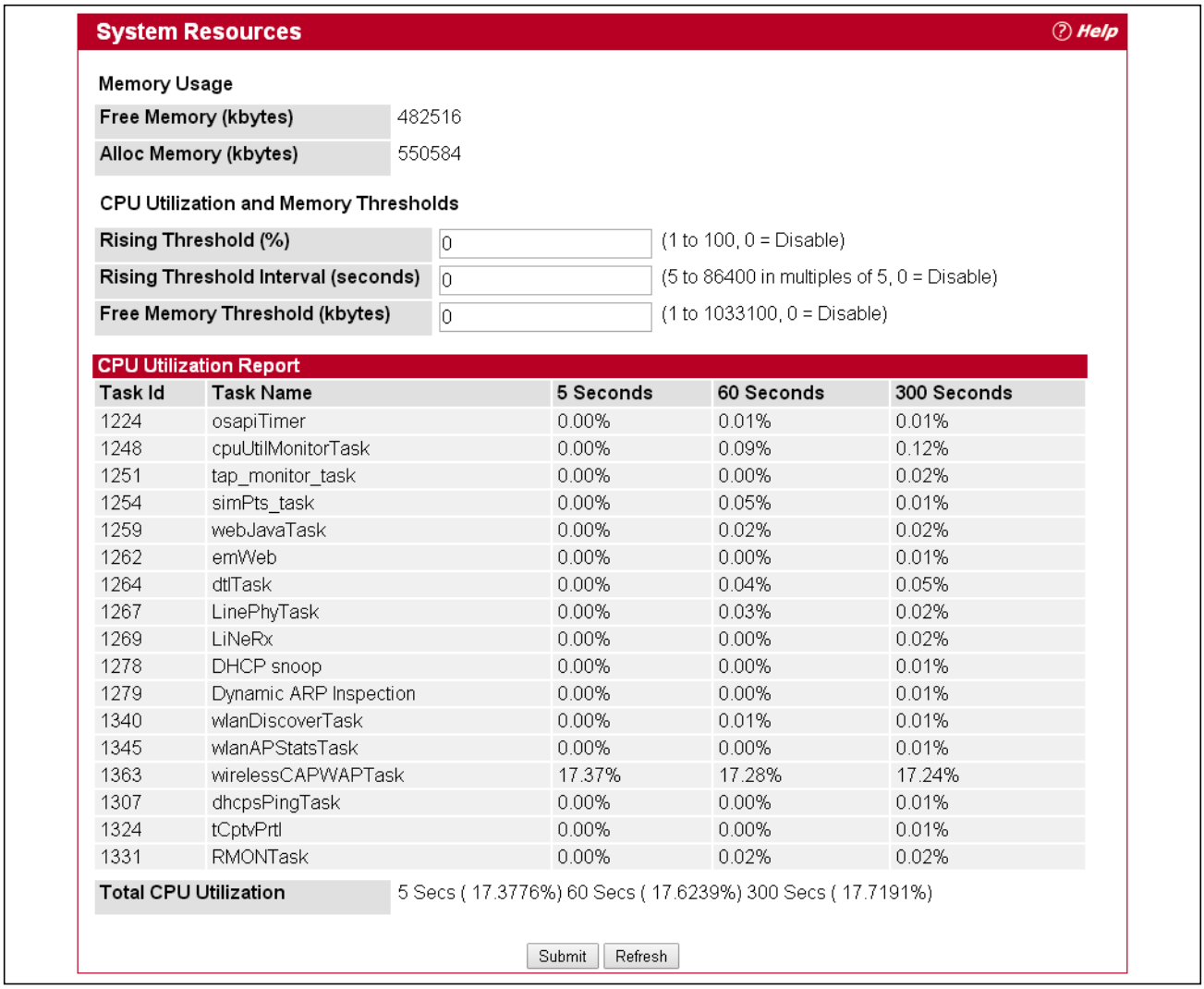
- Click **Refresh** to display the latest information from the router.
- For information about how to update or change the system images, see "Using System Utilities" on page 80.

Viewing System Resources

Use the System Resources page to display the following memory information for the switch:

- Free memory
- Allocated memory
- CPU utilization by task
- Total CPU utilization at the following intervals:
  - Five seconds
  - One minute
  - Five minutes

To display the System Resources page, click **System** > **System Resources** in the navigation menu.



System Resources Help

Memory Usage

Free Memory (kbytes)	482516
Alloc Memory (kbytes)	550584

CPU Utilization and Memory Thresholds

Rising Threshold (%)	0	(1 to 100, 0 = Disable)
Rising Threshold Interval (seconds)	0	(5 to 86400 in multiples of 5, 0 = Disable)
Free Memory Threshold (kbytes)	0	(1 to 1033100, 0 = Disable)

CPU Utilization Report

Task Id	Task Name	5 Seconds	60 Seconds	300 Seconds
1224	osapiTimer	0.00%	0.01%	0.01%
1248	cpuUtilMonitorTask	0.00%	0.09%	0.12%
1251	tap_monitor_task	0.00%	0.00%	0.02%
1254	simPts_task	0.00%	0.05%	0.01%
1259	webJavaTask	0.00%	0.02%	0.02%
1262	emWeb	0.00%	0.00%	0.01%
1264	dtlTask	0.00%	0.04%	0.05%
1267	LinePhyTask	0.00%	0.03%	0.02%
1269	LiNeRx	0.00%	0.00%	0.02%
1278	DHCP snoop	0.00%	0.00%	0.01%
1279	Dynamic ARP Inspection	0.00%	0.00%	0.01%
1340	wlanDiscoverTask	0.00%	0.01%	0.01%
1345	wlanAPStatsTask	0.00%	0.00%	0.01%
1363	wirelessCAPWAPTask	17.37%	17.28%	17.24%
1307	dhcpsPingTask	0.00%	0.00%	0.01%
1324	tCptvPrtl	0.00%	0.00%	0.01%
1331	RMONTask	0.00%	0.02%	0.02%

Total CPU Utilization	5 Secs (17.3776%) 60 Secs (17.6239%) 300 Secs (17.7191%)

Submit Refresh

Figure 11: System Resources

Table 8: System Resources Fields

Field	*Description*
Free Memory	Displays the available Free Memory on the switch.
Alloc Memory	Displays the allocated Memory for the switch.
Rising Threshold	The CPU Rising utilization threshold in percentage. A zero percent threshold indicates CPU Utilization Notification feature is disabled.
Rising Threshold Interval	The CPU Rising threshold interval in seconds. The time interval is configured in multiples of 5. A time interval of zero seconds indicates CPU Utilization Notification feature is disabled.
Falling Threshold	The CPU Falling utilization threshold in percentage. Configuration of this field is optional. If configured, the Falling threshold value must be equal to or less than the Rising threshold value. If not configured, it takes the same value as the Rising threshold.
Falling Threshold Interval	The CPU Falling threshold interval in seconds. Configuration of this field is optional. If configured, the Falling interval value must be equal to or less than the Rising interval value. If not configured, it takes the same value as the Rising interval. The time interval is configured in multiples of 5.
Free Memory Threshold	The CPU Free Memory threshold in kilobytes. A zero threshold value indicates CPU Free Memory Notification feature is disabled.
Task Id	Displays the Id of running tasks.
Task Name	Displays the name of the running tasks.
CPU Utilization(%)	Displays the CPU Utilization of tasks in terms of percentage of utilization.
Total CPU Utilization	Displays the Total CPU Utilization in terms of percentage. **Total CPU Utilization is shown in the following intervals:** • Five seconds • One minute • Five minutes

Defining General Device Information

The Configuration folder in the System menu contains links to pages that allow you to configure device parameters. The Configuration folder contains links to the following features:

- System Description
- Network Connectivity Configuration
- DHCP Client Options
- HTTP Configuration
- User Accounts
- Login Sessions
- Enable Password
- Denial of Service

System Description

After a successful login, the System Description page displays. Use this page to configure and view general device information.

To display the System Description page, click **System > Configuration > System Description** in the navigation tree.

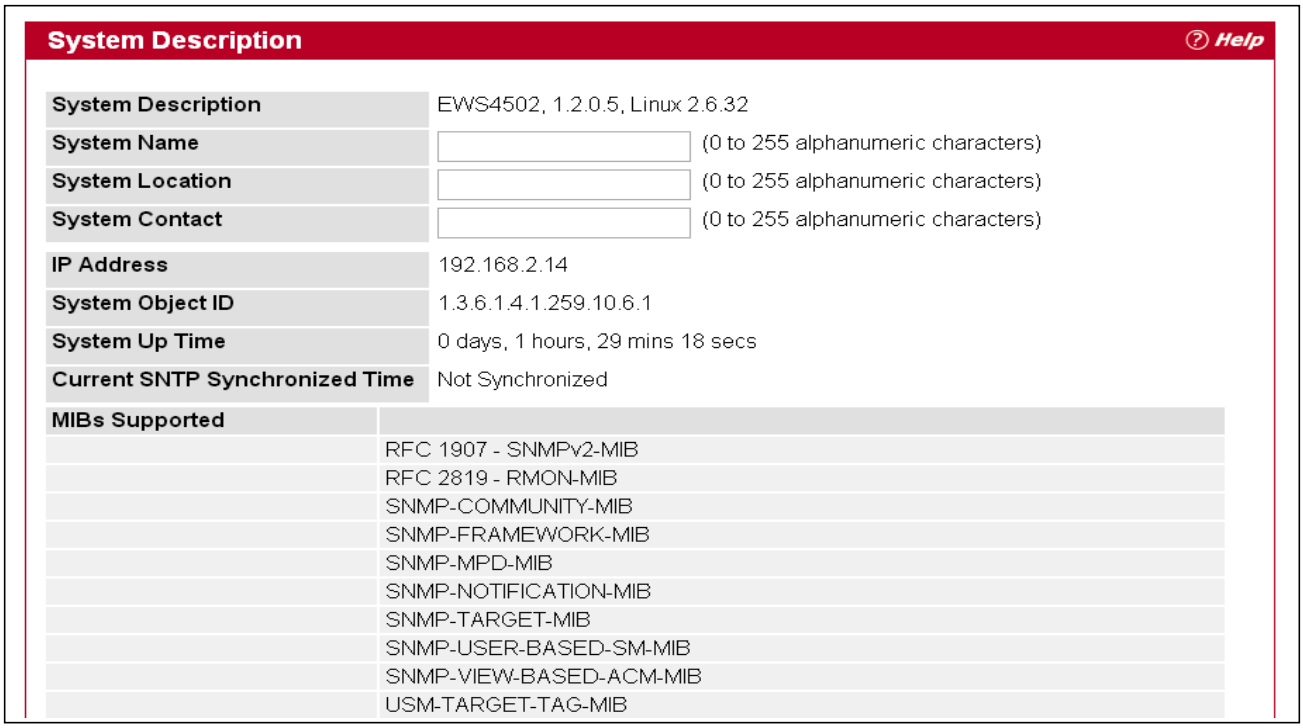


Figure 12: System Description

Table 9: System Description Fields

Field	*Description*
System Description	The product name of this switch.
System Name	Enter the name you want to use to identify this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
System Location	Enter the location of this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
System Contact	Enter the contact person for this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
IP Address	The IP Address assigned to the network interface. To change the IP address, see "Network Connectivity Configuration" on page 54.
System Object ID	The base object ID for the switch's enterprise MIB.
System Up Time	Displays the number of days, hours, and minutes since the last system restart.
Current SNTP Synchronized Time	Displays currently synchronized SNTP time in UTC. If no SNTP server has been configured and the time is not synchronized, this field displays "Not Synchronized." To specify an SNTP server, see "Configuring SNTP Settings" on page 110.
MIBs Supported	Displays the list of MIBs supported by the management agent running on this switch.

Defining System Information

1. Open the **System Description** page.
2. Define the following fields: **System Name**, **System Contact**, and **System Location**.
3. Click **Submit**.

   The system parameters are applied, and the device is updated.

Note: If you want the switch to retain the new values across a power cycle, you must perform a save.

Network Connectivity Configuration

The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

The Network Connectivity Configuration page allows you to change the IPv4 information using the Web interface. To access the page, click **System > Configuration > Network Connectivity** in the navigation tree.

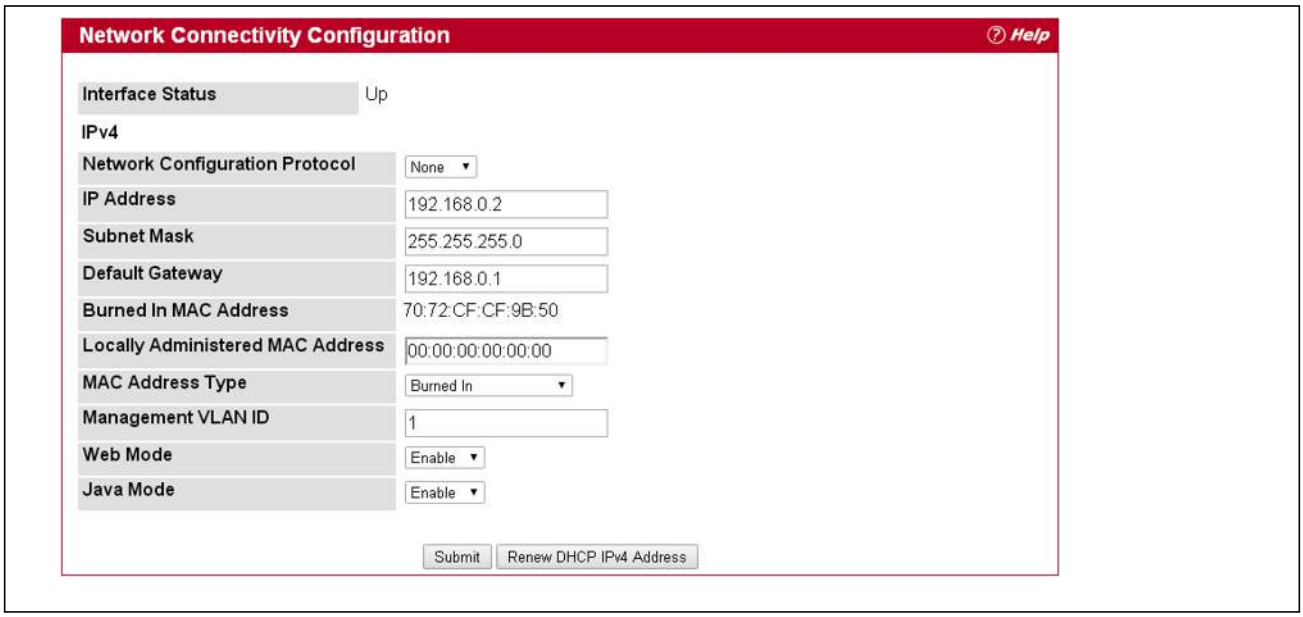


Figure 13: Network Connectivity Configuration for IPv4

Table 10: Network Connectivity Configuration for IPv4 Fields

Field	*Description*
Network Configuration Protocol	Specify what the switch should do following power-up. The factory default is None. The options are as follows: • **BOOTP:** Transmit a BOOTP request. • **DHCP:** Transmit a DHCP request. • **None:** Do not send any requests following power-up.
IP Address	The IP address of the network interface. The factory default value is 0.0.0.0 ***Note:*** Each part of the IP address must start with a number other than zero. For example, IP addresses 001.100.192.6 and 192.001.10.3 are not valid.
Subnet Mask	The IP subnet mask for the interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for the IP interface. The factory default value is 0.0.0.0.
Burned-in MAC Address	This read-only field displays the MAC address that is burned-in to the network card at the factory. This MAC address is used for in-band connectivity if you choose not to configure a locally administered address.

Table 10: Network Connectivity Configuration for IPv4 Fields (Cont.)

Field	*Description*
Locally Administered MAC Address	Specifies a locally administered MAC address for in-band connectivity instead of using the burned-in universally administered MAC address. In addition to entering an address in this field, you must also set the MAC address type to locally administered. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 must have a value between x'40' and x'7F'.
MAC Address Type	Specify whether the burned-in or the locally administered MAC address should be used for in-band connectivity. The factory default is to use the burned-in MAC address
Management VLAN ID	Specifies the management VLAN ID of the switch. It may be configured to any value in the range of (1 to 4093). The management VLAN is used for management of the switch. The default management VLAN ID is 1.
Web Mode	Enables/Disables Web Mode on the switch.
Java Mode	Enables/Disables Java mode on the switch.

If you change any of the network connectivity parameters, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

Click **Renew DHCP IPv4 Address** to force the interface to release the current DHCP-assigned information and submit a request for new information.

DHCP Client Options

Use the DHCP Client Options page to configure DHCP client settings on the system.

To access the DHCP Client Options page, click **System > Configuration > DHCP Client Options** in the navigation menu.

Figure 14: DHCP Client Options Configuration

Table 11: DHCP Client Options Configuration Fields

Field	*Description*
DHCP Vendor Class ID Mode	Enables/Disables the vendor class identifier mode.
DHCP Vendor Class ID String	The string added to DHCP requests as Option-60. i.e. Vendor Class Identifier option.

HTTP Configuration

Use the HTTP Configuration page to configure the HTTP server settings on the system.

To access the HTTP Configuration page, click **System > Configuration > HTTP Configuration** in the navigation menu.

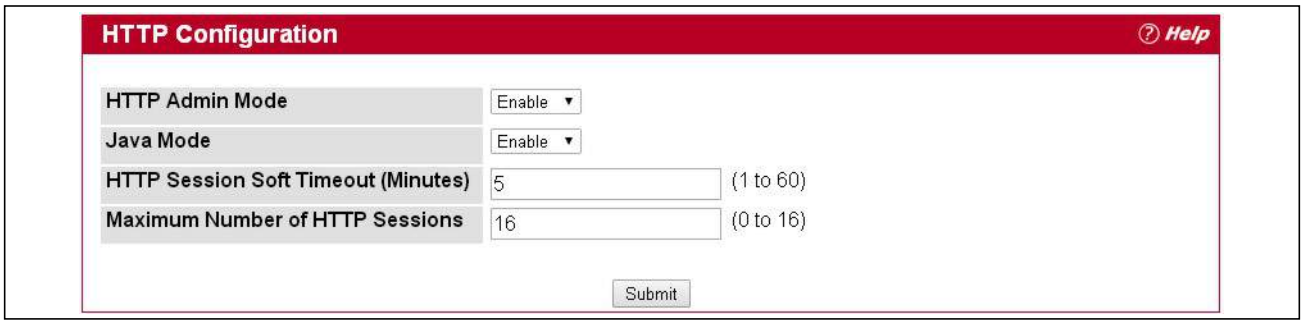


Figure 15: HTTP Configuration

Table 12: HTTP Configuration Fields

Field	*Description*
HTTP Admin Mode	This select field is used to Enable or Disable the Administrative Mode of HTTP. The currently configured value is shown when the web page is displayed. The default value is Enable. If you disable the HTTP admin mode, access to the web interface is limited to secure HTTP, which is disabled by default.
Java Mode	This select field is used to Enable or Disable the web Java Mode. This applies to both secure and un-secure HTTP connections. The currently configured value is shown when the web page is displayed. The default value is Enable.
HTTP Session Soft Timeout	This field is used to set the inactivity timeout for HTTP sessions. The value must be in the range of (1 to 60) minutes. A value of zero corresponds to an infinite timeout. The default value is 5 minutes. The currently configured value is shown when the web page is displayed.
Maximum Number of HTTP Sessions	This field is used to set the maximum allowable number of HTTP sessions. The value must be in the range of (0 to 16). The default value is 16. The currently configured value is shown when the web page is displayed.

If you make changes to the page, click **Submit** to apply the changes to the system.

User Accounts

By default, the switch contains two user accounts:

- admin, with 'Read/Write' privileges
- guest, with 'Read Only' privileges

Both of these accounts have blank passwords by default. The names are not case sensitive.

If you log on to the switch with the user account that has Read/Write privileges (i.e., as admin), you can use the **User Accounts** page to assign passwords and set security parameters for the default accounts. You can also add up to five read-only accounts. You can delete all accounts except for the Read/Write account.

Note: Only a user with Read/Write privileges may alter data on this screen, and only one account can exist with Read/Write privileges.

To access the User Accounts page, click **System > Configuration > User Accounts** in the navigation tree.

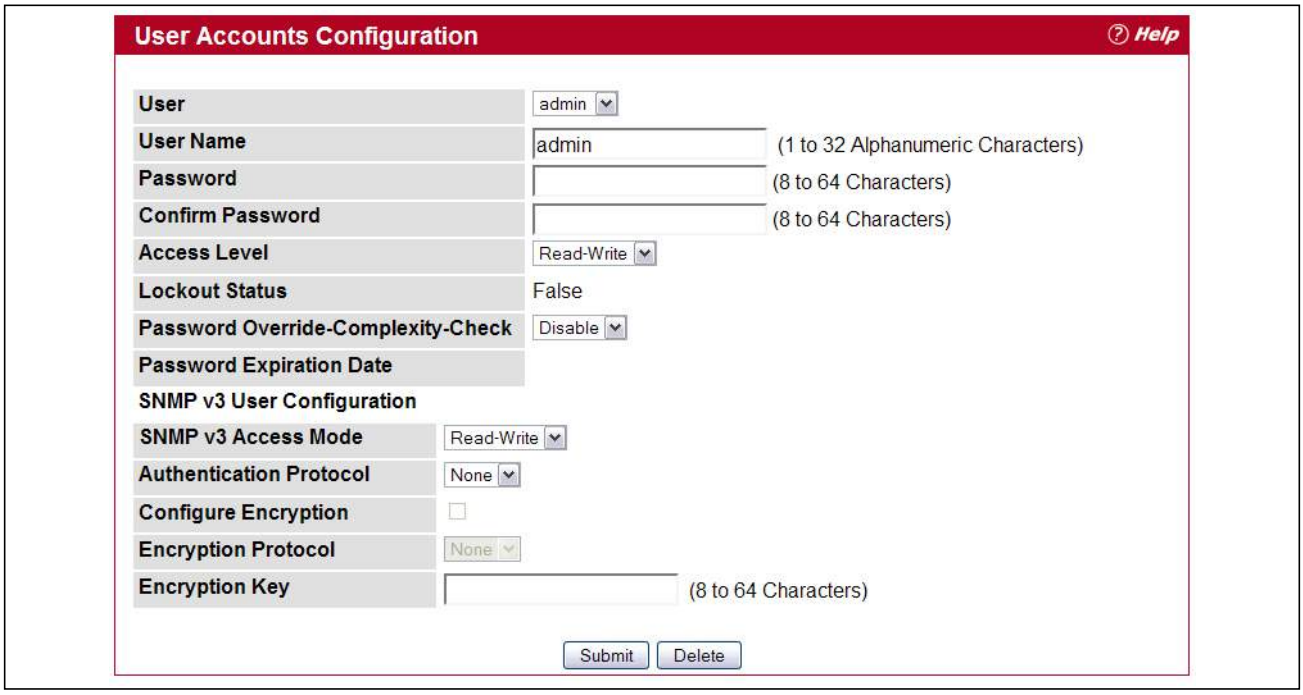


Figure 16: User Accounts

Table 13: User Accounts Fields

Field	*Description*
User	From the **User** menu, select an existing user to configure, or select **Create** to create a new user account. The system can have a maximum of five 'Read Only' accounts and one Read/Write account.
User Name	Enter the name you want to give to the new account. (You can only enter data in this field when you are creating a new account.) User names are up to 64 alphanumeric characters in length and are not case sensitive. Valid characters include all the alphanumeric characters and the dash ('-') and underscore ('_') characters. User name *default* is not valid. ***Note:*** You can change the Read/Write user name from “admin” to something else, but when you click **Submit**, you must re-authenticate with the new user name.
Password	Enter the optional new or changed password for the account. It will not display as it is typed, only asterisks (*) or dots(.) will show based on the browser used. Passwords must be greater than eight characters and can be up to 64 characters in length, and are case sensitive.
Confirm Password	Enter the password again, to confirm that you entered it correctly. This field will not display, but will show asterisks (*).
Access Level	Indicates the user's access level. The admin account always has Read/Write access, and all other accounts have Read Only access. A user with Read/Write access can also set a user’s access level to Suspend, which prevents the user from accessing the switch.
Lockout Status	Indicates whether the user is currently locked out. A user is locked out after a configurable number of failed login attempts. If the user is locked out, the status is True.
Password Override - Complexity-Check	When set to enable, the password strength checking is not in effect for this user.
Password Expiration Date	Indicates the date when this user’s current password will expire. This is determined by the date the password was created and the number of days specified in the Password Aging setting on the Password Management page.
SNMP v3 User Configuration	
SNMP v3 Access Mode	Shows the SNMPv3 access privileges for the user account. The admin account always has 'Read/Write' access, and all other accounts have 'Read Only' access.
Authentication Protocol	Specify the SNMPv3 Authentication Protocol setting for the selected user account. The valid Authentication Protocols are **None**, **MD5** or **SHA**. If you select **None**, the user will be unable to access the SNMP data from an SNMP browser. If you select **MD5** or **SHA**, the user login password will be used as the SNMPv3 authentication password, and you must specify a valid password.
Configure Encryption	Select the check box to change the Encryption Protocol and Encryption Key.
Encryption Protocol	Specify the SNMPv3 Encryption Protocol setting for the selected user account. The valid Encryption Protocols are **None** or **DES**. If you select the **DES** Protocol you must enter a key in the **Encryption Key** field. If **None** is specified for the Protocol, the **Encryption Key** field is not active for input.
Encryption Key	If you selected **DES** in the **Encryption Protocol** field enter the SNMPv3 Encryption Key here. Otherwise this field is not active. The key should be 8 characters in length.

Adding a User Account

Use the following procedures to add a user account. The system supports one Read/Write user and five Read Only users.

1. From the **User** menu, select **Create**.

   The screen refreshes.
2. Enter a user name and password for the new user, then re-enter the password in the **Confirm Password** field.
3. Click **Submit** to update the switch with the values on this screen.

   If you want the switch to retain the new values across a power cycle, you must perform a save.

Changing User Account Information

You cannot add or delete the Read/Write user, but you can change the user name and password. To change the password for an existing account or to overwrite the user name on an existing account, use the following procedures.

1. From the **User** menu, select the user to change.

   The screen refreshes.
2. To alter the user name or, delete the existing name in the **Username** field and enter the new user name.

   To change the password, delete any asterisks (*) in the **Password** and **Confirm Password** fields, and then enter and confirm the new password.
3. Click **Submit** to update the switch with the values on this screen.

   If you want the switch to retain the new values across a power cycle, you must perform a save.

Deleting a User Account

Use the following procedures to delete any of the Read Only user accounts.

1. From the **User** menu, select the user to delete.

   The screen refreshes.
2. Click **Delete** to delete the user.

   This button is only visible when you have selected a user account with 'Read Only' access. You cannot delete the 'Read/Write' user.

   If you want the switch to retain the new values across a power cycle, you must perform a save.

Login Sessions

Use the Login Session page to view information about users who have logged on to the switch.

To access the **Login Sessions** page, click **System > Configuration > Login Sessions** in the navigation tree.

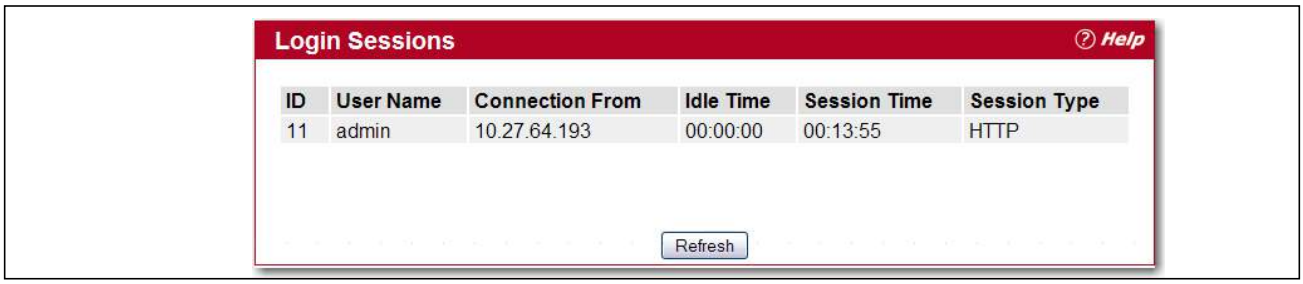


Figure 17: Login Session

The Login Session page has the following read-only fields:

Table 14: Login Session Fields

Field	*Description*
ID	Identifies the ID of this row.
User Name	Shows the user name of the user who is currently logged on to the switch.
Connection From	Shows the IP address of the system from which the user is connected. If the connection is a local serial connection, the **Connection From** field entry is EIA-232.
Idle Time	Shows the idle session time.
Session Time	Shows the total session time.
Session Type	Shows the type of session, which can be Telnet, Serial Port, HTTP, or SSH.

Click **Refresh** to update the information on the screen.

Select Authentication List

Use the Select Authentication List page to select the authentication methods used for the switch access methods.

To display this page, click **System > Configuration > Select Authentication List** in the navigation tree.

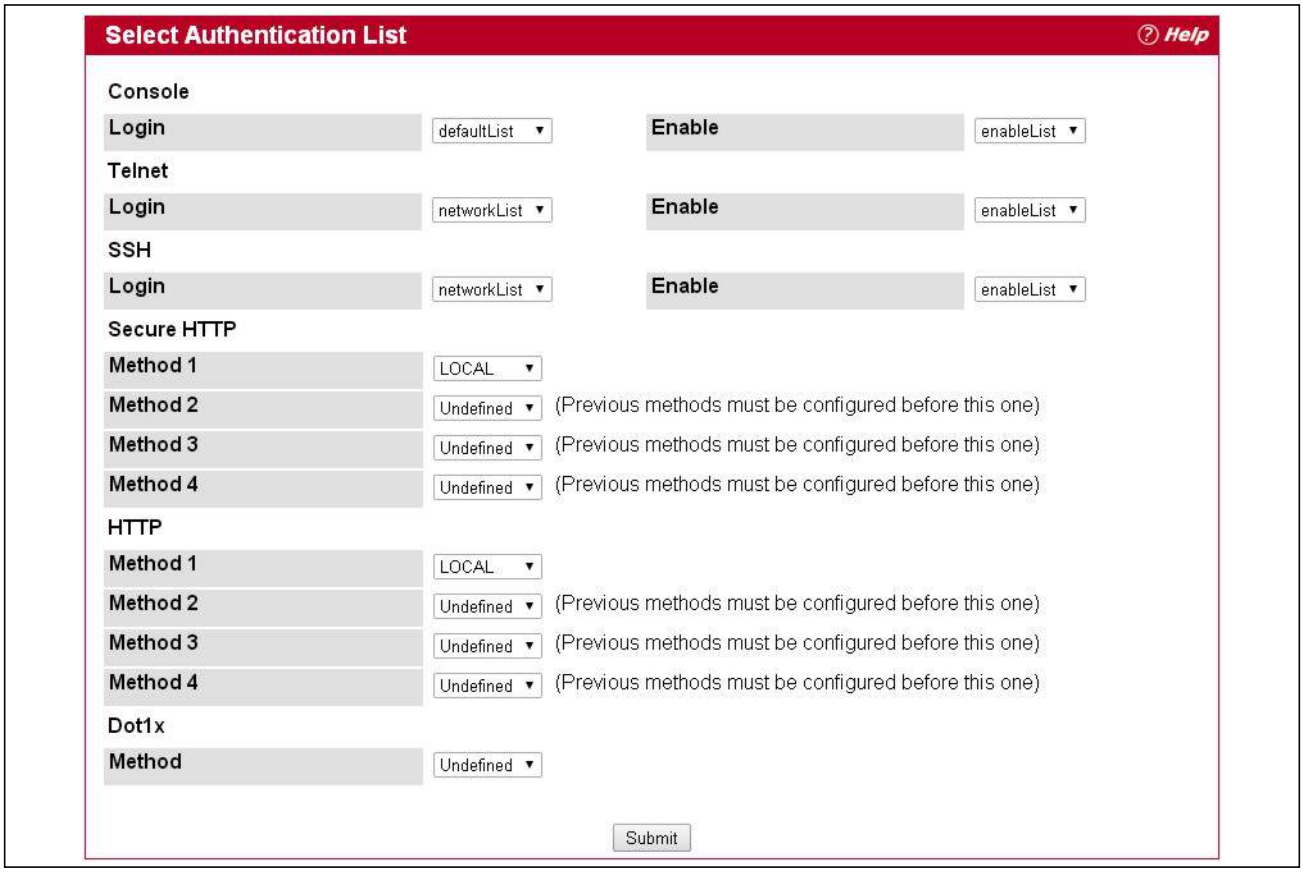


Figure 18: Select Authentication List

Table 15: Select Authentication List

Field	*Description*
Console	Authentication profiles used to authenticate console users. • **Login** or **Enable** - Specify the login list and enable list which will be used to validate switch or port access for the users associated with the list.
Telnet	Authentication profiles used to authenticate Telnet users. • **Login** or **Enable** - Specify the login list or enable list which will be used to validate switch or port access for the users associated with the list.
Secure Telnet (SSH)	Authentication profiles used to authenticate Secure Shell (SSH) users. SSH provides clients secure and encrypted remote connections to a device. • Login or Enable - Specify the login list or enable list which will be used to validate switch or port access for the users associated with the list.

Table 15: Select Authentication List (Cont.)

Field	*Description*

HTTP and Secure HTTP	Authentication method used for HTTP access and Secure HTTP access, respectively. Possible field values are:
	• **Method 1** - Use the drop-down menu to select the method that should appear first in the selected authentication list. If you select a method that does not time out as the first method, such as 'local' no other method will be tried, even if you have specified more than one method. The options are:
	  • **Undefined** - the authentication method is disabled (this may not be assigned as the first method)
	  • **Enable** - uses the enable password for authentication.
	  • **Line** - uses the Line password for authentication.
	  • **Local** - the user's locally stored ID and password will be used for authentication
	  • **None** - the user is not authenticated
	  • **Radius** - the user's ID and password will be authenticated using the RADIUS server instead of locally
	  • **TACACS**+ - the user's ID and password will be authenticated using the TACACS+ server
	• **Method 2** - Use the drop-down menu to select the method, if any, that should appear second in the selected authentication list. This is the method that will be used if the first method times out. If you select a method that does not time out as the second method, the third method will not be tried.
	• **Method 3** - Use the drop-down menu to select the method, if any, that should appear third in the selected authentication list. This is the method that will be used if the second method times out. If you select a method that does not time out as the third method, the fourth method will not be tried.
	• **Method 4** - Use the drop-down menu to select the method, if any, that should appear fourth in the selected authentication list.

DOT1X	Authentication method used for Dot1x access. Possible field values are:
	• **Method** - Use the drop-down menu to select the method that should appear in the selected authentication list. The options are:
	  • **Undefined** - the authentication method is disabled.
	  • **IAS** - the user's ID and password in Internal Authentication Server Database will be used for authentication.
	  • **Local**- the user's locally stored ID and password will be used for authentication.
	  • **None** - the user is not authenticated.
	  • **Radius** - the user's ID and password will be authenticated using the RADIUS server.

Enable Password

Use the Enable Password page to configure the enable password.

To display the page, click **System > Configuration > Enable Password** in the navigation tree.

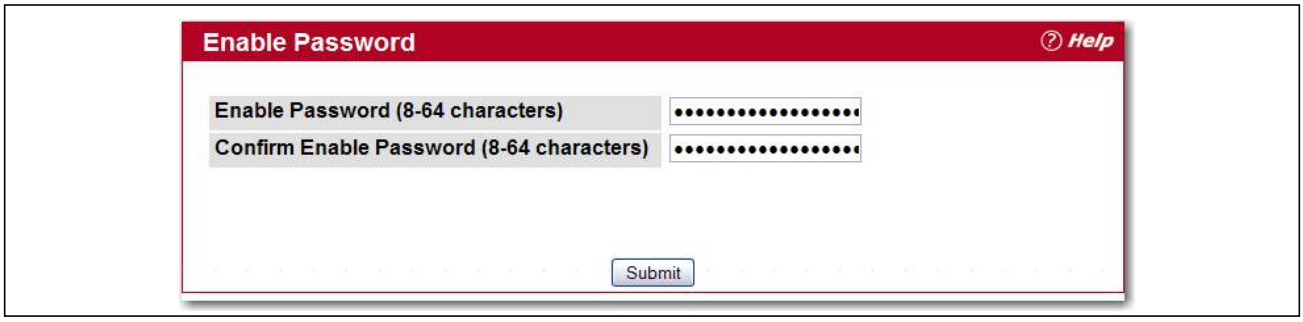


Figure 19: Enable Password

Table 16: Enable Password Fields

Field	*Description*
Enable Password (8-64 characters)	The enable password is for accessing the device via a console, Telnet, or Secure Telnet session.
Confirm Enable Password (8-64 characters)	Confirms the new enable password. The password appears in the ***** format.

If you change any data, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

Last Password Result

Use the Last Password Result page view information about the last attempt to set a user password. If the password set was unsuccessful, a reason for the failure is given.

To display the page, click **System > Configuration > Last Password Result** in the navigation tree.

Figure 20: Last Password Result

Table 17: Last Password Result

Field	*Description*
Last Password Set Result	Shows the results of the most recent attempt to set a password

Denial of Service

Use the Denial of Service (DoS) page to configure DoS control. EWS4502/EWS4606 software provides support for classifying and blocking specific types of DoS attacks. You can configure your system to monitor and block these types of attacks:

- **SIP=DIP**: Source IP address = Destination IP address.
- **First Fragment**: TCP Header size smaller then configured value.
- **TCP Fragment**: IP Fragment Offset = 1.
- **TCP Flag**: TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **L4 Port**: Source TCP/UDP Port = Destination TCP/UDP Port.
- **ICMP**: Limiting the size of ICMP Ping packets.
- **SMAC=DMAC:** Source MAC address=Destination MAC address.
- **TCP Por**t: Source TCP Port = Destination TCP Port.
- **UDP Port**: Source UDP Port = Destination UDP Port.
- **TCP Flag & Sequence:** TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.
- **TCP Offset:** TCP Header Offset = 1.
- **TCP SYN:** TCP Flag SYN set.
- **TCP SYN & FIN:** TCP Flags SYN and FIN set.
- **TCP FIN & URG & PSH:** TCP Flags FIN and URG and PSH set and TCP Sequence Number = 0.
- **ICMP V6**: Limiting the size of ICMPv6 Ping packets.
- **ICMP Fragment**: Checks for fragmented ICMP packets.

To access the **Denial of Service** page, click **System > Configuration > Denial of Service** in the navigation menu.

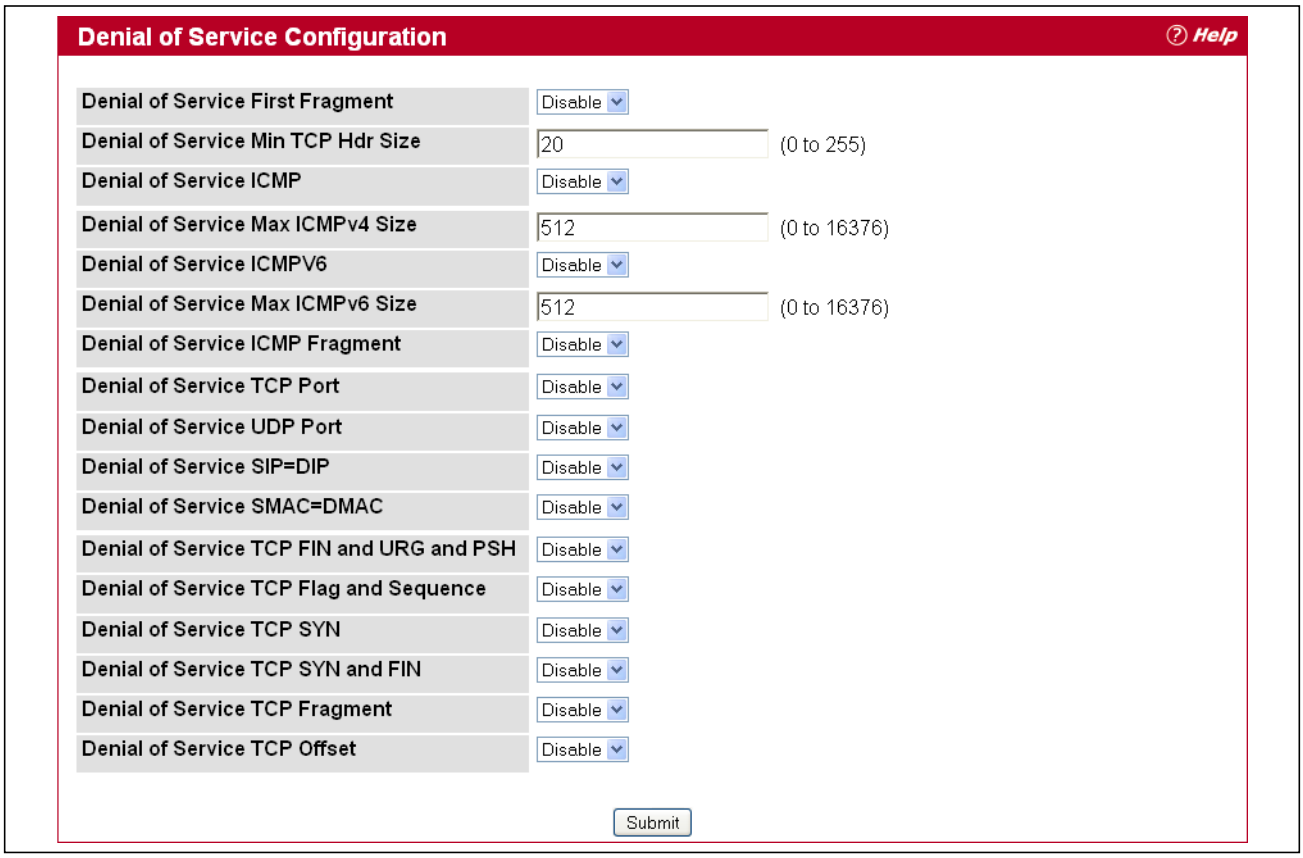


Figure 21: Denial of Service

Table 18: Denial of Service Configuration Fields

Field	*Description*
Denial of Service First Fragment	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling First Fragment DoS prevention causes the switch to drop packets that have a TCP header smaller then the configured Min TCP Hdr Size. The factory default is disabled.
Denial of Service Min TCP Hdr Size	Specify the Min TCP Hdr Size allowed. If First Fragment DoS prevention is enabled, the switch will drop packets that have a TCP header smaller then this configured Min TCP Hdr Size. The factory default is disabled.
Denial of Service ICMP	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling ICMP DoS prevention causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMP Pkt Size. The factory default is disabled.
Denial of Service Max ICMPv4 Pkt Size	Specify the Max ICMPv4 Pkt Size allowed. If ICMP DoS prevention is enabled, the switch will drop IPv4 ICMP ping packets that have a size greater than this configured Max ICMP Pkt Size. The factory default is disabled.
Denial of Service Max ICMPv6 Pkt Size	Specify the Max ICMPv6 ICMP Pkt Size allowed. If ICMP DoS prevention is enabled, the switch will drop IPv6 ICMP ping packets that have a size greater than this configured Max ICMP Pkt Size. The factory default is disabled.

Table 18: Denial of Service Configuration Fields (Cont.)

Field	*Description*
Denial of Service ICMP Fragment	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling ICMP Fragment DoS prevention causes the switch to drop ICMP Fragmented packets. The factory default is disabled.
Denial of Service SIP=DIP	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling SIP=DIP DoS prevention causes the switch to drop packets that have a source IP address equal to the destination IP address. The factory default is disabled.
Denial of Service SMAC=DMAC	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling SMAC=DMAC DoS prevention causes the switch to drop packets that have a source MAC address equal to the destination MAC address. The factory default is disabled.
Denial of Service TCP FIN&URG&PSH	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP FIN & URG & PSH DoS prevention causes the switch to drop packets that have TCP flags FIN, URG, and PSH set and TCP Sequence Number = 0. The factory default is disabled.
Denial of Service TCP Flag&Sequence	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP Flag DoS prevention causes the switch to drop packets that have TCP control flags set to 0 and TCP sequence number set to 0. The factory default is disabled.
Denial of Service TCP Fragment	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP Fragment DoS prevention causes the switch to drop packets that have an IP fragment offset equal to 1. The factory default is disabled.
Denial of Service TCP Offset	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP Offset DoS prevention causes the switch to drop packets that have a TCP header Offset equal to 1. The factory default is disabled.
Denial of Service TCP Port	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP Port DoS prevention causes the switch to drop packets that have TCP source port equal to TCP destination port. The factory default is disabled.
Denial of Service TCP SYN	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP SYN DoS prevention causes the switch to drop packets that have TCP Flags SYN set. The factory default is disabled.
Denial of Service TCP SYN&FIN	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP SYN & FIN DoS prevention causes the switch to drop packets that have TCP Flags SYN and FIN set. The factory default is disabled.
Denial of Service UDP Port	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling UDP Port DoS prevention causes the switch to drop packets that have UDP source port equal to UDP destination port. The factory default is disabled.

If you change any of the DoS settings, click **Submit** to apply the changes to the switch. To preserve the changes across a switch reboot, you must perform a save.

Defining SNMP Parameters

Simple Network Management Protocol (SNMP) provides a method for managing network devices. The device supports SNMP version 1, SNMP version 2, and SNMP version 3. The Web interfaces supports configuration of SNMPv1 and v2; SNMPv3 is supported only in the CLI.

SNMP v1 and v2

The SNMP agent maintains a list of variables, which are used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB presents the variables controlled by the agent. The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agent are controlled by access strings.

SNMP v3

SNMP v3 also applies access control and a new traps mechanism to SNMPv1 and SNMPv2 PDUs. In addition, the User Security Model (USM) is defined for SNMPv3 and includes:

- **Authentication**: Provides data integrity and data origin authentication.
- **Privacy**: Protects against disclosure of message content. Cipher-Bock-Chaining (CBC) is used for encryption. Either authentication is enabled on an SNMP message, or both authentication and privacy are enabled on an SNMP message. However privacy cannot be enabled without authentication.
- **Timeliness**: Protects against message delay or message redundancy. The SNMP agent compares incoming messages to the message time information.
- **Key Management**: Defines key generation, key updates, and key use.

The device supports SNMP notification filters based on Object IDs (OID). OIDs are used by the system to manage device features. SNMP v3 supports the following features:

- Security
- Feature Access Control
- Traps

Authentication or Privacy Keys are modified in the SNMPv3 User Security Model (USM).

Use the SNMP page to define SNMP parameters. To display the SNMP page, click **System > SNMP** in the navigation tree.

SNMP Community Configuration

Access rights are managed by defining communities on the SNMPv1, 2 Community page. When the community names are changed, access rights are also changed. SNMP Communities are defined only for SNMP v1 and SNMP v2.

Use the Community Configuration page to enable SNMP and Authentication notifications.

To display the Community Configuration page, click **System > SNMP > Community Configuration** in the navigation tree.

Figure 22: SNMP Community Configuration

Table 19: Community Configuration Fields

Field	*Description*
Community	Contains the predefined and user-defined community strings that act as a password and are used to authenticate the SNMP management station to the device. A community string can contain a maximum of 20 characters. By default, the options available in the menu are as follows: • **public**: This SNMP community has Read Only privileges and its status set to enable • **private**: This SNMP community has Read/Write privileges and its status set to enable.
Community Name	Use this field to reconfigure an existing community or to create a new one. A valid entry is a case-sensitive string of up to 16 characters.
Client IP Address	Taken together, the **Client IP Address** and **Client IP Mask** denote a range of IP addresses from which SNMP clients may use that community to access this device. If either the IP Address or IP Mask value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's IP address is ANDed with the mask, as is the Client IP Address, and, if the values are equal, access is allowed. For example, if the Client IP Address and Client IP Mask parameters are 192.168.1.0/255.255.255.0, then any client whose IP address is 192.168.1.0 through 192.168.1.255 (inclusive) will be allowed access. To allow access from only one station, use a Client IP Mask value of 255.255.255.255, and use that machine's IP address for Client IP Address.

Table 19: Community Configuration Fields (Cont.)

Field	*Description*
Client IP Mask	Along with the **Client IP Address**, the **Client IP Mask** denotes a range of IP addresses from which SNMP clients may use that community to access this device.
Access Mode	Specify the access level for this community: • **Read-Only**: The Community has read-only access to the MIB objects configured in the view. • **Read-Write**: The Community has read/modify access to the MIB objects configured in the view.
Status	Specify the status of this community: • **Enable**: The community is enabled, and the Community Name must be unique among all valid Community Names or the set request will be rejected. • **Disable**: The Community is disabled and the Community Name becomes invalid.

- If you make any changes to the page, click **Submit** to apply the changes to the system. If you create a new Community, it is added to the table below the **Submit** button.
- Click **Delete** to delete the selected SNMP Community.

Trap Receiver Configuration

Use the Trap Receiver Configuration page to configure information about the SNMP community and the trap manager that will receive its trap packets.

To access the Trap Receiver Configuration page, click **System > SNMP > Trap Receiver Configuration** from the navigation tree.

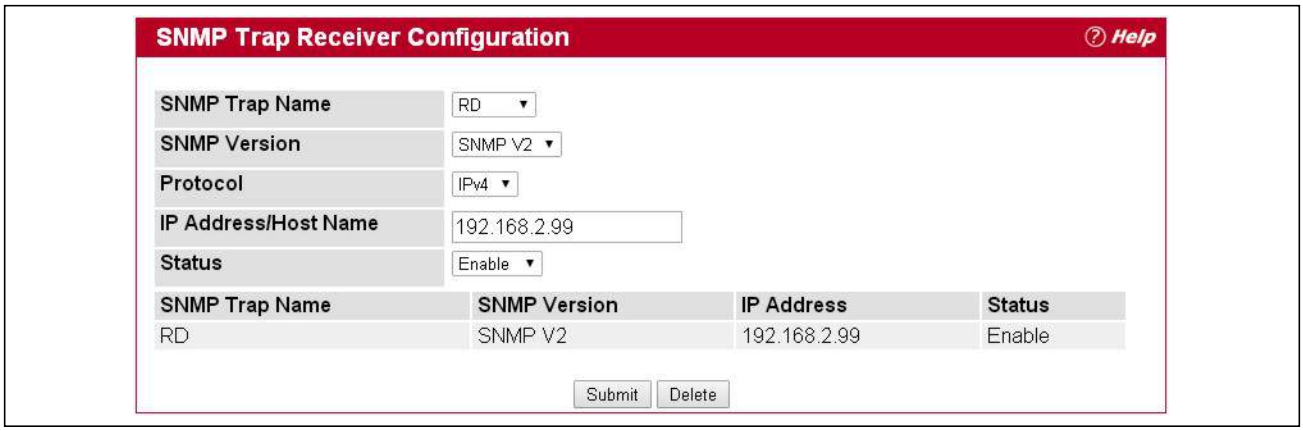


Figure 23: Trap Receiver Configuration

Table 20: Trap Receiver Configuration Fields

Field	*Description*
(Create) SNMP Trap Name	When this field is set to **Create**, you can configure new SNMP trap receiver information in the rest of the fields. If you have already configured an SNMP trap receiver, you can select it from the drop-down menu to change the settings or delete it.
SNMP Trap Name	Enter the SNMP trap name for the SNMP trap packet to be sent to the trap manager. This may be up to 16 characters and is case sensitive.
SNMP Version	Select the trap version to be used by the receiver from the pull down menu: • **SNMP v1**. Uses SNMP v1 to send traps to the receiver. • **SNMP v2**. Uses SNMP v2 to send traps to the receiver.
Protocol	Select the type of protocol used for the SNMP Trap Receiver Configuration: • **IPv4**. Choose IPv4 to enter the address in IPv4 format.
IP Address/Host Name	Enter the IP address or host name of the SNMP trap receiver.
Status	Select the receiver's status from the pull-down menu: • **Enable**: Send traps to the receiver • **Disable**: Do not send traps to the receiver.

If you make any changes to the page, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a **save**.

Supported MIBs

The Supported MIBs page lists the MIBs that the system currently supports.

To access the Supported MIBs page, click **System > SNMP > Supported MIBs** in the navigation menu. A portion of the web screen is shown Figure 24.

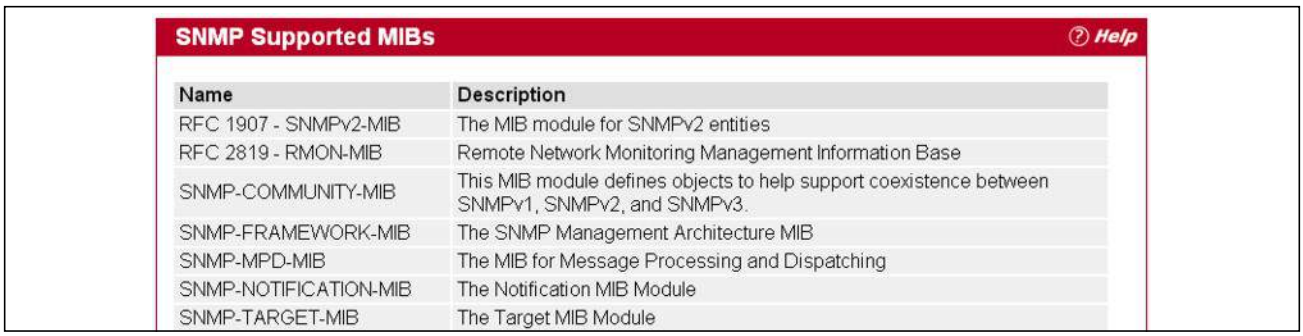


Figure 24: Supported MIBs

Table 21: Supported MIBs Fields

Field	*Description*
Name	The RFC number if applicable and the name of the MIB.
Description	The RFC title or MIB description.

Viewing System Statistics

The pages in the Statistics folder contain a variety of information about the number and type of traffic transmitted from and received on the switch.

Switch Detailed

The Switch Detailed Statistics page shows detailed statistical information about the traffic the switch handles.

To access the Switch Detailed Statistics page, click **System > Statistics > Switch Detailed** in the navigation menu.

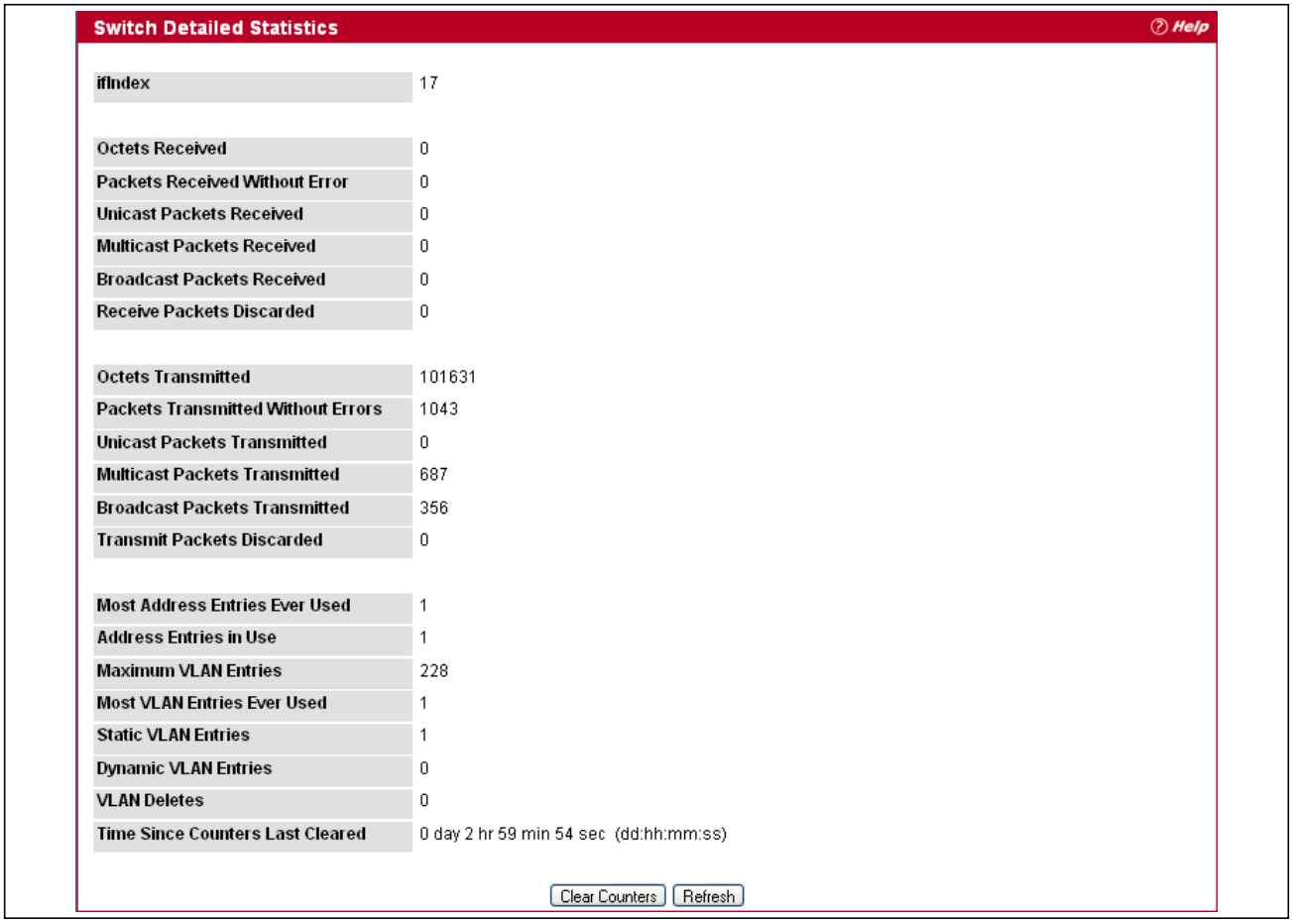


Figure 25: Switch Detailed

Table 22: Switch Detailed Statistics Fields

Field	*Description*
fIndex	This object indicates the ifIndex of the interface table entry associated with the processor of this switch.
Octets Received	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).

Table 22: Switch Detailed Statistics Fields (Cont.)

Field	*Description*
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted Without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
Address Entries in Use	The number of learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	The maximum number of Virtual LANs (VLANs) allowed on this switch.
Most VLAN Entries Ever Used	The largest number of VLANs that have been active on this switch since the last reboot.
Static VLAN Entries	The number of presently active VLAN entries on this switch that have been created statically.
Dynamic VLAN Entries	The number of presently active VLAN entries on this switch that have been created by GVRP registration.
VLAN Deletes	The number of VLANs on this switch that have been created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

- Click **Refresh** to refresh the data on the screen with the present state of the data in the switch.

- Click **Clear Counters** to clear all the statistics counters, resetting all switch summary and detailed statistics to default values. The discarded packets count cannot be cleared.

Switch Summary

Use the Switch Summary Statistics page to view a summary of statistics for traffic on the switch.

To access the Switch Summary Statistics page, click **System > Statistics > Switch Summary** in the navigation tree.

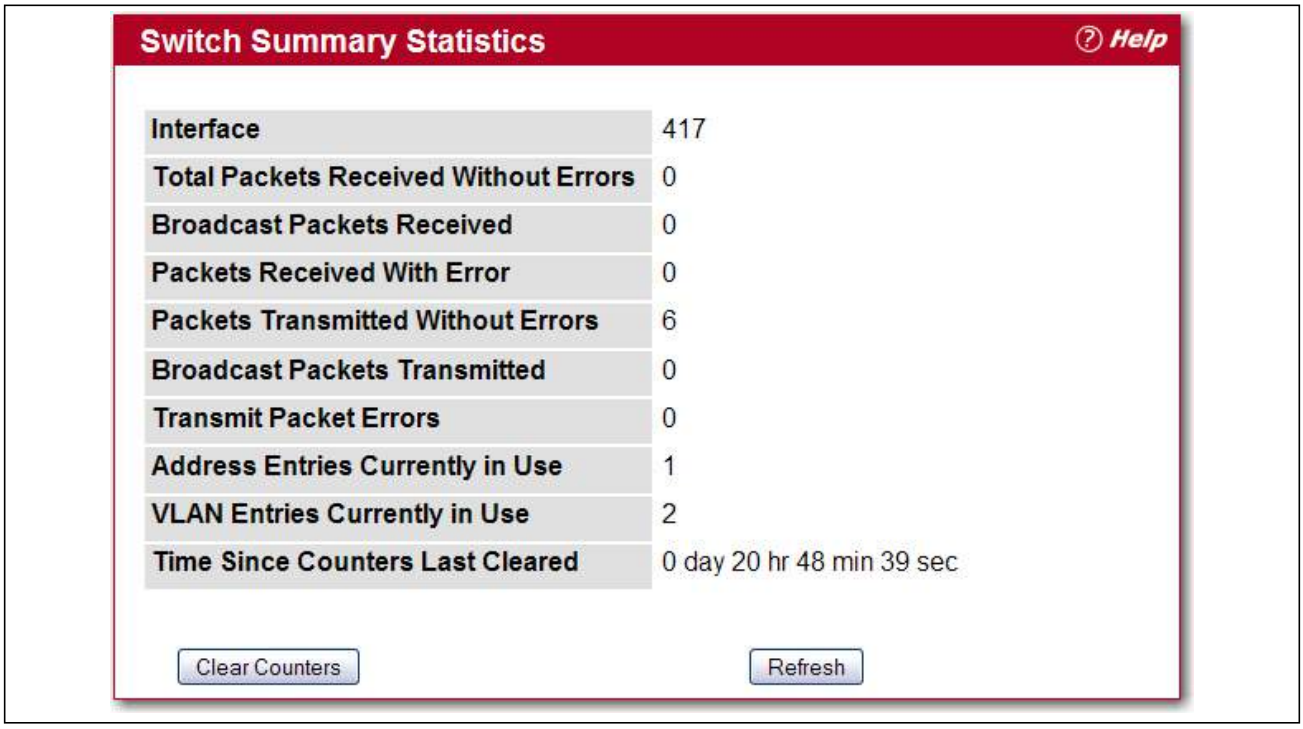


Figure 26: Switch Summary

Table 23: Switch Summary Fields

Field	*Description*
ifIndex	This object indicates the ifIndex of the interface table entry associated with the processor of this switch.
Total Packets Received Without Errors	The total number of packets, including multicast packets, that were directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Errors	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.

Table 23: Switch Summary Fields (Cont.)

Field	*Description*
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Address Entries Currently in Use	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
VLAN Entries Currently in Use	The number of VLAN entries presently occupying the VLAN table.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

- Click **Refresh** to refresh the data on the screen with the present state of the data in the switch.
- Click **Clear Counters** to clear all the statistics counters, resetting all summary and detailed statistics for this switch to default values. The discarded packets count cannot be cleared.
- Click **Clear All Counters** to clear counters for all switches in the stack.

Port Detailed

The Port Detailed Statistics page displays a variety of per-port traffic statistics.

To access the Port Detailed Statistics page, click **System > Statistics > Port Detailed** in the navigation tree.

Figure 27 shows some, but not all, of the fields on the Port Detailed page.

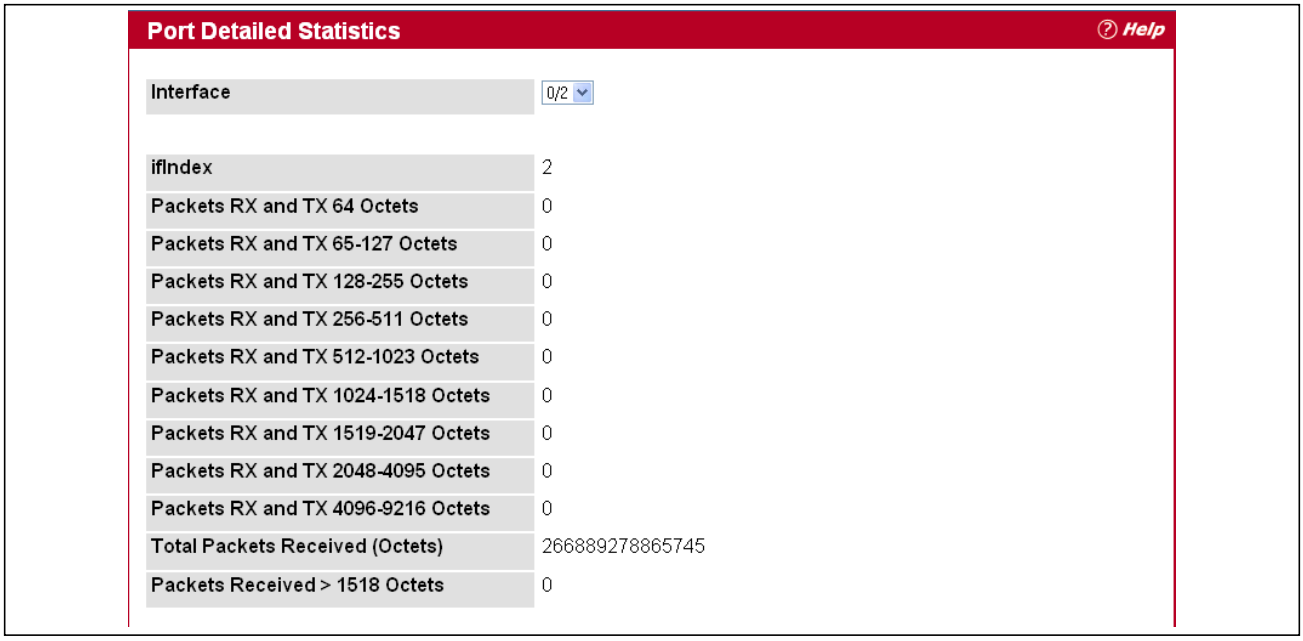


Figure 27: Port Detailed

Table 24: Port Fields

Field	*Description*
Interface	Use the drop-down menu to select the interface for which data is to be displayed or configured. For non-stacking systems, this field is **Slot/Port**.
ifIndex	This field indicates the ifIndex of the interface table entry associated with this port on an adapter.
Packets RX and TX 64 Octets	The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
Packets RX and TX 65-127 Octets	The total number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 128-255 Octets	The total number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 256-511 Octets	The total number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 512-1023 Octets	The total number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1024-1518 Octets	The total number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1519-1522 Octets	The total number of packets (including bad packets) received or transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1523-2047 Octets	The total number of packets (including bad packets) received or transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 2048-4095 Octets	The total number of packets (including bad packets) received or transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 4096-9216 Octets	The total number of packets (including bad packets) received or transmitted that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
Total Packets Received (Octets)	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets Received > 1518 Octets	The total number of packets (including bad packets) received that were greater than 1518 octets in length (excluding framing bits but including FCS octets).
Total Packets Received Without Errors	The total number of packets received that were without errors.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

Table 24: Port Fields (Cont.)

Field	*Description*
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Total Packets Received with MAC Errors	The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Jabbers Received	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Fragments Received	The total number of packets received that were less than 64 octets in length with ERROR CRC (excluding framing bits but including FCS octets).
Undersize Received	The total number of packets received that were less than 64 octets in length with GOOD CRC (excluding framing bits but including FCS octets).
Alignment Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.
Rx FCS Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
Overruns	The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Total Received Packets Not Forwarded	A count of valid frames received which were discarded (i.e., filtered) by the forwarding process.
802.3x Pause Frames Received	A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
Unacceptable Frame Type	The number of frames discarded from this port due to being an unacceptable frame type.
Total Packets Transmitted (Octets)	The total number of octets of data (including those in bad packets) transmitted on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets Transmitted > 1518 Octets	The total number of packets (including bad packets) received that were more than 1518 octets in length (excluding framing bits but including FCS octets).
Maximum Frame Size	The maximum ethernet frame size the interface supports or is configured, including ethernet header, CRC, and payload. (1518 to 9216). The default maximum frame size is 1518.
Total Packets Transmitted Successfully	The number of frames that have been transmitted by this port to its segment.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Table 24: Port Fields (Cont.)

Field	*Description*
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Total Transmit Errors	The sum of Single, Multiple, and Excessive Collisions.
Tx FCS Errors	The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
Underrun Errors	The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.
Total Transmit Packets Discarded	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Excessive Collision Frames	A count of frames for which transmission on a particular interface fails due to excessive collisions.
STP BPDUs Transmitted	Number of STP BPDUs transmitted from the selected port.
STP BPDUs Received	Number of STP BPDUs received at the selected port.
RSTP BPDUs Transmitted	Number of RSTP BPDUs transmitted from the selected port.
RSTP BPDUs Received	Number of RSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	Number of MSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	Number of MSTP BPDUs received at the selected port.
802.3x Pause Frames Transmitted	A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
GVRP PDUs Received	The count of GVRP PDUs received in the GARP layer.
GVRP PDUs Transmitted	The count of GVRP PDUs transmitted from the GARP layer.
GVRP Failed Registrations	The number of times attempted GVRP registrations could not be completed.
GMRP PDUs Received	The count of GMRP PDUs received from the GARP layer.
GMRP PDUs Transmitted	The count of GMRP PDUs transmitted from the GARP layer.
GMRP Failed Registrations	The number of times attempted GMRP registrations could not be completed.
EAPOL Frames Transmitted	The number of 802.1X EAPOL authentication frames transmitted.
EAPOL Start Frames Received	The number of 802.1X EAPOL start frames received.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

- Click **Clear Counters** to clear all the counters. This resets all statistics for this port to the default values.
- Click **Clear All Counters** to clear all the counters for all ports on the switch. The button resets all statistics for all ports to default values.

- Click **Refresh** to refresh the data on the screen and display the most current statistics.

Port Summary

The Port Statistics Summary page shows a summary of per-port traffic statistics on the switch.

To access the Port Statistics Summary page, click **System > Statistics > Port Summary** in the navigation tree.

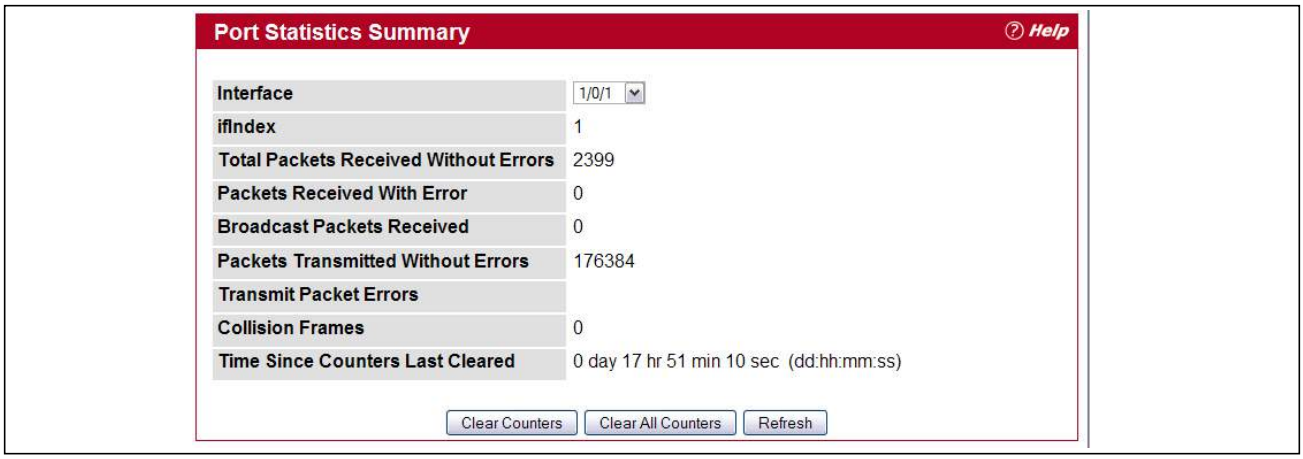


Figure 28: Port Summary

Table 25: Port Summary Fields

Field	*Description*
Interface	Use the drop-down menu to select the interface for which data is to be displayed or configured. For non-stacking systems, this field is **Slot/Port**.
ifIndex	This field indicates the ifIndex of the interface table entry associated with this port on an adapter.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Without Errors	The number of frames that have been transmitted by this port to its segment.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Collision Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

- Click **Clear Counters** to clear all the counters. This resets all statistics for this port to the default values.
- Click **Clear All Counters** to clear all the counters for all ports on the switch. The button resets all statistics for all ports to default values.

- Click **Refresh** to refresh the data on the screen and display the most current statistics.

Using System Utilities

The System Utilities folder contains links to the following Web pages that help you manage the switch:

- Save All Applied Changes
- System Reset
- Reset Configuration to Defaults
- Reset Passwords to Defaults
- Upload File To Switch (TFTP)
- Download File From Switch (TFTP)
- Dual Image Configuration
- HTTP File Upload
- Ping
- TraceRoute

Save All Applied Changes

When you click **Submit**, the changes are applied to the system and saved in the running configuration file. However, these changes are not saved to non-volatile memory and will be lost if the system resets. Use the Save All Applied Changes page to make the changes you submit persist across a system reset.

To access the Save All Applied Changes page, click **System > System Utilities > Save All Applied Changes** in the navigation tree.

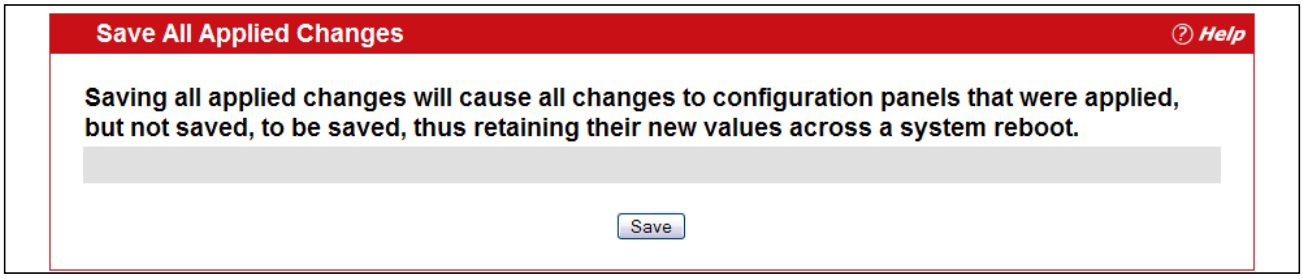


Figure 29: Save All Applied Changes

Click **Save** to save all changes applied to the system to NVRAM so that they are retained if the system reboots.

System Reset

Use the System Reset page to reboot the system. If the platform supports stacking, you can reset any of the switches in the stack, or all switches in the stack from this page.

To access the System Reset page, click **System > System Utilities > System Reset** in the navigation tree.

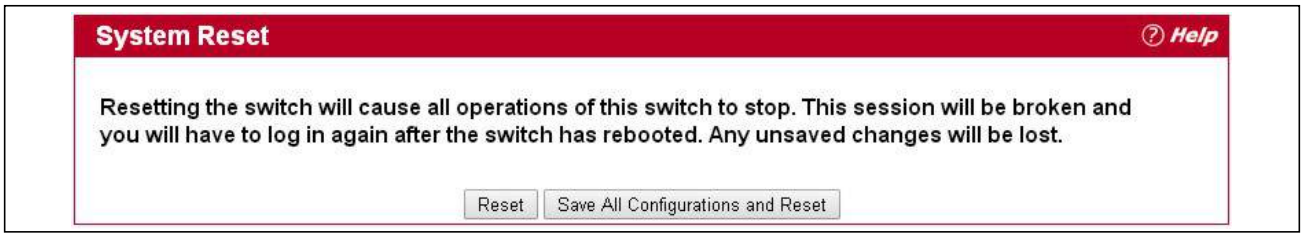


Figure 30: System Reset

Click **Reset** to initiate the system reset. If you have not saved the changes that you submitted since the last system reset, click **Save All Configurations and Reset**. to apply the changes to the system after the reset.

Reset Configuration to Defaults

Use the Reset Configuration to Defaults page to reset the system configuration to the factory default values.

Note: By default, the switch does not have an IP address, and the DHCP client is disabled. When you reset the system to its default values, you will not be able to access the Web interface until you connect to the CLI through the serial port and configure network information. For information about configuring network information, see "Connecting the Switch to the Network" on page 33.

To access the Reset Configuration to Defaults page, click **System > System Utilities > Reset Configuration to Defaults** in the navigation tree.

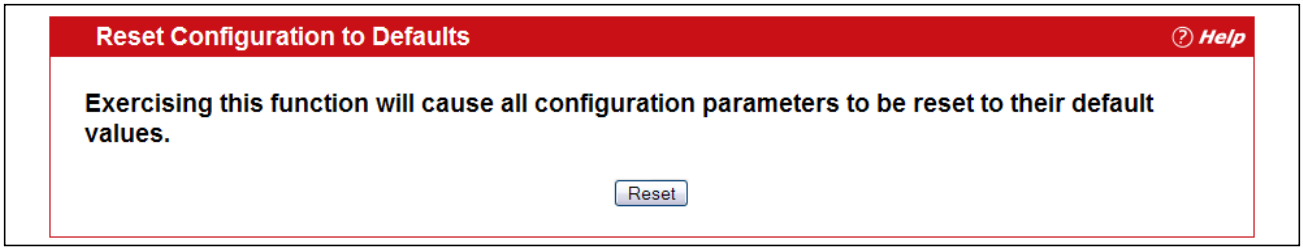


Figure 31: Reset Configuration to Defaults

Click **Reset** to restore the factory default settings. The screen refreshes and asks you to confirm the reset. Click **Reset** again to complete the action.

Reset Passwords to Defaults

Use the Reset Passwords to Defaults page to reset the passwords for the default read/write (admin) and read-only (guest) users on the system. By default, the passwords are blank. If you have configured additional read-only users on your system, their passwords are not affected.

To access the Reset Passwords to Defaults page, click **System > System Utilities > Reset Passwords to Defaults** in the navigation tree.

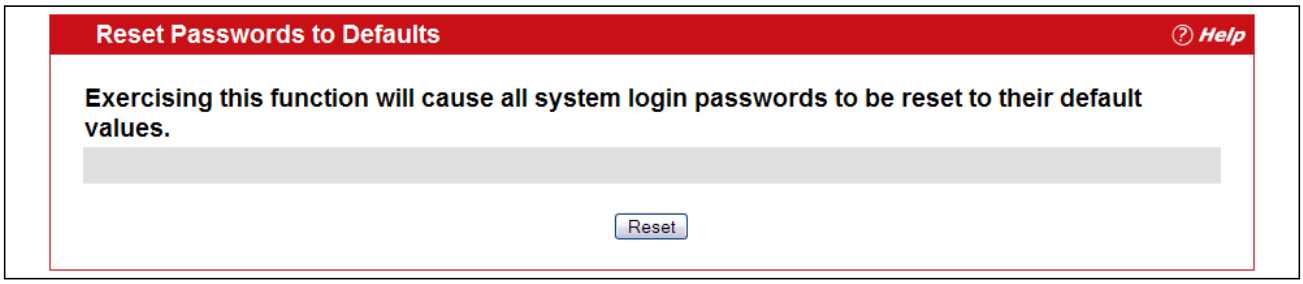


Figure 32: Reset Passwords to Defaults

Click **Reset** to restore the passwords for the default users to the factory defaults.

Note: When the password for the read/write user (admin) changes, you must re-authenticate with the user name and default password.

Upload File To Switch (TFTP)

Use the Upload File To Switch page to upload device software, the image file, the configuration files, and SSH or SSL files from a TFTP server to the switch.

You can also upload files via HTTP. See "HTTP File Upload" on page 89 for more information.

To access the Upload File To Switch page, click **Syste**m > **System Utilities** > **Upload File To Switch** in the navigation tree. To start file transfer, fill in the appropriate information in the text boxes, check the Start File Transfer button, and then click Submit.

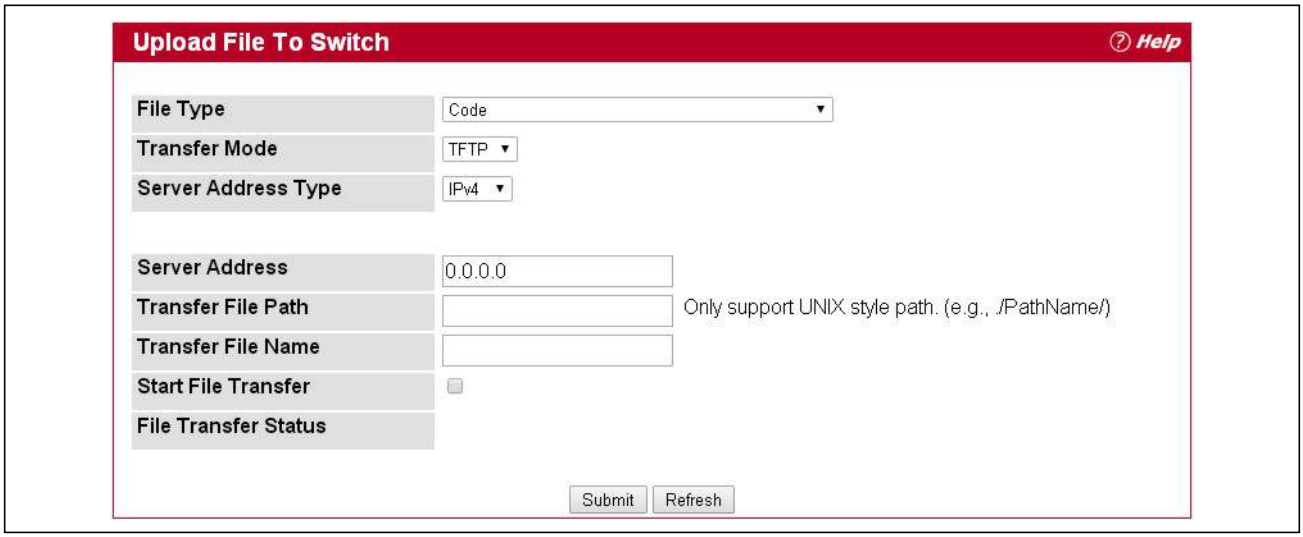


Figure 33: Upload File to Switch

Table 26: Upload File to Switch Fields

Field	*Description*
File Type	Specify what type of file you want to download to the switch: • **CLI Banner:** The CLI banner is the text that displays in the command-line interface before the login prompt. The CLI banner to download is a text file and displays when a user connects to the switch by using telnet, SSH, or a serial connection. • **Code:** The code is the system software image, which is saved in one of two designated files in the file system called images (active and backup). The active image stores the active copy; while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image. This is a safety feature for faults occurring during the boot upgrade process. • **Configuration:** If you have a copy of a valid configuration file on a TFTP server, you can download it to the switch to overwrite the running and startup configuration files. Upon a successful file transfer, the settings in the configuration file you upload are applied to the switch, and the configuration persists across a system reset. If the file has errors, the update is stopped. The configuration file is not a text file and cannot be edited by using a text editor. • **Text Configuration**: A text-based configuration file enables you to edit a configured text file (startup-config) offline as needed without having to translate the contents for FASTPATH to understand. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (i.e., change the device name, serial number, IP address, etc.), and download it to that device. • **SSH-1 RSA Key File:** SSH-1 Rivest-Shamir-Adleman (RSA) Key File. To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions. • **SSH-2 RSA Key PEM File:** SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded). To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions. • **SSH-2 DSA Key PEM File:** SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded). To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions. • **SSL Trusted Root Certificate PEM File:** SSL Trusted Root Certificate File (PEM Encoded). • **SSL Server Certificate PEM File:** SSL Server Certificate File (PEM Encoded). • **SSL DH Weak Encryption Parameter PEM File:** SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded). • **SSL DH Strong Encryption Parameter PEM File:** SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded). • **IAS Users:** Internal Authentication Server Users Database File to be used for local IEEE 802.1X authentication. • **License Certificate PEM File:** An X.509 certificate file that contains license information for the access controller system, including the maximum number of APs that can be managed. • **AP Image File:** AP image file to store on AC.
Transfer Mode	Specifies the protocol to be used for the transfer: TFTP or FTP.

Table 26: Upload File to Switch Fields (Cont.)

Field	*Description*
Server Address Type	Specify either IPv4 or DNS address to indicate the format of the TFTP Server Address field. The factory default is IPv4.
Server Address	Enter the IP address of the TFTP server in accordance with the format indicated by the TFTP Server Address Type. The factory default is the IPv4 address 0.0.0.0.
Transfer File Path	Enter the path on the TFTP server where the selected file is located. You may enter up to 32 characters. The factory default is blank.
Transfer File Name	Enter the name of the file you want to upload from the TFTP server. You may enter up to 32 characters. The factory default is blank.
User Name	Enter the user name for remote login to FTP server where the file resides. This field is visible only when FTP transfer modes are selected.
Password	Enter the password for remote login to FTP server where the file resides. This field is visible only when FTP transfer modes are selected.
Start File Transfer	To initiate the upload, check this box before clicking **Submit**.

Uploading a File to the Switch

Before you upload a file to the switch, the following conditions must be true:

- The file to upload is on the server in the appropriate directory.
- The file is in the correct format.
- The switch has a path to the server.

Use the following procedures to upload a file from a TFTP server to the switch.

1. From the **File Type** field, select the type of file to upload.

Note: It is recommended that you not overwrite the active image.

2. Verify the IP address of the TFTP server and ensure that the software image or other file to upload is available on the TFTP server.
3. Complete the **Server IP Address**, **Transfer File Path** (full path without TFTP server IP address) fields, and **Transfer File Name**.
4. Click the Start File Transfer check box, and then click **Submit**.

   After you click **Submit**, the screen refreshes and a “File transfer operation started” message appears. After the software is uploaded to the device, a message appears indicating that the file transfer operation completed successfully.

To activate a software image that you download to the switch, see “Dual Image Configuration” on page 88.

Download File From Switch (TFTP)

Use the Download File from Switch page to download configuration (ASCII) and image (binary) files from the switch to the TFTP server.

To display the Download File From Switch page, click **System > System Utilities > Download File From Switch** in the navigation tree.

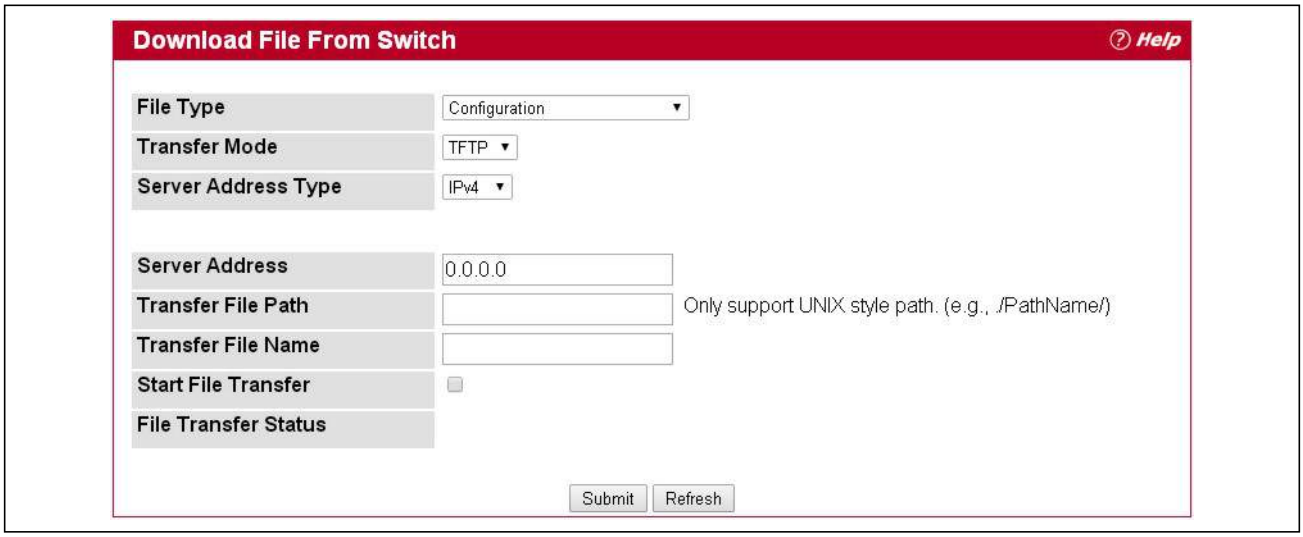


Figure 34: Download File from Switch

Table 27: Download File from Switch Fields

Field	*Description*
File Type	Specify what type of file you want to download: • **CLI Banner**: Retrieves the CLI banner file. • **Configuration**: Retrieves the stored startup configuration (.cfg) and copy it to a TFTP server. • **Text Configuration:** Retrieves the text configuration file startup-config. • **Error Log:** Retrieves the system error (persistent) log, sometimes referred to as the event log. • **Buffered Log**: Retrieves the system buffered (in-memory) log. • **Startup Log:** Retrieves the specified log file generated during system boot up. • **Trap Log**: Retrieves the system trap records. • **License Certificate PEM File:** An X.509 certificate file that contains license information for the access controller system, including the maximum number of APs that can be managed. • **AP Image File**: Retrieves the specified AP image file.
Transfer Mode	Specifies the TFTP protocol as the transfer method.
Server Address Type	Specifies either IPv4 or IPv6 address to indicate the format of the TFTP Server Address field. The factory default is IPv4.

Table 27: Download File from Switch Fields (Cont.)

Field	*Description*
Server Address	Enter the IP address of the TFTP server in accordance with the format indicated by the TFTP Server Address Type. The factory default is the IPv4 address 0.0.0.0.
Transfer File Path	Enter the path on the TFTP server where you want to put the file. You may enter up to 32 characters. The factory default is blank.
Transfer File Name	Enter a destination file name for the file to download. You may enter up to 32 characters. The factory default is blank.
Start File Transfer	To initiate the file download, check this box before clicking **Submit**.

Downloading Files

Use the following procedures to download a file to a TFTP server from the switch.

1. From the **File Type** field, select the type of file to copy from the switch to the TFTP server.
2. Complete the **Server Address Type**, **Server Address, Transfer File Path** (full path without TFTP server IP address), and **Transfer File Name** fields.
3. Click the **Start File Transfe**r check box, and then click **Submit**.

   After you click **Submit**, the screen refreshes and a “File transfer operation started” message appears. After the software is downloaded to the server, a message appears indicating that the file transfer operation completed successfully.

Copy Configuration Files

Use the Copy Configuration Files page to change the configuration files on the switch to startup or backup configuration files.

To display this page, click **System > System Utilities > Copy Configuration Files** in the navigation menu.

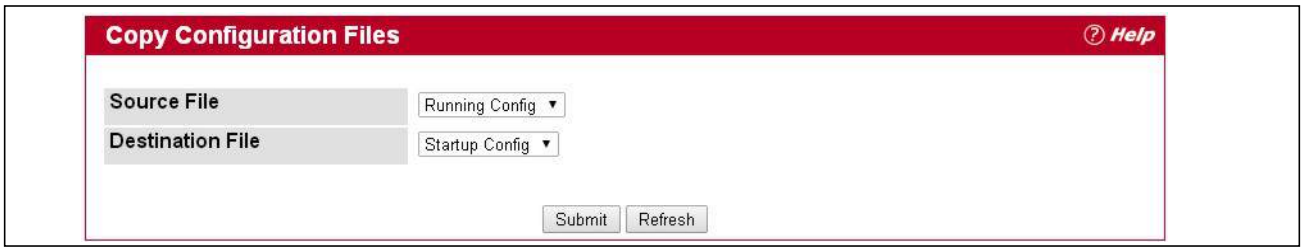


Figure 35: Copy Configuration Files

The Copy Configuration Files page contains the following fields:

Table 28: Copy Configuration Files Fields

Field	*Description*
Source File	Specifies the configuration file to copy: • Running Config • Startup Config • Backup Config
Destination File	Specifies the configuration file to overwrite: • Startup Config • Backup Config

Dual Image Configuration

The system maintains two versions of the software in permanent storage. One image is the active image, and the second image is the backup image. The active image is loaded during subsequent switch restarts. This feature reduces switch down time when upgrading/downgrading the software.

A system running an older software version will ignore (not load) a configuration file created by the newer software version. When a configuration file created by a newer software version is discovered by the system running an older version of the software, the system will display an appropriate warning to the user.

Use the Dual Image Configuration page to set the boot image.

To display the Dual Image Configuration page, click **System > System Utilities > Dual Image Configuration** in the navigation menu.

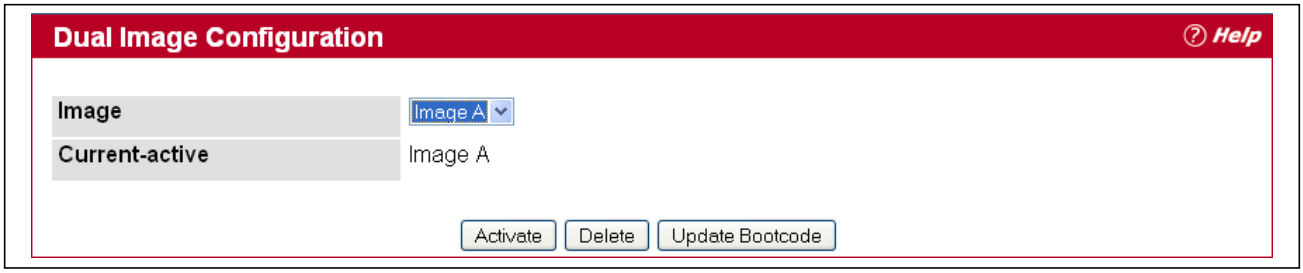


Figure 36: Dual Image Configuration

The Active Image page contains the following fields:

Table 29: Dual Image Configuration Fields

Field	*Description*
Image	Select Image A or Image B from the drop-down menu to set a software image as the active image.
Current Active	Displays name of current active image.

Click **Activate** to make the image that is selected in the **Image** field the next active image for subsequent reboots.

Note: After activating an image, you must perform a system reset of the switch in order to run the new code.

- Click **Delete** to remove the selected image from permanent storage on the switch.You cannot delete the active image.
- If the file you uploaded contains the boot loader code only, click **Update Bootcode**.
- Click **Submit** to update the image on the switch.

HTTP File Upload

Use the HTTP File Upload page to upload files of various types to the switch using an HTTP session (i.e., via your web browser).

To display this page, click **System > System Utilities > HTTP File Upload** in the navigation menu.

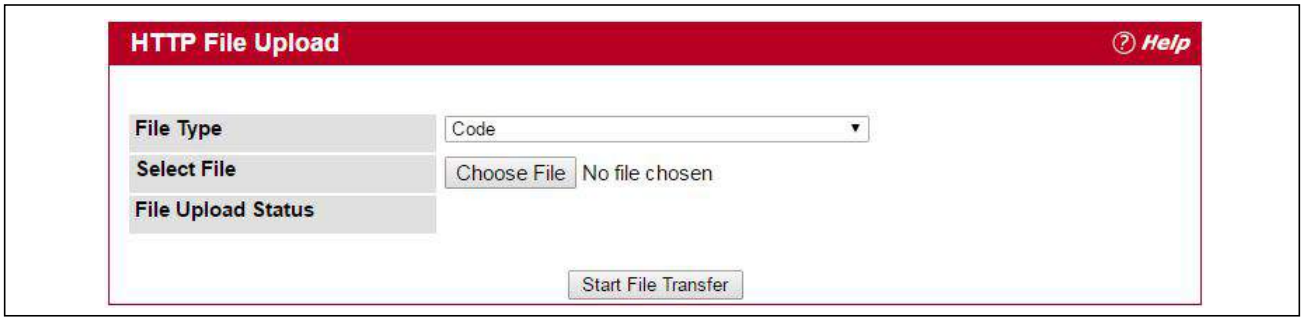


Figure 37: HTTP File Upload

Table 30: HTTP File Upload Fields

Field	*Description*

File Type	Specify the type of file you want to upload:
	• **Code**: Choose this option to upgrade the operational software in flash (default).
	• **Configuration**: Choose this option to update the switch's configuration. If the file has errors the update will be stopped.
	• **Text Configuration**: Uploads a text configuration file startup-config. Specify the text configuration to be updated. If the file has errors, the update will be stopped.
	• **SSH-1 RSA Key File**: SSH-1 Rivest-Shamir-Adleman (RSA) Key File
	• **SSH-2 RSA Key PEM File**: SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded)
	• **SSH-2 DSA Key PEM File**: SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded)
	• **SSL Trusted Root Certificate PEM File**: SSL Trusted Root Certificate File (PEM Encoded)
	• **SSL Server Certificate PEM File**: SSL Server Certificate File (PEM Encoded)
	• **SSL DH Weak Encryption Parameter PEM File**: SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded)
	• **SSL DH Strong Encryption Parameter PEM File**: SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded)
	• **CLI Banner**: Choose this option to upload a banner file to be displayed before the login prompt appears.
	• **License Certificate PEM File**: An X.509 certificate file that contains license information for the access controller system, including the maximum number of APs that can be managed.
	• **AP Image File**: Choose this option to copy AP image. Files will be stored under the AP Image Availability List.
	• **Text Default Configuration**: This feature allows you to preserve a particular segment of the configuration when performing configuration upload/download. This feature allows user to preserve a particular segment of the configuration when doing the config upload/download. This segment includes the following:
	  • Security > Captive Portal > CP configuration > Default config
	  • Security > Radius > Configuration > Default configuration (Default servername: Default-RADIUS-SERVER)
	  • WLAN > WLAN Configuration > Networks > 1~17 Networks (GuestNetwork, ManagedSSID_1, ManagedSSID_2, …, ManagedSSID_16)
	  • WLAN > WLAN Configuration > AP Profiles > Default config
	
	The factory default is code.
	
	Note: To upload SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.

Select File	Enter the path and filename or browse for the file you want to upload. You may enter up to 80 characters.

Click the **Start File Transfer** button to initiate the file download.

Ping

Use the Ping page to tell the switch to send a Ping request to a specified IP address. You can use this feature to check whether the switch can communicate with a particular network host.

To access the Ping page, click **System > System Utilities > Ping** in the navigation menu.

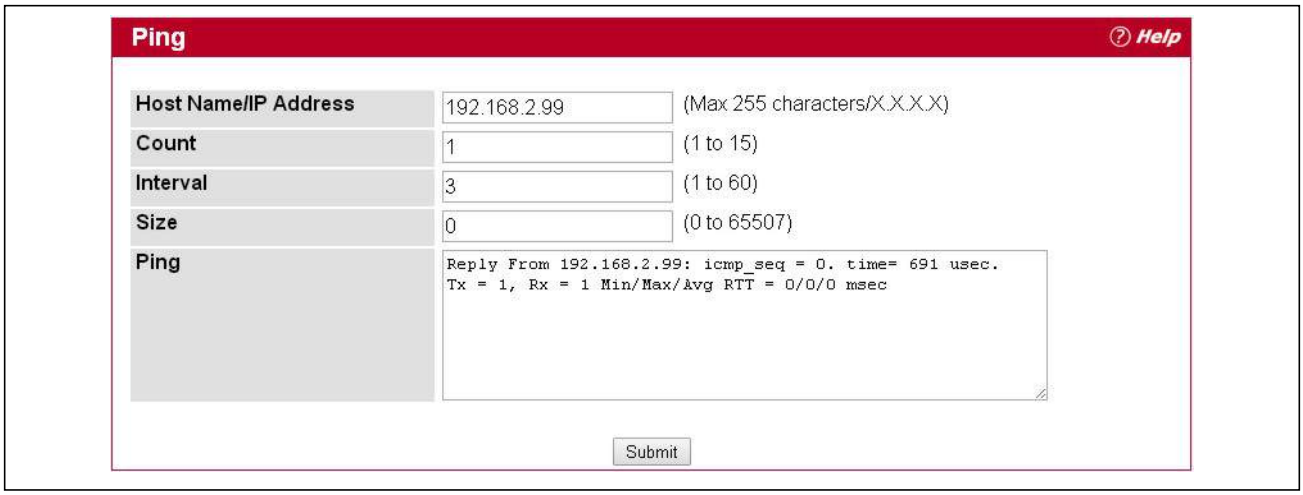


Figure 38: Ping

Table 31: Ping Fields

Field	*Description*
Hostname/IP Address	Enter the IP address or the host name of the station you want the switch to ping. The initial value is blank. This information is not retained across a power cycle.
Count	Specify the number of pings to send.
Interval	Specify the number of seconds between pings sent.
Size	Specify the size of the ping packet to send.
Ping	Display the results of the ping.

Click **Submit** to send the ping. If successful, the results display as shown in Figure 39.

TraceRoute

You can use the TraceRoute utility to discover the paths that a packet takes to a remote destination.

To display this page, click **System > System Utilities> TraceRoute** in the navigation tree.

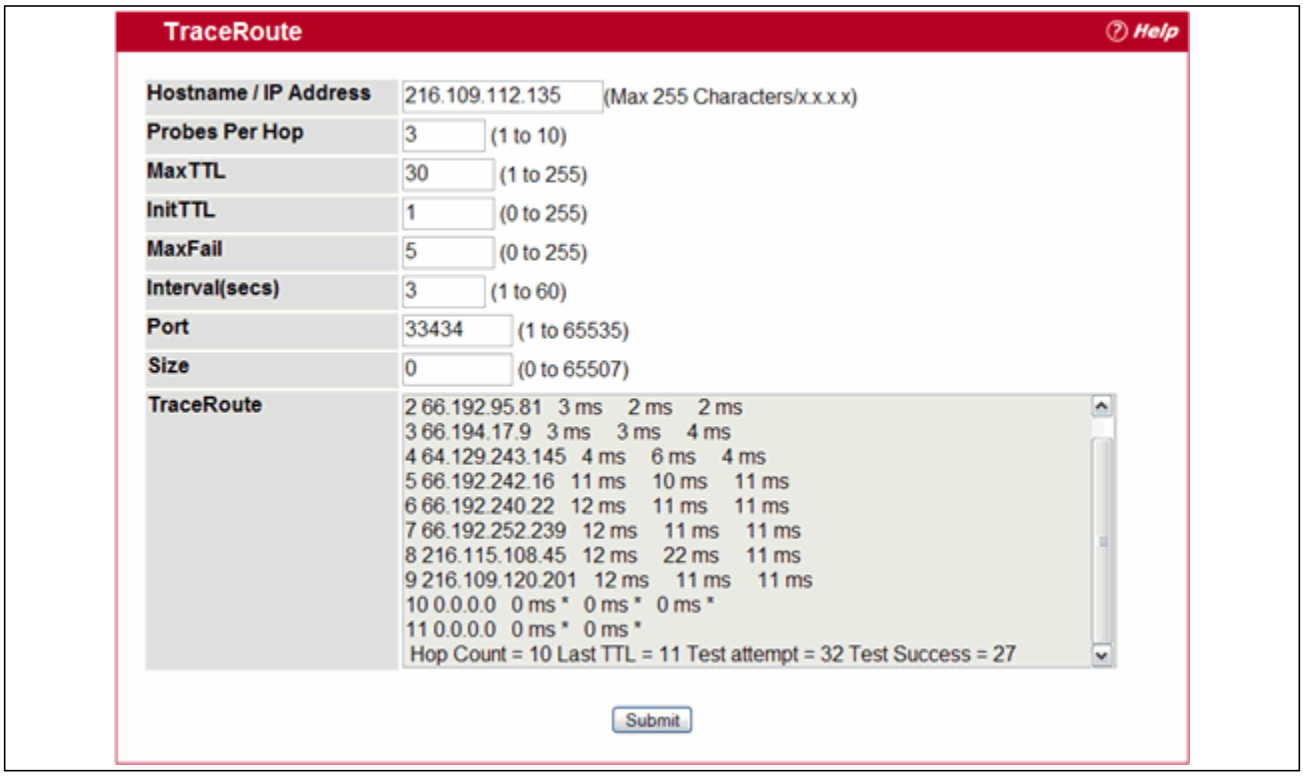


Figure 39: TraceRoute

Table 32: TraceRoute Fields

	Definition
Hostname/IP Address	Enter the IP address or the hostname of the station you want the switch to discover path for.
Probes Per Hop	Enter the number of times each hop should be probed.
MaxTTL	Enter the maximum time-to-live for a packet in number of hops.
InitTTL	Enter the initial time-to-live for a packet in number of hops.
MaxFail	Enter the maximum number of failures allowed in the session.
Interval	Enter the time between probes in seconds.
Port	Enter the UDP destination port in probe packets.
Size	Enter the size of probe packets.
TraceRoute	Displays the output from a traceroute.

Click **Submit** to initiate the traceroute. The results display in the TraceRoute box.

Managing SNMP Traps

The pages in the Trap Manager folder allow you to view and configure information about SNMP traps the system generates.

Trap Flags

Use the Trap Flags page to enable or disable traps the switch can send to an SNMP manager. When the condition identified by an active trap is encountered by the switch, a trap message is sent to any enabled SNMP trap receivers, and a message is written to the trap log.

To access the Trap Flags page, click **System > Trap Manager > Trap Flags** page.

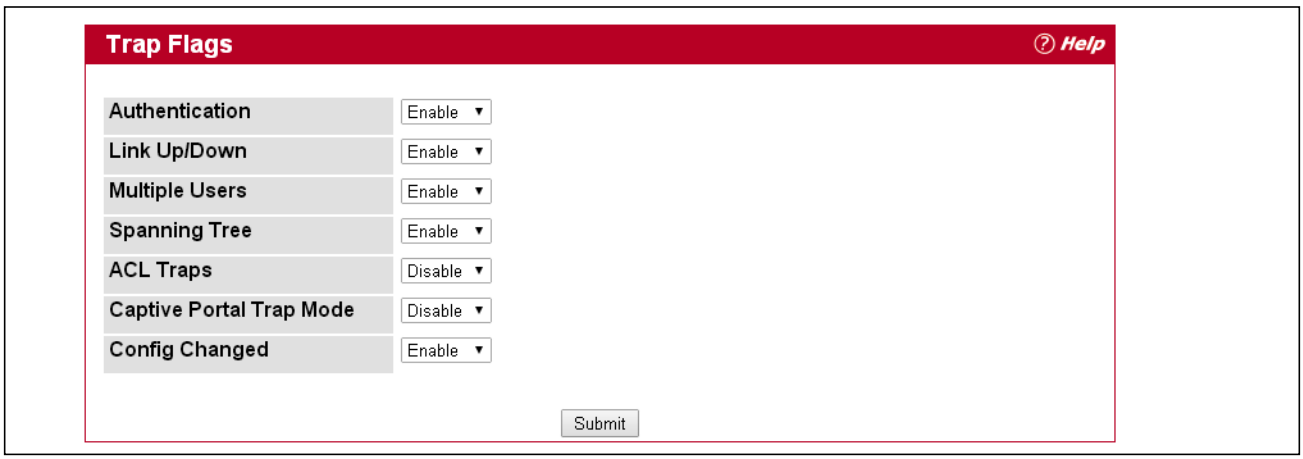


Figure 40: Trap Flags Configuration

The fields available on the Trap Flags page depends on the packages installed on your system. For example, if your system does not have the BGP4 package installed, the BGP Traps field is not available. Figure 40 and Table 33 show the fields that are available on a system with all packages installed.

Table 33: Trap Flags Configuration Fields

Field	*Description*
Authentication	Enable or disable activation of authentication failure traps by selecting the corresponding line on the pull-down entry field. The factory default is enabled.
Link Up/Down	Enable or disable activation of link status traps by selecting the corresponding line on the pull-down entry field. The factory default is enabled.
Multiple Users	Enable or disable activation of multiple user traps by selecting the corresponding line on the pull-down entry field. The factory default is enabled. This trap is triggered when the same user ID is logged into the switch more than once at the same time (either via telnet or the serial port).
Spanning Tree	Enable or disable activation of spanning tree traps by selecting the corresponding line on the pull-down entry field. The factory default is enabled.

Table 33: Trap Flags Configuration Fields (Cont.)

Field	*Description*
ACL Traps	Enable or disable activation of ACL traps by selecting the corresponding line on the pulldown entry field. The factory default is disabled.
Captive Portal	Select Enable to allow the SNMP agent on the switch to generate captive portal SNMP traps that are enabled. Select Disable to prevent the SNMP agent on the switch from generating any captive portal SNMP traps, even if they are individually enabled.
Config Changed	Enable or disable activation of a trap when the system configuration is changed.

If you make any changes to this page, click **Submit** to apply the changes to the system.

Trap Logs

Use the Trap Log page to view the entries in the trap log. For information about how to copy the file to a TFTP server, see "Download File From Switch (TFTP)" on page 86.

To access the Trap Log page, click **System > Trap Manager > Trap Logs** in the navigation menu.

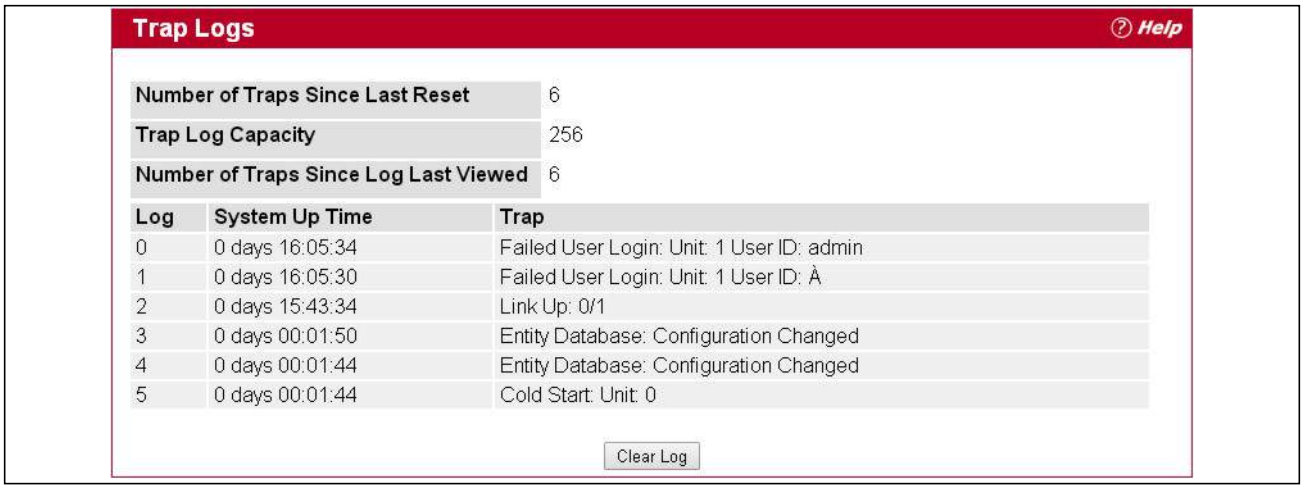


Figure 41: Trap Log

Table 34: Trap Log Fields

Field	*Description*
Number of Traps Since Last Reset	The number of traps generated since the trap log entries were last cleared.
Trap Log Capacity	The maximum number of traps stored in the log. If the number of traps exceeds the capacity, new entries will overwrite the oldest entries.
Number of Traps Since Log Last Viewed	The number of traps that have occurred since the traps were last displayed. Displaying the traps by any method (terminal interface display, Web display, upload file from switch, etc.) will cause this counter to be cleared to 0.
Log	The sequence number of this trap.

Table 34: Trap Log Fields (Cont.)

Field	*Description*
System Up Time	The time at which this trap occurred, expressed in days, hours, minutes and seconds since the last reboot of the switch.
Trap	Displays information identifying the trap.

Click **Clear Log** to clear all entries in the log. Subsequent displays of the log will only show new log entries.

Managing the DHCP Server

DHCP is generally used between clients (e.g., hosts) and servers (e.g., routers) for the purpose of assigning IP addresses, gateways, and other networking definitions such as DNS, NTP, and/or SIP parameters. The DHCP Server folder contains links to web pages that define and display DHCP parameters and data. The following pages are accessible from this DHCP Server folder:

- Global Configuration
- Pool Configuration
- Pool Options
- Reset Configuration
- Binding Information
- Server Statistics
- Conflict Information

Global Configuration

Use the **DHCP Server Global Configuration** page to configure DHCP global parameters.

To display this page, click **System > DHCP Server > Global Configuration** in the navigation menu.

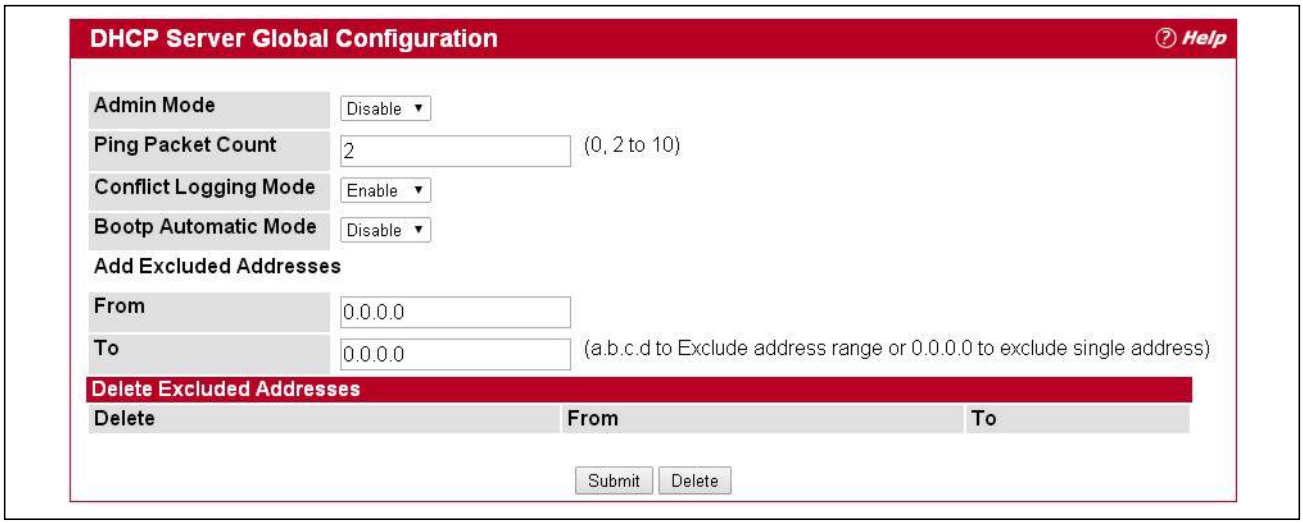


Figure 42: DHCP Server Global Configuration

Table 35: DHCP Server Global Configuration Fields

Field	*Description*
Admin Mode	Enables or disables the DHCP server administrative mode. When enabled, the device can be configured to automatically allocate TCP/IP configurations for clients.

Table 35: DHCP Server Global Configuration Fields

Field	*Description*
Ping Packet Count	The number of packets the server sends to a pool address to check for duplication as part of a ping operation. If the server receives a response to the ping, the address is considered to be in conflict and is removed from the pool.
Conflict Logging Mode	Enables or disables the logging mode for IP address conflicts. When enabled, the system stores information about IP address conflicts that are detected by the DHCP server.
BOOTP Automatic Mode	Enables or disables the BOOTP automatic mode. When enabled, the DHCP server supports the allocation of automatic addresses for BOOTP clients. When disabled the DHCP server supports only static addresses for BOOTP clients.
Enable	Allows the allocation of the addresses in the automatic address pool to the BOOTP client.
Disable	Does not use the automatic address pool addresses for BOOTP clients. This is the default value.
Add Excluded Addresses	Use the **From** and **To** fields to specify the IP addresses that the server should not assign to the client. If you want to exclude a range of addresses, set the range boundaries.
From	To exclude an address range, specify the low address in the range. To specify a single address to exclude, enter the address in the **From** field and leave the **To** field at the default value of 0.0.0.0.
To	To exclude an address range, specify the high address in the range. To exclude a single address, do not enter a value in this field.
Delete Excluded Addresses	After you add excluded addresses, they appear below this field title. Each address or address range has a check box next to it.

- If you change any settings or add an excluded address range, click **Submit** to apply the changes to the system. Each time you enter a value in the **From** or **To** fields, click **Submit** to add the address or address range to the excluded address list.
- To Delete an address or address range from the excluded address list, select one or more check boxes beneath the Delete Excluded Addresses field and click Submit.

Pool Configuration

Use the DHCP Pool Configuration page to create the pools of addresses that can be assigned by the server.

To access the DHCP Server Pool Configuration page, click **System > DHCP Server > Pool Configuration** in the navigation menu.

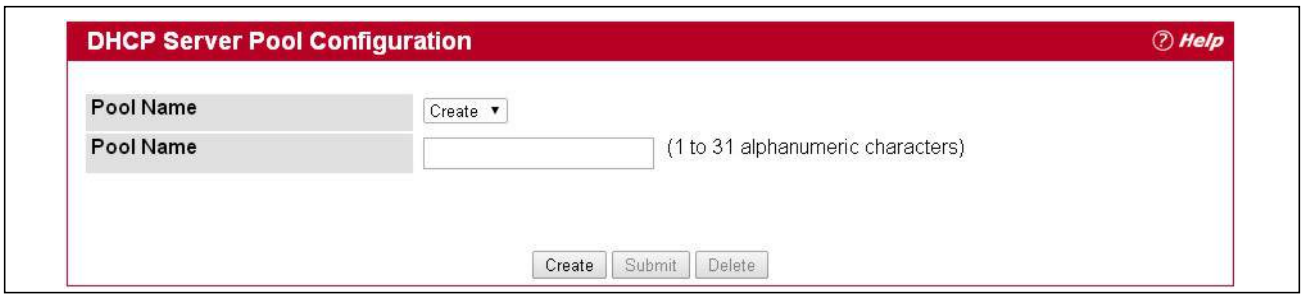


Figure 43: DHCP Server Pool Configuration

Table 36: DHCP Server Pool Configuration Fields

Field	*Description*
Pool Name	For a user with read/write permission, this field would show names of all the existing pools along with an additional option Create. When the user selects Create, another text box, Pool Name, appears where the user may enter the name for the Pool to be created. For a user with read-only permission, this field would show names of the existing pools only.
Pool Name	This field appears when a user with read-write permission has selected Create in the Drop Down list against Pool Name. Specifies the Name of the Pool to be created. Pool Name can be up to 31 characters in length.

In Figure 44, some of the blank fields where you add IP addresses have been edited out of the image for display purposes. You can add up to eight addresses in the Default Router Addresses, DNS Server Addresses, NetBIOS name Server Addresses and IP Address Value fields.

If you select Automatic or Manual from the Type of Binding drop-down menu, the screen refreshes and a slightly different set of fields appears.

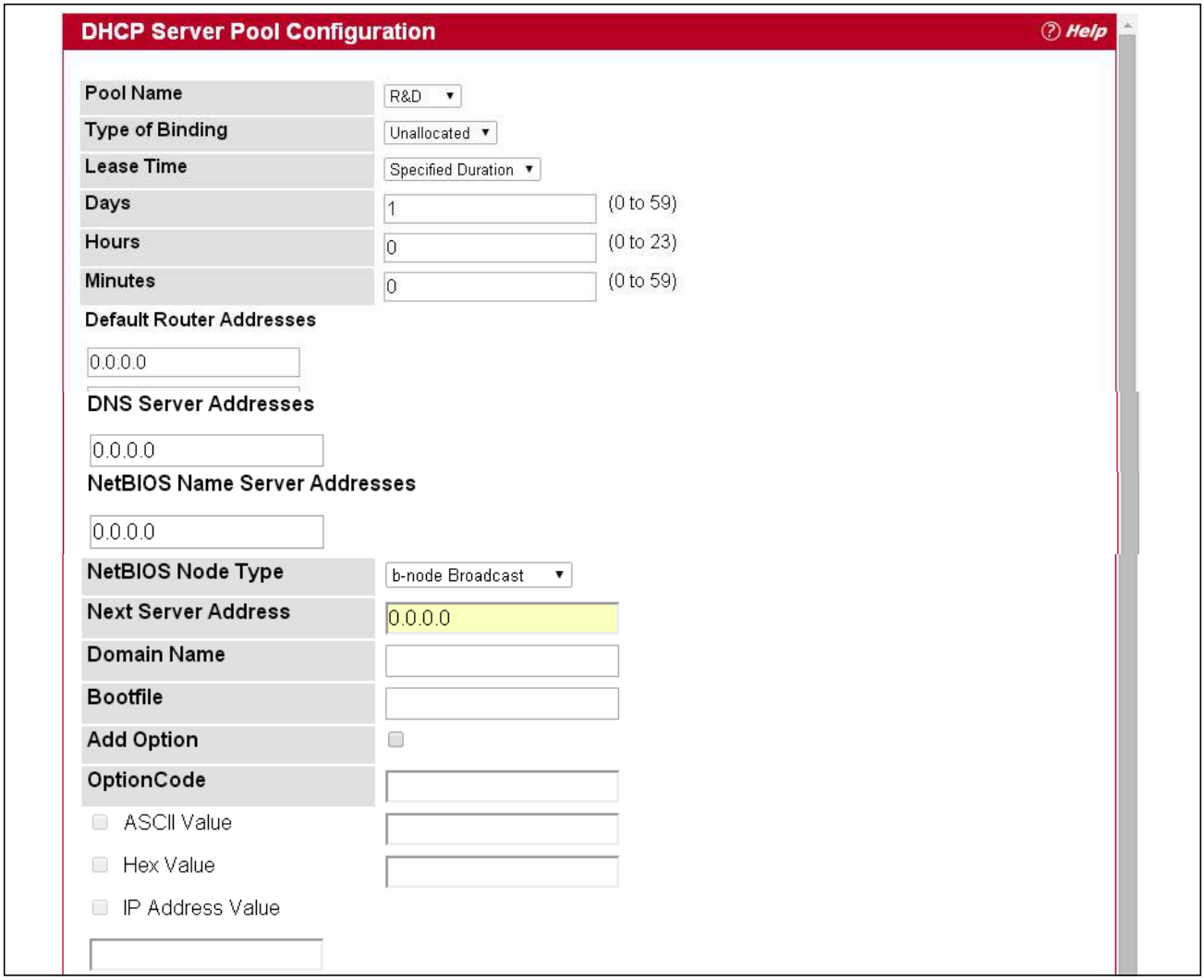


Figure 44: DHCP Server Pool Configuration (Continued)

Table 37: DHCP Server Pool Configuration Fields

Field	*Description*
Pool Name	This field shows the names of existing pools.
Type of Binding	Specifies the type of binding for the pool. • **Unallocated**: The addresses are not assigned to a client. • **Automatic**: The IP address is automatically assigned to a client by the DHCP server. • **Manual**: You statically assign an IP address to a client based on the client's MAC address.
Lease Time	Specifies the type of lease to assign clients: • Infinite: For dynamic bindings, an infinite lease time is a lease period of 60 days. For manual bindings, an infinite lease time means the lease period does not expire. • Specified Duration: Allows you to specify the lease period. The default value is Specified Duration.

Table 37: DHCP Server Pool Configuration Fields (Cont.)

Field	*Description*
Days	For a Specified Duration lease time, this field specifies the number of days for the lease period. The default value is 1, and the valid range is 0-59.
Hours	For a Specified Duration lease time, this field specifies the number of hours for the lease period. The default value is 1, and the valid range is 0-1439.
Minutes	For a Specified Duration lease time, this field specifies the number of minutes for the lease period. The default value is 1, and the valid range is 0-86399.
Vlan ID	
Network Number	If you specify Dynamic as the type of binding, this field appears. Specifies the network number (host bits) for a DHCP address of a dynamic pool. For example, if 192.168.5.0 is the network number and 255.255.255.0 is the network mask (or a prefix length of 24) for the pool, the IP addresses in the pool range from 192.168.5.1 - 192.168.5.254.
Network Mask	For dynamic bindings, this field specifies the subnet mask for a DHCP address of a dynamic pool. You can enter a value in **Network Mask** or **Prefix Length** to specify the subnet mask, but do not enter a value in both fields.
Prefix Length	For dynamic bindings, this field specifies the subnet number for a DHCP address of a dynamic pool. You can enter a value in Network Mask or Prefix Length to specify the subnet mask, but do not enter a value in both fields. The valid range is 0 to 32.
Client Name	For manual bindings, this field specifies a name for the client to which the DHCP server will statically assign an IP address. This field is optional.
Hardware Address	For manual bindings, this field specifies the MAC address of the hardware platform of the DHCP client.
Hardware Address Type	For manual bindings, this field specifies the protocol of the hardware platform of the DHCP client. Valid types are ethernet and ieee802. Default value is ethernet.
Host Number	For manual bindings, this field specifies the IP address to be statically assigned to a DHCP client. The host can be set only if at least one among of Client Identifier or Hardware Address is specified. Deleting Host would delete Client Name, Client ID, Hardware Address for the Manual Pool and set the Pool Type to Unallocated.
Host Mask	For manual bindings, this field specifies the subnet mask to be statically assigned to a DHCP client. You can enter a value in Host Mask or Prefix Length to specify the subnet mask, but do not enter a value in both fields.
Default Router Addresses	Lists the IP address of each router to which the client(s) in the pool should send traffic. The default router should be in the same subnet as the client.
DNS Server Addresses	Lists the IP address of each DNS server the client(s) in the pool can contact to perform address resolution.
NetBIOS Name Server Addresses	Lists the IP address of each NetBIOS Windows Internet Naming Service (WINS) name server that is available for the selected pool.
NetBIOS Node Type	Specifies the NetBIOS node type for DHCP clients. • b-node Broadcast • p-node Peer-to-Peer • m-node Mixed • h-node Hybrid
Next Server Address	Specifies the Next Server Address for the pool.

Table 37: DHCP Server Pool Configuration Fields (Cont.)

Field	*Description*
Domain Name	Specifies the domain name for a DHCP client. Domain Name can be up to 255 characters in length.
Bootfile	Specifies the name of the default boot image for a DHCP client. File Name can be up to 128 characters in length.
Add Option	This field is used to configure the DHCP server options.
Option Code	Specifies the DHCP option code. Valid Range is (1 to 254)
ASCII Value	Specifies an NVT ASCII character string.
Hex Value	Specifies hexadecimal data. Each byte in hexadecimal character strings is 2 hexadecimal digits. Each byte can be separated by a colon or white space. A period can be used to separate 2 bytes/4 hexadecimal digits.
IP Address Value	Specifies the Option IP addresses.

- After you configure values for the DHCP address pool, click **Submit** to create the pool and apply the changes to the system.
- To delete a pool, select the pool from the **Pool Name** drop-down menu and click **Delete**.

Pool Options

Use the Pool Options page to configure additional DHCP pool options, including vendor-defined options. DHCP options are collections of data with type codes that indicate how the options should be used. When a client broadcasts a request for information, the request includes the option codes that correspond to the information the client wants the DHCP server to supply.

To access the DHCP Server Pool Options page, click **System** > **DHCP Server** > **Pool Options** in the navigation menu.

If no DHCP pools exist, the DHCP Server Pool Options page does not display the fields shown in Figure 45.

Figure 45: DHCP Server Pool Options

If any DHCP pools are configured on the system, the DHCP Server Pool Options page contains the following fields:

Table 38: DHCP Server Pool Options Fields

Field	*Description*
Pool Name	Select the DHCP pool with the options you want to view or configure.
Option Code	Displays the DHCP option code configured for the selected Pool.
ASCII Value	Specifies the Option ASCII Value for the selected pool.

Table 38: DHCP Server Pool Options Fields

Field	*Description*
Hex Value	Specifies the Option Hex Value for the selected pool.
IP Address Value	Specifies the Option IP Address Value for the selected pool.
Delete	To delete an option code for the selected Pool, mark the check box for the option code and click **Delete**. This button is not visible to a user with read-only permission.

Reset Configuration

Use the **DHCP Server Reset Configuration** page to clear IP address bindings that the DHCP server assigned to the client.

To access this page, click **System > DHCP Server > Reset Configuration** in the navigation menu.

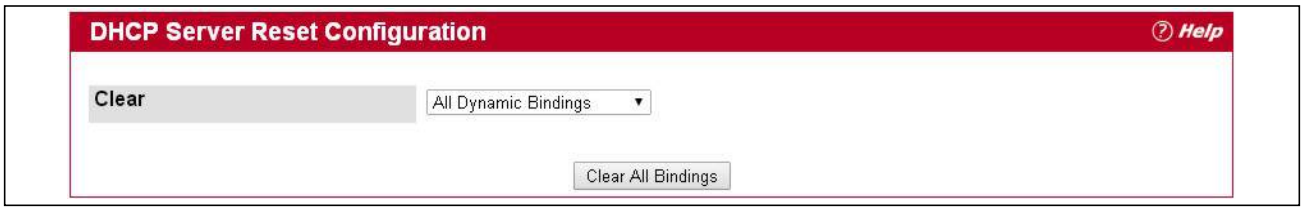


Figure 46: DHCP Server Reset Configuration

Table 39: DHCP Server Reset Configuration Fields

Field	*Description*
Clear	Specifies what to clear from the DHCP server database: • All Dynamic Bindings: Deletes all dynamic bindings from all address pools. • Specific Dynamic Binding: Deletes the specified binding. • All Address Conflicts: Deletes all address conflicts from the DHCP server database. • Specific Address Conflict: Deletes a specified conflicting address from the database.
Clear All Bindings	If you select **Specific Dynamic Bindings** or **Specific Address Conflicts** from the **Clear** field, the screen refreshes and the **Clear IP Address** field appears. Enter the specific IP address to clear from the DHCP server.

After you select the bindings or conflicts to clear and, if necessary, enter the specific IP address, click Clear to remove the binding from the DHCP server.

Binding Information

Use the DHCP Server Bindings Information page to view information about the IP address bindings in the DHCP server database.

To access the DHCP Server Bindings Information page, click **System** > **DHCP Server** > **Bindings Information** in the navigation tree.

Figure 47: DHCP Server Bindings Information

Table 40: DHCP Server Bindings Information Fields

Field	*Description*
DHCP Binding	Select the bindings to display: • **All Bindings**: Show all bindings. • **Specific Binding**: Show a specific binding. When you select this option, the screen refreshes, and the **Binding IP Address** field appears.
Binding IP Address	Specify the IP address for which you want to view binding information. This field is only available if you select **Specific Binding** from the **DHCP Binding** field.
IP Address	Displays the client IP address.
Hardware Address	Displays the client MAC address.
Lease Time Left	Shows the remaining time left in the lease in Days, Hours and Minutes dd:hh:mm format.
Pool Allocation Type	Shows the type of binding, which is dynamic or manual.

If you change any settings, click **Submit** to apply the changes to the system.

Click the **Detail** tab to display detailed information about configured address pools.

Figure 48: DHCP Pool Bindings Information

Table 41: DHCP Pool Bindings Information

Field	*Description*
Pool Name	Select the DHCP pool you want to view.
Leased addresses count	The number of addresses leased to this pool.
Total addresses count	The number of addresses available.
IP Address	Displays the client IP address.
Hardware Address	Displays the client MAC address.
Lease Time Left	Shows the remaining time left in the lease in Days, Hours and Minutes dd:hh:mm format.
Pool Allocation Type	Shows the type of binding, which is dynamic or manual.

Server Statistics

Use the DHCP Server Statistics page to view information about the DHCP server bindings and messages.

To access the DHCP Server Statistics page, click **System** > **DHCP Server** > **Server Statistics** in the navigation menu.

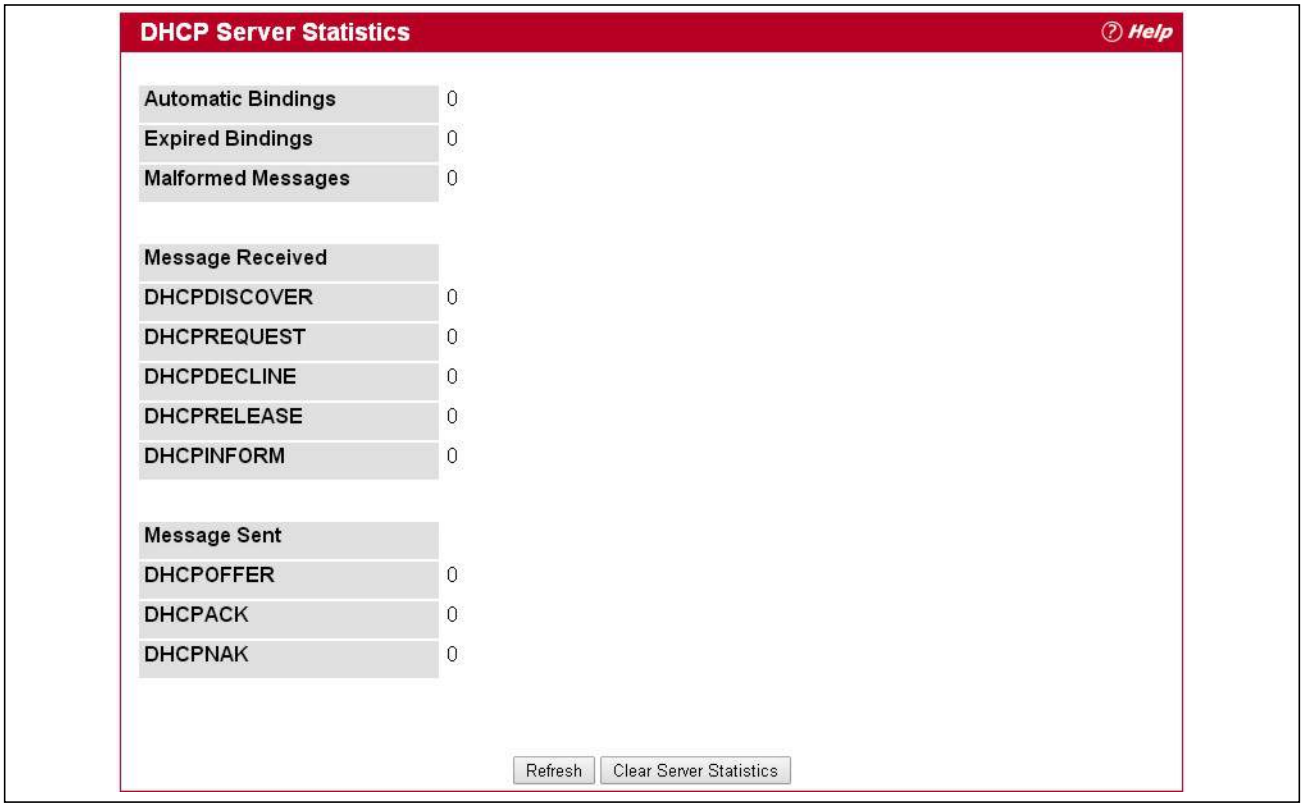


Figure 49: DHCP Server Statistics

Table 42: DHCP Server Statistics

Field	*Description*
Automatic Bindings	Shows the number of automatic bindings on the DHCP server.
Expired Bindings	Shows the number of expired bindings on the DHCP server.
Malformed Messages	Shows the number of the malformed messages.
Message Received	
DHCPDISCOVER	Shows the number of DHCPDISCOVER messages received by the DHCP server.
DHCPREQUEST	Shows the number of DHCPREQUEST messages received by the DHCP server.
DHCPDECLINE	Shows the number of DHCPDECLINE messages received by the DHCP server.
DHCPRELEASE	Shows the number of DHCPRELEASE messages received by the DHCP server.
DHCPINFORM	Shows the number of DHCPINFORM messages received by the DHCP server.
Message Sent	
DHCPOFFER	Shows the number of DHCPOFFER messages sent by the DHCP server.
DHCPACK	Shows the number of DHCPACK messages sent by the DHCP server.

Table 42: DHCP Server Statistics (Cont.)

Field	*Description*
DHCPNAK	Shows the number of DHCPNAK messages sent by the DHCP server.

Conflict Information

Use the DHCP Server Conflicts Information page to view information on hosts that have address conflicts; i.e., when the same IP address is assigned to two or more devices on the network.

To access the DHCP Server Conflicts Information page, click **System** > **DHCP Server** > **Conflicts Information** in the navigation tree.

Figure 50: DHCP Server Conflicts Information

Table 43: DHCP Server Conflicts Information Fields

Field	*Description*
DHCP Conflicts	Select the DHCP conflicts to display: • **All Conflicts**: Show all conflicts. • **Specific Conflict**: Show a specific conflict. When you select this option, the screen refreshes, and the Conflict IP Address field appears.
Conflict IP Address	Specify the IP address for which you want to view conflict information. This field is only available if you select **Specific Conflicts** from the **DHCP Conflict** field.
IP Address	Displays the client IP address.
Detection Method	Specifies the manner in which the IP address of the hosts were found on the DHCP server.
Detection Time	Specifies the time when the conflict was detected in N days NNh:NNm:NNs format with respect to the system up time.

Configuring DNS

You can use these pages to configure information about DNS servers the network uses and how the switch/router operates as a DNS client.

Global Configuration

Use this page to configure global DNS settings and to view DNS client status information.

To access this page, click **System > DNS > Global Configuration**.

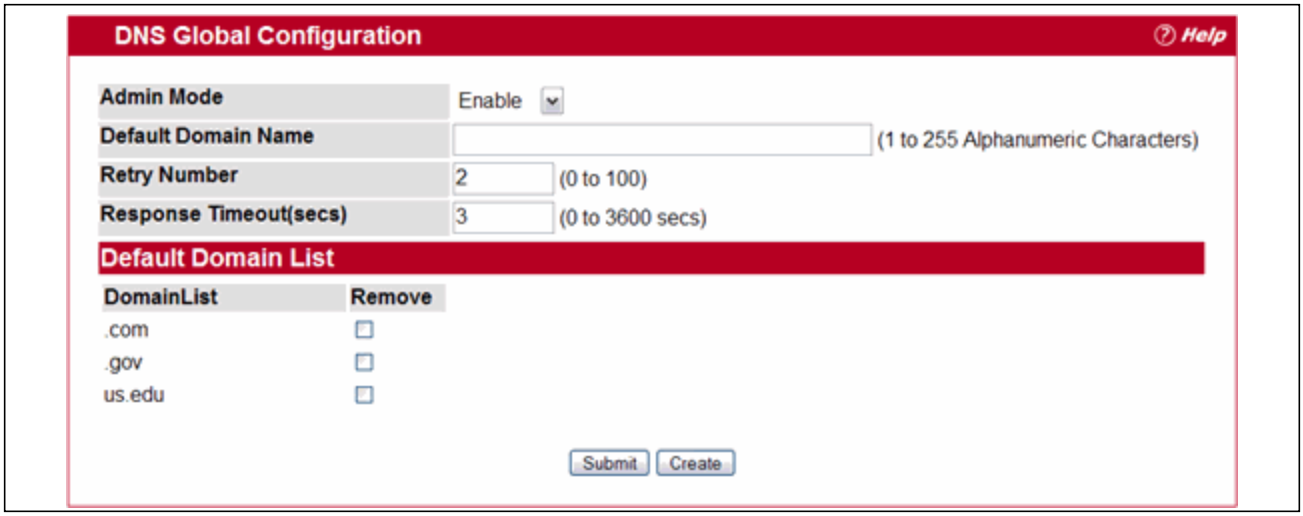


Figure 51: DNS Global Configuration

Table 44: DNS Global Configuration Fields

Field	*Description*
Admin Mode	Select **Enable** or **Disable** from the pull-down menu to set the administrative status of DNS Client. The default is Disable.
Default Domain Name	Enter the default domain name for DNS client messages. The name should be no longer than 255 characters. When the system is performing a lookup on an unqualified hostname, this field is provided as the domain name (e.g., if default domain name is *.com* and the user enters *hotmail*, then hotmail is changed to *hotmail.com* to resolve the name). By default, no default domain name is configured in the system.
Retry Number	Enter the number of times to retry sending DNS queries. Valid values are from 0 to 100. The default value is 2.
Response Timeout	Enter the number of seconds to allow a DNS server to respond to a request before issuing a retry. Valid values are 0 to 3600. The default value is 3.
Domain List	The domain name list for DNS Client. If there is no domain list, the default domain name configured is used.

- If you change any settings, click **Submit** to send the information to the system.

- To create a new list of domain names, click **Create**. Then enter a name of the list and click **Submit**. Repeat this step to add multiple domains to the default domain list. Domain names are composed of series of labels concatenated with dots. Each label must be between 1 and 63 characters long, and the entire domain name has a maximum of 255 characters.
- To remove a domain from the default list select the **Remove** option next to the item you want to remove and click **Submit**.

Server Configuration

Use this page to configure information about DNS servers that the router will use. The order in which you create them determines their precedence; i.e., DNS requests will go to the higher precedence server first. If that server is unavailable or does not respond in the configured response time, then the request goes to the server with the next highest precedence.

To access this page, click **System > DNS > Server Configuration**.

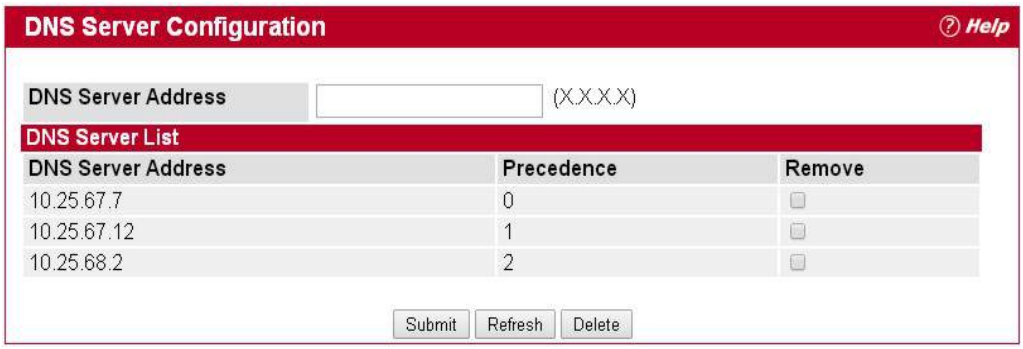


Figure 52: DNS Server Configuration

Table 45: DNS Server Configuration Fields

Field	*Description*
DNS Server Address	To add a new DNS server to the list, enter the DNS server IPv4 or IPv6 address in numeric notation.
Precedence	Shows the precedence value of the server that determines which server is contacted first; a lower number indicates a higher precedence.

- To create a new DNS server, enter an IP address in standard IPv4 or IPv6 dot notation in the **DNS Server Address** and click **Submit**. The server appears in the list below. The precedence is set in the order created.
- To change precedence, you must remove the server(s) by clicking the **Remove** box and then **Submit**, and add server(s) in the preferred order.

DNS Host Name IP Mapping Summary

Use this page to configure static and dynamic DNS host names for hosts on the network. The host names are associated with IPv4 or IPv6 addresses on the network, which are assigned to particular hosts.

To access this page, click **System > DNS > Host Name IP Mapping Summary** in the navigation tree.

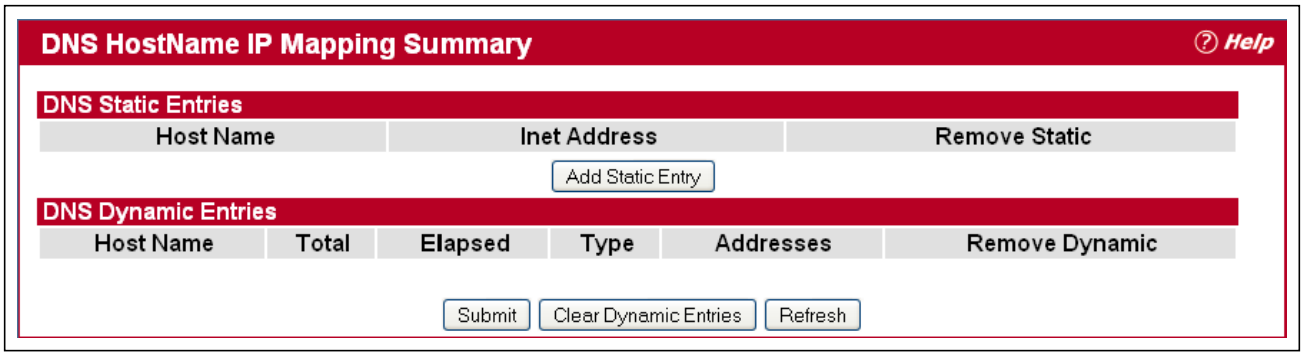


Figure 53: DNS Host Name IP Mapping Summary

Table 46: DNS Host Name IP Mapping Summary Fields

Field	*Description*
DNS Static Entries	
Host Name	The host name of the static entry.
Inet Address	The IP4 or IPv6 address of the static entry.
Remove Static	Select to remove a Host Name IP Mapping entry from the Host Name IP Mapping list.
DNS Dynamic Entries	
Host Name	The host name of the dynamic entry.
Total	The total time of the dynamic entry.
Elapsed	The elapsed time of the dynamic entry.
Type	The type of the dynamic entry.
Addresses	The IP4 or IPv6 address of the dynamic entry.
Remove Dynamic	Select to remove a Host Name IP Mapping entry from the Host Name IP Mapping list.

- Click **Add Static Entry** to load the Host Name IP Mapping Configuration page in order to configure the Host Name IP Mapping entries.
- Click **Submit** to apply the new configuration and cause the change to take effect immediately. These changes will not be retained across a power cycle unless a Save is performed.
- Click **Clear Dynamic Entries** to remove all Host Name IP Mapping entries. A confirmation prompt will be displayed. Click the button to confirm removal and the Host Name IP Mapping dynamic entries are cleared.
- Click **Refresh** to refresh the page with the most current data from the switch.

Configuring SNTP Settings

EWS4502/EWS4606 software supports the Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. EWS4502/EWS4606 software operates only as an SNTP client and cannot provide time services to other systems.

Time sources are established by Stratums. Stratums define the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. The device receives time from stratum 1 and above since it is itself a stratum 2 device.

The following is an example of stratums:

- **Stratum 0:** A real time clock is used as the time source, for example, a GPS system.
- **Stratum 1:** A server that is directly linked to a Stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.
- **Stratum 2**: The time source is distanced from the Stratum 1 server over a network path. For example, a Stratum 2 server receives the time over a network link, via NTP, from a Stratum 1 server.

Information received from SNTP servers is evaluated based on the time level and server type.

SNTP time definitions are assessed and determined by the following time levels:

- **T1**: Time at which the original request was sent by the client.
- **T2**: Time at which the original request was received by the server.
- **T3**: Time at which the server sent a reply.
- **T4**: Time at which the client received the server's reply.

The device can poll Unicast and Broadcast server types for the server time.

Polling for Unicast information is used for polling a server for which the IP address is known. SNTP servers that have been configured on the device are the only ones that are polled for synchronization information. T1 through T4 are used to determine server time. This is the preferred method for synchronizing device time because it is the most secure method. If this method is selected, SNTP information is accepted only from SNTP servers defined on the device using the SNTP Server Configuration page.

Broadcast information is used when the server IP address is unknown. When a Broadcast message is sent from an SNTP server, the SNTP client listens to the message. If Broadcast polling is enabled, any synchronization information is accepted, even if it has not been requested by the device. This is the least secure method.

The device retrieves synchronization information, either by actively requesting information or at every poll interval. If Unicast and Broadcast polling are enabled, the information is retrieved in this order:

- Information from servers defined on the device is preferred. If Unicast polling is not enabled or if no servers are defined on the device, the device accepts time information from any SNTP server that responds.
- If more than one Unicast device responds, synchronization information is preferred from the device with the lowest stratum.
- If the servers have the same stratum, synchronization information is accepted from the SNTP server that responded first.

MD5 (Message Digest 5) Authentication safeguards device synchronization paths to SNTP servers. MD5 is an algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication.

The SNTP folder contains links to view or configure the following features:

- SNTP Global Configuration
- SNTP Global Status
- SNTP Server Configuration
- SNTP Server Status

SNTP Global Configuration

Use the SNTP Global Configuration page to view and adjust SNTP parameters.

To display the SNTP Global Configuration page, click **System > SNTP** > **Global Configuration** in the navigation menu.

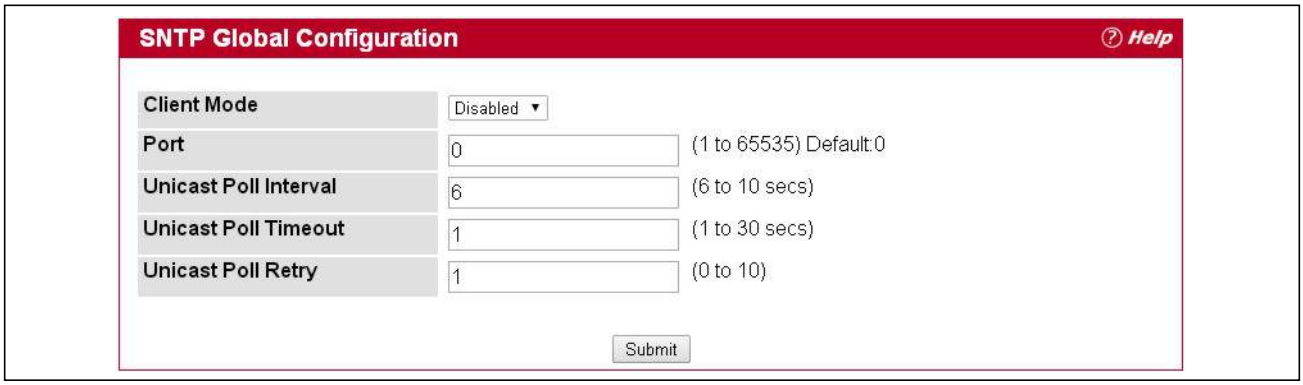


Figure 54: SNTP Global Configuration

Table 47: SNTP Global Configuration Fields

Field	*Description*
Client Mode	Use drop-down list specify the SNTP client mode, which is one of the following modes: • **Disabled**: SNTP is not operational. No SNTP requests are sent from the client nor are any received SNTP messages processed. • **Unicast**: SNTP operates in a point to point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally the round-trip delay and local clock offset relative to the server.
Port	Specifies the local UDP port to listen for responses/broadcasts. Allowed range is 1 to 65535. Default value is 123.
Unicast Poll Interval	Specifies the number of seconds between unicast poll requests expressed as a power of two when configured in unicast mode. Allowed range is 6 to 10. Default value is 6.
Unicast Poll Timeout	Specifies the number of seconds to wait for an SNTP response when configured in unicast mode. Allowed range is 1 to 30. Default value is 5.

Table 47: SNTP Global Configuration Fields (Cont.)

Field	*Description*
Unicast Poll Retry	Specifies the number of times to retry a request to an SNTP server after the first time-out before attempting to use the next configured server when configured in unicast mode. Allowed range is 0 to 10. Default value is 1.

If you change any of the settings on the page, click **Submit** to apply the changes to system.

SNTP Global Status

Use the SNTP Global Status page to view information about the system's SNTP client.

To access the SNTP Global Status page, click **System > SNTP > Global Status** in the navigation menu.

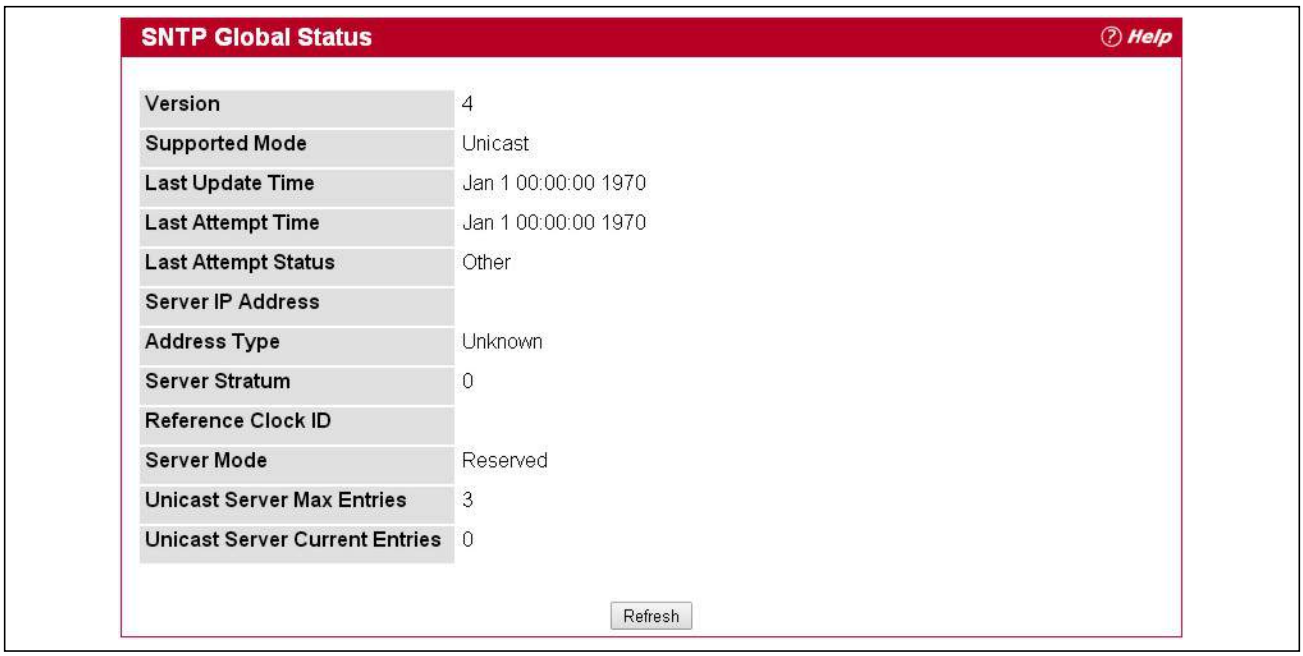


Figure 55: SNTP Global Status

Table 48: SNTP Global Status Fields

Field	*Description*
Version	Specifies the SNTP Version the client supports.
Supported Mode	Specifies the SNTP modes the client supports. Multiple modes may be supported by a client.
Last Update Time	Specifies the local date and time (UTC) the SNTP client last updated the system clock.
Last Attempt Time	Specifies the local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.

Table 48: SNTP Global Status Fields (Cont.)

Field	*Description*
Last Attempt Status	Specifies the status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message has been received from a server, a status of Other is displayed. These values are appropriate for all operational modes: • **Other**: None of the following enumeration values. • **Success**: The SNTP operation was successful and the system time was updated. • **Request Timed Out**: A directed SNTP request timed out without receiving a response from the SNTP server. • **Bad Date Encoded**: The time provided by the SNTP server is not valid. • **Version Not Supported**: The SNTP version supported by the server is not compatible with the version supported by the client. • **Server Unsynchronized**: The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message. • **Server Kiss Of Death**: The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.
Server IP Address	Specifies the IP address of the server for the last received valid packet. If no message has been received from any server, an empty string is shown.
Address Type	Specifies the address type of the SNTP Server address for the last received valid packet.
Server Stratum	Specifies the claimed stratum of the server for the last received valid packet.
Reference Clock ID	Specifies the reference clock identifier of the server for the last received valid packet.
Server Mode	Specifies the mode of the server for the last received valid packet.
Unicast Sever Max Entries	Specifies the maximum number of unicast server entries that can be configured on this client.
Unicast Server Current Entries	Specifies the number of current valid unicast server entries configured for this client.

Click **Refresh** to display the latest information from the router.

SNTP Server Configuration

Use the SNTP Server Configuration page to view and modify information for adding and modifying Simple Network Time Protocol SNTP servers.

To display the SNTP Server Configuration page, click **System > SNTP > Server Configuration** in the navigation tree.

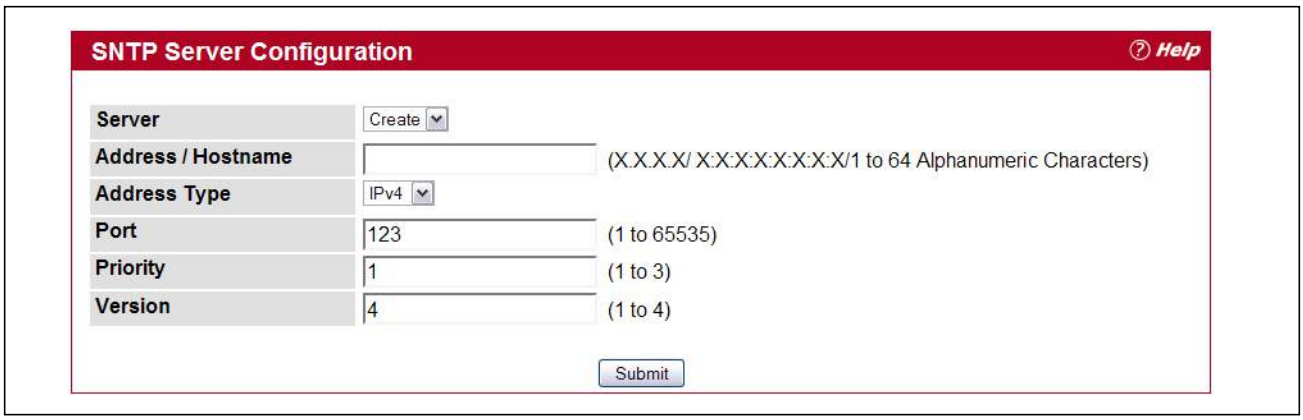


Figure 56: SNTP Server Configuration

Table 49: SNTP Server Configuration Fields

Field	*Description*
Server	Select the IP address of a user-defined SNTP server to view or modify information about an SNTP server, or select **Create** to configure a new SNTP server. You can define up to three SNTP servers.
Address / Hostname	Enter the IP address or the host name of the SNTP server.
Address Type	Select **IPv4** if you entered an IPv4 address or **DNS** if you entered a host name.
Port	Enter a port number from 1 to 65535. The default is 123.
Priority	Enter a priority from 1 to 3, with 1 being the highest priority. The router will attempt to use the highest priority server and, if it is not available, will use the next highest server.
Version	Enter the protocol version number.
Priority	Specifies the priority of this server entry in determining the sequence of servers to which SNTP requests are sent. Values are 1 to 3, and the default is 1. Servers with lowest numbers have priority.

- To add an SNTP server, select Create from the **Server** list, complete the remaining fields as desired, and click **Submit**. The SNTP server is added, and is now reflected in the Server list. You must perform a save to retain your changes over a power cycle.
- To remove an SNTP server, select the IP address of the server to remove it from the **Server** list, and then click **Delete**. The entry is removed, and the device is updated.

SNTP Server Status

The SNTP Server Status page displays status information about the SNTP servers configured on your switch.

To access the SNTP Server Status page, click **System > SNTP > Server Status** in the navigation menu.

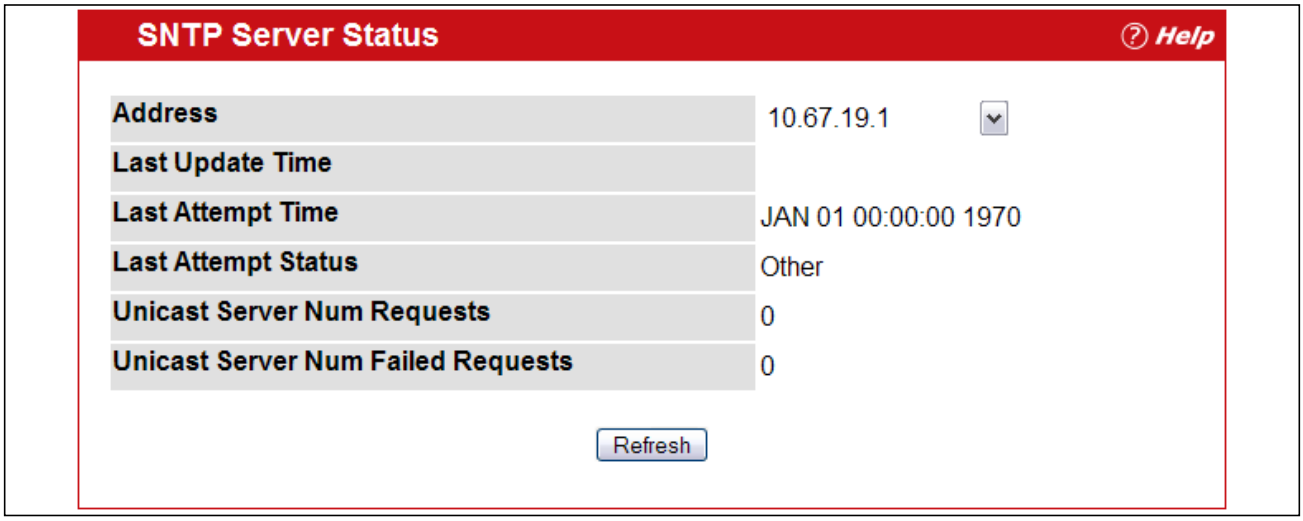


Figure 57: SNTP Server Status

Table 50: SNTP Server Status Fields

Field	*Description*
Address	Specifies all the existing Server Addresses. If no Server configuration exists, a message saying “No SNTP server exists” flashes on the screen.
Last Update Time	Specifies the local date and time (UTC) that the response from this server was used to update the system clock.
Last Attempt Time	Specifies the local date and time (UTC) that this SNTP server was last queried.
Last Attempt Status	Specifies the status of the last SNTP request to this server. If no packet has been received from this server, a status of Other is displayed: • **Other**: None of the following enumeration values. • **Success**: The SNTP operation was successful and the system time was updated. • **Request Timed Out**: A directed SNTP request timed out without receiving a response from the SNTP server. • **Bad Date Encoded**: The time provided by the SNTP server is not valid. • **Version Not Supported**: The SNTP version supported by the server is not compatible with the version supported by the client. • **Server Unsynchronized**: The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message. • **Server Kiss Of Death**: The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.
Unicast Server Num Requests	Specifies the number of SNTP requests made to this server since last agent reboot.

Table 50: SNTP Server Status Fields (Cont.)

Field	*Description*
Unicast Server Num Failed Requests	Specifies the number of failed SNTP requests made to this server since last reboot.

Click **Refresh** to display the latest information from the router.

Section 3: Configuring Switching Information

Managing VLANs

Adding Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security and management of multicast traffic.

A VLAN is a set of end stations and the switch ports that connect them. You may have many reasons for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support one default VLAN ID.

The VLAN folder contains links to the following features:

- VLAN Configuration
- VLAN Status
- VLAN Port Configuration
- VLAN Port Summary
- Reset VLAN Configuration

VLAN Configuration

Use the VLAN Configuration page to define VLAN groups stored in the VLAN membership table. Your switch supports up to 3965 VLANs. VLAN 1 is the default VLAN of which all ports are members.

To display the VLAN Configuration page, click **Switching > VLAN > Configuration** in the navigation tree. (Note that six ports are shown to cover both the EWS4502 and EWS4606 switches.)

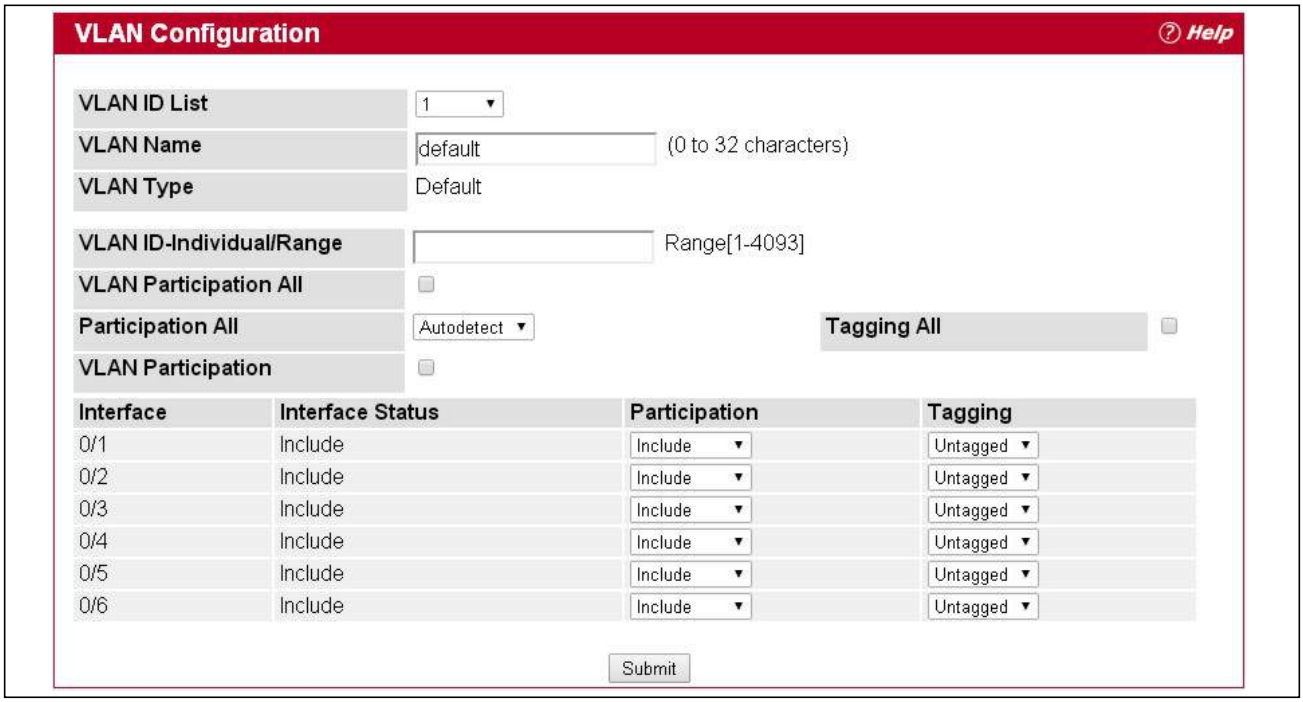


Figure 58: VLAN Configuration

Table 51: VLAN Configuration Fields

Field	*Description*
VLAN ID List	You can use this screen to create a new VLAN or delete or reconfigure an existing VLAN. Use this pull-down menu to select one of the existing VLANs, or select **Create** to add a new one.
VLAN ID - Individual/Range	When Create is select from the VLAN ID List, specify the VLAN Identifier for the new VLAN. You can also enter a range of VLAN IDs. For example, 3-5, 101 creates VLANs 3, 4, 5, and 101. This field is configurable only when you are creating a new VLAN.
VLAN Name	Use this optional field to specify a name for the VLAN. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 is always named “Default.”
VLAN Type	This field identifies the type of the VLAN you are configuring. You cannot change the type of the default VLAN (VLAN ID = 1): it is always type “Default.” When you create a VLAN, using this screen, its type will always be “Static.” A VLAN that is created by GVRP registration initially has a type of “Dynamic.” You can use this pull-down menu to change its type to “Static.”

Table 51: VLAN Configuration Fields (Cont.)

Field	*Description*
VLAN Participation All	Use this field to specify VLAN to participate on all the interfaces. By default, the field is disabled. Set the checkbox to enable the field.
Participation All	Use this field to specify whether a port will participate in this VLAN. The factory default is "Autodetect." The possible values are: • **Include**: This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • **Exclude**: This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • **Autodetect**: Specifies that port may be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless it receives a GVRP request. This is equivalent to registration normal in the IEEE 802.1Q standard.
VLAN Participation	Use this field to specify VLAN to participate. By default, the field is disabled. Set the checkbox to enable the field.
Tagging All	Sets the tagging behavior for all the ports in this VLAN. The factory default is "Untagged." The possible values are: • **Tagged**: all frames transmitted for this VLAN will be tagged. • **Untagged**: all frames transmitted for this VLAN will be untagged.
Interface	Indicates which port is associated with the fields on this line.
Interface Status	Indicates the current value of the participation parameter for the port.
Participation	• This field has the same definition as that of **Partition All**, except that it applies to individual ports.
Tagging	Select the tagging behavior for this port in this VLAN. The factory default is "Untagged." The possible values are: • **Tagged**: all frames transmitted for this VLAN will be tagged. • **Untagged**: all frames transmitted for this VLAN will be untagged.

If you make any changes to the page, click **Submit** to apply the changes to the system. To delete a VLAN, select the VLAN from the **VLAN ID and Name** field, and click **Delete**. You cannot delete the default VLAN.

VLAN Status

Use the VLAN Status page to view information about the VLANs configured on your system.

To access the VLAN Status page, click **Switching > VLAN > Status** in the navigation tree.

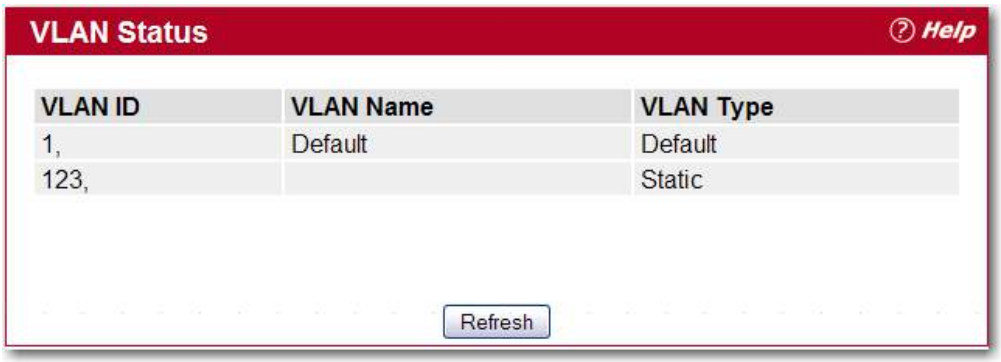


Figure 59: VLAN Status

Table 52: VLAN Status Fields

Field	*Description*
VLAN ID	The VLAN Identifier (VID) of the VLAN. The range of the VLAN ID is 1 to 3965.
VLAN Name	The name of the VLAN. VLAN ID 1 is always named Default.
VLAN Type	The VLAN type, which can be one of the following: • **Default**: (VLAN ID = 1) -- always present • **Static**: A VLAN you have configured • **Dynamic**: A VLAN created by GVRP registration that you have not converted to static, and that GVRP may therefore be removed

Click **Refresh** to display the latest information from the router.

VLAN Port Configuration

Use the VLAN Port Configuration page to configure a virtual LAN on a port.

To access the VLAN Port Configuration page, click **Switching > VLAN > Port Configuration** in the navigation tree.

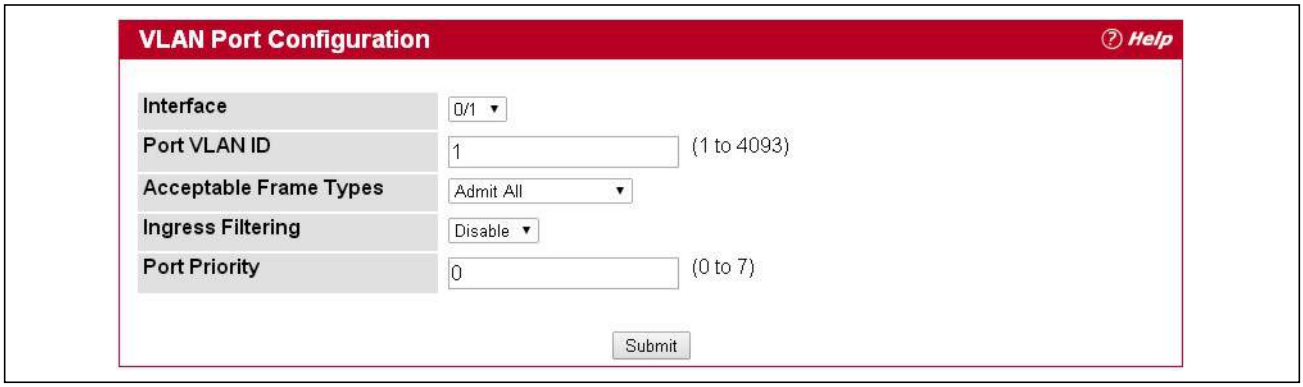


Figure 60: VLAN Port Configuration

Table 53: VLAN Port Configuration Fields

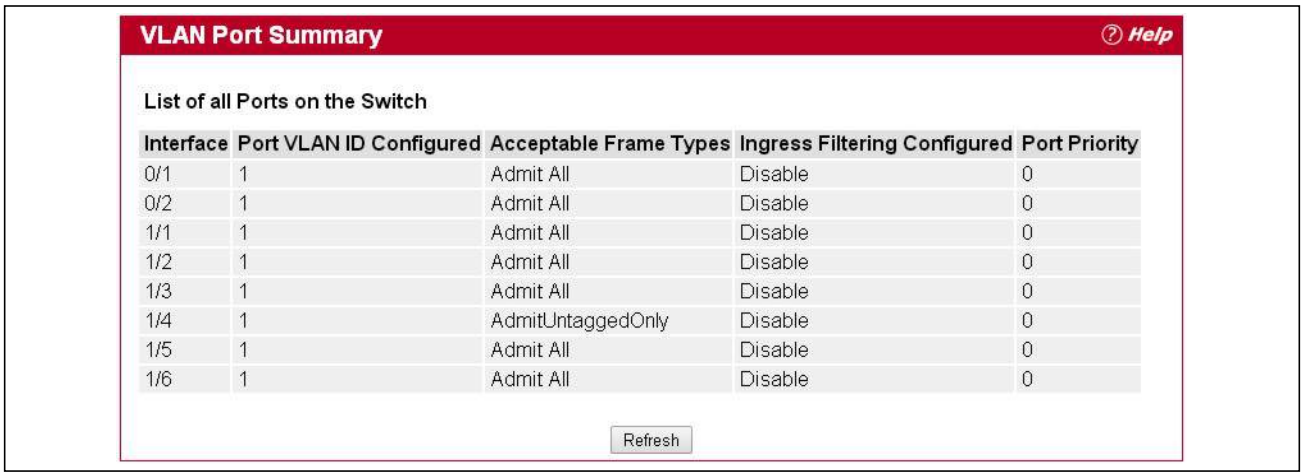
Field	*Description*
Interface	Select the interface for which you want to display or configure data. Select **All** to set the parameters for all ports to same values.
Port VLAN ID	Specify the VLAN ID you want assigned to untagged or priority tagged frames received on this port. The factory default is 1.
Acceptable Frame Types	Specify how you want the port to handle untagged and priority tagged frames. Whichever you select, VLAN tagged frames will be forwarded in accordance with the IEEE 802.1Q VLAN standard. The factory default is Admit All. • **Admit All**: Untagged and priority tagged frames received on the port will be accepted and assigned the value of the Port VLAN ID for this port. • **AdmitTaggedOnly**: The port will discard any untagged or priority tagged frames it receives. • **AdmitUntaggedOnly**: Only untagged frames received on the port are accepted.
Ingress Filtering	Specify how you want the port to handle tagged frames: • **Enable**: A tagged frame will be discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. • **Disable**: All tagged frames will be accepted. The factory default is disable.
Port Priority	Specify the default 802.1p priority assigned to untagged packets arriving at the port. The value ranges from 0 to 7. The default value is 0.

If you change any information on the page, click **Submit** to apply the changes to the system.

VLAN Port Summary

Use the VLAN Port Summary page to view VLAN configuration information for all the ports on the system.

To access the VLAN Port Summary page, click **Switching > VLAN > Port Summary** in the navigation menu.



Interface	Port VLAN ID Configured	Acceptable Frame Types	Ingress Filtering Configured	Port Priority
0/1	1	Admit All	Disable	0
0/2	1	Admit All	Disable	0
1/1	1	Admit All	Disable	0
1/2	1	Admit All	Disable	0
1/3	1	Admit All	Disable	0
1/4	1	AdmitUntaggedOnly	Disable	0
1/5	1	Admit All	Disable	0
1/6	1	Admit All	Disable	0

Figure 61: VLAN Port Summary

Table 54: VLAN Port Summary Fields

Field	*Description*
Interface	Identifies the physical interface associated with the rest of the data in the row.
Port VLAN ID Configured	Identifies the VLAN ID assigned to untagged or priority-tagged frames received on this port. The factory default is 1.
Acceptable Frame Types	Shows how the port handles untagged and priority tagged frames. • **Admit All**: Untagged and priority tagged frames received on the port are accepted and assigned the value of the Port VLAN ID for this port. • **AdmitTaggedOnly**: The port discards any untagged or priority tagged frames it receives. • **AdmitUntaggedOnly**: Only untagged frames received on the port are accepted.
Ingress Filtering Configured	Shows how the port handles tagged frames. • **Enable**: A tagged frame is discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. • **Disable**: All tagged frames are accepted, which is the factory default.
Port Priority	Identifies the default 802.1p priority assigned to untagged packets arriving at the port.

Click **Refresh** to reload the page and view the most current information.

Reset VLAN Configuration

Use the Reset VLAN Configuration page to return all VLAN parameters for all interfaces to the factory default values.

To access the Reset VLAN Configuration page, click **Switching > VLAN > Reset Configuration** in the navigation tree.

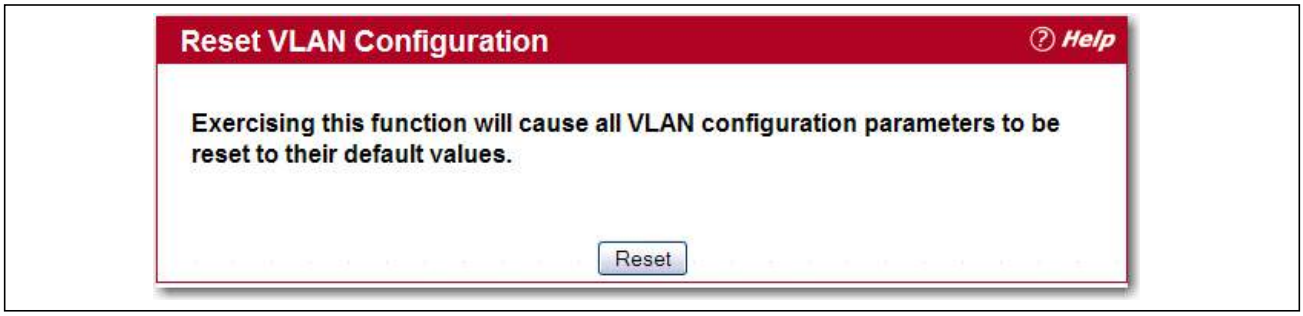


Figure 62: Reset VLAN Configuration

When you click **Reset**, the screen refreshes, and you are asked to confirm the reset. Click **Reset** again to restore all default VLAN settings for the ports on the system.

GARP Configuration

Use this page to set the administrative mode for the features that use the Generic Attribute Registration Protocol (GARP), including GARP VLAN Registration Protocol (GVRP). GARP is a general-purpose protocol that registers any network connectivity or membership-style information. GARP defines a set of switches interested in a given network attribute, such as VLAN ID or multicast address.

The GARP folder contains links to the following features:

- GARP Status
- GARP Switch Configuration
- GARP Port Configuration

GARP Status

Use the GARP Status page to display the global and port-based settings for GVRP, and the port-based settings for the GVRP timers.

To access the GARP Status page, click **Switching** > **GARP** > **Status** in the navigation tree.

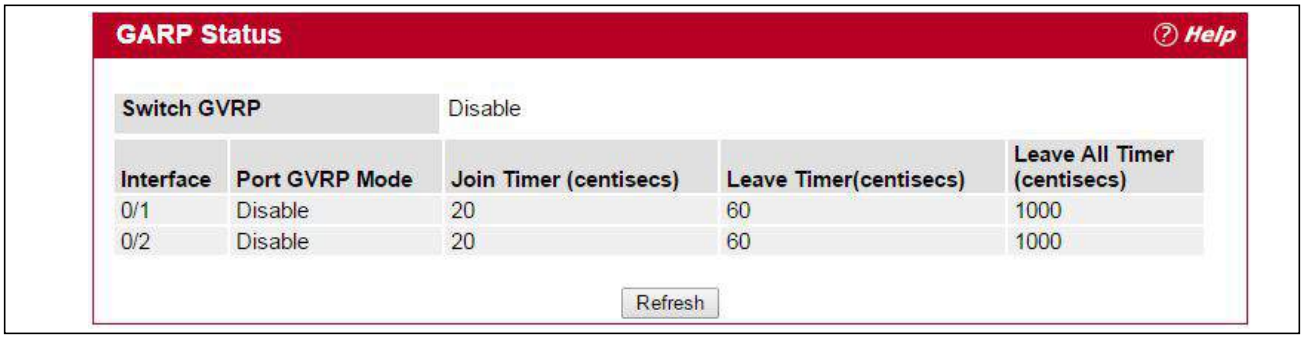


Figure 63: GARP Status

Click **Refresh** to update the page with the most current information.

GARP Switch Configuration

To access the GARP Switch Configuration page, click **Switching** > **GARP** > **Switch** in the navigation menu.

Figure 64: GARP Switch Configuration

Table 55: GARP Switch Configuration Fields

Field	*Description*
GVRP Mode	The administrative mode of GVRP on the system. When enabled, GVRP can help dynamically manage VLAN membership on trunk ports.

Click **Refresh** to update the page with the most current information.

GARP Port Configuration

Use this page to set the per-interface administrative mode for GARP VLAN Registration Protocol (GVRP). On this page you can also set the GARP timers for each interface. GVRP uses the same set of GARP timers to specify the amount of time to wait before transmitting various GARP messages.

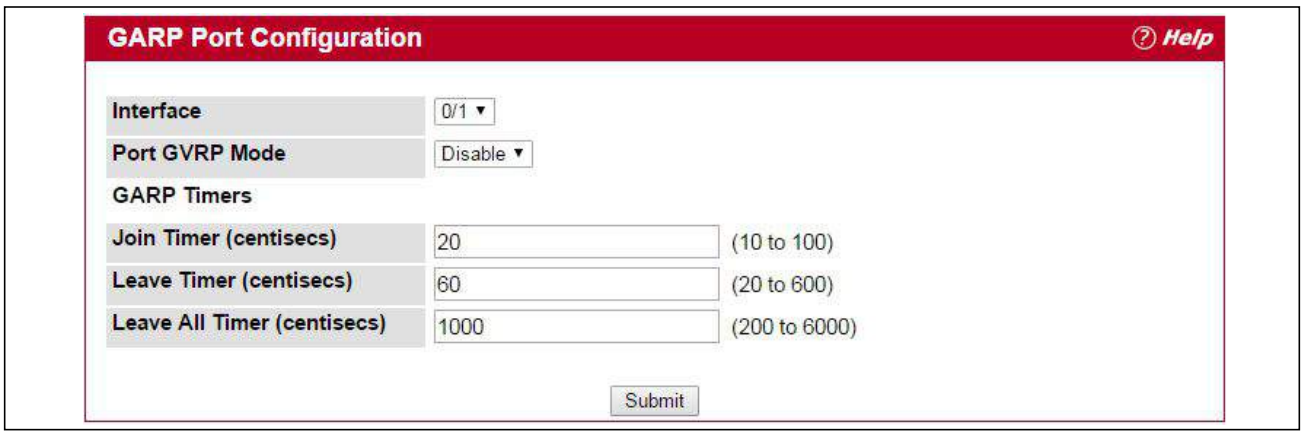


Figure 65: GARP Port Configuration

To change the GARP settings for an interface, select the interface to configure and edit the required fields.

Table 56: GARP Port Configuration Fields

Field	*Description*
Interface	The interface associated with the rest of the data in the row.
Port GVRP Mode	The administrative mode of GVRP on the interface. When enabled, GVRP can help dynamically manage VLAN memberships on the trunk ports. GVRP must also be enabled globally for the protocol to be active on the interface. When disabled, the protocol will not be active on the interface, and the GARP timers have no effect.
Join Timer (Centisecs)	The amount of time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group.
Leave Timer (Centisecs)	The amount of time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry. The timer allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service.

Table 56: GARP Port Configuration Fields (Cont.)

Field	*Description*
Leave All Timer r (Centisecs)	The amount of time to wait before sending a LeaveAll PDU after the GARP application has been enabled on the interface or the last LeaveAll PDU was sent. A LeaveAll PDU indicates that all registrations will shortly be derigistered. Participants will need to rejoin in order to maintain membership

Click **Refresh** to refresh the page with the most current data from the switch.

Creating Port Channels

Port-channels, which are also known as link aggregation groups (LAGs), allow you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. You assign the port-channel (LAG) VLAN membership after you create a port-channel. The port channel by default becomes a member of the management VLAN.

A port-channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols. A static port-channel interface does not require a partner system to be able to aggregate its member ports.

Note: If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

Static LAGs are supported. When a port is added to a LAG as a static member, it neither transmits nor receives LACPDUs.

Port Channel Configuration

Use the Port Channel Configuration page to group one or more full duplex Ethernet links to be aggregated together to form a port-channel, which is also known as a link aggregation group (LAG). The switch treats the port-channel as if it were a single link.

To access the Port Channel Configuration page, click **Switching > Port Channel > Configuration** in the navigation tree.

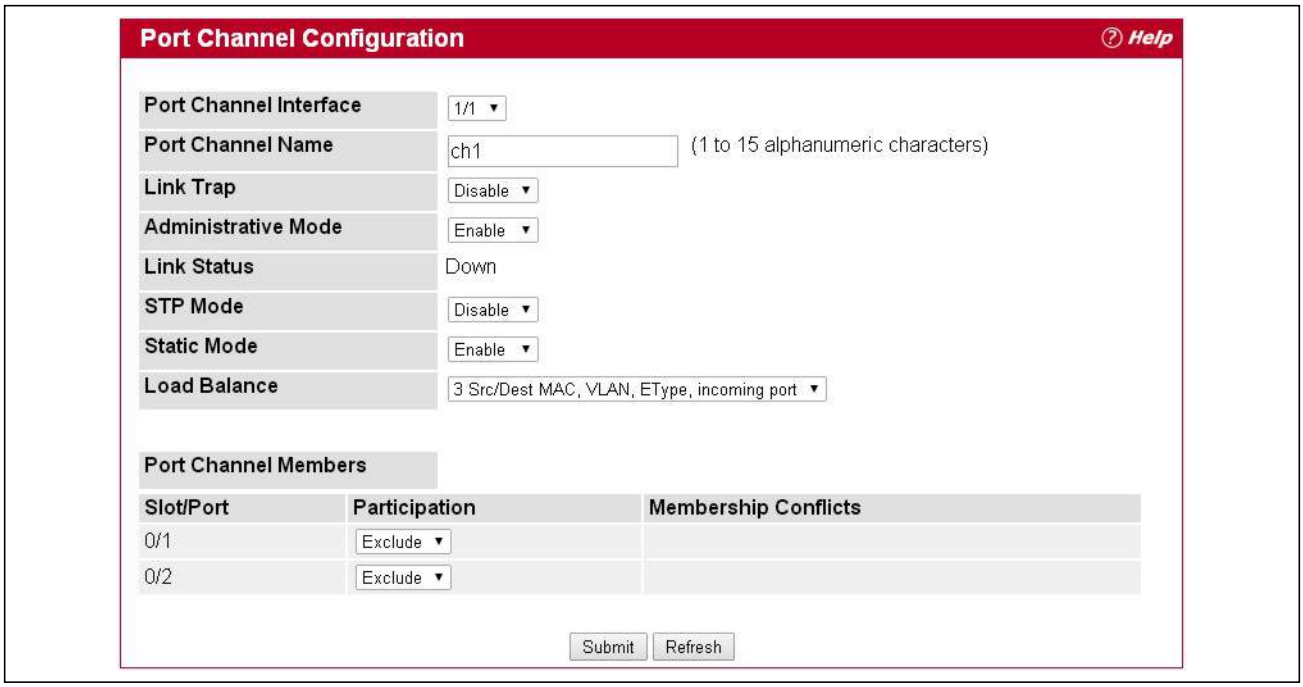


Figure 66: Port Channel Configuration

Table 57: Port Channel Configuration Fields

Field	*Description*
Port Channel Interface	Select the port channel to configure. The port channel follows a Slot/Port (or Unit/Slot/Port for stacking platforms) interface naming convention, where the slot is 3.
Port Channel Name	Enter the name you want assigned to the Port Channel. You may enter any string of up to 15 alphanumeric characters. You must specify a valid name in order to create the Port Channel.
Link Trap	Specify whether you want to have a trap sent when link status changes. The factory default is enable, which will cause the trap to be sent.
Administrative Mode	Select enable or disable from the pull-down menu. When the Port Channel is disabled no traffic will flow and LACPDUs will be dropped, but the links that form the Port Channel will not be released. The factory default is enable.
Link Status	Indicates whether the link is Up or Down.
STP Mode	Select the Spanning Tree Protocol (STP) Administrative Mode associated with the Port Channel: • **Disable**: Spanning tree is disabled for this Port Channel. • **Enable**: Spanning tree is enabled for this Port Channel.
Static Mode	Select enable or disable from the pull-down menu. The factory default is Disable. • **Enable**: The port channel is statically maintained, which means it does not transmit or process received LAGPDUs. The member ports do not transmit LAGPDUs and all the LAGPDUs it may receive are dropped. A static port-channel interface does not require a partner system to be able to aggregate its member ports. • **Disable**: The port channel is dynamically maintained. The interface transmits and processes LAGPDUs and requires a partner system
Load Balance	Select the hashing algorithm used to distribute the traffic load among available physical ports in the LAG. The range of possible values may vary with the type of switch. The possible values are: • Source MAC, VLAN, EtherType, and source port • Destination MAC, VLAN, EtherType and source port • Source/Destination MAC, VLAN, EtherType, and source port • Source IP and Source TCP/UDP Port • Destination IP and Destination TCP/UDP Port • Source/Destination IP and source/destination TCP/UDP Port • Enhanced hashing mode
Port Channel Members	After you create one or more port channels, this field lists the members of the Port Channel in Slot/Port form. If there are no port channels on the system, this field is not present.
Slot/Port	This column lists the physical ports available on the system.
Participation	Select each port's membership status for the Port Channel you are configuring. There can be a maximum of 8 ports assigned to a Port Channel. • **Include**: The port participates in the port channel. • **Exclude**: The port does not participate in the port channel, which is the default.

Table 57: Port Channel Configuration Fields (Cont.)

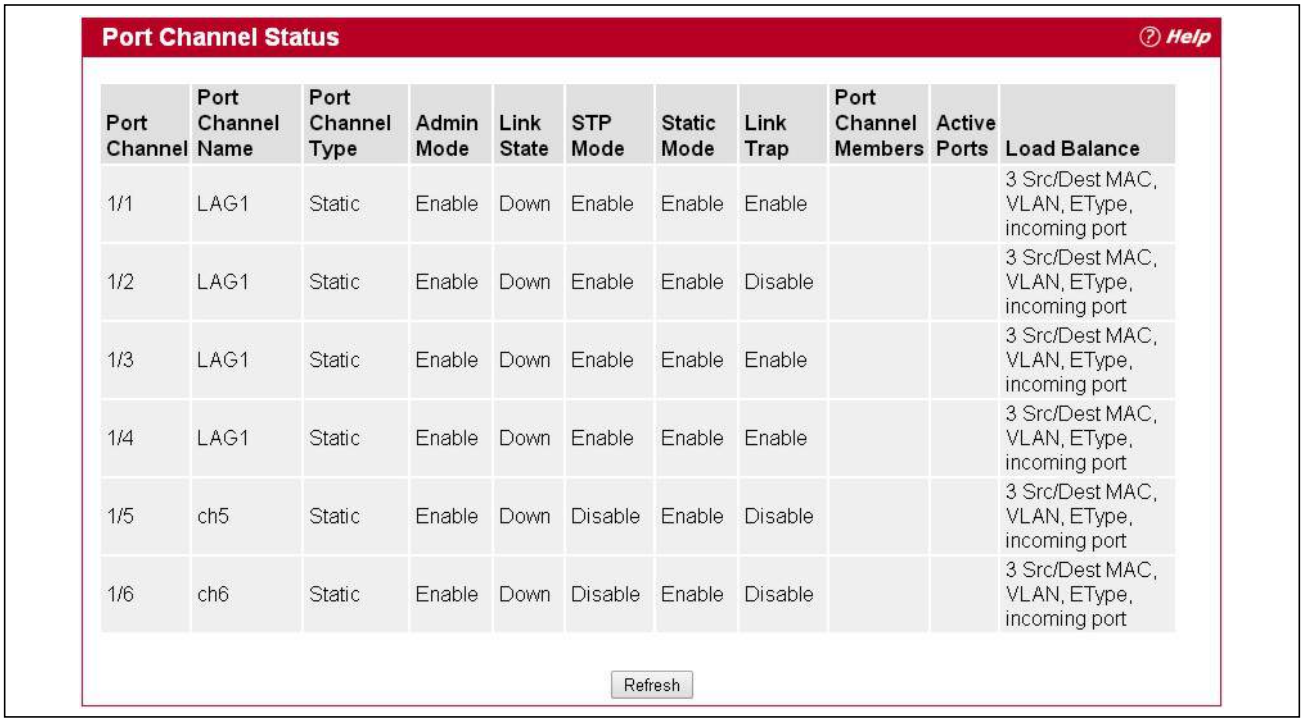
Field	*Description*
Membership Conflicts	Shows ports that are already members of other Port Channels. A port may only be a member of one Port Channel at a time. If the entry is blank, the port is not currently a member of any Port Channel

- If you make any changes to this page, click **Submit** to apply the changes to the system.
- To remove a port channel, select it from the **Port Channel Name** drop-down menu and click delete. All ports that were members of this Port Channel are removed from the Port Channel and included in the default VLAN. This field will not appear when a new Port Channel is being created.

Port Channel Status

Use the Port Channel Status page to group one or more full duplex Ethernet links to be aggregated together to form a port-channel, which is also known as a link aggregation group (LAG). The switch can treat the port-channel as if it were a single link.

To access the Port Channel Status page, click **Switching > Port Channel > Status** in the navigation tree.



Port Channel Status

Help

Port Channel	Port Channel Name	Port Channel Type	Admin Mode	Link State	STP Mode	Static Mode	Link Trap	Port Channel Members	Active Ports	Load Balance
1/1	LAG1	Static	Enable	Down	Enable	Enable	Enable			3 Src/Dest MAC, VLAN, EType, incoming port
1/2	LAG1	Static	Enable	Down	Enable	Enable	Disable			3 Src/Dest MAC, VLAN, EType, incoming port
1/3	LAG1	Static	Enable	Down	Enable	Enable	Enable			3 Src/Dest MAC, VLAN, EType, incoming port
1/4	LAG1	Static	Enable	Down	Enable	Enable	Enable			3 Src/Dest MAC, VLAN, EType, incoming port
1/5	ch5	Static	Enable	Down	Disable	Enable	Disable			3 Src/Dest MAC, VLAN, EType, incoming port
1/6	ch6	Static	Enable	Down	Disable	Enable	Disable			3 Src/Dest MAC, VLAN, EType, incoming port

Refresh

Figure 67: Port Channel Status

Table 58: Port Channel Status Fields

Field	*Description*
Port Channel	Identifies the port channel with the Slot/Port (or Unit/Slot/Port for stacking platforms) interface naming convention.

Table 58: Port Channel Status Fields (Cont.)

Field	*Description*
Port Channel Name	Identifies the user-configured text name of the port channel.
Port Channel Type	The type of this Port Channel, which is one of the following: • **Static**: The port channel is statically maintained. • **Dynamic**: The port channel is dynamically maintained.
Admin Mode	Select enable or disable from the pull-down menu. When the Port Channel is disabled no traffic will flow and LACPDUs will be dropped, but the links that form the Port Channel will not be released. The factory default is enable.
Link State	Indicates whether the link is Up or Down.
STP Mode	Shows whether the Spanning Tree Protocol (STP) Administrative Mode is enabled or disabled on the port channel
Static Mode	Shows whether static mode is enabled for this port channel.
Link Trap	Shows whether to send traps when link status changes. If the status is Enabled, traps are sent.
Port Channel Members	Lists the ports that are members of the Port Channel, in Slot/Port notation (Unit/Slot/Port for stackable systems). There can be a maximum of 8 ports assigned to a Port Channel.
Active Ports	Lists the ports that are actively participating members of this Port Channel, in Slot/Port notation (Unit/Slot/Port for stackable systems).
Load Balance	Shows the hashing algorithm used to distribute the traffic load among available physical ports in the LAG. The range of possible values may vary with the type of switch. The possible values are: • 1 Source MAC, VLAN, EtherType, and incoming port • 2 Destination MAC, VLAN, EtherType and incoming port • 3 Source/Destination MAC, VLAN, EtherType, and incoming port • 4 Source IP and Source TCP/UDP Port incoming • 5 Destination IP and Destination TCP/UDP Port incoming • 6 Source/Destination IP and source/destination TCP/UDP Port fields

Section 4: Managing Device Security

Use the features in the Security folder on the navigation tree menu to set management security parameters for port, user, and server security. The Security folder contains links to the following features:

- Captive Portal Configuration
- RADIUS Settings
- TACACS+ Settings
- Secure HTTP
- Secure Shell

Captive Portal Configuration

The Captive Portal (CP) feature allows you to block wired and wireless clients from accessing the network until user verification has been established. You can configure CP verification to allow access for both guest and authenticated users. Authenticated users must be validated against a database of authorized Captive Portal users before access is granted. The database can be stored locally on the switch or on a RADIUS server.

The Captive Portal folder contains links to the following pages that help you view and configure system Captive Portal settings:

- Captive Portal Global Configuration
- CP Configuration
- Local User Summary
- Interface Association
- CP Status
- Interface Status
- Client Connection Status
- SNMP Trap Configuration

Captive Portal Global Configuration

From the CP **Global Configuration** page, you can control the administrative state of the CP feature and configure global settings that affect all captive portals configured on the switch.

To configure the global CP settings, click **Security > Captive Portal > Global Configuration**.

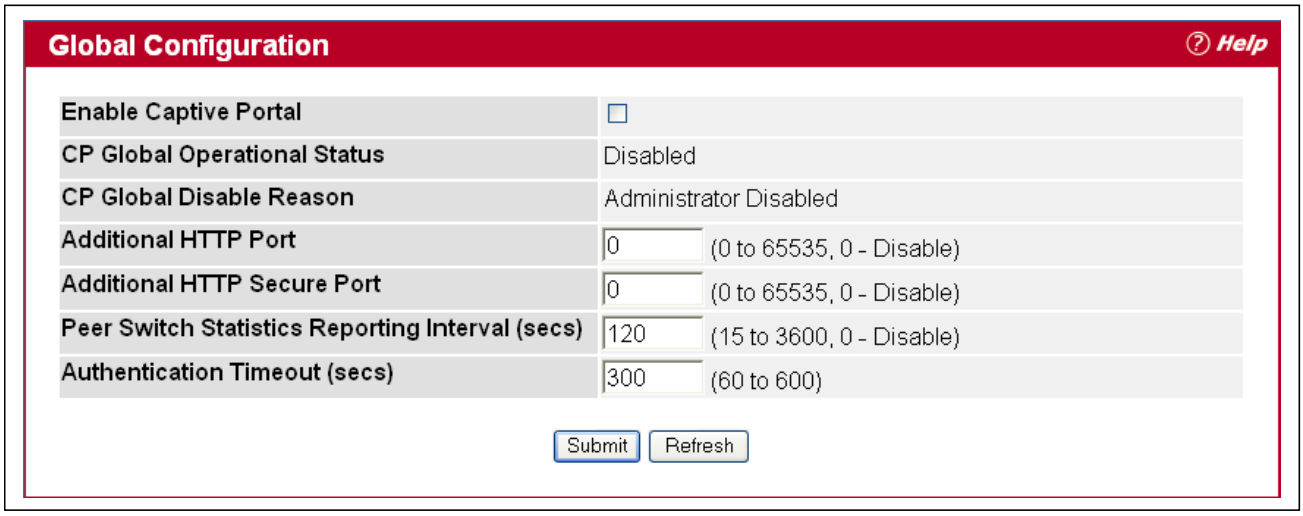


Figure 68: Global Captive Portal Configuration

The following table describes the global CP fields you can view or configure.

Table 59: Global Captive Portal Configuration

Field	*Description*
Enable Captive Portal	Select the check box to enable the CP feature on the switch. Clear the check box to disable the captive portal feature.
CP Global Operational Status	Shows whether the CP feature is enabled.
CP Global Disable Reason	If CP is disabled, this field displays the reason, which can be one of the following: • None • Administratively Disabled • No IPv4 Address
Additional HTTP Port	HTTP traffic uses port 80, but you can configure an additional port for HTTP traffic. Enter a port number between 0-65535 (excluding ports 80, 443, and the configured switch management port).
Additional HTTP Secure Port	HTTP traffic over SSL (HTTPS) uses port 443, but you can configure an additional port for HTTPS traffic. Enter a port number between 0-65535 (excluding ports 80, 443, and the configured switch management port).
Peer Switch Statistics Reporting Interval	When clustering is supported on the switch, enter a value to determine how often the switch sends its authenticated client statistics to the Cluster Controller. The interval is in seconds. Enter a value of 0 to prevent the switch from reporting the statistics.
Authentication Timeout	To access the network through a portal, the client must first enter authentication information on an authentication Web page. Enter the number of seconds to keep the authentication session open with the client. When the timeout expires, the switch disconnects any active TCP or SSL connection with the client.
SMS Provider	Short Message Service (SMS) is a text messaging service component of phone, Web, or mobile communication systems. It uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages. SMS gateway providers facilitate SMS traffic between businesses and mobile subscribers, including SMS for enterprises, content delivery, and entertainment services.
SMS Account	The SMS account name. Range (1-128 alphanumeric characters)
SMS Password	The SMS password. Range (1-128 alphanumeric characters)

CP Configuration

From the CP Configuration page, you can view summary information about captive portals on the system, add a captive portal, and configure existing captive portals.

Use the **CP Summary** page to create or delete captive portal configurations. The switch supports 10 CP configurations. CP configuration 1 is created by default and can not be deleted. Each captive portal configuration can have unique guest or group access modes and a customized acceptance use policy that displays when the client connects.

To view summary information about existing captive portals, or to add or delete a captive portal, click **Security > Captive Portal > CP Summary**.

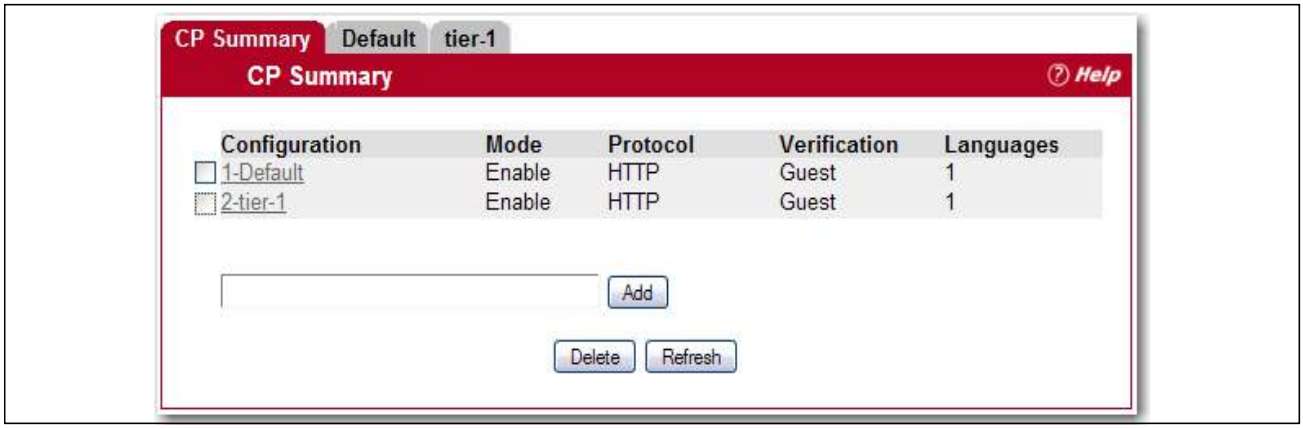


Figure 69: Captive Portal Summary

To create a CP configuration, enter the configuration name in the text box and click **Add**. After you add the configuration, the CP Configuration page for that configuration displays, and a new tab with the name of that configuration appears.

To delete an existing CP, select the check box for the CP to remove, and then click **Delete**.

To configure the settings for an existing CP, click the name in the Configuration column or click the appropriate tab.

Table 60 describes the fields on the **CP Summary** page.

Table 60: Captive Portal Summary

Field	*Description*
Configuration	Shows the captive portal ID and name. To access the configuration page for an exiting CP, click the configuration name.
Mode	Shows whether the CP is enabled.
Protocol	Indicates whether the portal uses HTTP or HTTPS.
Verification	Specifies which type of user verification to perform: • **Guest**: The user does not need to be authenticated by a database. • **Local**: The switch uses a local database to authenticated users. • **RADIUS**: The switch uses a database on a remote RADIUS server to authenticate users. • **Self-Service Local**: Tool designed to add or edit local business listings. To configure authorized users on the local or remote RADIUS database, see "Local User Summary" on page 144.
Languages	Shows the number of languages that are configured for this captive portal.

Changing the Captive Portal Settings

By default, the switch has one captive portal. You can change the settings for that captive portal, and you can also create and configure up to nine additional portals. After you create a captive portal from the **CP Summary** page, you can change its settings.

To view information about existing captive portals, or to add or delete a captive portal, click **Security > Captive Portal > CP Summary**. Then click the tab for a configured portal.

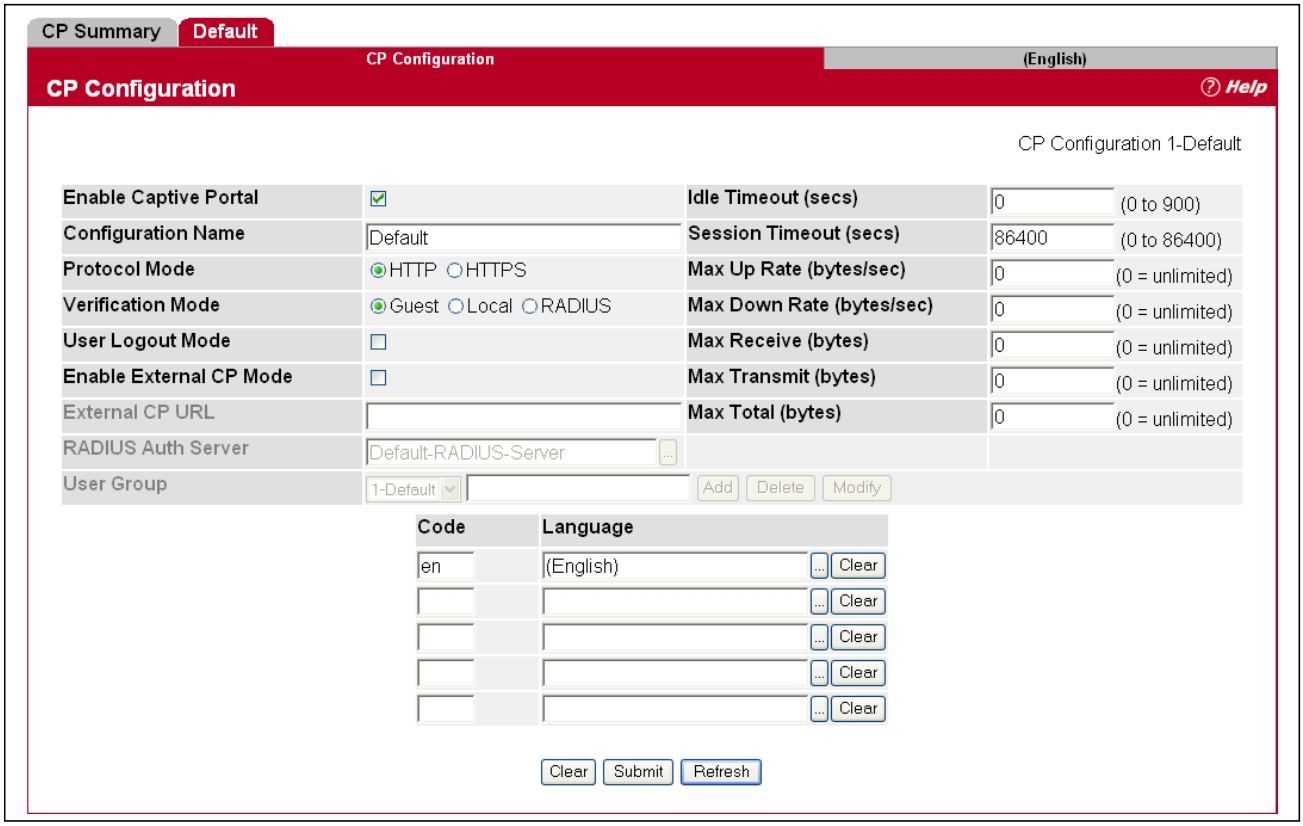


Figure 70: Captive Portal Configuration

Table 61 describes the fields on the **CP Configuration** page.

Table 61: CP Configuration

Field	*Description*
Enable Captive Portal	Select the check box to enable the CP. Clear the check box to disable it.
Configuration Name	This field allows you to change the name of the portal added from the **CP Summary** page.
Protocol Mode	Choose whether to use HTTP or HTTPs as the protocol for the portal to use during the verification process. • **HTTP:** Does not use encryption during verification • **HTTPS**: Uses the Secure Sockets Layer (SSL), which requires a certificate to provide encryption. The certificate is presented to the user at connection time.

Table 61: CP Configuration (Cont.)

Field	*Description*
Verification Mode	Select the mode for the CP to use to verify clients: • **Guest**: The user does not need to be authenticated by a database. • **Local**: The switch uses a local database to authenticated users. • **RADIUS**: The switch uses a database on a remote RADIUS server to authenticate users. • **Self-Service Local**: Tool designed to add or edit local business listings.
User Logout Mode	Select this option to allow an authenticated client to deauthenticate from the network. If this option is clear or the user does not specifically request logout, the client connection status remains authenticated until the CP deauthenticates the user, for example by reaching the idle timeout or session timeout values.
Enable Redirect Mode	Select this option to specify that the CP should redirect the newly authenticated client to the configured URL. If this option is clear, the user sees the locale-specific welcome page after a successful verification.
Redirect URL	Specify the URL to which the newly authenticated client is redirected if Enable Redirect Mode is enabled. This field is only displayed if the Enable Redirect Mode is enabled.
Notification Method	This field is displayed when the Verification Method is set to Self-Service Local. The notification options include: • **Displayed Directly**: The notification method is displayed on the connected device. • **SMS**: The notification method uses Short Message Service (SMS) text messaging.
External Login URL	Allows users to log into your site using their existing credentials from other applications such as Facebook, Twitter, and Google.
Allowed White List	A list of people considered to be acceptable or trustworthy. When a white list is specified, no other people can access the captive portal.
RADIUS Auth Server	If the verification mode is RADIUS, click the **...** button and select the name of the RADIUS server used for client authentications. The switch acts as the RADIUS client and performs all RADIUS transactions on behalf of the clients. To configure RADIUS server information, go to **Security > RADIUS > Server Configuration**.
User Group	If the Verification Mode is Local or RADIUS, assign an existing User Group to the captive portal or create a new group. All users who belong to the group are permitted to access the network through this portal. The User Group list is the same for all CP configurations on the switch. The User Group field also allows you to add, delete, or rename user groups for all captive portals. • To assign an existing user group to the CP, select it from the drop-down menu. • To create a new user group, enter the group name in the blank field and click **Add**. • To change the name of an existing user group, select the name to change from the drop-down menu, enter the new name in the blank field, and click **Modify**. • To delete a user group, select it from the drop-down menu and click **Delete**. **Note:** The User Group fields are unavailable if the Verification Mode is Guest.
Idle Timeout	Enter the number of seconds a user can remain idle before automatically being logged out. If the value is set to 0, the timeout is not enforced. The default value is 0.
Session Timeout	Enter the number of seconds to wait before terminating a session. A user is logged out once the session timeout is reached. If the value is set to 0, the timeout is not enforced. The default value is 86400 (24 hours).

Table 61: CP Configuration (Cont.)

Field	*Description*
Max Up Rate	Enter the maximum speed, in bytes per second, that a client can transmit traffic when using the captive portal. This setting limits the bandwidth at which the client can send data into the network.
Max Down Rate	Enter the maximum speed, in bytes per second, that a client can receive traffic when using the captive portal. This setting limits the bandwidth at which the client can receive data from the network.
Max Receive	Enter the maximum number of bytes that a client is allowed to receive when using the captive portal. After this limit has been reached the user will be disconnected.
Max Transmit	Enter the maximum number of bytes that a client is allowed to transmit when using the captive portal. After this limit has been reached the user will be disconnected.
Max Total	Enter the maximum number of bytes the user is allowed to transfer (sum of bytes transmitted and received). After this limit has been reached the user will be disconnected.
Age Timeout	Shows the number of seconds a user is permitted to remain connected to the network. Once the Age Timeout is reached, the user is logged out automatically. This field is only enabled if the verification mode is set to Self-Service Local. ***Note:*** When the Age Timeout is set to a value of 0, the timeout is not enforced.
Code	Enter the IANA Language Subtag code for the language. All codes are listed in the IANA Language Subtag Registry. If the language is currently supported by the switch, the code is filled in automatically when you select the language.
Language	To add a captive portal configuration in a language that is supported by the switch, click the **...** button to display and select the language to use for the captive portal.

Customizing the Captive Portal Web Page

When a client connects to the access point, the user sees a Web page. Open the tab for a specific language (such as **English**) to access the **CP Web Customization** page. The CP Web Customization page allows you to customize the appearance of that page with specific text and images.

You can create up to five location-specific web pages for each captive portal as long as the pages all use the same verification type; either guest or authorized user web pages. This allows you to create pages in a variety of languages to accommodate a diverse group of users.

To configure the portal users in a remote RADIUS server, see “Configuring Users in a Remote RADIUS Server” on page 145.

To customize the page that wireless clients see when they access the captive portal, on the **CP Configuration** page first click the **English** tab. Click **Security** > **Captive Portal** > **Global Configuration**, and then select Global Parameters from the drop-down list. The **CP WEB Customization** (Global Parameters) page will appear.

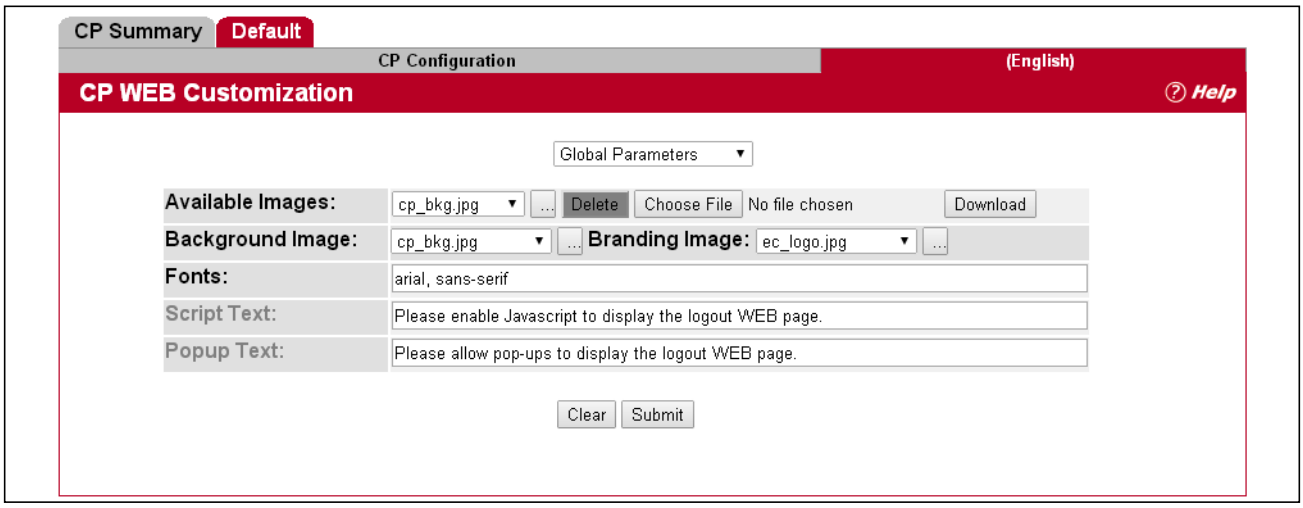


Figure 71: CP Web Customization

The **CP Web Page Customization** page defaults to the **Global Parameters** page. It provides access to the five pages that allow CP web customization:

- Global Parameters Page
- Authentication Page
- Welcome Page
- Logout Page
- Logout Success Page

Table 62 describes the fields on the **CP Web Page Customization** > **Global Parameters** page.

Table 62: CP Web Customization > Global Parameters Page Fields

Field	*Description*
Available Images	The menu shows the images that are available to use for the page branding and the account image. To add images, click **Browse** and select an image on your local system (or accessible from your local system). Click **Download** to download the image to the switch. The image should be 5KB max, 200x200 pixels, GIF or JPG format. To delete an image from the list, select the file name from the menu and click **Delete**. You can only delete images that you download.
Background Image	Select the name of the image to display as the page background. Use the drop-down menu to display the file names of the available images. Click the ... button to display the available images. Click the image to select it. To specify that no background image is to be used, select <No Selection>.
Branding Image	Select the name of the image file to display on the top left corner of the page. This image is used for branding purposes, such as the company logo.
Fonts	Enter the name of the font to use for all text on the CP page.

Table 62: CP Web Customization > Global Parameters Page (Cont.)Fields

Field	*Description*
Script Text	Specify the text to indicate that users must enable JavaScript to display the logout WEB page. This field is only applicable when the User Logout Mode is enabled, but you can modify the text whether the feature is enabled or disabled.
Popup Text	Specify the text to indicate that users must allow pop-up windows to display the logout WEB page. This field is only applicable when the User Logout Mode is enabled, but you can modify the text whether the feature is enabled or disabled.

CP Web Page Customization > Authentication Page

To customize the page that wireless clients see when they access the captive portal authentication page, on the **CP Configuration** page first click the **English** tab. **Security** > **Captive Portal** > **Global Configuration**, and then select Authentication Page from the drop-down list. The **CP WEB Customization** (Authentication Page) page will appear.

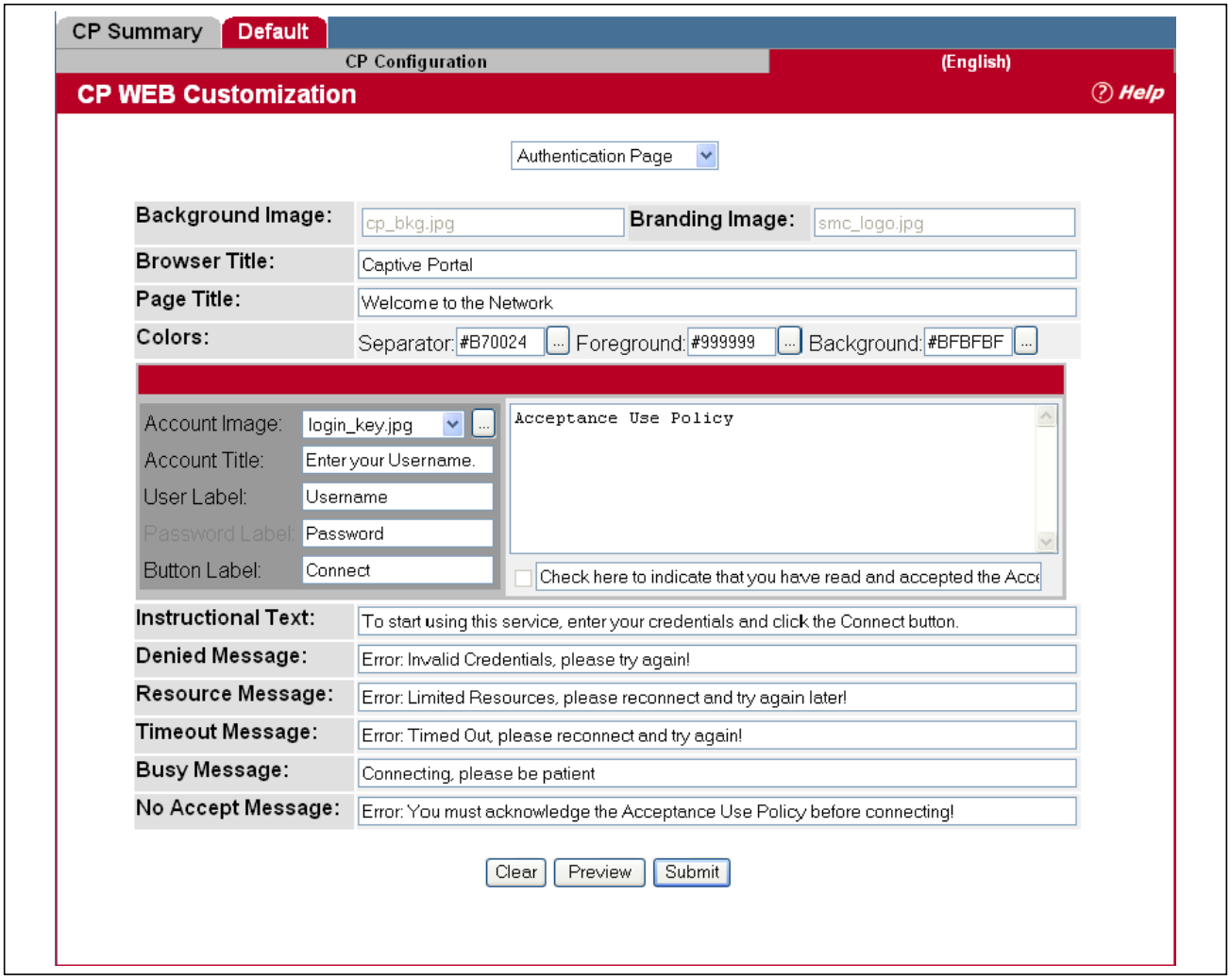


Figure 72: CP Web Customization > Authentication Page

Table 63 describes the fields on the **CP Web Page Customization** > **Authentication** page.

Table 63: CP Web Customization > Authentication Page Fields

Field	*Description*
Background Image	Shows the name of the current background image on the Authentication Page. This field can be modified from the CP WEB Customization (Authentication Page) page.
Branding Image	Shows the name of the current branding image on the (Authentication Page). This field can be modified from the CP WEB Customization (Authentication Page) page.
Browser Title	Enter the text to display on the client's Web browser title bar or tab.
Page Title	Enter the text to use as the page title. This is the text that identifies the page.
Colors	Select the colors to use for the CP page. Click the **...** button, and then select the color to use. The sample account information is updated with the colors you choose.
Account Image	Select the image that will display on the Captive Portal page above the login field. The image display area is 55H X 310W pixels. ***Note:*** Your image will be resized to fit the display area. To download a new image, use the Available Images field.
Account Title	Enter the summary text to display that instructs users to authenticate.
User Label	Enter the text to display next to the field where the user enters the user name.
Password Label	Enter the text to display next to the field where the user enters the password.
Button Label	Enter the text to display on the button the user clicks to connect to the network.
Acceptance Use Policy Text Box	Enter the text to display in the Acceptance Use Policy field. The acceptance use policy instructs users about the conditions under which they are allowed to access the network. The policy can contain up to 8192 text characters.
Acceptance Check Box Prompt	Enter the text to display next to the box that the user must select to indicate that he or she accepts the terms of use.
Instructional Text	Enter the detailed text to display that instructs users to authenticate. This text appears under the button.
Denied Message	Enter the text to display when the user does not provide valid authentication information. This message displays after the user clicks the button to connect to the network.
Resource Message	Enter the text to display when the system has rejected authentication due to system resource limitations. This message displays after the user clicks the button to connect to the network.
Timeout Message	Enter the text to display when the system has rejected authentication because the authentication transaction took too long. This could be due to user input time, or a timeout due to the overall transaction.
Busy Message	Enter the text to display when the user does not provide valid authentication information. This message displays after the user clicks the button to connect to the network.
No Accept Message	Enter the text to display when the user did not accept the acceptance use policy. This message displays after the user clicks the button to connect to the network.

CP Web Customization > Welcome Page

To customize the page that wireless clients see when they access the captive portal, on the **CP Configuration** page first click the **English** tab. The **CP WEB Customization** (Welcome Page) page will appear.

To customize the page that wireless clients see when they access the captive portal welcome page, on the **CP Configuration** page first click the **English** tab. **Security** > **Captive Portal** > **Global Configuration**, and then select Welcome Page from the drop-down list. The **CP WEB Customization** (Welcome Page) page will appear.

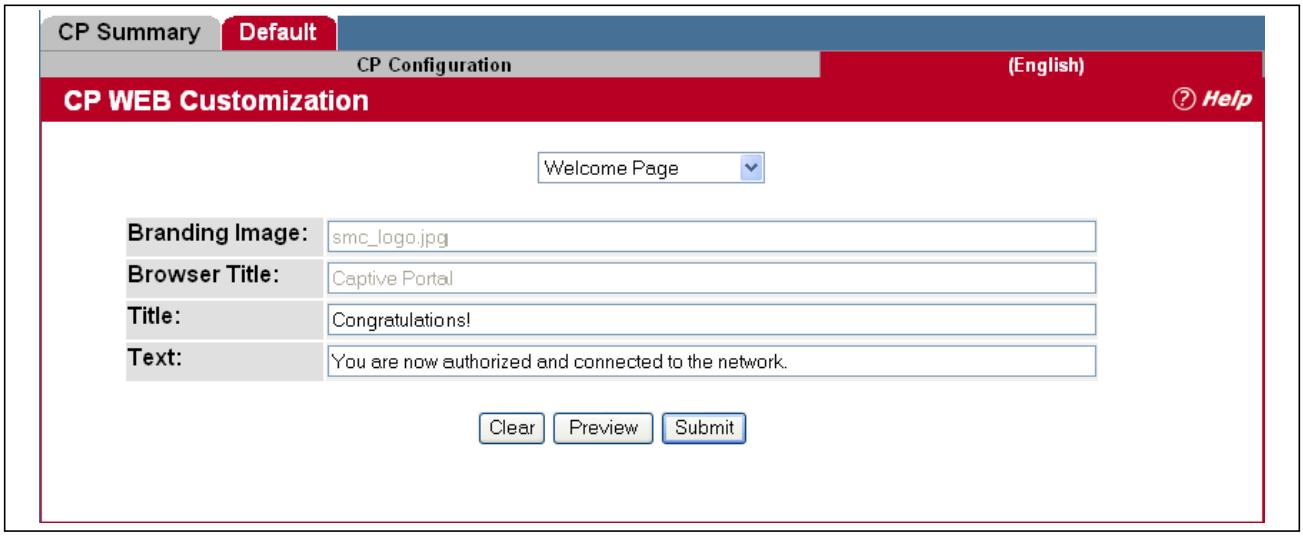


Figure 73: CP Web Customization > Welcome Page

Table 62 describes the fields on the **CP Web Customization** > **Welcome** page.

Table 64: CP Web Customization > Welcome Page Fields

Field	*Description*
Branding Image	Shows the name of the current branding image on the Welcome Page. This field can be modified from the CP WEB Customization (Welcome Page).
Browser Title	Enter the text to display on the client's Web browser title bar or tab.
Title	Enter the title to display to greet the user after he or she successfully connects to the network.
Text	Enter the optional text to display to further identify the network to be access by the CP user. This message displays under the Welcome Title.

CP Web Page Customization > Logout Page

To customize the page that wireless clients see when they logout from the captive portal, on the **CP Configuration** page first click the **English** tab. **Security** > **Captive Portal** > **Global Configuration**, and then select Logout Page from the drop-down list. The **CP WEB Customization** (Logout Page) page will appear.

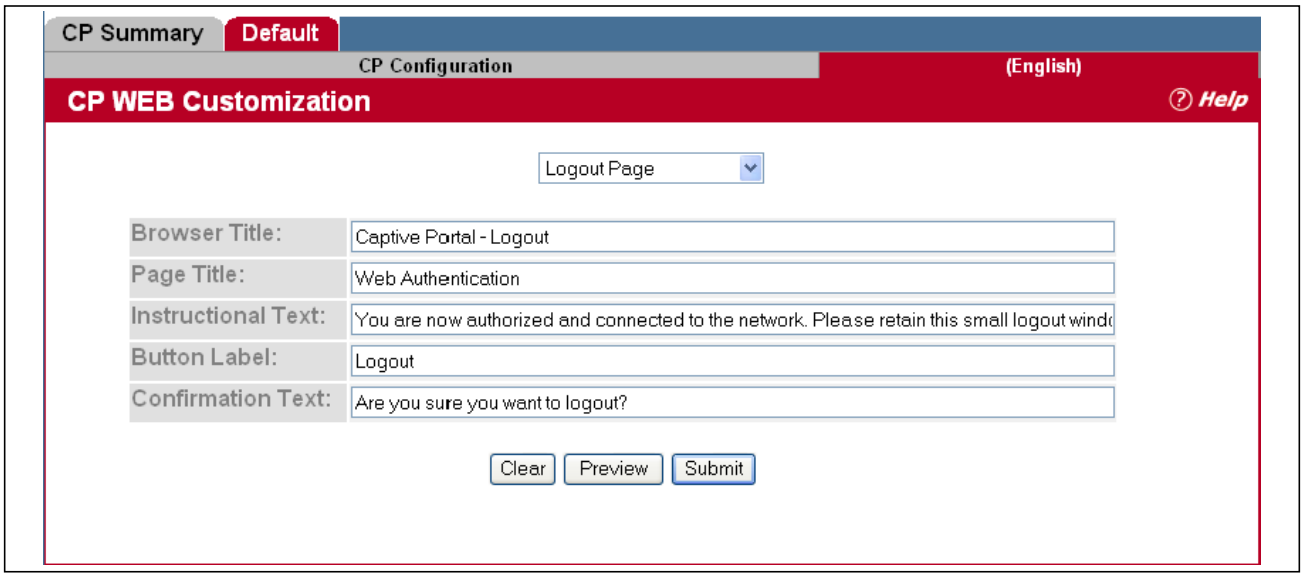


Figure 74: CP Web Customization > Logout Page

Table 62 describes the fields on the **CP Web Page Customization** > **Logout** page.

Table 65: CP Web Customization > Logout Page Fields

Field	*Description*
Note: The fields on this page are only applicable when the User Logout Mode is enabled; you can modify the fields whether the feature is enabled or disabled.	
Browser Title	Enter the text to display on the title bar of the Logout page.
Page Title	Enter the text to use as the page title. This is the text that identifies the page.
Instructional Text	Enter the detailed text to display that confirms that the user has been authenticated and instructs the user how to deauthenticate.
Button Label	Enter the text to display on the button the user clicks to deauthenticate.
Confirmation Text	Enter the detailed text to display that prompts users to confirm the deauthentication process.

CP Web Page Customization > Logout Success Page

To customize the page that wireless clients see when they successfully logout from the captive portal, on the **CP Configuration** page first click the **English** tab. **Security** > **Captive Portal** > **Global Configuration**, and then select Logout Success from the drop-down list. The **CP WEB Customization** (Logout Success) page will appear.

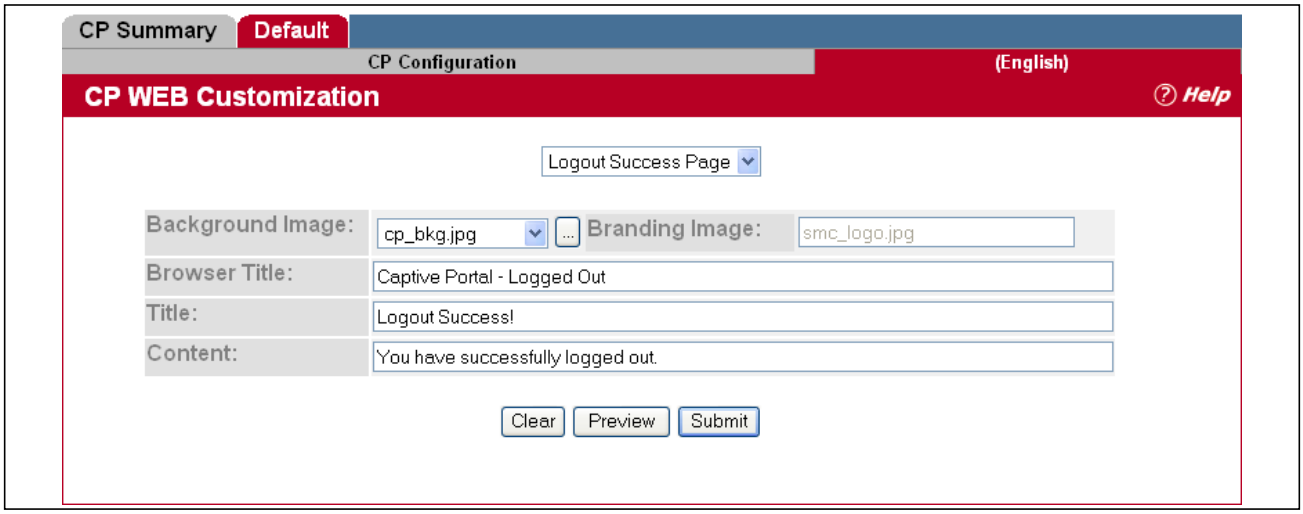


Figure 75: CP Web Page Customization > Logout Success Page

Table 62 describes the fields on the **CP Web Page Customization** > **Logout Success** page.

Table 66: CP Web Customization > Logout Success Page Fields

Field	*Description*
Background Image	Shows the name of the current background image on the Logout Success page. This field can be modified from the CP WEB Customization (Logout Success Page) page.
Branding Image	Shows the name of the current branding image on the Logout Success page. This field can be modified from the CP WEB Customization (Logout Success Page) page.
Browser Title	Enter the text to display on the title bar of the Logout Success page.
Title	Enter the text to use as the page title. This is the text that identifies the page.
Content	Enter the text to display that confirms that the user has been deauthenticated.

Local User Summary

You can configure a portal to accommodate guest users and authorized users. Guest users do not have assigned user names and passwords. Authorized users provide a valid user name and password that must first be validated against a local database or RADIUS server. Authorized users can gain network access once the switch confirms the user's credentials.

The **Local User Summary** page allows you to add authorized users to the local database, which can contain up to 1024 user entries. You can also delete users from the local database from the **Local User Summary** page.

To view and configure CP users in the local database, click **Security > Captive Portal > Local User**.

Any users that are already configured are listed on the **Local User Summary** page. To display existing users or add new users to the local user database for captive portals, click **Security** > **Captive Portal** > **Local User Summary**.

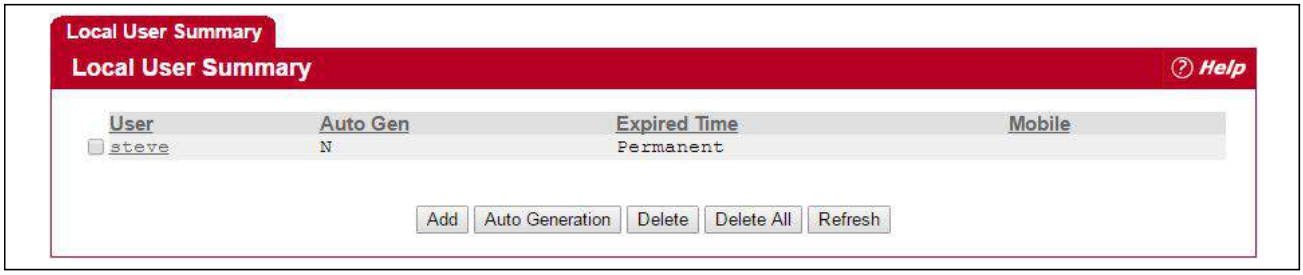


Figure 76: Captive Portal Local User Summary

Table 67 describes the fields on the **Local User Summary** page.

Table 67: Local User Summary Fields

Field	*Description*
User	Identifies the name of the user.
Auto Gen	Identifies if the account is generated by "Auto generator", "Y" for yes and "N" for no.
Age Timeout	Shows the number of seconds a user is permitted to remain connected to the network. Once the Session Timeout value is reached, the user is logged out automatically. This value is only used for an "Auto Gen" account. ***Note:*** A value of 0 signifies that the Session Timeout in the global configuration is used (no local user Session Timeout is specified). When the global configuration for Session Timeout is set to a value of 0, the timeout is not enforced.
Expired Time	Shows the number of seconds a user has been connected to the network.
Mobile	A one day account feature is supported for Captive Portal which allows users to self-register their account. The AC will automatically add that self-registered account to the local user database. The mobile number is one of the fields (optional) to be filled when doing the self-registration. If the user fills in his/her own mobile phone number, the AC will show this information on the local user database.

To access the configuration page for a specific user listed on the page, click the user name.

The following buttons are available at the bottom of the Local User table:

- **Add**: Click **Add** to add a new user to the Local User database.
- **Auto Generation**: Click **Auto Generation** to add a new user to the Local User database using auto generator.

- **Delete:** Select the check box next to the user to remove and click **Delete**. Select multiple check boxes to delete more than one user at a time.
- **Delete All**: Click **Delete All** to remove all configured users from the local database.
- **Refresh**: Click **Refresh** to update the page with the most current information.

Adding a Local User

When you click **Add** from the Local User Summary page, the screen refreshes, and you can add a new user to the Local User database. To configure additional parameters for the new user, return to the Local User Summary page and click the name of the new user. The captive portal Global Status page displays the maximum number of users the Local User database supports.

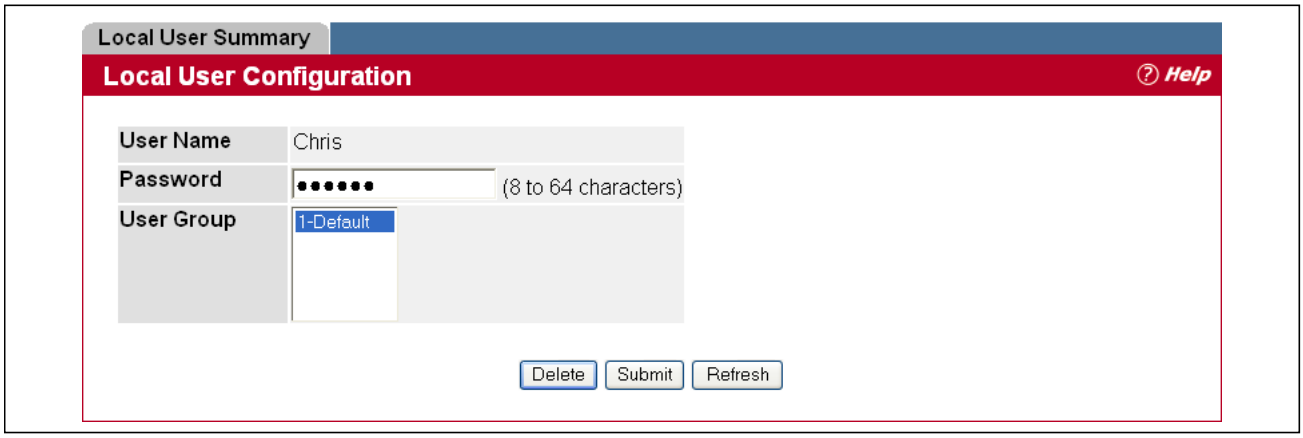


Figure 77: Adding a New User

The following table describes the fields available when you add a new user to the local CP database. After you complete the fields, click **Add** to add the user and return to the Local User Summary page.

Table 68: Local User Configuration Fields

Field	*Description*
User Name	Enter the name of the user.
Password	Enter a password for the user. The password length can be from 8 to 64 characters.
User Group	Assign the user to at least one User Group. To assign a user to more than one group, press the Ctrl key and click each group. New users are assigned to the 1-Default user group by default.

Configuring Users in a Remote RADIUS Server

You can use a remote RADIUS server for client authorization if enabled in the **CP Configuration** page. You must add all users to the RADIUS server. The local database in the switch does not share any information with the remote RADIUS database.

Table 69 indicates the RADIUS attributes you use to configure authorized captive portal clients. The table indicates both RADIUS attributes and vendor-specific attributes (VSA). VSAs are denoted in the Attribute column and are comma delimited (vendor id, attribute id).

Note: For Radius Attributes that are set manually on the server (not set using the switch's user interface), a value of 0 signifies that the attribute value set on the **CP Configuration** page is used (no manually set RADIUS attribute value is specified).

Manually set RADIUS attribute values that are not specified are assumed to be 0.

Table 69: Captive Portal User RADIUS Attributes

Attribute	*Vendor ID*	*Attribute ID*	*Description*	*Range*	*Usage*	*Default*
User-Name	–	1	User name to be authorized	1-32 characters	Required	None
User-Password	–	2	User password	8-64 characters	Required	None
Session-Timeout	–	27	Logout once session timeout is reached (seconds). If the attribute is 0 or not present then use the value configured for the captive portal.	Integer (seconds)	Optional	0
Idle-Timeout	–	28	Logout once idle timeout is reached (seconds). If the attribute is 0 or not present then use the value configured for the captive portal.	Integer (seconds)	Optional	0
LVL7-Max-Input-Octets	6132	124	Maximum number of bytes that the user is allowed to receive when using the captive portal.	0-unlimited Integer bytes/sec	Optional	0
LVL7-Max-Output-Octets	6132	125	Maximum number of bytes that the user is allowed to transmit when using the captive portal.	0-unlimited Integer bytes/sec	Optional	0
LVL7-Max-Total-Octets	6132	126	Maximum number of bytes the user is allowed to transfer (sum of bytes transmitted and received).	0-unlimited Integer bytes	Optional	0
LVL7-Captive-Portal-Groups	6132	127	User Group(s) assigned to the user.	Comma delimited list	Optional	1-Default
WISPr-Bandwidth-Max-Up	14122	7	Maximum speed, in bytes per second, that the user can transmit traffic when using the captive portal.	0-unlimited Integer bytes/sec	Optional	0
WISPr-Bandwidth-Max-Down	14122	8	Maximum speed, in bytes per second, that the user can receive traffic when using the captive portal.	0-unlimited Integer bytes/sec	Optional	0

Interface Association

From the **Interface Association** page, you can associate a configured captive portal with a specific wired or wireless network (SSID). The CP feature only runs on the interfaces (or wireless networks) that you specify. A CP can have multiple interfaces associated with it, but an interface can be associated to only one CP at a time.

To associate interfaces with CPs, click **Security > Captive Portal > Interface Association**.

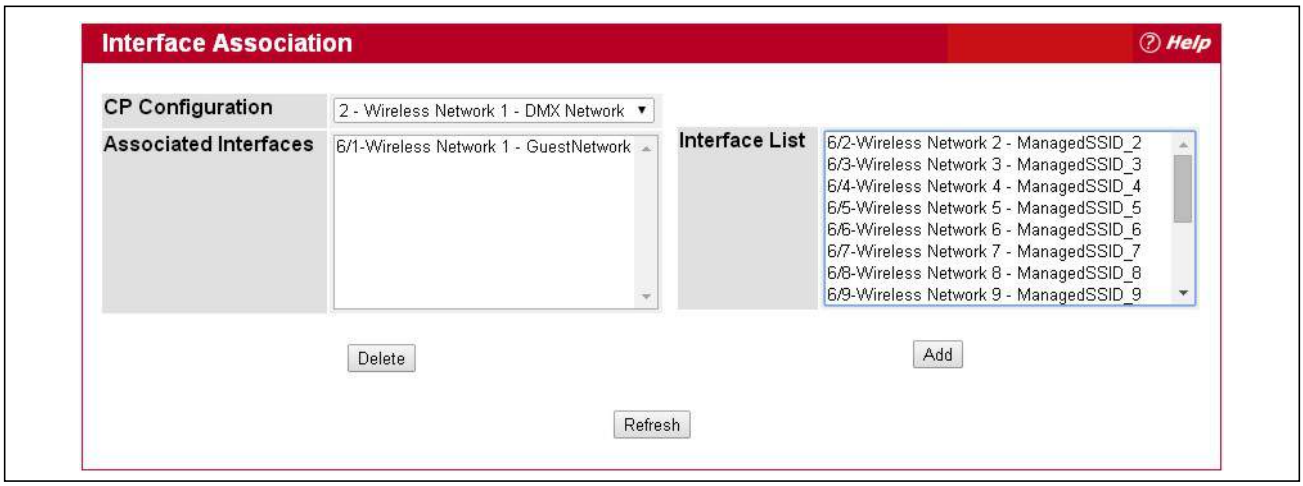


Figure 78: Interface Association

Table 70 describes the fields on the **Interface Association** page.

Table 70: Global Captive Portal Configuration Fields

Field	*Description*
CP Configuration	Lists the captive portals configured on the switch by number and name.
Associated Interfaces	Lists the wireless interfaces that are currently associated with the selected captive portal. The interface is identified by its wireless network number and SSID.
Interface List	Lists the wireless interfaces available on the switch that are not currently associated with a CP. Each interface is identified by its wireless network number and SSID.

Use the following steps to associate one or more interfaces with a captive portal.

1. Select the desired captive portal from the CP Configuration list.
2. Select the interface or interfaces from the Interface List. To select more than one interface, hold CTRL and click multiple interfaces.
3. Click **Add**.

Note: When you associate an interface with a captive portal, the interface is removed from the Interface List. Each interface can be associated with only one CP at a time.

Use the following steps to remove an interface from the Associated Interfaces list for a captive portal.

1. Select the desired captive portal from the CP Configuration list.

2. In the Associated Interfaces field, select the interface or interfaces to remove. To select more than one interface, hold CTRL and click multiple interfaces.
3. Click Delete.

   The interface is removed from the Associated Interface list and appears in the Interface List.

CP Status

The **CP Global Status** page contains a variety of information about the CP feature. From the **CP Global Status** page, you can access information about the CP activity and interfaces.

To view captive portal status information, click **Security > Captive Portal > CP Status**, and then click the CP Status tab.

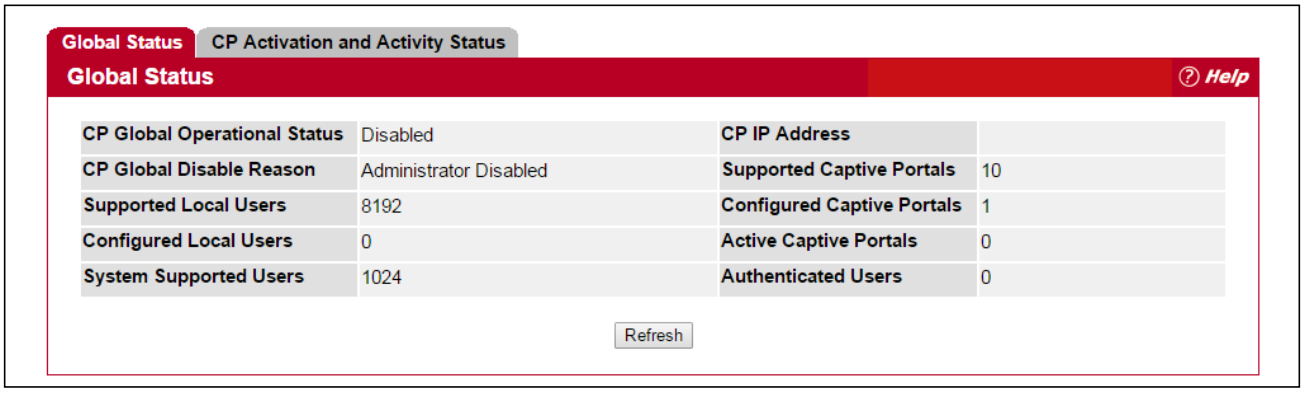


Figure 79: Global Captive Portal Status

Table 71 describes the fields displayed on the **CP Global Status** page.

Table 71: Global Captive Portal Status Fields

Field	*Description*
CP Global Operational Status	Shows whether the CP feature is enabled.
CP Global Disable Reason	Indicates the reason for the CP to be disabled, which can be one of the following: • None • Administratively Disabled • No IPv4 Address • Routing Enabled, but no IPv4 routing interface
Supported Local Users	Shows the number of entries that the Local User database supports.
Configured Local Users	Shows the number of configured local users.
System Supported Users	Shows the number of authenticated users that the system can support.
CP IP Address	Shows the captive portal IP address
Supported Captive Portals	Shows the number of supported captive portals in the system.
Configured Captive Portals	Shows the number of captive portals configured on the switch.
Active Captive Portals	Shows the number of captive portal instances that are operationally enabled.

Table 71: Global Captive Portal Status (Cont.)Fields

Field	*Description*
Authenticated Users	Shows the number of users currently authenticated to all captive portal instances on this switch.

CP Activation and Activity Status

The **CP Activation and Activity Status** page provides information about each CP configured on the switch.

To open this page, click **Security > Captive Portal > CP Status**, then click the CP Activation and Activity Status tab.

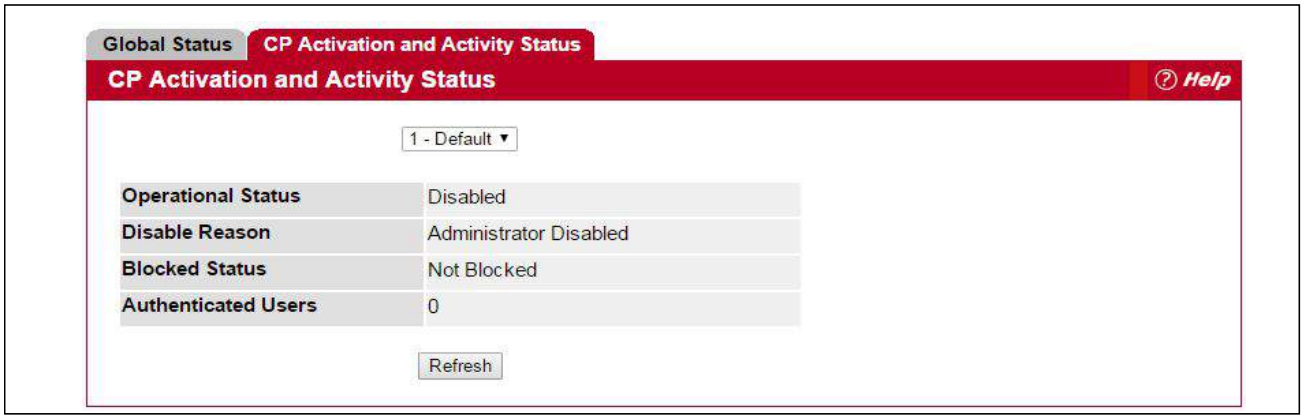


Figure 80: CP Activation and Activity Status

The **CP Activation and Activity Status** page has a drop-down menu that contains all captive portals configured on the switch. When you select a captive portal, the activation and activity status for that portal displays.

Table 72 describes the information that displays for each portal.

Table 72: CP Activation and Activity Status Fields

Field	*Description*
Operational Status	Indicates whether the captive portal is enabled or disabled.
Disable Reason	If the captive portal is disabled, then this field indicates the reason. The portal instance may be disabled for the following reasons: • None - CP is enabled. • Administratively Disabled RADIUS Authentication mode enabled, but RADIUS server is not defined. • Not associated with any interfaces. • The associated interfaces do not exist or do not support the CP capability.
Blocked Status	Indicates whether the captive portal is temporarily blocked for authentications.
Authenticated Users	Shows the number of users that successfully authenticated to this captive portal and are currently using the portal.

The following buttons are available on the **CP Activation and Activity** page:

- **Refresh**—Click **Refresh** to update the screen with the most current information.

Interface Status

The pages available from the **Interface Status** link provide information about the captive portal interfaces and their capabilities.

Interface Activation Status

The **Interface Activation Status** page shows information for every interface assigned to a captive portal instance. Use the drop-down menus to select the portal or interface for which you want to view information

To open this page, click **Security > Captive Portal > Interface Status**, then click the Interface Activation Status tab.

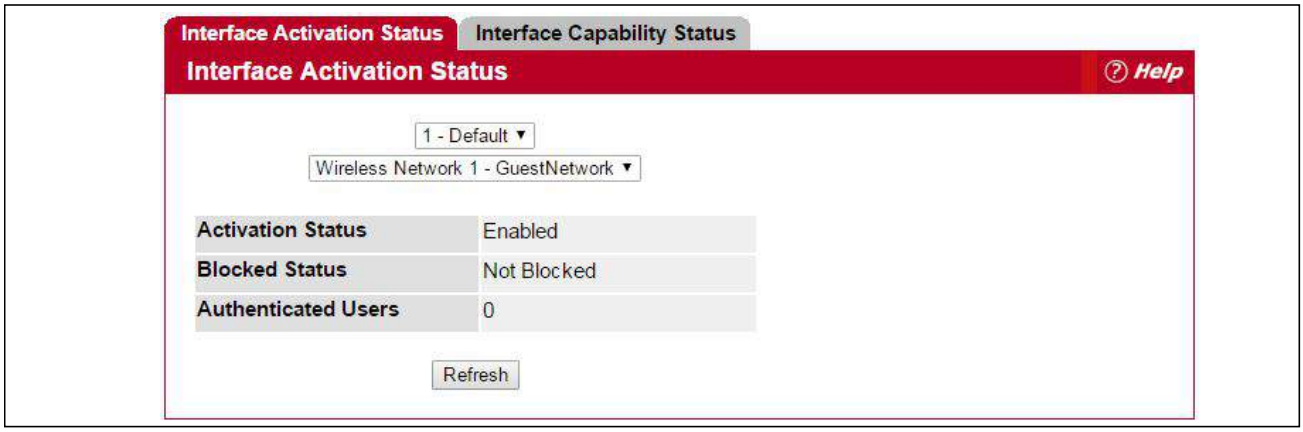


Figure 81: Interface Activation Status

The following table describes the fields on the **Interface Activation Status** page.

Table 73: Interface Activation Status Fields

Field	*Description*
Activation Status	Shows whether the portal is active on the specified interface.
Blocked Status	Indicates whether the captive portal is temporarily blocked for authentications.
Authenticated Users	Displays the number of authenticated users using the captive portal instance on this interface.

Interface Capability Status

The **Interface Capability Status** page contains information about interfaces that can have CPs associated with them. The page also contains status information for various capabilities. Specifically, this page indicates what services are provided through the CP to clients connected on this interface. The list of services is determined by the interface capabilities.

To open this page, click **Security > Captive Portal > Interface Status**, then click the Interface Capability Status tab.

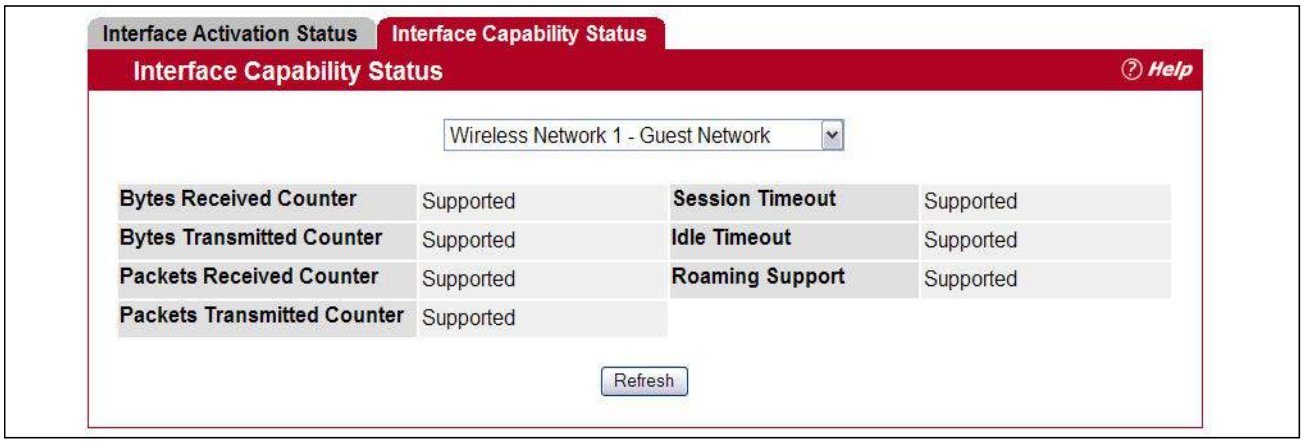


Figure 82: Interface Capability Status

The drop-down menu contains all the wireless interfaces available on the switch. Each interface is identified by its wireless network number and SSID. Use the drop-down menu to select the interface with the information to display.

Table 74 describes the fields on the **Interface Capability Status** page.

Table 74: Interface and Capability Status Fields

Parameter	*Description*
Bytes Received Counter	Shows whether the interface supports displaying the number of bytes received from each client.
Bytes Transmitted Counter	Shows whether the interface supports displaying the number of bytes transmitted to each client.
Packets Received Counter	Shows whether the interface supports displaying the number of packets received from each client.
Packets Transmitted Counter	Shows whether the interface supports displaying the number of packets transmitted to each client.
Session Timeout	Shows whether the interface supports client session timeout. This attribute is supported on all interfaces.
Idle Timeout	Shows whether the interface supports a timeout when the user does not send or receive any traffic.
Roaming Support	Shows whether the interface supports client roaming. Only wireless interfaces support client roaming.

Client Connection Status

From the Client Connection Status page, you can access several pages that provide information about clients that are connected to the switch through the CP.

Client Summary

Use the **Client Summary page to view summary information** about all authenticated wireless clients that are connected through the captive portal. From this page, you can manually force the captive portal to disconnect one or more authenticated clients. The list of wireless clients is sorted by client MAC address.

If the switch supports clustering and there are peer switches in the cluster, some of the clients displayed on the page might be connected to the network through other switches. For more information about the client, and to view information about which the switch handled authentication for the client, click the MAC address of the client.

To view information about the wireless clients connected to the switch through the captive portal, click **Security > Captive Portal > Client Connection Status**, and then click the **Client Summary** tab.

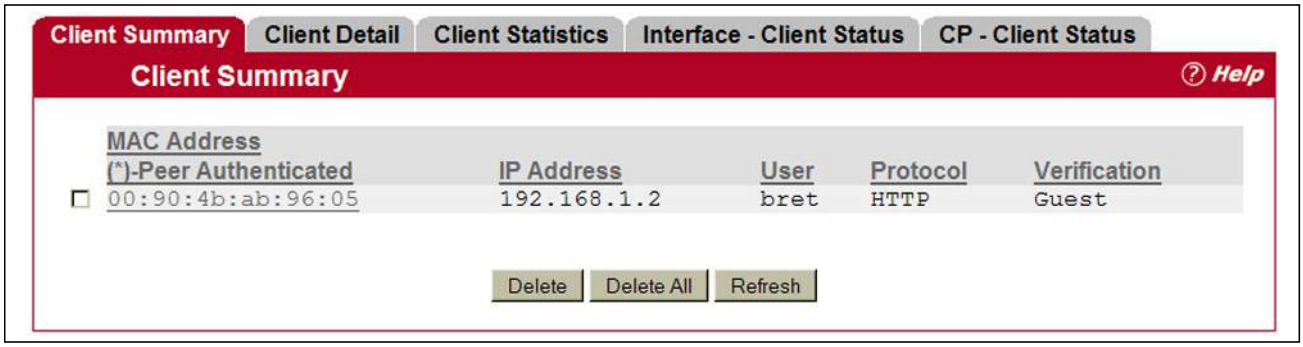


Figure 83: Client Summary

The following table describes the fields on the **Client Summary** page.

Table 75: Client Summary Fields

Field	*Description*
MAC Address	Identifies the MAC address of the wireless client (if applicable). If the MAC address is marked with an asterisk (*), the authenticated client is authenticated by a peer switch. In order words, the cluster controller was not the authenticator.
IP Address	Identifies the IP address of the wireless client (if applicable).
User	Displays the user name (or Guest ID) of the connected client.
Protocol	Shows the current connection protocol, which is either HTTP or HTTPS.
Verification	Shows the current account type, which is Guest, Local, or RADIUS.

To force the captive portal to disconnect an authenticated client, select the check box next to the client MAC address and click **Delete**. To disconnect all clients from all captive portals, click **Delete All**.

Client Detail

The **Client Detail** page shows detailed information about each client connected to the network through a captive portal.

To open this page, click **Security > Captive Portal > Client Connection Status**, and then click the **Client Detail** tab.

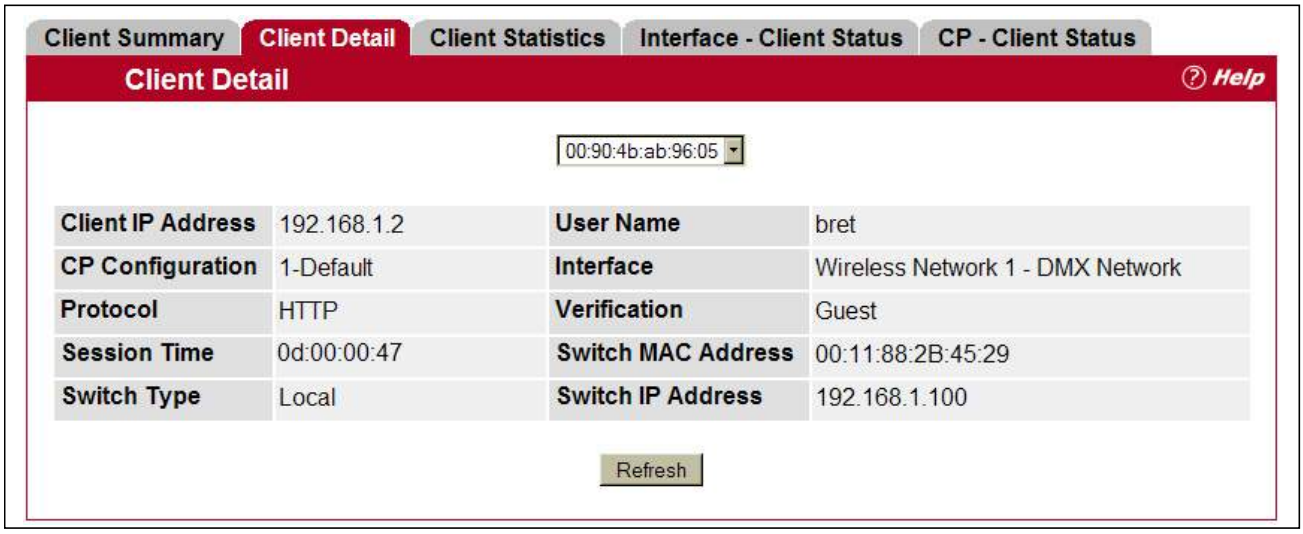


Figure 84: Client Detail

The drop-down menu lists each associated client by MAC address. To view status information for a different client, select its MAC address from the list.

Table 76 describes the fields on the **Client Detail** page.

Table 76: Client Detail Fields

Field	*Description*
Client IP Address	Identifies the IP address of the wireless client (if applicable).
CP Configuration	Identifies the CP configuration the wireless client is using.
Protocol	Shows the current connection protocol, which is either HTTP or HTTPS.
Session Time	Shows the amount of time that has passed since the client was authorized.
Switch Type	Shows whether the switch handling authentication for this client is the local switch or a peer switch in the cluster.
User Name	Displays the user name (or Guest ID) of the connected client.
Interface	Identifies the interface the wireless client is using.
Verification	Shows the current account type, which is Guest, Local, or RADIUS.
Switch MAC Address	Shows the MAC address of the switch handling authentication for this client. If clustering is supported, this field might display the MAC address of a peer switch in the cluster.
Switch IP Address	Shows the IP address of the switch handling authentication for this client. If clustering is supported, this field might display the IP address of a peer switch in the cluster.

Client Statistics

Use the **Client Statistics** page to view information about the traffic a client has sent or received.

To open this page, click **Security > Captive Portal > Client Connection Status**, and then click the **Client Statistics** tab.

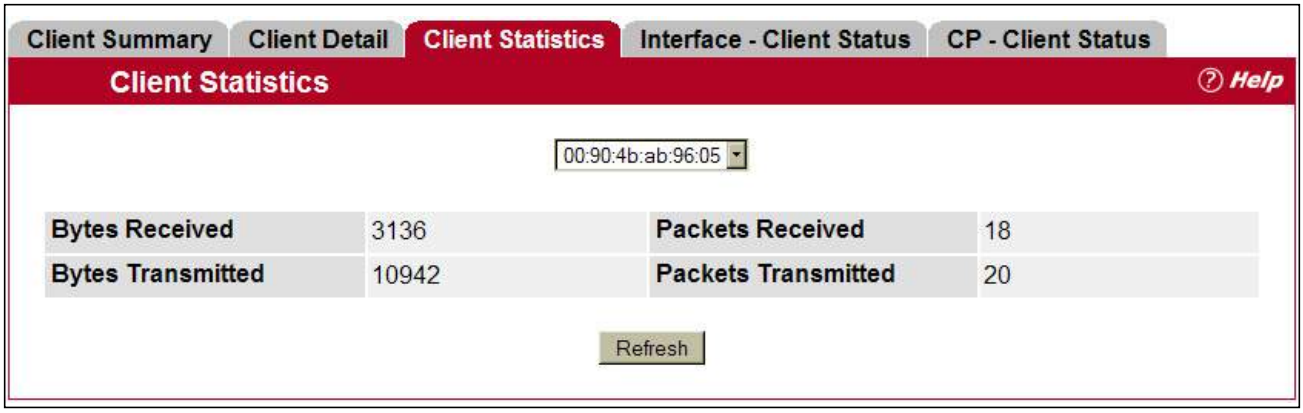


Figure 85: Client Statistics

The drop-down menu lists each associated client by MAC address. To view statistical information for a client, select it from the list.

Table 77 describes the fields on the **Client Statistics page**.

Table 77: Client Interface Association Connection Statistics Fields

Field	*Description*
Bytes Received	Total bytes the client has received
Bytes Transmitted	Total bytes the client has transmitted
Packets Received	Total packets the client has received
Packets Transmitted	Total packets the client has transmitted

Interface - Client Status

Use the **Interface - Client Status** page to view clients that are authenticated to a specific interface.

To open this page, click **Security > Captive Portal > Client Connection Status**, and then click the **Interface - Client Status** tab.

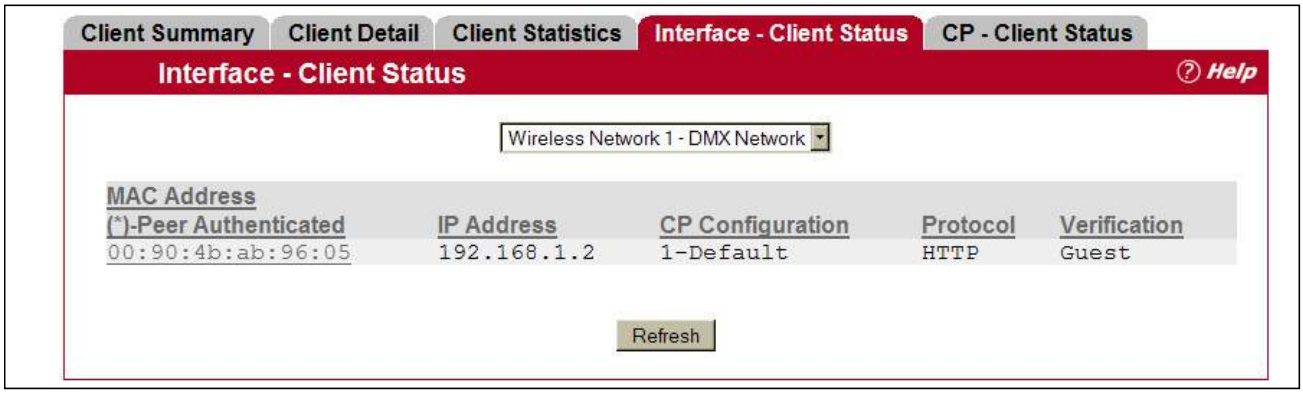


Figure 86: Interface - Client Status

The drop-down menu lists each interface on the switch. To view information about the clients connected to a CP on this interface, select it from the list.

Table 78 describes the fields on the **Interface - Client Status page**.

Table 78: Interface - Client Status Fields

Field	*Description*
MAC Address	Identifies the MAC address of the wireless client. If the MAC address is marked with an asterisk (*), the authenticated client is authenticated by a peer switch. In order words, the cluster controller was not the authenticator.
IP Address	Identifies the IP address of the wireless client.
CP Configuration	Identifies the captive portal the client used to access the network.
Protocol	Shows the current connection protocol, which is either HTTP or HTTPS.
Verification	Shows the current account type, which is Guest, Local, or RADIUS.

CP - Client Status

Use the **CP - Client Status** page to view clients that are authenticated to a specific CP configuration.

To open this page, click **Security > Captive Portal > Client Connection Status**, and then click the **CP - Client Status** tab.

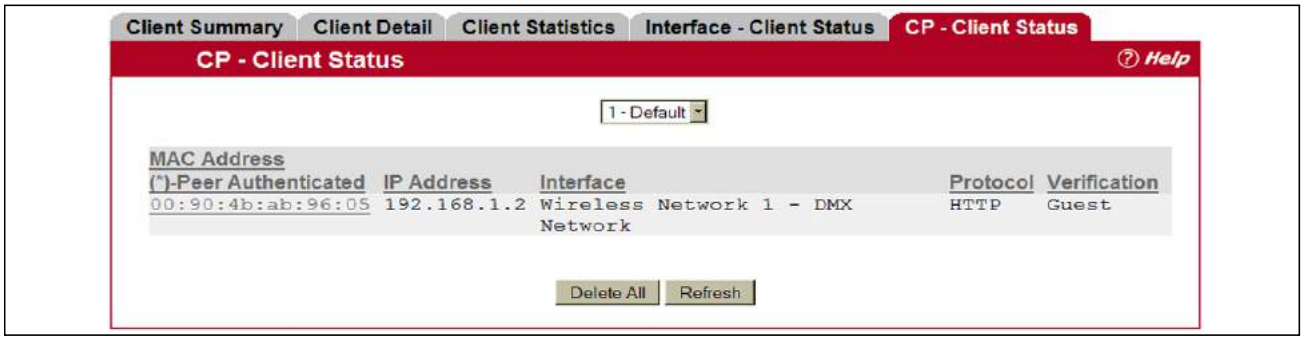


Figure 87: CP - Client Status

The drop-down menu lists each CP configured on the switch. To view information about the clients connected to the CP, select it from the list.

The following table describes the fields on the **Client CP Association Status page**.

Table 79: CP - Client Status Fields

Field	*Description*
MAC Address	Identifies the MAC address of the wireless client. If the MAC address is marked with an asterisk (*), the authenticated client is authenticated by a peer switch. In order words, the cluster controller was not the authenticator.
IP Address	Identifies the IP address of the wireless client.
Interface	Identifies the interface the client used to access the network.
Protocol	Shows the current connection protocol, which is either HTTP or HTTPS.
Verification	Shows the current account type, which is Guest, Local, or RADIUS.

SNMP Trap Configuration

Use the **SNMP Trap Configuration** page to configure whether or not SNMP traps are sent from the Captive Portal and to specify captive portal events that will generate a trap.

Note: You can configure the Captive Portal traps only if the Captive Portal Trap Mode is enabled, which you configure on the **System >Trap Manager > Trap Flags** page.

All CP SNMP traps are disabled by default.

To configure SNMP trap settings for various captive portal features, click **Security > Captive Portal > SNMP Trap Configuration**.

Figure 88: SNMP Trap Configuration

The following table describes the events that generate SNMP traps when the status is Enabled.

Table 80: SNMP Trap Configuration Fields

Field	*Description*
Captive Portal Trap Mode	Displays the captive portal trap mode status. To enable or disable the mode, use Captive Portal menu on the **System > Trap Manager > Trap Flags** page.
Client Authentication Failure Traps	If you enable this field, the SNMP agent sends a trap when a client attempts to authenticate with a captive portal but is unsuccessful.
Client Connection Traps	If you enable this field, the SNMP agent sends a trap when a client authenticates with and connects to a captive portal.
Client Database Full Traps	If you enable this field, the SNMP agent sends a trap each time an entry cannot be added to the client database because it is full.
Client Disconnection Traps	If you enable this field, the SNMP agent sends a trap when a client disconnects from a captive portal.

RADIUS Settings

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. The RADIUS server maintains a user database, which contains per-user authentication information. RADIUS servers provide a centralized authentication method for:

- Telnet Access
- Web Access
- Console to Switch Access
- Access Control Port (802.1x)

The RADIUS folder contains links to the following pages that help you view and configure system RADIUS settings:

- RADIUS Configuration
- Server Configuration
- Named Server Status
- Server Statistics
- Accounting Server Configuration
- Named Accounting Server Status
- Accounting Server Statistics
- Clear Statistics

RADIUS Configuration

Use the RADIUS Configuration page to view and configure various settings for the RADIUS servers configured on the system.

To access the **RADIUS Configuration** page, click **Security > RADIUS > Configuration** in the navigation menu.

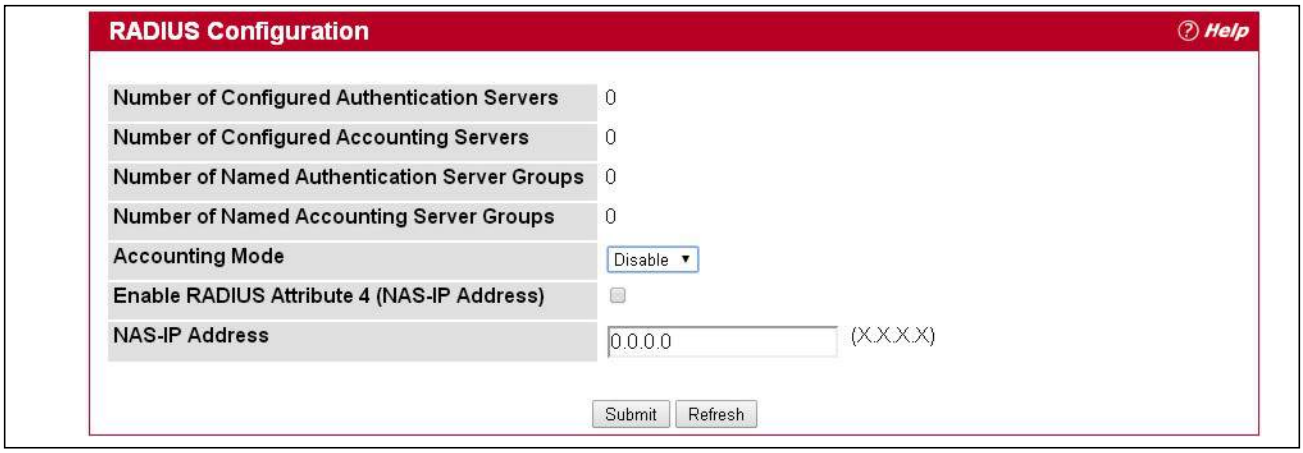


Figure 89: RADIUS Configuration

Table 81: RADIUS Configuration Fields

Field	*Description*
Number of Configured Authentication Servers	The number of RADIUS authentication servers configured on the system. The value can range from 0 to 32.
Number of Configured Accounting Servers	The number of RADIUS accounting servers configured on the system. The value can range from 0 to 32.
Number of Named Authentication Server Groups	The number of authentication server groups configured on the system. An authentication server group contains one or more configured authentication servers that share the same RADIUS server name.
Number of Named Accounting Server Groups	The number of accounting server groups configured on the system. An accounting server group contains one or more configured authentication servers that share the same RADIUS server name.
Accounting Mode	Use the menu to select whether the RADIUS accounting mode is enabled or disabled on the current server.
Enable RADIUS Attribute 4 (NAS-IP Address	Select the check box to allow the switch to include the network access server (NAS) IP address in Access-Request packets.
NAS-IP Address	Enter the IP address of the NAS. This field can be edited only when the Enable RADIUS Attribute 4 field is selected. The address should be unique to the NAS within the scope of the RADIUS server. The NAS IP address is only used in Access-Request packets.

Use the buttons at the bottom of the page to perform the following actions:

- Click **Refresh** to update the page with the most current information.
- If you make changes to the page, click **Submit** to apply the changes to the system.

Server Configuration

From the **Server Configuration** page, you can add a new RADIUS server, configure settings for a new or existing RADIUS server, and view RADIUS server status information. The RADIUS client on the switch supports up to 32 named authentication and accounting servers.

To access the RADIUS Server Configuration page, click **Security > R**AD**IUS > Server Configuration** in the navigation menu.

If there are no RADIUS servers configured on the system or if you select Add from the RADIUS Server Host Address menu, the fields described in the following table are available.

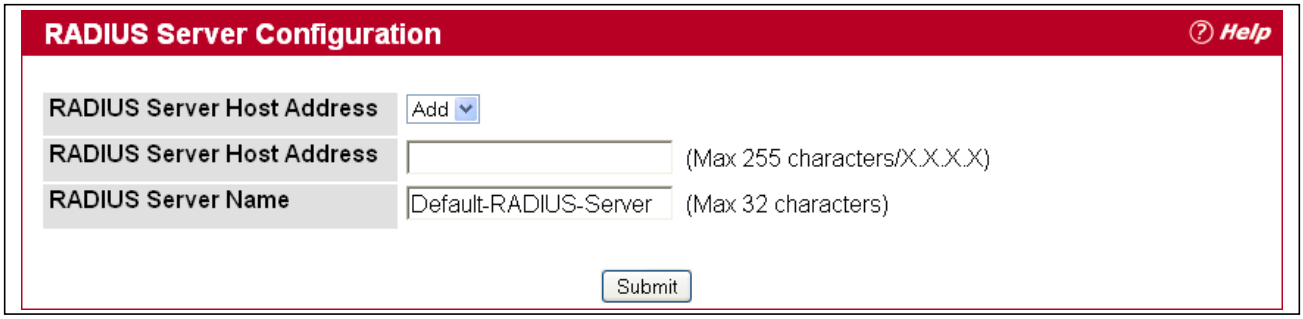


Figure 90: RADIUS Server Configuration—Add Server

Table 82: RADIUS Server Configuration Fields

Field	*Description*
RADIUS Server Host Address	To configure a new RADIUS server, select the Add option from the menu. To view or configure a RADIUS server that is already configured on the system, select its IP address from the menu.
RADIUS Server Host Address	Enter the IP address of the RADIUS server to add. This field is only available when Add is selected in the **RADIUS Server Host Address** field.
RADIUS Server Name	Enter the name of the RADIUS server. The name can contain up to 32 alphanumeric characters. Spaces, hyphens, and underscores are also permitted. If you do not assign a name, the server is assigned the default name Default-RADIUS-Server. You can use the same name for multiple RADIUS Authentication servers. RADIUS clients can use RADIUS servers with the same name as backups for each other.

After you enter RADIUS server information, click **Submit** to apply the changes to the system. The page refreshes, and additional RADIUS server configuration fields appear.

If at least one RADIUS server is configured on the switch, and a host address is selected in the RADIUS Server Host Address field, then additional fields are available on the RADIUS Server Configuration page. After you add a RADIUS server, use the Server Configuration page to configure the server settings.

If you select **Add** from the RADIUS Server Host Address field, the page refreshes and several of the configuration options are hidden.

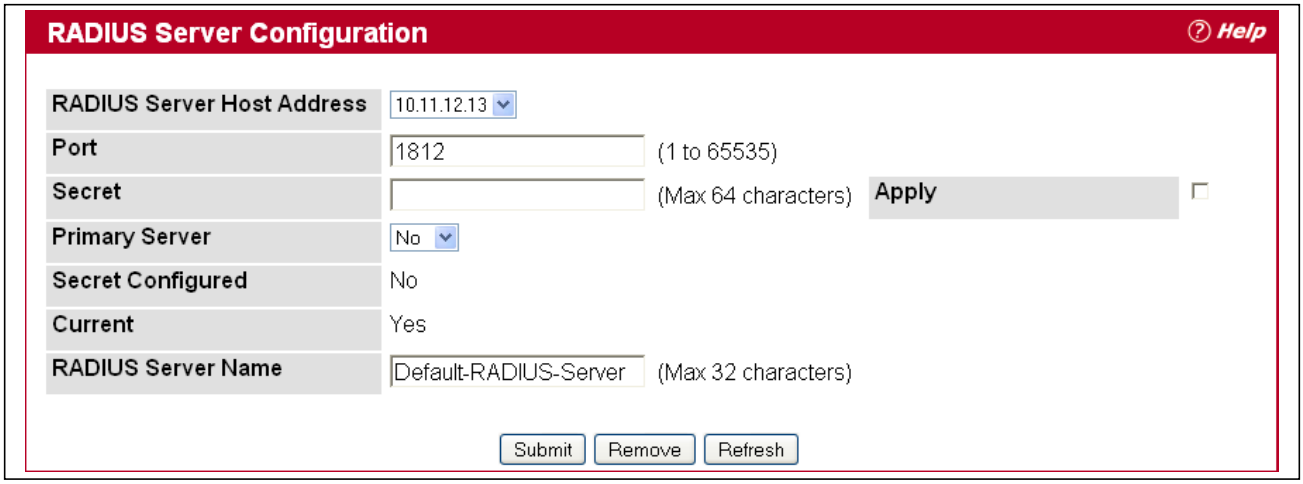


Figure 91: RADIUS Server Configuration—Server Added

Table 83: RADIUS Server Configuration Fields

Field	*Description*
RADIUS Server Host Address	Use the drop-down menu to select the IP address of the RADIUS server to view or configure. Select Add to configure additional RADIUS servers.
Port	Identifies the authentication port the server uses to verify the RADIUS server authentication. The port is a UDP port, and the valid range is 1-65535. The default port for RADIUS authentication is 1812.
Secret	Shared secret text string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This secret must match the RADIUS encryption.
Apply	The Secret will only be applied if this box is checked. If the box is not checked, anything entered in the Secret field will have no affect and will not be retained. This field is only displayed if the user has READWRITE access.
Primary Server	Sets the selected server to the Primary (Yes) or Secondary (No) server. If you configure multiple RADIUS servers with the same RAIDUS Server Name, designate one server as the primary and the other(s) as the backup server(s). The switch attempts to use the primary server first, and if the primary server does not respond, the switch attempts to use one of the backup servers with the same RADIUS Server Name.
Secret Configured	Indicates whether the shared secret for this server has been configured.
Current	Indicates whether the selected RADIUS server is the current server (Yes) or a backup server (No). If more than one RADIUS server is configured with the same name, the switch selects one of the servers to be the *current* server from the group of servers with the same name. When the switch sends a RADIUS request to the named server, the request is directed to the server selected as the current server. Initially the primary server is selected as the current server. If the primary server fails, one of the other servers becomes the current server. If the primary server is not configured, the current server is the most recently configured RADIUS server.

Table 83: RADIUS Server Configuration Fields (Cont.)

Field	*Description*
RADIUS Server Name	Shows the RADIUS server name. To change the name, enter up to 32 alphanumeric characters. Spaces, hyphens, and underscores are also permitted. If you do not assign a name, the server is assigned the default name Default-RADIUS-Server. You can use the same name for multiple RADIUS Authentication servers. RADIUS clients can use RADIUS servers with the same name as backups for each other.

Use the buttons at the bottom of the page to perform the following actions:

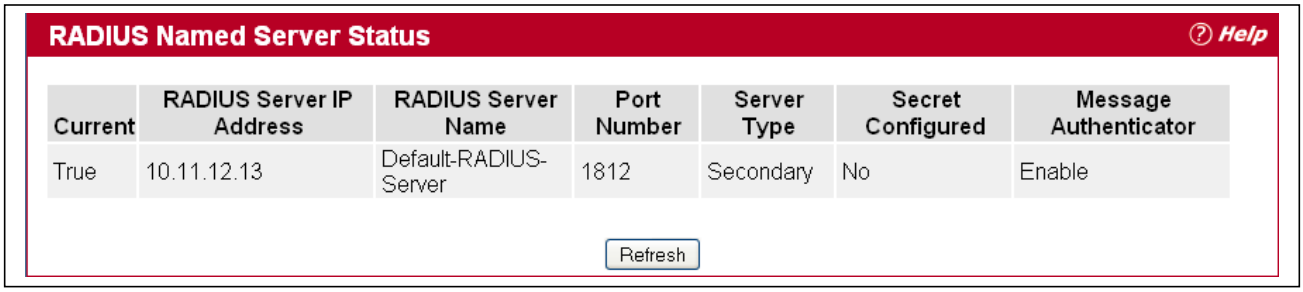
- If you make changes to the page, click **Submit** to apply the changes to the system.

To delete a configured RADIUS authentication server, select the IP address of the server from the **RADIUS Server Host Address** menu, and then click **Remove**.

- Click **Refresh** to update the page with the most current information.

Named Server Status

The RADIUS Named Server Status page shows summary information about the RADIUS servers configured on the system.



Current	RADIUS Server IP Address	RADIUS Server Name	Port Number	Server Type	Secret Configured	Message Authenticator
True	10.11.12.13	Default-RADIUS-Server	1812	Secondary	No	Enable

Figure 92: Named Server Status

Table 84: RADIUS Server Configuration Fields

Field	*Description*
Current	An asterisk (*) in the column Indicates that the server is the current server for the authentication server group. If no asterisk is present, the server is a backup server. If more than one RADIUS server is configured with the same name, the switch selects one of the servers to be the current server from the group of servers with the same name. When the switch sends a RADIUS request to the named server, the request is directed to the server selected as the current server. Initially the primary server is selected as the current server. If the primary server fails, one of the other servers becomes the current server.
RADIUS Server IP Address	Shows the IP address of the RADIUS server.

Table 84: RADIUS Server Configuration Fields (Cont.)

Field	*Description*
RADIUS Server Name	Shows the RADIUS server name. Multiple RADIUS servers can have the same name. In this case, RADIUS clients can use RADIUS servers with the same name as backups for each other.
Port Number	Identifies the authentication port the server uses to verify the RADIUS server authentication. The port is a UDP port.
Server Type	Shows whether the server is a Primary or Secondary server.
Secret Configured	Indicates whether the shared secret for this server has been configured.
Message Authenticator	Shows whether the message authenticator attribute for the selected server is enabled or disabled.

Click **Refresh** to update the page with the most current information.

Server Statistics

Use the RADIUS Server Statistics page to view statistical information for each RADIUS server configured on the system.

To access the RADIUS Server Statistics page, click **Security > RADIUS > Server Statistics** in the navigation menu.

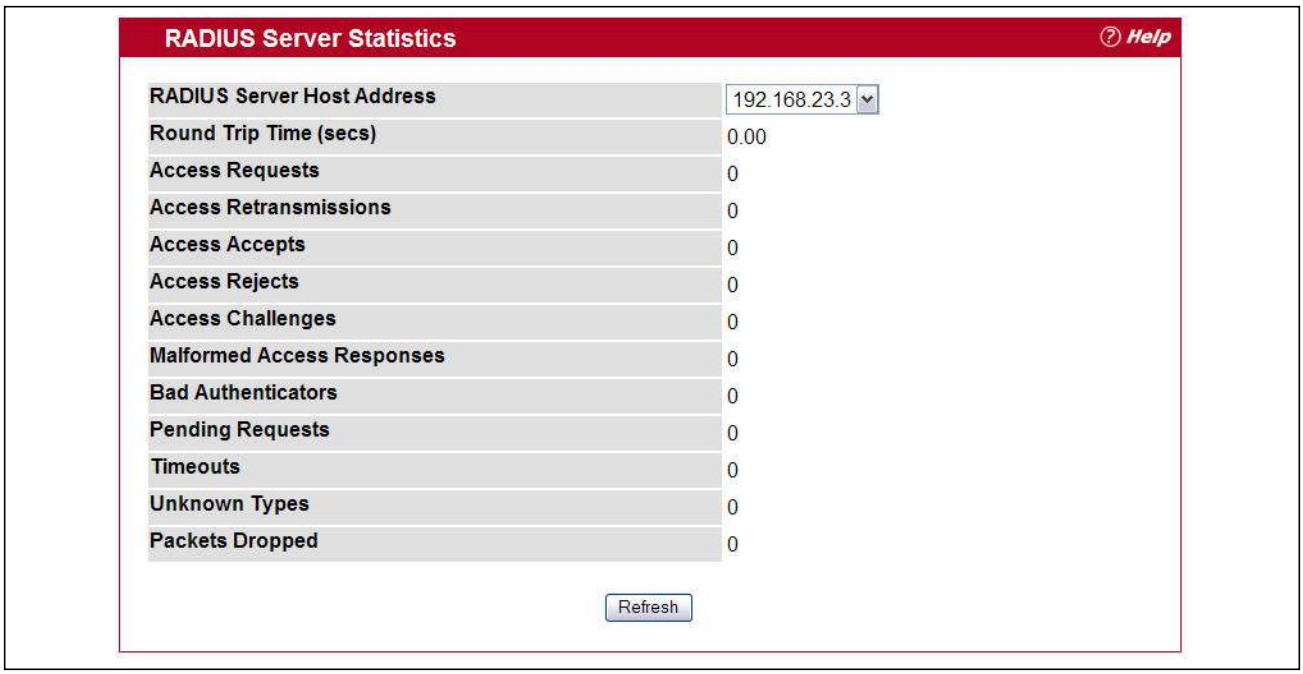


Figure 93: RADIUS Server Statistics

Table 85: RADIUS Server Statistics Fields

Field	*Description*
RADIUS Server Host Address	Use the drop-down menu to select the IP address of the RADIUS server for which to display statistics.
Round Trip Time (secs)	The time interval, in hundredths of a second, between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.

Table 85: RADIUS Server Statistics Fields (Cont.)

Field	*Description*
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access-responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

Click **Refresh** to update the page with the most current information.

Accounting Server Configuration

From the **Accounting Server Configuration** page, you can add a new RADIUS accounting server, configure settings for a new or existing RADIUS accounting server, and view RADIUS accounting server status information. The RADIUS client on the switch supports up to 32 named authentication and accounting servers.

If there are no RADIUS accounting servers configured on the system or if you select Add from the Accounting Server Host Address menu, the fields described in the following table are available.

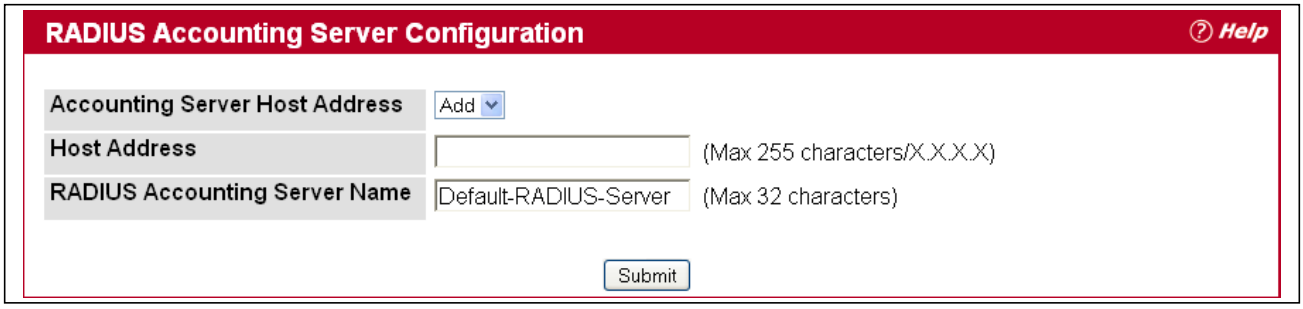


Figure 94: Add RADIUS Accounting Server

Table 86: RADIUS Server Configuration Fields

Field	*Description*
Accounting Server Host Address	To configure a new RADIUS accounting server, select the Add option from the menu. To view or configure an accounting server that is already configured on the system, select its IP address from the menu.
Host Address	Enter the IP address of the RADIUS accounting server to add. This field is only available when Add is selected in the **Accounting Server Host Address** field.

Table 86: RADIUS Server Configuration Fields (Cont.)

Field	*Description*
RADIUS Accounting Server Name	Enter a name for the RADIUS accounting server. The name can contain up to 32 alphanumeric characters. Spaces, hyphens, and underscores are also permitted. If you do not assign a name, the server is assigned the default name Default-RADIUS-Server. You can use the same name for multiple RADIUS accounting servers. RADIUS clients can use accounting servers with the same name as backups for each other.

After you enter the RADIUS accounting server information, click **Submit** to apply the changes to the system.The page refreshes, and additional accounting server configuration fields appear.

If at least one RADIUS accounting server is configured on the switch, and a host address is selected in the Accounting Server Host Address field, then additional fields are available on the Accounting Server Configuration page. After you add an accounting server, use the Accounting Server Configuration page to configure the server settings.

If you select **Add** from the Accounting Server Host Address field, the page refreshes and several of the configuration options are hidden.

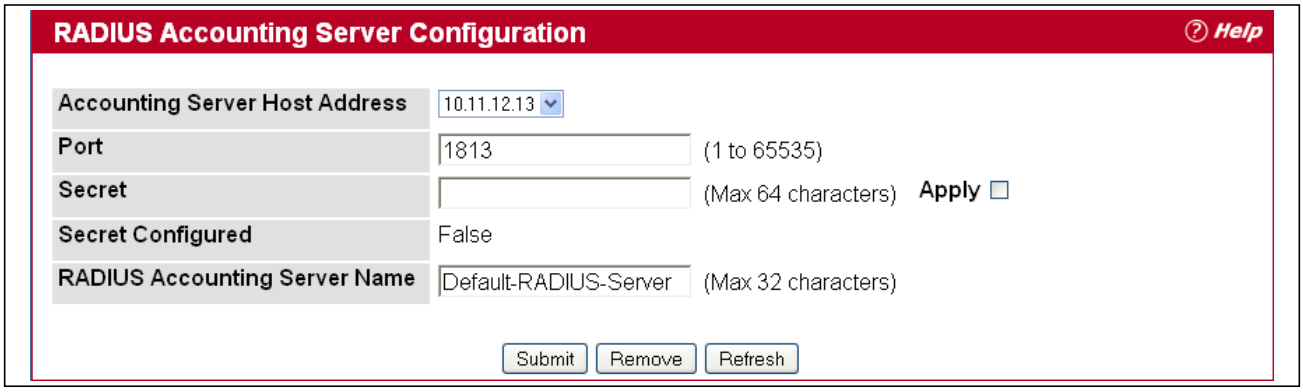


Figure 95: RADIUS Accounting Server Configuration—Server Added

Table 87: RADIUS Accounting Server Configuration Fields

Field	*Description*
Accounting Server Host Address	Use the drop-down menu to select the IP address of the accounting server to view or configure. Select Add to configure additional RADIUS servers.
Port	Identifies the authentication port the server uses to verify the RADIUS accounting server authentication. The port is a UDP port, and the valid range is 1-65535. The default port for RADIUS accounting is 1813.
Secret	Specifies the shared secret to use with the specified accounting server. This field is only displayed if you are logged into the switch with READWRITE access.
Apply	The Secret will only be applied if this box is checked. If the box is not checked, anything entered in the Secret field will have no affect and will not be retained. This field is only displayed if you are logged into the switch with READWRITE access.

Table 87: RADIUS Accounting Server Configuration Fields (Cont.)

Field	*Description*
Secret Configured	Indicates whether the shared secret for this server has been configured.
RADIUS Accounting Server Name	Enter the name of the RADIUS accounting server. The name can contain up to 32 alphanumeric characters. Spaces, hyphens, and underscores are also permitted. If you do not assign a name, the server is assigned the default name Default-RADIUS-Server. You can use the same name for multiple RADIUS accounting servers. RADIUS clients can use accounting servers with the same name as backups for each other.

Use the buttons at the bottom of the page to perform the following actions:

- If you make changes to the page, click **Submit** to apply the changes to the system.

To delete a configured RADIUS accounting server, select the IP address of the server from the **RADIUS Server IP Address** drop-down menu, and then click **Remove**.

- Click **Refresh** to update the page with the most current information.

Named Accounting Server Status

The RADIUS Named Accounting Server Status page shows summary information about the accounting servers configured on the system.

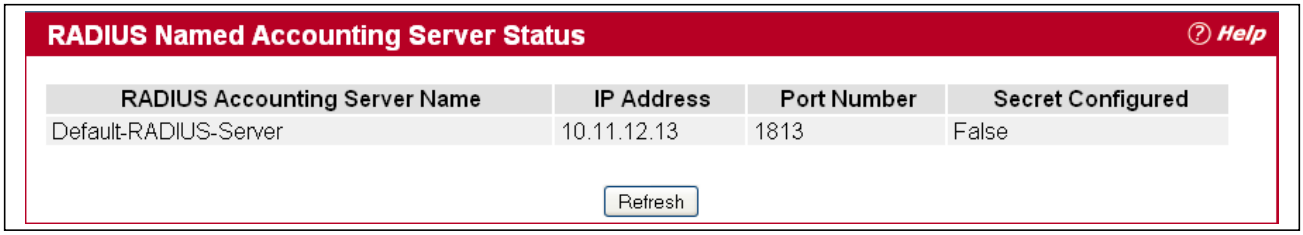


Figure 96: RADIUS Server Configuration—Server Added

Table 88: Named Accounting Server Fields

Field	*Description*
RADIUS Accounting Server Name	Shows the RADIUS accounting server name. Multiple RADIUS accounting servers can have the same name. In this case, RADIUS clients can use RADIUS servers with the same name as backups for each other.
P Address	Shows the IP address of the RADIUS server.
Port Number	Identifies the authentication port the server uses to verify the RADIUS server authentication. The port is a UDP port.
Secret Configured	Indicates whether the shared secret for this server has been configured.

Click **Refresh** to update the page with the most current information.

Accounting Server Statistics

Use the RADIUS Accounting Server Statistics page to view statistical information for each RADIUS server configured on the system.

To access the RADIUS Accounting Server Statistics page, click **Security > RADIUS > Accounting Server Statistics** in the navigation menu.

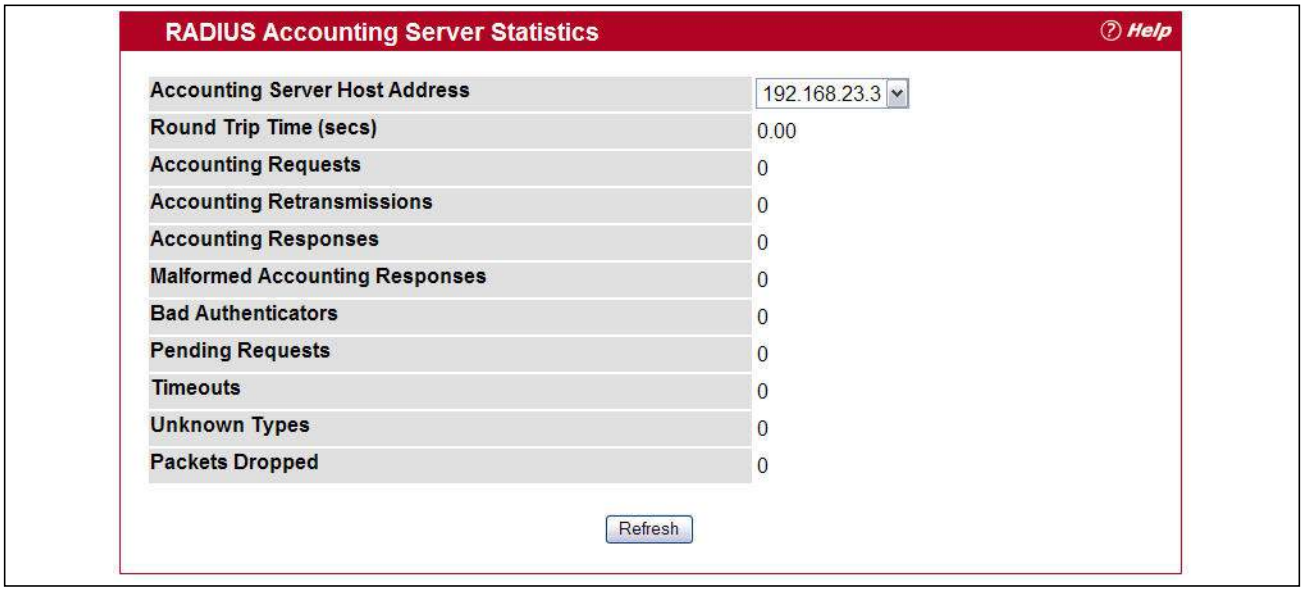


Figure 97: RADIUS Accounting Server Statistics

Table 89: RADIUS Accounting Server Fields

Field	*Description*
Accounting Server Host Address	Use the drop-down menu to select the IP address of the RADIUS accounting server for which to display statistics.
Round Trip Time (secs)	Displays the time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Accounting Requests	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
Accounting Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this server.
Accounting Responses	Displays the number of RADIUS packets received on the accounting port from this server.
Malformed Access Responses	Displays the number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	Displays the number of RADIUS Accounting-Response packets that contained invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets destined for this server that have not yet timed out or received a response.

Table 89: RADIUS Accounting Server Fields (Cont.)

Field	*Description*
Timeouts	The number of accounting timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

Clear Statistics

Use the RADIUS Clear Statistics page to reset all RADIUS authentication and accounting statistics to zero.

To access the RADIUS Clear Statistics page, click **Security > RADIUS > Clear Statistics** in the navigation menu.

Figure 98: RADIUS Clear Statistics

To clear all statistics for the RADIUS authentication and accounting server, click **Clear**.

TACACS+ Settings

To access the TACACS+ Configuration page, click **Security** > **TACACS+** > **Configuration** in the navigation menu.

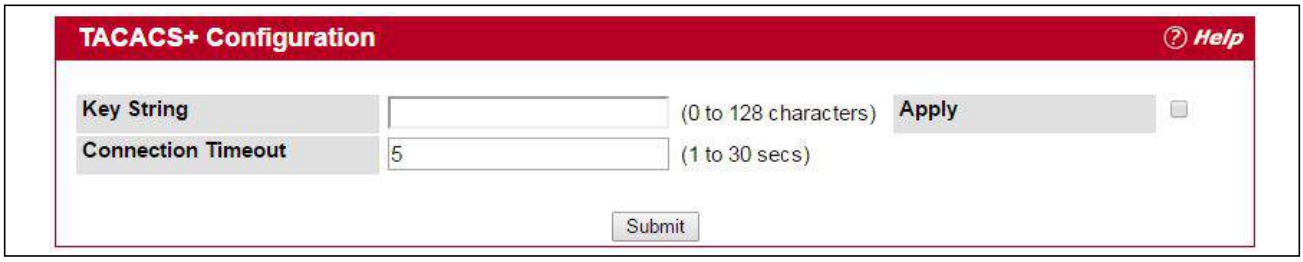


Figure 99: TACACS+ Configuration

Table 90: TACACS+ Configuration Fields

Field	*Description*
Key String	Specifies the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The key must match the key configure on the TACACS+ server.
Connection Timeout	The maximum number of seconds allowed to establish a TCP connection between the device and the TACACS+ server.

Click **Refresh** to update the page with the most current information.

If make any changes to the page, click **Submit** to apply the changes to the system.

TACACS+ Server Configuration

To access the TACACS+ Server Configuration page, click **Security** > **TACACS+** > **Server Configuration** in the navigation menu

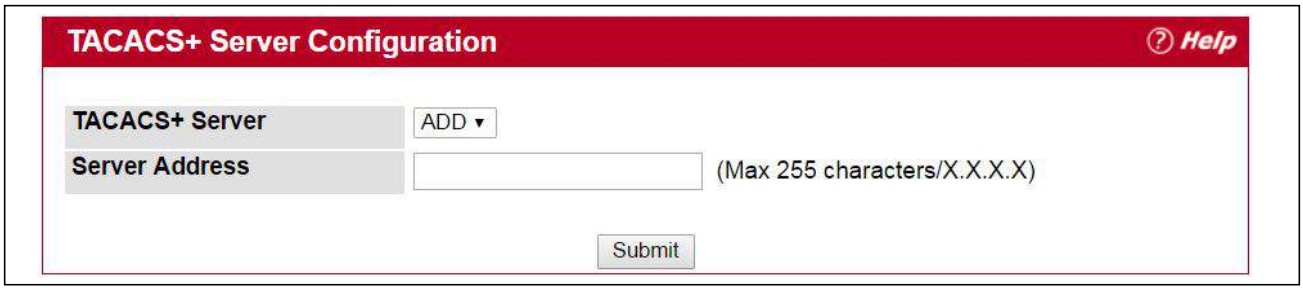


Figure 100: TACACS+ Server Configuration

Table 91: TACACS+ Server Configuration Fields

Field	*Description*
TACACS+ Server	To add a TACACS+ server to the list of servers the TACACS+ client can contact, click Add. If the maximum number of servers is exceeded, this selection is disabled.
Server Address	Specifies the TACACS+ server IP address or hostname.

If a TACACS+ server is added to the list or an existing server is selected, the following TACACS+ server configuration page is displayed.

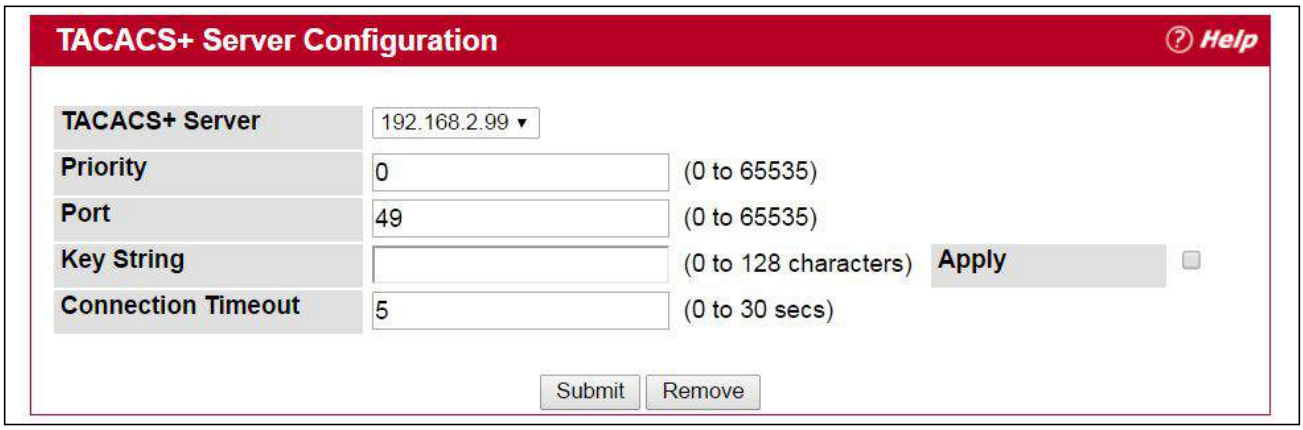


Figure 101: TACACS+ Server Configuration (Details)

Table 92: TACACS+ Server Configuration Details

Field	*Description*
TACACS+ Server	Specifies the TACACS+ server IP address or host name.
Priority	Specifies the order in which the TACACS+ servers are used.
Port	Specifies the authentication port.
Key String	Specifies the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The key must match the encryption used on the TACACS+ server.
Connection Timeout	The amount of time that passes before the connection between the device and the TACACS+ server times out.

Secure HTTP

Secure HTTP enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. When you manage the switch by using a Web interface, secure HTTP can help ensure that communication between the management system and the switch is protected from eavesdroppers and man-in-the-middle attacks.

Secure HTTP Configuration

Use the Secure HTTP Configuration page to configure the settings for HTTPS communication between the management station and the switch.

To display the Secure HTTP Configuration page, click **Security** > **Secure HTTP** > **Configuration** in the navigation menu.

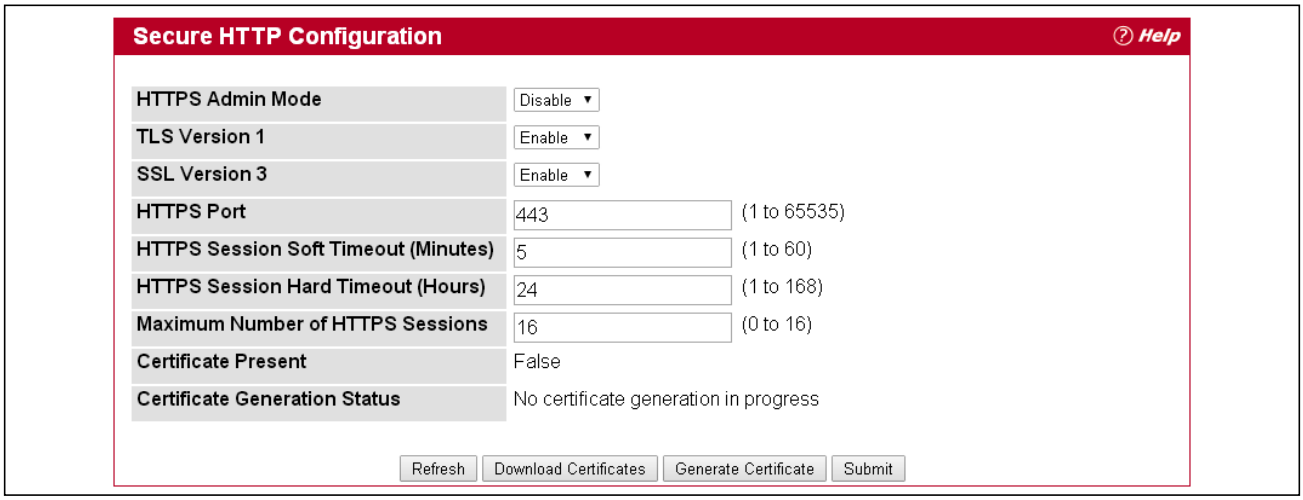


Figure 102: Secure HTTP Configuration

Table 93: Secure HTTP Configuration Fields

Field	*Description*
Admin Mode	Enables or Disables the Administrative Mode of Secure HTTP. The currently configured value is shown when the web page is displayed. The default value is Disable. You can only download SSL certificates when the HTTPS Admin mode is disabled.
TLS Version 1	Enables or Disables Transport Layer Security Version 1.0. The currently configured value is shown when the web page is displayed. The default value is Enable.
SSL Version 3	Enables or Disables Secure Sockets Layer Version 3.0. The currently configured value is shown when the web page is displayed. The default value is Enable.
HTTPS Port	Sets the HTTPS Port Number. The value must be in the range of 1 to 65535. Port 443 is the default value. The currently configured value is shown when the web page is displayed.

Table 93: Secure HTTP Configuration Fields (Cont.)

Field	*Description*
HTTPS Session Soft Timeout	Sets the inactivity timeout for HTTPS sessions. The value must be in the range of (1 to 60) minutes. The default value is 5 minutes. The currently configured value is shown when the web page is displayed.
HTTPS Session Hard Timeout	Sets the hard timeout for HTTPS sessions. This timeout is unaffected by the activity level of the session. The value must be in the range of (1 to 168) hours. The default value is 24 hours. The currently configured value is shown when the web page is displayed.
Maximum Number of HTTPS Sessions	Sets the maximum allowable number of HTTPS sessions. The value must be in the range of (0 to 16). The default value is 16. The currently configured value is shown when the web page is displayed.
Certificate Present	Displays whether there is a certificate present on the device is true or false.
Certificate Generation Status	Displays whether SSL certificate generation is in progress or no certificate generation is in progress.

For the Web server on the switch to accept HTTPS connections from a management station, the Web server needs a public key certificate. The switch can generate its own certificates, or you can generate these externally (i.e., off-line) and download them to the switch.

Generating Certificates

To have the switch generate the certificates:

1. Click **Generate Certificates**.

   The page refreshes with the message “Certificate generation in progress”.

2. Click **Submit** to complete the process.

   The page refreshes with the message “No certificate generation in progress” and the Certificate Present field displays as “True”.

Downloading SSL Certificates

Before you download a file to the switch, the following conditions must be true:

- The file to download from the TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch has a path to the TFTP server.

Use the following procedures to download an SSL certificate.

1. Click the **Download Certificates** button at the bottom of the page.

Note: The **Download Certificates** button is only available if the HTTPS admin mode is disabled. If the mode is enabled, disable it and click Submit. When the page refreshes, the **Download Certificates** button appears.

The Download Certificates button links to the File Download page, as Figure 103 shows.

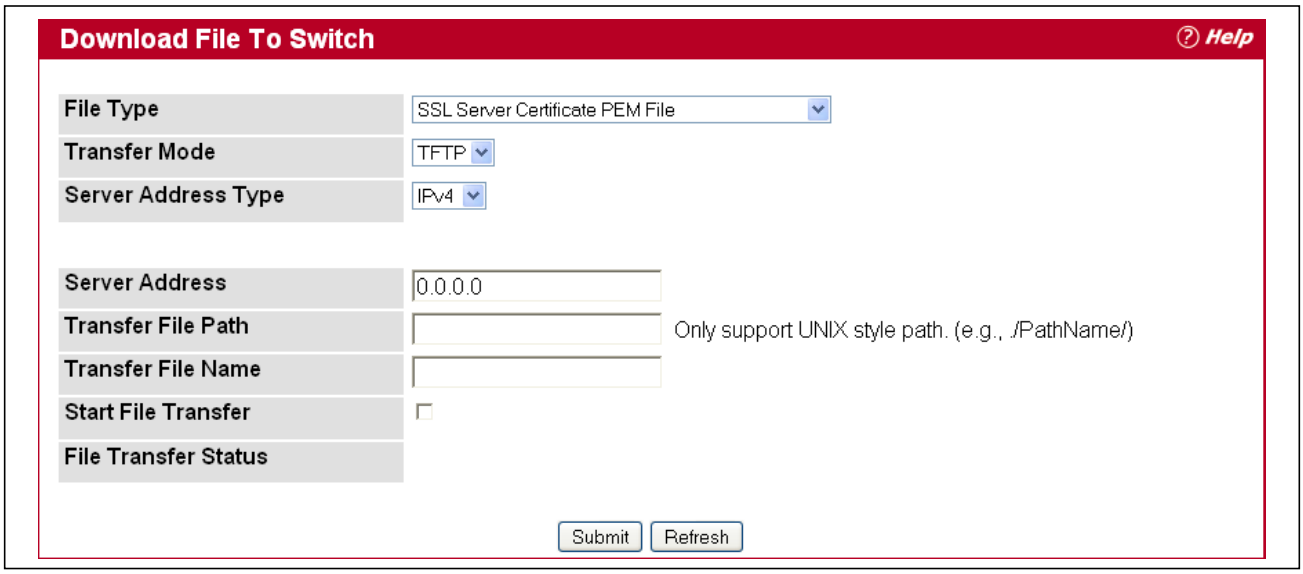


Figure 103: File Download

2. From the **File Type** field on the File Download page, select one of the following types of SSL files to download:
   - SSL Trusted Root Certificate PEM File: SSL Trusted Root Certificate File (PEM Encoded).
   - SSL Server Certificate PEM File**:** SSL Server Certificate File (PEM Encoded).
   - SSL DH Weak Encryption Parameter PEM File**:** SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
   - SSL DH Strong Encryption Parameter PEM File**:** SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).
3. Verify the IP address of the TFTP server and ensure that the software image or other file to be downloaded is available on the TFTP server.
4. Complete the **TFTP Server IP Address** and **TFTP File Name** (full path without TFTP server IP address) fields.
5. Select the **Start File Transfe**r check box, and then click **Submit**.

   After you click Submit, the screen refreshes and a “File transfer operation started” message appears. After the software is downloaded to the device, a message appears indicating that the file transfer operation completed successfully.
6. To return to the Secure HTTP Configuration page, click **Security > Secure HTTP > Configuration** in the navigation menu.
7. To enable the HTTPS admin mode, select Enable from the **HTTPS Admin Mode** field, and then click **Submit**.

Secure Shell

If you use the command-line interface (CLI) to manage the switch from a remote system, you can use Secure Shell (SSH) to establish a secure connection. SSH uses public-key cryptography to authenticate the remote computer.

Secure Shell Configuration

Use the Secure Shell Configuration page to configure the settings for secure command-line based communication between the management station and the switch.

To display the Secure Shell Configuration page, click **Security** > **Secure Shell** > **Configuration** in the navigation menu.

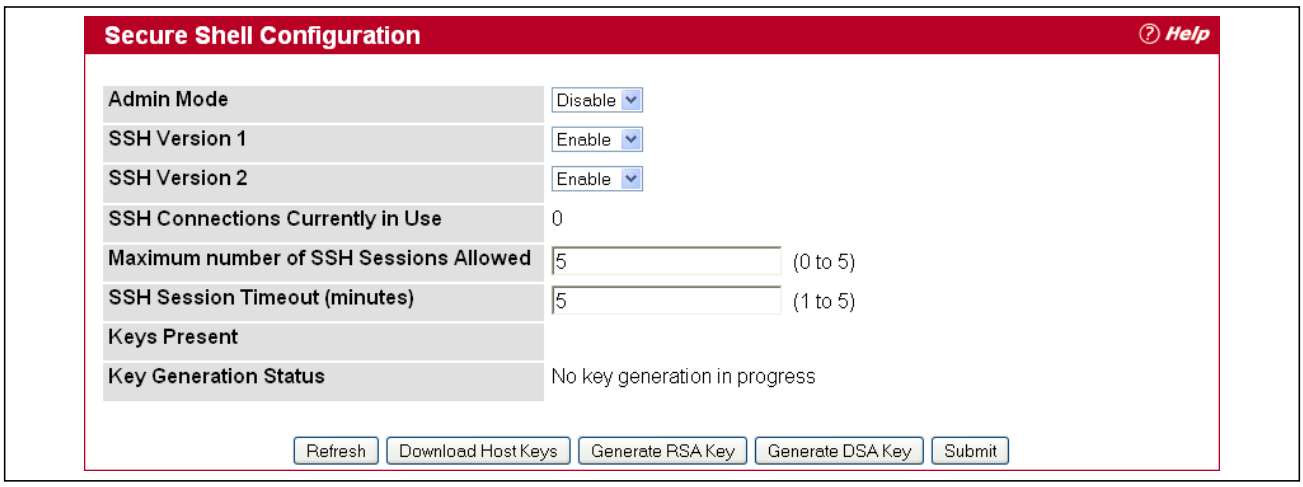


Figure 104: Secure Shell Configuration

Table 94: Secure Shell Configuration Fields

Field	*Description*
Admin Mode	This select field is used to Enable or Disable the administrative mode of SSH. The currently configured value is shown when the web page is displayed. Setting this value to disable shuts down the SSH port. If the admin mode is set to disable, then all existing SSH connections remain connected until timed-out or logged out, but new SSH connections cannot be established. The default value is Disable.
SSH Version 1	This select field is used to Enable or Disable Protocol Level 1 for SSH. The currently configured value is shown when the web page is displayed. The default value is Enable.
SSH Version 2	This select field is used to Enable or Disable Protocol Level 2 for SSH. The currently configured value is shown when the web page is displayed. The default value is Enable.
SSH Connections in Use	Displays the number of SSH connections currently in use in the system.
Maximum Number of SSH Sessions Allowed	This select field is used to configure the maximum number of inbound SSH sessions allowed on the switch. The currently configured value is shown when the web page is displayed. The range of acceptable values for this field is 0-5.

Table 94: Secure Shell Configuration Fields (Cont.)

Field	*Description*
SSH Session Timeout (Minutes)	This text field is used to configure the inactivity timeout value for incoming SSH sessions to the switch. The acceptable range for this value is 1-160 minutes.
Keys Present	Displays which keys RSA, DSA are present. This field is blank when no keys are present.
Key Generation Status	Displays what key files RSA, DSA, Both or None are currently being generated.

Downloading SSH Host Keys

For the switch to accept SSH connections from a management station, the switch needs SSH host keys or certificates. The switch can generate its own keys or certificates, or you can generate these externally (i.e., off-line) and download them to the switch.

To download an SSH host key from a TFTP server to the switch, use the instructions in "Downloading SSL Certificates" on page 173. However, from the File Type field on the File Download page, select one of the following key file types to download:

- **SSH-1 RSA Key File:** SSH-1 Rivest-Shamir-Adleman (RSA) Key File.
- **SSH-2 RSA Key PEM File:** SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded).
- **SSH-2 DSA Key PEM File:** SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded).

Section 5: Configuring the Wireless Features

The Unified Wireless Switch is a wireless local area network (WLAN) solution that enables WLAN deployment while providing state-of-the-art wireless networking features. It is a scalable solution that provides secure wireless connectivity and seamless layer 2 roaming for end users.

This section contains information about the features available in the WLAN folder, which includes the following:

- Unified Wireless System Components
- Setup Wizard
- WLAN Configuration
- AP Management
- Monitoring Status and Statistics
- Monitoring and Managing Intrusion Detection
- WDS Configuration

Unified Wireless System Components

The EWS4502/EWS4606 Wireless System components include:

- EWS4502/EWS4606 Unified Wireless Switch (UWS)
- EWS4502/EWS4606 Unified Access Point (UAP)

Each EWS4502 can manage up to 200 UAPs and each EWS4606 up to 800 UAPs[1], and each access point can handle up to 100 clients. The switch tracks the status and statistics for all associated WLAN traffic and devices.

To support larger networks, wireless switches can be configured to belong to a cluster (peer group). Clusters can contain up to 4 switches that share various information about UAPs and their associated wireless clients. Each cluster can support up to 1500 APs (see footnote 1) and a total of 45000 wireless clients (see footnote 1). Switches within the cluster enable L2 roaming between managed APs in a routing configuration. This means that wireless clients can roam among the access points within the cluster without losing network connections. Additionally, you can push portions of the wireless configuration to one or more switches within the cluster.

One switch in the cluster is automatically elected or configured to be the Cluster Controller. The Cluster Controller gathers status and statistics about all APs and clients in the cluster so you can view network status information and manage all devices in the cluster from a single switch.

Devices in the wireless system can be directly connected to each other, separated by layer 2 bridges, or located in different IP subnets.

Whether or not you have a cluster, the UWS can support a total of 30000 wireless clients.

1. The supported number of APs and wireless clients is based on the existing reference design and the access controller license certificate downloaded to the switch. For more information on access controller licenses, see "UWS Licenses" on page 178.

Unified Wireless Switch

The UWS handles Layer 2 switching functions for traffic on the wired and wireless LAN and manages up to 200 APs, based on the existing reference design. The UWS user interface allows you to configure and monitor all AP settings and maintain a consistent configuration among all APs in the network.

The UWS supports advanced data path connectivity, mobility control, security safeguards, control over radio and power parameters, and management features for both network and element control. The UWS allows you to control the discovery, validation, authentication, and monitoring of peer wireless switches, APs, and clients on the WLAN, including discovery and status of rogue APs and clients.

UWS Licenses

Each UWS requires a license certificate file to be downloaded to the device. The UWS license solution is based on Public Key Infrastructure (PKI) using X.509 certificates. Each certificate file can be signed by a trusted Certificate Authority (CA) or self-signed by a local CA. The certificates are verified by a pre-trusted public key, which is built into the UWS release software.

The certificate files contain information on the device, user, and the capability of the UWS, which defines the number of APs that can be managed. By default, the UWS can only manage six APs without a license certificate file. Up to 500 license certificates can be downloaded to the switch and the sum of all valid certificates will equal the total number of APs that can be managed (plus the six APs included in the default licenses).

When switches are in a cluster, licenses are shared amongst all UWS devices. That is, if three switches in a cluster each have licenses to manage 50 APs, the cluster together can manage up to 150 APs.

For information on downloading license certificate files to a UWS, see “Upload File To Switch (TFTP)” on page 82.

Unified Access Point

The UAP can operate in one of two modes: Standalone Mode or Managed Mode. In Standalone Mode, the UAP acts as an individual access point in the network, and you manage it by connecting to the UAP and using the Administrator Web User Interface (UI), command-line interface (CLI) or SNMP. In Managed Mode, the UAP is part of the Unified Wireless Switch, and you manage it by using the UWS. If a UAP is in Managed Mode, the Administrator Web UI and SNMP services on the UAP are disabled. Access is limited to the CLI through a serial-cable connection.

The Standalone Mode is appropriate for small networks with only a few APs. The Managed Mode is useful for any size network. If you start out with APs in Standalone Mode, you can easily transition the APs to Managed Mode when you add a UWS to the network. By using the AP in Managed Mode, you can centralize AP management and streamline the AP upgrade process by pushing configuration profiles and software upgrades from the UWS to the managed APs.

The UAP has two radios and is capable of broadcasting in the following wireless modes:

- IEEE 802.11b mode
- IEEE 802.11g mode
- IEEE 802.11a mode
- IEEE 802.11n mode (2.4 GHz and 5 GHz)
- IEEE 802.11ac mode (5 GHz)

Each access point supports up to 16 virtual access points (VAPs) on each radio. The VAP feature allows you to segment each physical access point into up to 32 logical access points that each support a unique SSID, VLAN ID, and security policy.

UWS and AP Discovery Methods

The UWS and AP can use the following methods to discover each other:

- L2 Discovery
- IP Address of AP Configured in the Switch
- IP Address of Switch Configured in the AP

Note: For an AP to be managed by a switch, the managed mode on the AP must be enabled. To enable managed mode on the AP, log on to the AP CLI and use the command required for your access point, or access the Web UI and go to the appropriate page to enable the managed mode option.

L3/IP Discovery (WLAN > WLAN Configuration > Discovery) can be used for discovery in different subnets between AP and AC or between peer ACs.

The ECW7220-L APs are set to managed mode by default.

L2 Discovery

When the AP and UWS are directly connected or in the same layer 2 broadcast domain and use the default VLAN settings, the UWS automatically discovers the AP through its broadcast of a L2 discovery message. The L2 discovery works automatically when the devices are directly connected or connected by using a layer 2 bridge.

For more information about L2 Discovery, see “L2/VLAN Discovery” on page 230.

IP Address of AP Configured in the Switch

If APs are in a different broadcast domain than the UWS or use different management VLANs, you can add the IP addresses of the APs to the L3 Discovery list on the switch. The UWS sends UDP discovery messages to the IP addresses in its list. When the AP receives the messages and decides that it can connect to the switch, it initiates an SSL TCP connection to the switch. For more information about configuring the IP address of the AP in the switch, see “L3/IP Discovery” on page 229.

IP Address of Switch Configured in the AP

You can connect to the access point in Standalone mode and statically configure the IP addresses or DNS name of up to two switches that are allowed to manage the AP.

The AP sends a UDP discovery message to the first IP address configured in its list. When the switch receives the message, it verifies that the vendor ID on the AP is valid, there is no existing SSL TCP connection to the access point, and the maximum number of managed APs has not been reached. If all these conditions are met then the switch sends an invitation message to the AP to start the SSL TCP connection.

If the AP does not receive an invitation from the first UWS configured in its list, it sends a UDP discovery message to the second UWS configured in the list five seconds after sending the message to the first UWS.

When an IP address of a UWS is configured on the AP, the AP only associates with that switch even if other switches discover the AP by using other mechanisms.

Note: For this method to work, the AP must be able to find a route to the Unified Switch.

To use the access point CLI to manually configure AP and switch IP address information in the AP, use the following procedure. However, note that the exact commands may vary depending on the AP you are using.

1. Use a serial or Telnet connection to log on to the AP.
2. Press [Ctrl+c] to stop the DHCP process of the AP.
3. At the prompt, enter "cli enter" then press return to access the CLI prompt.
4. Use the following command to set the IP address for the AP.
   `configure interface ethernet ip address [IPv4] [netmask] [gateway]`
   Example:
   `configure interface ethernet ip address 10.7.9.25 255.255.255.0 10.7.9.254`

Note: To set the AP back to DHCP mode, use the command `configure interface ethernet ip dhcp`.

5. Enter "exit" to leave the CLI prompt.
6. Set the switch (access controller) primary and secondary IP addresses using the following commands:
   `set_sys_ac_ip_primary x.x.x.x`
   `set_sys_ac_ip_secondary x.x.x.x`
   Example:
   `# set_sys_ac_ip_primary 10.7.9.251`
   `# set_sys_ac_ip_secondary 10.7.9.252`
7. Use the command "`apconf_cmd Saveall`" to save the AP settings:
8. Reboot the AP using the "`reboot`" command.

Configuring the DHCP Option

You can configure the IP address of the UWS as an option in the DHCP response to the DHCP request that the AP sends the DHCP server.

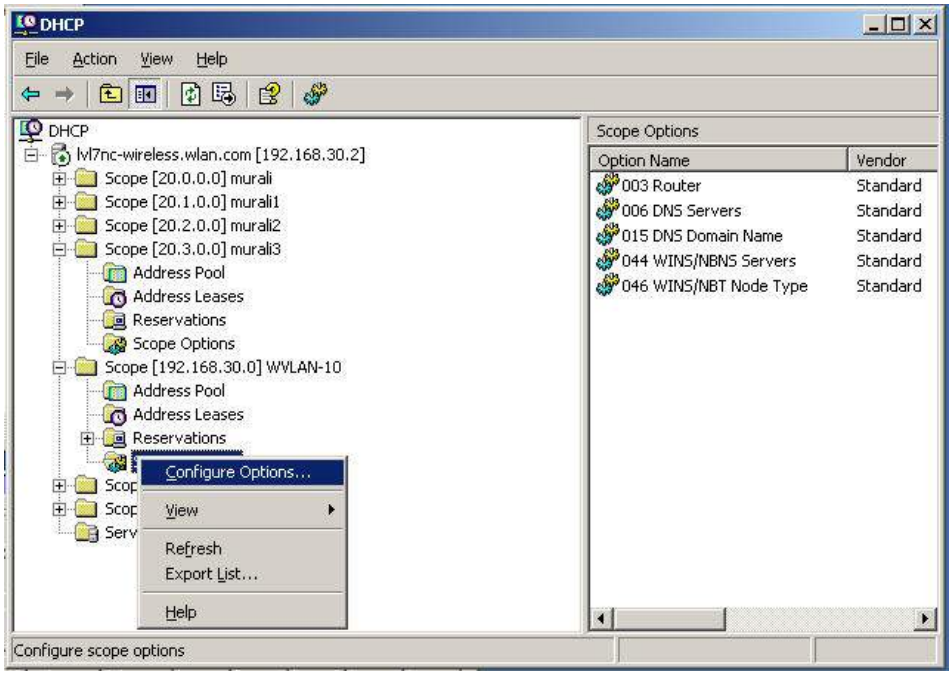
The AP can learn up to two switch IP addresses or DNS names through DHCP option 43 (the Vendor Information option) in the DHCP response. If you configured a static IP address in the AP, the AP ignores DHCP option 43.

Note: This discovery method only works if you configure the DHCP option before the AP receives its network information from the DHCP server.

The format for DHCP option 43 values are defined by RFC 2132.

The procedures to add the DHCP option to the DHCP server depend on the type of DHCP server you use on your network. If you use a Microsoft Windows 2000 or Microsoft Windows 2003 DHCP Server, you configure the scope you use with the access points with DHCP Option 43, as the following procedures describe.

1. From the DHCP manager, right-click the applicable scope and select **Configure Options...**



2. From the Available Options list, scroll to Option 43 and select the **043 Vendor Specific Info** check box.
3. Enter the Option 43 data into the Data Entry field.

   The format for DHCP option 43 values are defined by RFC 2132. To enter an IP address of 192.168.1.10 into the Binary column, you enter the data type code (01) and the address length (04), followed by the IP address in hexadecimal format. You repeat the data type and address length codes for each address you enter.

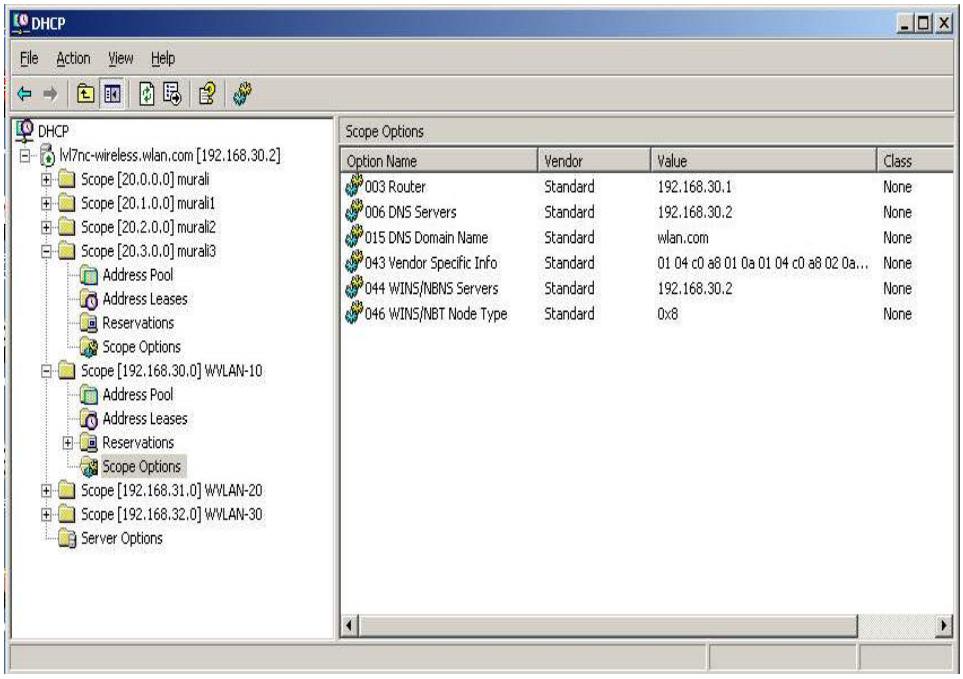
   Note: If you do not know the hexadecimal format for a specific IP address, use an IP address converter (dotted decimal-to-hex) available on the Internet.

   For example, to add the two switch IP addresses 192.168.1.10 and 192.168.2.10 to Option 43, you enter the following hexadecimal numbers into the Data Entry field:

   01 04 0C A8 01 0A 01 04 0C A8 02 0A

4. Click OK.

The following figure shows a scope with Option 43 configured.



Discovery and Peer Switches

When multiple peer switches are present in the network, you can control which switch or switches are allowed to discover a particular AP by the discovery method you use.

If you want to make sure that an AP is discovered by one specific switch, use one of the following methods:

- Disable L2 Discovery on all switches and configure the IP address of the AP in only one UWS.
- Configure the IP address of one UWS in the AP.
- Configure the DHCP option 43 with the IP address of only one UWS.

An alternative approach is to configure the RADIUS server to return a switch IP address during AP MAC address checking in the AP authentication process. If the RADIUS server indicates that the AP is a valid managed AP and returns an IP address of a switch that is not the same as this switch, then the switch sends a re-link message to the access point with the IP address of the wireless switch to which the AP should be talking to. When the AP gets the re-link message it modifies or sets the wireless switch IP address, breaks the TCP connection with the current switch and starts a new discovery process.

You can also configure the UWS so that each AP is allowed to be managed by any switch in a cluster. If the UWS that manages an AP goes down, one of the backup switches takes over the management responsibilities.

To use one or more switches as a backup for an AP, use one of the following discovery methods:

- If the AP and any of the peer switches are in the same L2 broadcast domain, L2 Discovery is enabled, and all the devices use the default VLAN settings, a peer switch will automatically discover the AP if the primary UWS becomes unavailable.
- Configure the IP address of the AP in multiple switches.

- Configure the IP address of one or more switches in the AP while it is in Standalone Mode. The number of configurable switches depends on the AP. For example you can configure up to four switches on the UAP, and up to two switches on the ECS5110-L.
- Configure the DHCP option 43 with the IP addresses of additional switches in the cluster.

Setup Wizard

From the tabs at the top of the *System* > **Setup Wizard** page, you can access the following pages:

- Wireless Global Configuration
- AP Image Settings
- Profile Configuration
- Radio Configuration
- VAP Configuration
- Valid AP Configuration
- Network Connectivity Configuration

Wireless Global Configuration

For the UWS to be able to discover and manage access points, both the WLAN switch and its operational status must be enabled. However, before you enable the WLAN switch, set the correct country code for the switch so that the access points can operate only in the modes permitted in your country. The default country code is US for operation in the United States. To set the country code and enable the switch by using the Web interface, click *System* **> Setup Wizard**.

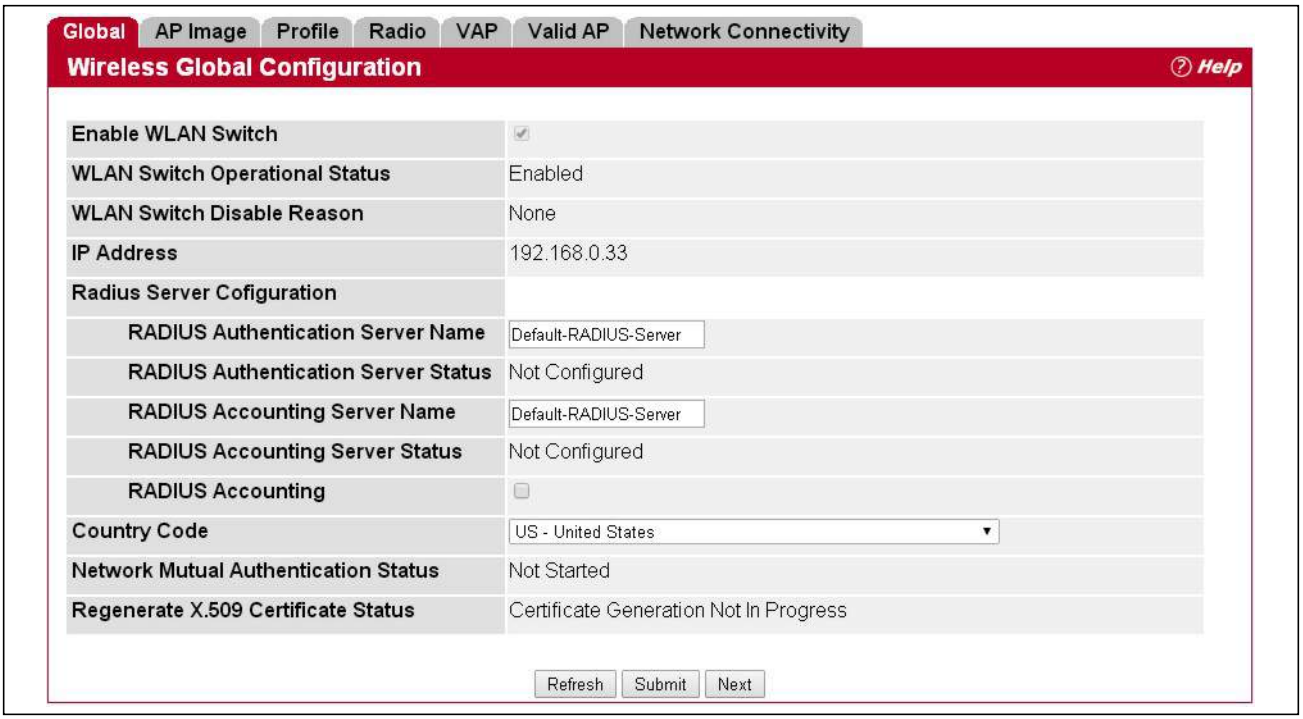


Figure 105: Wireless Global Configuration

The following table describes the fields available on the Wireless Global Configuration page.

Table 95: Basic Wireless Global Configuration

Field	*Description*
Enable WLAN Switch	Select this option to enable WLAN switching functionality on the system. Clear the option to administratively disable the WLAN switch. If you clear the option, all peer switches and APs that are associated with this switch are disassociated. Disabling the WLAN switch does not affect non-WLAN features on the switch, such as VLAN or STP functionality.
WLAN Switch Operational Status	Shows the operational status of the switch. The status can be one of the following values: • Enabled • Enable-Pending • Disabled • Disable-Pending If the status is pending, click **Refresh** to update the screen with the latest information.
WLAN Switch Disable Reason	If the status is disabled, this field appears and one of the following reasons is listed: • None: The cause for the disabled status is unknown. • Administrator disabled: The Enable WLAN Switch check box has been cleared. • No IP Address: The WLAN interface does not have an IP address. • No SSL Files: The UWS communicates with the APs it manages by using Secure Sockets Layer (SSL) connections. The first time you power on the UWS, it automatically generates a server certificate that will be used to set up the SSL connections. The SSL certificate and key generation typically completes within a few minutes.
IP Address	IP address of the switch.
RADIUS Server Configuration	
RADIUS Authentication Server Name	Enter the name of the RADIUS server used for AP and client authentications when a network-level RADIUS server is not defined on the **Basic Setup > VAP > Wireless Network Configuration** page. The name can contain up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted. The switch acts as the RADIUS client and performs all RADIUS transactions on behalf of the APs and wireless clients.
RADIUS Authentication Server Status	Indicates whether the RADIUS authentication server is configured. To configure RADIUS server information, go to **Security > RADIUS > Server Configuration**.
RADIUS Accounting Server Name	Enter the name of the RADIUS server used for reporting wireless client associations and disassociations when a network-level RADIUS accounting server is not defined on the **Basic Setup > VAP > Wireless Network Configuration** page. The name can contain up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted.
RADIUS Accounting Server Status	Indicates whether the RADIUS accounting server is configured. To configure RADIUS accounting server information, go to **Security > RADIUS > Accounting Server Configuration**.
RADIUS Accounting	Select this option to enable RADIUS accounting for wireless clients.

Table 95: Basic Wireless Global Configuration (Cont.)

Field	*Description*
Country Code	Select the country code that represents the country where your switch and APs operate. When you click **Submit**, a pop-up message asks you to confirm the change. Wireless regulations vary from country to country. Make sure you select the correct country code so that your WLAN system complies with the regulations in your country. ***Note:*** Changing the country code disables and re-enables the switch. Channel and radio mode settings that are invalid for the regulatory domain are reset to the default values. The country code (IEEE 802.11d) is transmitted in beacons and probe responses from the access points.
Network Mutual Authentication Status	The mutual authentication feature allows authentication between switches and APs and between peer switches. Mutual authentication is accomplished by using X.509 certificate exchange. This field shows the status of the mutual authentication feature. The field has one of the following values: • Not Started • In Progress—Mutual authentication is in the process of being enabled or disabled. • Complete Without Errors—The mutual authentication process finished without any problems. • Complete With Errors —Mutual authentication finished, but problems were detected. This means that you may need to provision some switches or APs separately.
Regenerate X.509 Certificate Status	Status of the request to generate an X.509 certificate. To initiate X.509 certificate generation, go to the **Advanced Configuration > Switch Provisioning** page. The field has one of the following values: • Certificate Generation is not in progress • Start Certificate Generation • Certificate Generation is in progress.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click System > System Utilities > Save All Applied Changes.
- **Next**—Navigates to the next page in the Setup Wizard configuration. Any changes you made to the current page are saved before the next page is displayed. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click System > System Utilities > Save All Applied Changes.

AP Image Settings

The UWS can upgrade software on the APs that it manages. The Cluster Controller can update code on APs managed by peer wireless switches.

A switch might manage APs that have different hardware types that require different software images. The AP Image page allows you to select the AP hardware for different images. The required AP image is derived from the AP hardware type.

To upgrade an Edge-Core AP from the switch that manages it, click the *System* **> Setup Wizard > AP Image** tab.

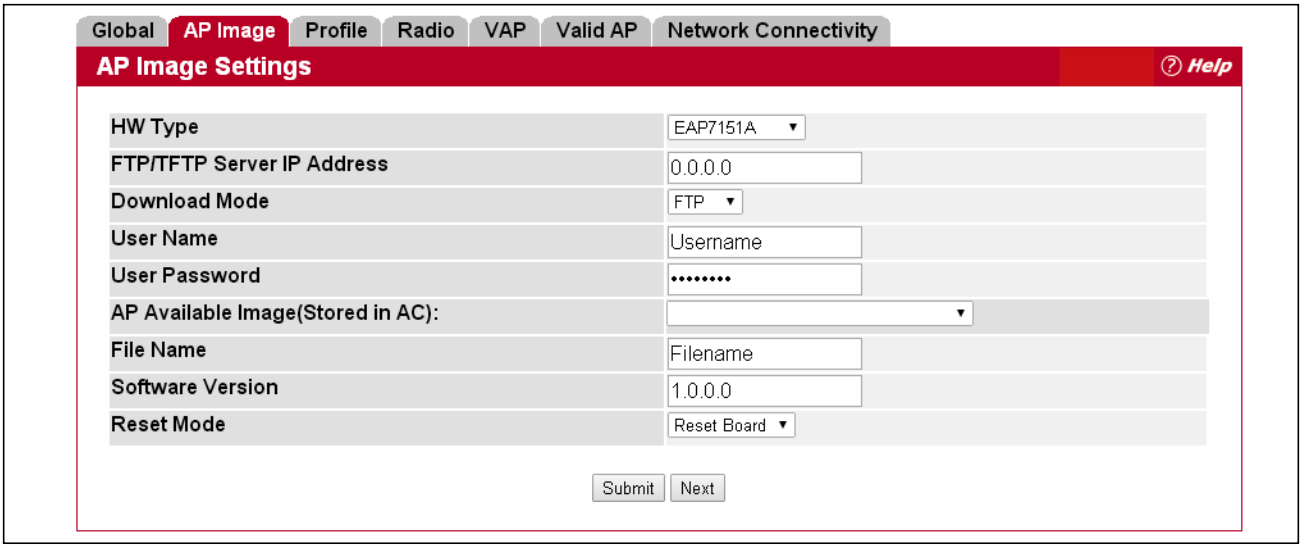


Figure 106: AP Image Settings

After you provide the information about the upgrade file, as described in the following table, click **Submit** to begin the upgrade process. Additional fields appear after the download begins and provide information about upgrade status and success.

Note: The APs automatically reset after the code is successfully downloaded and installed.

Table 96 describes the fields you must complete to upgrade APs.

Table 96: AP Image Settings

Field	*Description*
HW Type	Selects the AP hardware type.
FTP/TFTP Server IP Address	Enter the IP address of the host where the upgrade file is located. The host must have an FTP or TFTP server installed and running.
Download Mode	Selects FTP or TFTP as the download protocol, depending on the host server.
User Name	The FTP server access name.
User Password	The FTP server access password.
AP Available Image (Stored in AC)	Shows the AP images which have been stored in the switch using the System > System Utilities > Upload File to Switch page.

Table 96: AP Image Settings (Cont.)

Field	*Description*
File Name	Enter the name of the upgrade file. You may enter up to 32 characters, and the file extension must be included. Edge-Core APs with a hardware type that requires this software will use this file name.
Software Version	A string of up to 32 characters that identify the software version on the server. If the code on the AP is a different version, the AP will upgrade itself automatically.
Reset Mode	Specifies the AP restart mode after the software is downloaded: • **Reset Board**. Restarts the AP using the current saved configuration.

Command Buttons

The page includes the following buttons:

- **Submit**—Initiates the software download.
- **Next**—Navigates to the next page in the Setup Wizard configuration. Any changes you made to the current page are saved before the next page is displayed. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click System > System Utilities > Save All Applied Changes.

Profile Configuration

The switch can support APs that have different hardware capabilities, such as the supported number of radios and the supported IEEE 802.11 modes. APs that use the same profile should have the same hardware capabilities so that the settings you configure in the profile are valid for all APs within the profile. Different hardware platforms might also require different software images.

You configure the default radio settings from the *System* **> Setup Wizard > Profile** tab, which the following figure shows.

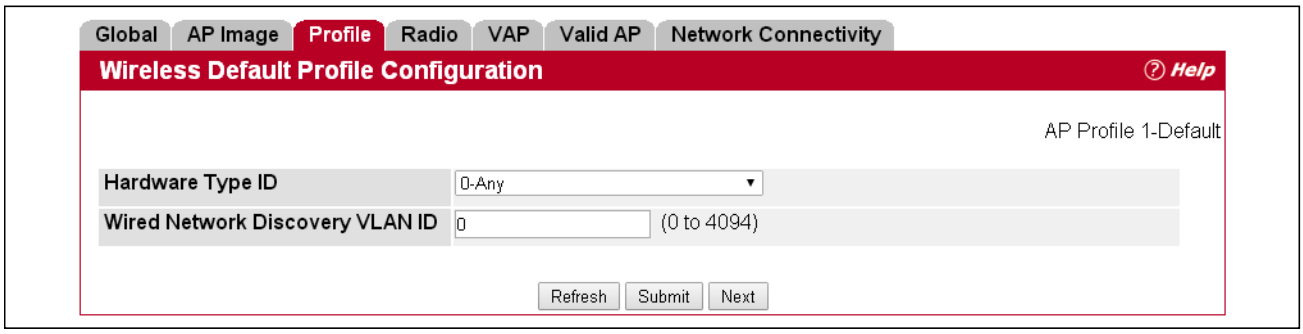


Figure 107: AP Hardware Capabilities

Table 97 describes the fields available on the Profile page.

Table 97: Profile

Field	*Description*
Hardware Type ID	Select the hardware type for the APs that use this profile. The hardware type is determined, in part, by the number of radios the AP supports (single or dual) and the IEEE 802.11 modes that the radio supports (a/b/g, a/b/g/n, or a/n/ac). The options available in the Hardware Type ID are as follows: • Any • MJ Dual Radio a/b/g • MJ Single Radio a/b/g • MJ Dual Radio a/b/g/n • MJ Single Radio a/b/g/n • Enterprise Dual Radio a/b/g/n • Enterprise Single Radio a/b/g/n • AP-64 Dual Radio a/b/g/n • ECW7220-L AP Dual Radio anac/bgn • ECWO7220-L OAP Dual Radio anac/bgn • EAP7151A Single Radio b/g/n • EAP7011CA Single Radio b/g/n • EAP9012CA Dual Radio a/b/g/n • OAP9112CA Dual Radio a/b/g/n • EAP7015A Single Radio b/g/n • EAP7315A Single Radio b/g/n • EAP7311A Single Radio b/g/n • EAP9012A Dual Radio a/b/g/n
Wired Network Discovery VLAN ID	Enter the VLAN ID that the AP uses to send tracer packets in order to detect APs connected to the wired network. The tracer packets help APs identify unauthorized APs that do not belong to the Unified Wireless Switch but are connected to the wired network.

To add a new profile, go to the **WLAN** > **WLAN Configuration > AP Profiles** page, enter a name for the new profile in the available field, and click **Add**.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click System > System Utilities > Save All Applied Changes.
- **Next**—Navigates to the next page in the Setup Wizard configuration. Any changes you made to the current page are saved before the next page is displayed. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click System > System Utilities > Save All Applied Changes.

Radio Configuration

To accommodate a broad range of wireless clients and wireless network requirements, the AP can support up to two radios. Each radio can broadcast in one of the following modes:

- IEEE 802.11a mode
- IEEE 802.11b and IEEE 802.11g modes
- IEEE 802.11a and IEEE 802.11n modes
- IEEE 802.11a and IEEE 802.11n modes
- IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n modes
- IEEE 802.11a, IEEE 802.11n, and IEEE 802.11ac modes
- 5 GHz IEEE 802.11n mode
- 2.4 GHz IEEE 802.11n mode

By default, Radio 1 operates in the IEEE 802.11b/g/n mode, and Radio 2 operates in the IEEE 802.11a/n/ac mode. The difference between these modes is the frequency in which they operate. IEEE 802.11b/g/n operates in the 2.4 GHz frequency, and IEEE 802.11a/n/ac operates in the 5 GHz frequency of the radio spectrum.

You configure the default radio settings from the *System* **> Setup Wizard > Radio** tab, which the following figure shows.

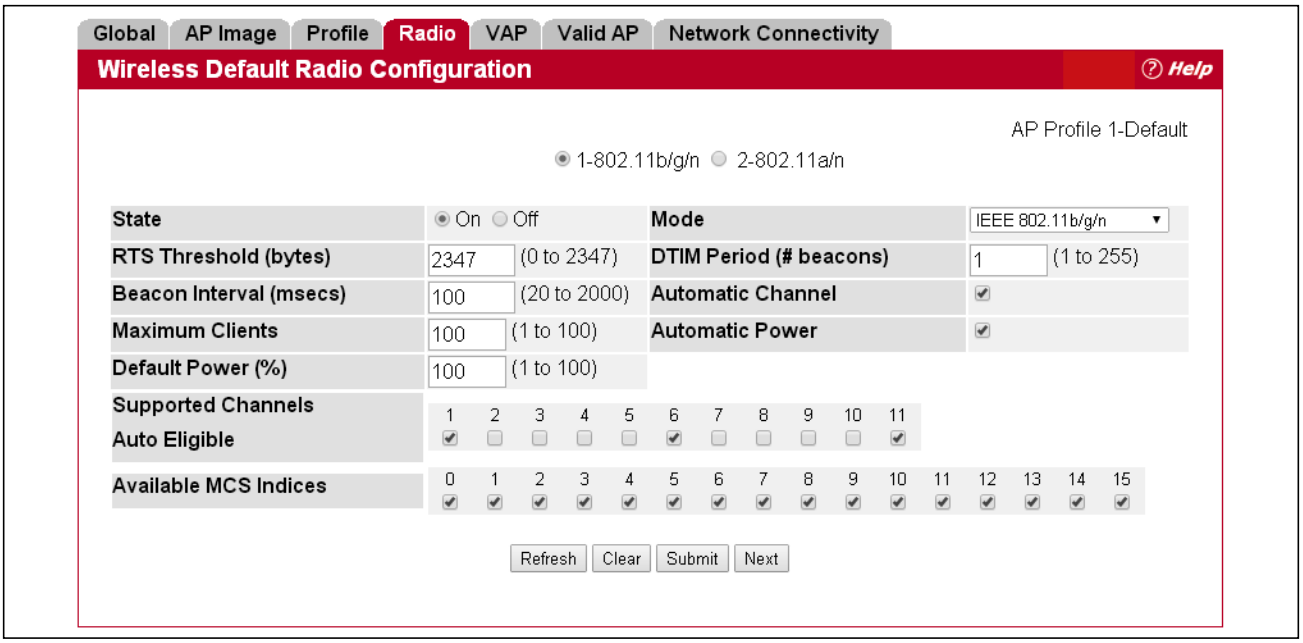


Figure 108: Radio Settings

The following table describes the fields you can configure from the **Radio** tab on the **Setup Wizard** page. To change the settings on this page, you must first select the radio you want to configure (1 or 2). After you change the settings, click **Submit** to apply the settings. Changes to the settings apply only to the selected radio.

Table 98: Radio Settings

Field	*Description*
1-802.11b/g/n **2-802.11a/n/ac**	From this field, you can select the radio that you want to configure. By default, Radio 1 operates in IEEE 802.11b/g/n mode, and Radio 2 operates in IEEE 802.11a/n/ac mode. If you change the mode, the labels for the radios change accordingly. Changes to the settings apply only to the selected radio.
State	Specify whether you want the radio on or off by clicking **On** or **Off**. If you turn off a radio, the AP sends disassociation frames to all the wireless clients it is currently supporting so that the radio can be gracefully shut down and the clients can start the association process with other available APs.
Mode	The Mode defines the Physical Layer (PHY) standard the radio uses. Select one of the following modes for each radio interface: • **IEEE 802.11a** is a PHY standard that specifies operating in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 6 to 54 Mbps. • I**EEE 802.11b/g** operates in the 2.4 GHz ISM band. IEEE 802.11b is an enhancement of the initial 802.11 PHY to include 5.5 Mbps and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps. IEEE 802.11g is a higher speed extension (up to 54 Mbps) to the 802.11b PHY. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps. • **IEEE 802.11a/n/ac** operates in the 5 GHz ISM band and includes support for 802.11a, 802.11n, and 802.11ac devices. IEEE 802.11n is an extension of the 802.11 standard that includes multiple-input multiple-output (MIMO) technology. IEEE 802.11n supports data ranges of up to 248 Mbps and nearly twice the indoor range of 802.11 b, 802.11g, and 802.11a. 802.11ac has expected multi-station WLAN throughput of at least 1 Gigabit per second and a single link throughput of at least 500 megabits per second (500 Mbit/s). This is accomplished by using wider RF bandwidth (up to 160 MHz), more MIMO spatial streams (up to eight), downlink multi-user MIMO (up to four clients), and high-density modulation (up to 256-QAM). • **IEEE 802.11b/g/n** operates in the 2.4 GHz ISM band and includes support for 802.11b, 802.11g, and 802.11n devices. • **5 GHz IEEE 802.11n** is the recommended mode for networks with 802.11n devices that operate in the 5 GHz frequency that do not need to support 802.11a or 802.11b/g devices. IEEE 802.11n can achieve a higher throughput when it does not need to be compatible with legacy devices (802.11b/g or 802.11a). • **2.4 GHz IEEE 802.11n** is the recommended mode for networks with 802.11n devices that operate in the 2.4 GHz frequency that do not need to support 802.11a or 802.11b/g devices. IEEE 802.11n can achieve a higher throughput when it does not need to be compatible with legacy devices (802.11b/g or 802.11a).

Table 98: Radio Settings (Cont.)

Field	*Description*
RTS Threshold	Specify a Request to Send (RTS) Threshold value between 0 and 2347. The RTS threshold indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed. Changing the RTS threshold can help control traffic flow through the AP, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.
DTIM Period	The Delivery Traffic Information Map (DTIM) message is an element included in some Beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the access point awaiting pickup. The DTIM period you specify indicates how often the clients served by this access point should check for buffered data still on the AP awaiting pickup. Specify a DTIM period within the given range (1–255). The measurement is in beacons. For example, if you set this field to 1, clients will check for buffered data on the AP at every beacon. If you set this field to 10, clients will check on every 10th beacon.
Beacon Interval	Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second). The Beacon Interval value is set in milliseconds. Enter a value from 20 to 2000.
Automatic Channel	The channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface. When the AP boots, the AP scans the RF area for occupied channels and selects a channel from the available non-interfering or clear channels. However, channel conditions can change during operation. Enabling the **Automatic Channel** makes APs assigned to this profile eligible for auto-channel selection. You can automatically or manually run the auto-channel selection algorithm to allow the UWS to adjust the channel on APs as WLAN conditions change. By default, the global auto-channel mode is set to manual. To enable the automatic channel selection mode, go to the **AP Management > RF Management** page and select Fixed or Interval for the Channel Plan mode. You can also run the automatic channel selection algorithm manually from the **Manual Channel Plan** page. ***Note:*** If you assign a static channel to an AP in the Valid AP database or on the Advanced AP Management page, the AP will not participate in the auto-channel selection.
Maximum Clients	Specify the maximum number of stations allowed to associate with this access point at any one time. You can enter a value between 1 and 100.

Table 98: Radio Settings (Cont.)

Field	*Description*
Automatic Power	The power level affects how far an AP broadcasts its RF signal. If the power level is too low, wireless clients will not detect the signal or experience poor WLAN performance. If the power level is too high, the RF signal might interfere with other APs within range. Automatic power uses a proprietary algorithm to automatically adjust the RF signal to broadcast far enough to reach wireless clients, but not so far that it interferes with RF signals broadcast by other APs. The power level algorithm increases or decreases the power level in 10% increments based on presence or absence of packet retransmission errors.
Default Power	The automatic power algorithm will not reduce the power below the number you set in the default power field. By default, the power level is 100%. Therefore, even if you enable the automatic power, the power of the RF signal will not decrease. The power level is a percentage of the maximum transmission power for the RF signal.
Supported Channels	This field displays the channels that are supported for the radio mode currently selected on the page and for the country configured on the **Global Wireless Settings** page.
Auto Eligible	Select the **Auto Eligible** option beneath each channel to include the channel in the automatic channel assignment process.
Available MCS Indices	This field shows the Modulation and Coding Scheme (MCS) index values supported by the radio. Each index can be enabled and disabled independently.

Note: If you access the Access Point Profile Radio configuration through the **Radio** tab for a profile from the **WLAN** > **WLAN Configuration > AP Profiles** page, additional fields are available for configuration.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Clear**—Resets the settings on the page to the default values.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP).
- **Next**—Navigates to the next page in the Setup Wizard configuration. Any changes you made to the current page are saved to the running configuration (but not startup configuration) before the next page is displayed.

VAP Configuration

The **VAP** tab displays the virtual access point (VAP) settings associated with the default AP profile. Each VAP has an associated network, which is identified by its network number and Service Set Identifier (SSID). You can configure and enable up to 16 VAPs per radio on each physical access point.

You configure default Valid Access Point settings from the *System* **> Setup Wizard > VAP** tab, which the following figure shows.

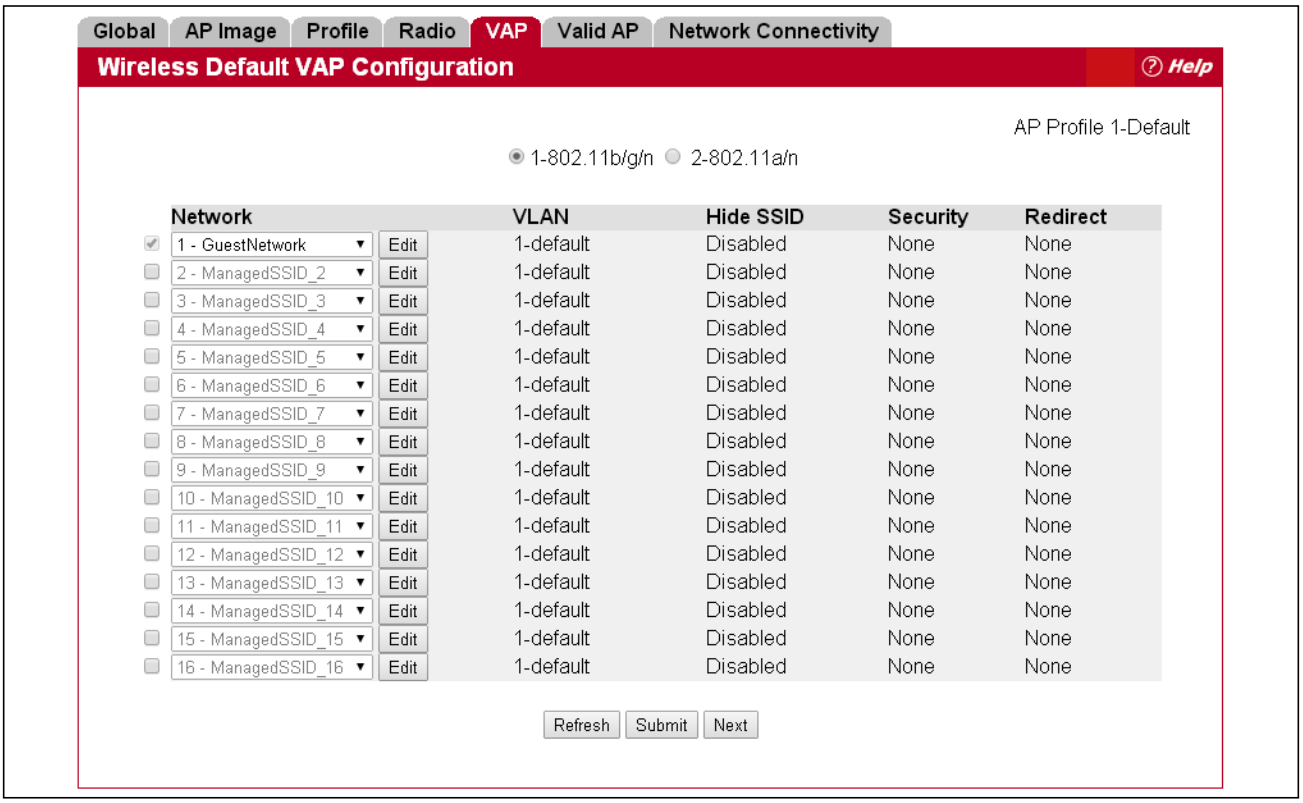


Figure 109: VAP Settings

VAPs segment the wireless LAN into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. To a wireless client, each VAP appears to be a single physical access point. However, since the VAPs use the same channel, there is no risk of RF interference among the networks that are on a single AP.

VAPs can help you maintain better control over broadcast and multicast traffic, which affects network performance. You can also configure different security mechanisms for each VAP.

A VAP is a physical entity. Each VAP maps directly to a MAC address. A network is a logical entity that you apply to a VAP. Networks are identified by a network number and an associated SSID. The SSID does not need to be unique for each network. You can create and modify a network in one place and apply the network to one or more VAP as needed. This allows you to mix networks within different profiles without having to reconfigure everything. When you edit a network configuration that is applied to more than one VAP, you edit it for every VAP that uses the network.

Managing Virtual Access Point Configuration

The Default AP profile has one VAP on each radio enabled by default. The default VAP uses the Guest Network SSID, and there is no security to prevent wireless clients from associating with the VAP. To enable additional VAPs, select the check box next to the VAP. Once you enable a VAP, you can select the network (SSID) to use from the drop-down menu. To change Network settings, click **Edit**.

The following table describes the fields on the **VAP** page.

Table 99: Default VAP Configuration

Field	*Description*
Radio 1 **Radio 2**	You configure the VAPs for Radio 1 and Radio 2 separately. Select the radio to configure the settings for before you enable the VAP.
Network	Use the option to the left of the network to enable or disable the corresponding VAP on the selected radio. When enabled, use the menu to select a networks to assign to the VAP. You can configure up to 250 separate networks on the switch and apply them across multiple radio and VAP interfaces. By default, 16 networks are pre-configured and applied in order to the VAPs on each radio. Enabling a VAP on one radio does not automatically enable it on the other radio. ***Note:*** You cannot disable the default VAP, VAP0. To configure additional networks, click **WLAN** > **WLAN Configuration > Networks**.
Edit	Click **Edit** to modify settings for the corresponding network. When you click **Edit**, the Wireless Network Configuration page appears.
VLAN	Shows the VLAN ID of the VAP. To change this setting, click **Edit**.
Hide SSID	Shows whether the VAP broadcasts the SSID. If enabled, the SSID for this network is not included in AP beacons. To change this setting, click **Edit**.
Security	Shows the current security settings for the VAP. To change this setting, click **Edit**.
Redirect	Shows whether HTTP redirect is enabled. The possible values for the field are as follows: • HTTP: HTTP Redirect is enabled • None: HTTP Redirect is disabled

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click System > System Utilities > Save All Applied Changes.
- **Next**—Navigates to the next page in the Setup Wizard configuration. Any changes you made to the current page are saved before the next page is displayed. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click System > System Utilities > Save All Applied Changes.

Configuring the Default Network

Each network is identified by its Service Set Identifier (SSID), which is an alphanumeric key that identifies a wireless local area network. You can configure up to 64 different networks on the UWS. Each network can have a unique SSID, or you can configure multiple networks with the same SSID.

When you click **Edit** for one of the networks that display on the VAP page, the Wireless Network Configuration page appears, as the following figure shows.

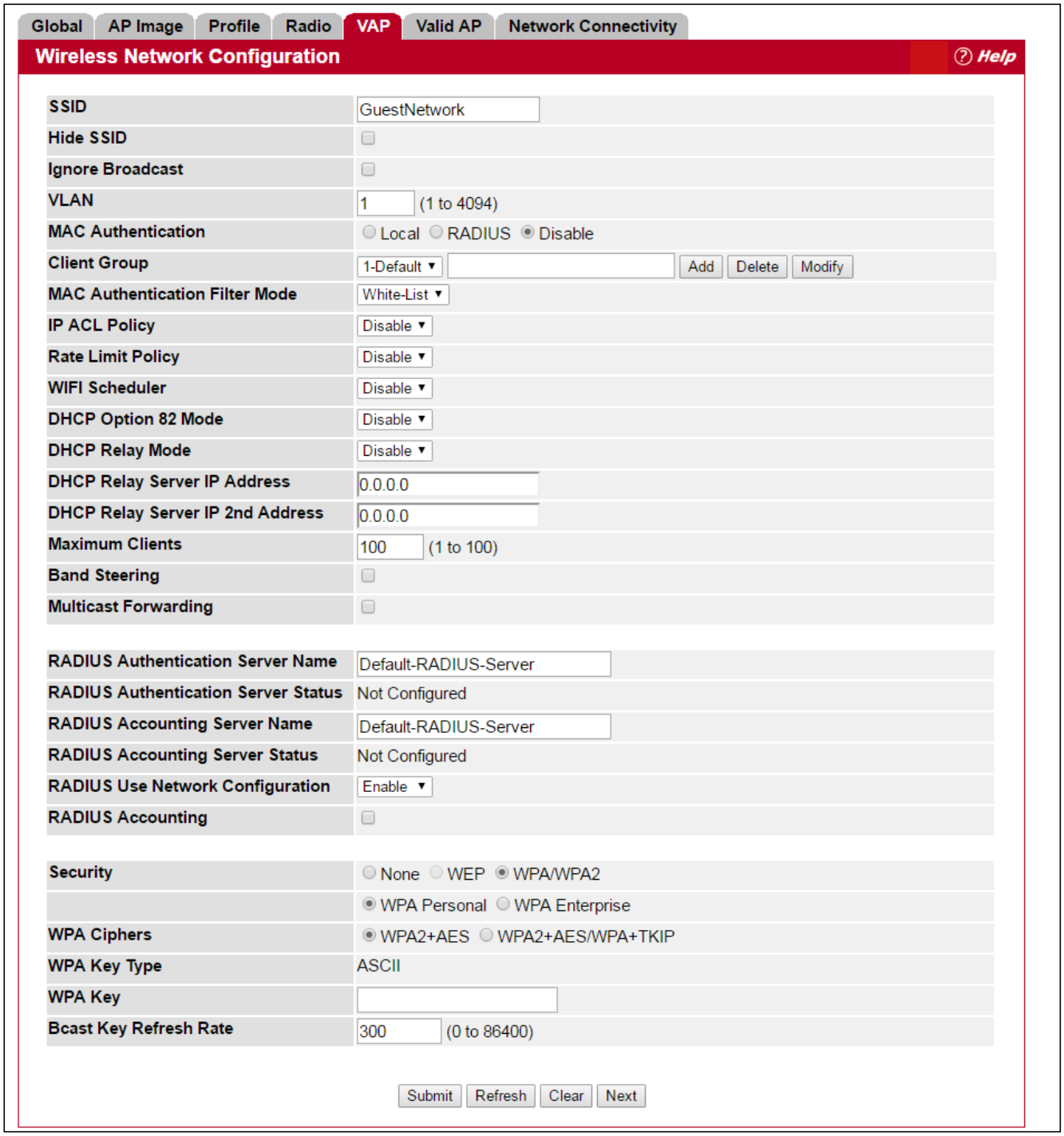


Figure 110: Configuring Network Settings

The following table describes the fields on the Wireless Network Configuration page. After you change the wireless network settings, click **Submit** to save the changes.

Table 100: Wireless Network Configuration

Field	*Description*
SSID	Wireless clients identify a wireless network by the SSID, which is an alphanumeric key that uniquely identifies a wireless local area network. The SSID can be up to thirty-two characters in length, and there are no restrictions on the characters that may be used in an SSID.
Hide SSID	You can hide the SSID broadcast to discourage stations from automatically discovering your access point. When the broadcast SSID of the AP is hidden, the network name is not displayed in the list of available networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it is able to connect. Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect, or monitor unencrypted traffic. Hiding the SSID offers a very minimal level of protection on an otherwise exposed network (such as a guest network) where the priority is making it easy for clients to get a connection and where no sensitive information is available.
Ignore Broadcast	If a wireless client broadcasts probe requests to all available SSIDs, this option controls whether the AP will respond to the probe request. • Select this option to prohibit the AP from responding to client probe requests • Clear this option to allow the AP to respond to client probe requests.
VLAN	A virtual LAN (VLAN) is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be. The nodes in a VLAN share resources and bandwidth and are isolated on that network. The Unified Wireless Switch supports the configuration of a wireless VLAN. You can configure each VAP to be on a unique VLAN or on the same VLAN as other VAPs. When a wireless client connects to the AP by using this network (SSID), the AP tags the client's traffic with the VLAN ID you configure in this field. By default, all networks use VLAN 1, which is also untagged by default. ***Note:*** The VLAN ID you configure in this field can be overwritten by the VLAN ID configured for the AP in the RADIUS server. In other words, if your network uses a RADIUS server to assign wireless clients to VLANs, the wireless client uses the VLAN ID from the RADIUS server and ignores the VLAN ID configured on the VAP.
MAC Authentication	If you enable MAC authentication, wireless clients must be authenticated by the AP in order to connect to the network. To use MAC authentication, configure the client MAC addresses in one of the following databases: • Local • RADIUS In the database, you set a default action to either accept or deny that client or use the global action configured on the **Advanced Configuration > Global** page. MAC authentication is useful in networks that operate in Open mode to grant or deny access to clients with specific MAC addresses. MAC Authentication can also be used in conjunction with 802.1X security methods, in which case the MAC Authentication is done prior to the 802.1X authentication.
Client Group	The name of a group of clients (VAP) to which the settings on this page apply.
MAC Authentication Filter Mode	Uses black list of prohibited clients, or white list of allowed clients. If white list is selected, any clients not in the list are prohibited access to the AP.

Table 100: Wireless Network Configuration (Cont.)

Field	*Description*
IP ACL Policy	Enables or disables IP address filtering for the profile. See "IP ACL Configuration" on page 220.
Rate Limit Policy	Selects a rate limit policy which sets the maximum transfer rate between the AP VAP and the client based on address or other QoS parameters. See "Rate Limit Configuration" on page 225
WIFI Scheduler	Selects an ACL policy which impose a limitation on the time range during which the WLAN is enabled. See "WIFI Scheduler" on page 223.
DHCP Option 82 Mode	When DHCP Option82 is enabled, the UWS sends information about its DHCP clients to the DHCP server. When enabled, the client will get an IP address from the DHCP server according to its VLAN ID.
DHCP Relay Mode	Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients that broadcast a request. To receive the broadcast request, the DHCP server would normally have to be on the same subnet as the client. However, when the DHCP relay agent is enabled, received client requests can be forwarded directly to a known DHCP server on another subnet. Responses from the DHCP server are returned to the switch, which then broadcasts them back to clients.
DHCP Relay Server IP Address	The IP address of the DHCP relay server.
DHCP Relay Server IP 2nd Address	The IP address of a secondary DHCP server to be used if the first DHCP server does not repond.
Maximum Clients	Specifies the maximum number of stations allowed to associate with this access point at any one time. You can enter a value between 0 and 100.
Band Steering	The band steering mode allows higher connection priority for clients using the 5GHz band. Use the menu to enable or disable the mode.
Multicast Forwarding	Enables or disables multicast forwarding. Use the menu to enable or disable the mode.
RADIUS Authentication Server Name	Enter the name of the RADIUS server that the VAP uses for AP and client authentications. The name can contain up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted. Any RADIUS information you configure for the wireless network overrides the global RADIUS information configured on the **Wireless Global Configuration** page. The switch acts as the RADIUS client and performs all RADIUS transactions on behalf of the APs and wireless clients.
RADIUS Authentication Server Status	Indicates whether the RADIUS authentication server is configured for the VAP. To configure RADIUS server information, go to the **Security > RADIUS > Server Configuration** page.
RADIUS Accounting Server Name	Enter the name of the RADIUS server that the VAP uses for reporting wireless client associations and disassociations. The name can contain up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted. Any RADIUS information you configure for the wireless network overrides the global RADIUS information configured on the **Wireless Global Configuration** page.
RADIUS Accounting Server Status	Indicates whether the RADIUS accounting server is configured. To configure RADIUS accounting server information, go to **Security > RADIUS > Accounting Server Configuration**.

Table 100: Wireless Network Configuration (Cont.)

Field	*Description*
RADIUS Use Network Configuration	This field controls whether the VAP uses the network RADIUS settings or the global RADIUS settings. • Enable: Use RADIUS Servers defined on the Wireless Network Configuration page. • Disable: Use RADIUS servers defined on the Wireless Global Configuration page.
RADIUS Accounting	Select this option to enable RADIUS accounting for wireless clients.
Security	The default AP profile does not use any security mechanism by default. To protect your network, Edge-Core strongly recommends that you select a security mechanism so that unauthorized wireless clients cannot gain access to your network. The following WLAN network security options are available: • None • WEP • WPA/WPA2 If you select WEP or WPA/WPA2 as your security mechanism, additional fields appear. "Configuring AP Security" on page 199 describes the security mechanisms and the additional fields you can configure if you select WEP or WPA/WPA2.

Configuring AP Security

The Default AP profile does not use any security mechanism by default. To protect your network, Edge-Core strongly recommends that you select a security mechanism so that unauthorized wireless clients cannot gain access to your network.

From the **VAP** tab of the **Wireless Network Configuration** page, you can select **None**, **WEP** or **WPA/WPA2** as the WLAN security mechanisms, as the following figure shows. The default is **None**.

Figure 111: AP Network Security Options

The following sections describe the security mechanicians.

Using No Security

If you select **None** as your security mode, no further options are configurable on the AP. This mode means that any data transferred between the AP and the associated wireless clients is not encrypted, and any wireless client can associate with the AP.

This security mode can be useful during initial network configuration or for problem solving, but it is not recommended for regular use on the internal network because it is not secure.

Using Static WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. If you select this security mechanism, all wireless clients and access points on the network are configured with a 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

Static WEP is not the most secure mode available, but it offers more protection than setting the security mode to **None** as it does prevent an outsider from easily sniffing out unencrypted wireless traffic.

WEP encrypts data moving across the wireless network based on a static key. (The encryption algorithm is a stream cipher called RC4.)

If you select WEP as the Security Mode, additional fields display, as the following figure shows.

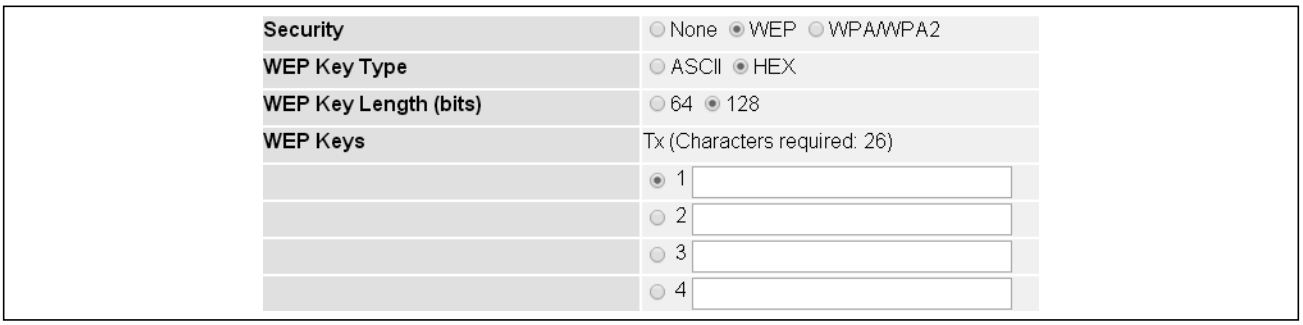


Figure 112: Static WEP Configuration

Table 101 describes the configuration options for WEP.

Table 101: Static WEP

Field	*Description*
Static WEP	Static WEP uses static key management. You manually configure the same keys to encrypt data on both the wireless client and the AP.
WEP Key Type	Select the key type by clicking one of the radio buttons: • ASCII: Includes upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #. • HEX: Includes digits 0 to 9 and the letters A to F.

Table 101: Static WEP (Cont.)

Field	*Description*
WEP Key Length	Specify the length of the key by clicking one of the radio buttons: • 64 bits • 128 bits
Tx	The Transfer Key Index indicates which WEP key the access point uses to encrypt the data it transmits. To select a transfer key, click the button located between the key number and the field where you enter the key.
WEP Keys	You can specify up to four WEP keys. In each text box, enter a string of characters for each key. These are the RC4 WEP keys shared with the stations using the access point. Use the same number of characters for each key. The number of keys you enter depends on the Key Type and Key Length. The following list shows the number of keys to enter in the field: • 64 bit: ASCII: 5 characters; Hex: 10 characters • 128 bit: ASCII: 13 characters; Hex: 26 characters Each client station must be configured to use one of these same WEP keys in the same slot as specified here on the AP.

Static WEP Rules

If you use Static WEP, the following rules apply:

- All client stations must have the Wireless LAN (WLAN) security set to WEP and all clients must have one of the WEP keys specified on the AP in order to de-code AP-to-station data transmissions.
- The AP must have all keys used by clients for station-to-AP transmit so that it can de-code the station transmissions.
- The same key must occupy the same slot on all nodes (AP and clients). For example if the AP defines *abc12* key as WEP key 3, then the client stations must define that same string as WEP key 3.
- Client stations can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)
- On some wireless client software, you can configure multiple WEP keys and define a client station “transfer key index”, and then set the stations to encrypt the data they transmit using different keys. This ensures that neighboring APs cannot decode each other’s transmissions.
- You cannot mix 64-bit, 128-bit, and 152-bit WEP keys between the access point and its client stations.

Using WPA/WPA2 Personal or Enterprise

WPA and WPA2 are Wi-Fi Alliance IEEE 802.11i standards, which include AES-CCMP and TKIP mechanisms. The WPA/WPA2 Personal employs a pre-shared key to perform an initial check of credentials. The WPA/WPA2 Enterprise security uses a RADIUS server to authenticate users.

Note: The 802.11n clients cannot use the TKIP cipher. Therefore if only TKIP is enabled then the 802.11 clients will not be able to authenticate with the network.

If you select WPA/WPA2 as the security mode, additional fields display, as the following figure shows.

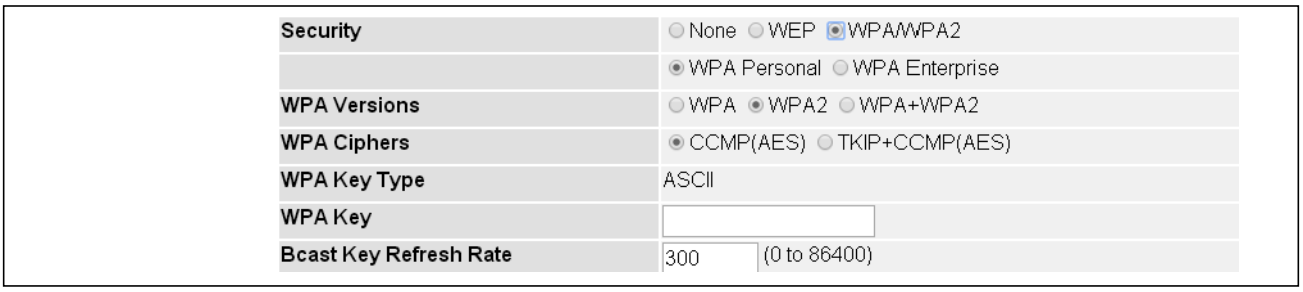


Figure 113: WPA Personal Configuration

The following table describes the configuration options for the WPA Personal and WPA Enterprise security mode.

Table 102: WPA Security

Field	*Description*
WPA Personal or WPA Enterprise	WPA/WPA2 Personal uses static key management. You manually configure the same keys to encrypt data on both the wireless client and the AP. WPA/WPA2 Enterprise uses a RADIUS server and dynamically generated keys to encrypt client-to- AP traffic. WPA Enterprise is more secure than WPA Personal, but you need a RADIUS server to manage the keys. If you select WPA Enterprise, the screen refreshes, and the WPA Key Type and WPA Key fields are hidden. The AP uses the global RADIUS server or the RADIUS server you specify for the wireless network For information about how to configure the global RADIUS server settings on the UWS, see "WLAN Switch Configuration" on page 214.
WPA Versions	Select the types of client stations you want to support: • WPA: If all client stations on the network support the original WPA but none support the newer WPA2, then select WPA. • WPA2: If all client stations on the network support WPA2, Edge-Core suggests using WPA2 which provides the best security per the IEEE 802.11i standard. • WPA + WPA2: If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select this box. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.
WPA Ciphers	Select the cipher suite you want to use: • CCMP (AES) • TKIP + CCMP (AES) Both TKIP and AES clients can associate with the access point. WPA clients must have one of the following to be able to associate with the AP: • A valid TKIP key • A valid AES-CCMP key ***Note:*** The 802.11n clients cannot use the TKIP cipher. Therefore if only TKIP is enabled then the 802.11 clients will not be able to authenticate with the network.
WPA Key Type	The key type is ASCII, which includes upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.

Table 102: WPA Security (Cont.)

Field	*Description*
WPA Key	The WPA Key is the shared secret key for WPA Personal. Enter a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.
Bcast Key Refresh Rate	Enter a value to set the interval at which the broadcast (group) key is refreshed for clients associated to this VAP. The valid range is 0-86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.
Additional Fields for WPA/WPA2 Enterprise	
Pre-Authentication	If you select WPA/WPA2 Enterprise, you can enable Pre-Authentication. Click the **Pre-Authentication** check box if you want WPA2 wireless clients to send pre-authentication packets. The pre-authentication information is relayed from the access point the client is currently using to the target access point. Enabling this feature can help speed up authentication for roaming clients who connect to multiple access points. Only clients that connect by using WPA2 can use this feature. It is not supported by the original WPA.
Pre-Authentication Limit	Enter the number of pre-authentications that can be in progress simultaneously on an AP. The limit prevents too much load on the RADIUS server. This does not prevent the pre-authentication from being attempted again when the load is lighter. A value of 0 represents no limit.
Key Caching Hold Time	Enter the amount of minutes a PMK will be held by the AP. This applies to Pairwise Master Keys (PMKs) generated by RADIUS, those that come from pre-authentication, and those that are forwarded to the AP. Note that this time limit can be overridden by RADIUS if the RADIUS server returns a longer time in the Session-Timeout attribute for a particular user. The valid values of this are from 1–1440 minutes. If you do not enter a value, APs will not forward the PMK for the wireless client to other APs in case the client roams to another AP.
Session Key Refresh Rate	Enter a value to set the interval at which the AP will refresh session (unicast) keys for each client associated to the VAP. The valid range is 0-86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).
- **Refresh**—Updates the page with the latest information.
- **Clear**—Resets the settings on the page to the default values.
- **Next**—Navigates to the next page in the Setup Wizard configuration. Any changes you made to the current page are saved before the next page is displayed. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click System > System Utilities > Save All Applied Changes.

Valid AP Configuration

The VAP tab contains a field to select whether to use a local or RADIUS database for AP Validation. When you click the **Valid AP** tab, the Valid Access Point Summary page displays information about APs configured in the local database. If AP Validation is set to RADIUS on the VAP tab, information about the APs to be managed by the switch must be added to the external RADIUS database.

Adding a Valid Access Point

You can add an AP into the local list of Valid APs from the **Setup Wizard > Valid Access Point Summary > Valid VAP** tab, as the following figure shows, or you can add an AP from the AP Authentication Failures or Rogue AP/RF Scan lists.

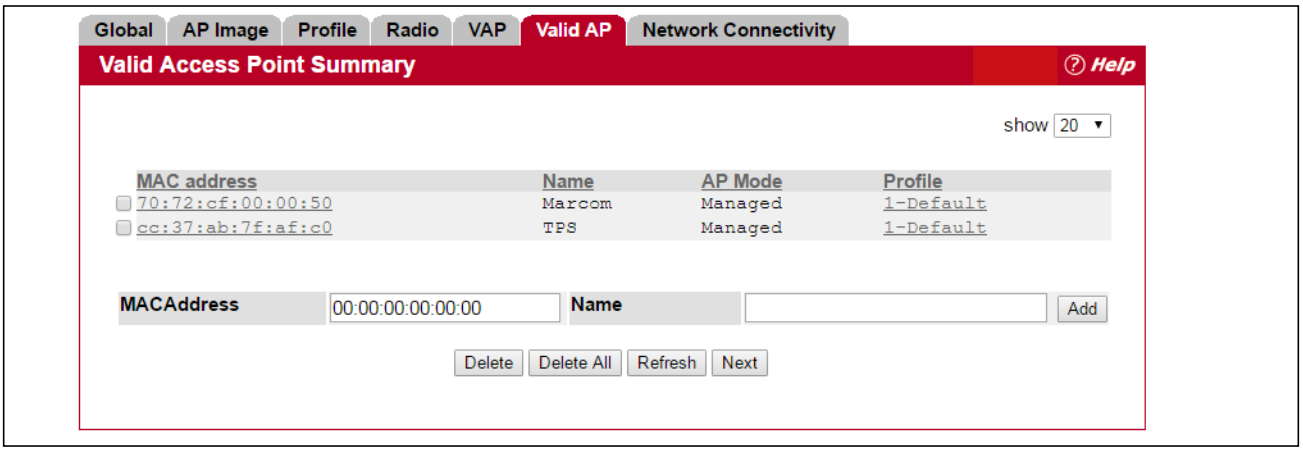


Figure 114: Adding a Valid AP

Table 103: Local Access Point Database

Field	*Description*
MAC Address	Enter the MAC address of the AP in this field. When you add the MAC address, you add the AP to the local database on the switch.
Name	Enter a name to help identify the AP. This field is optional and accepts up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted.
AP Mode	This field displays the current mode of the AP, which can be one of the following: • Managed • Standalone • Rogue To configure a different mode, click the MAC address of the AP to go to the Valid Access Point Configuration page.
Profile	This field displays the AP profile assigned to the AP. To assign a different profile to the AP, click the MAC address of the AP to go to the Valid Access Point Configuration page. Click the profile name to access the configuration pages for the profile.

After you enter the MAC address and location of the AP to add to the list, click **Add** to add the AP to the database and to access the configuration page for the AP. For an AP that is already in the database, click the MAC address of the AP to access its configuration page.

Command Buttons

The page includes the following buttons:

- **Add**—Adds the AP MAC Address and Name to the local Valid AP database.
- **Delete**—Deletes any selected APs from the local Valid AP database. This button is available if the check box next to at least one AP MAC address is selected. Managed APs must be reset to complete their removal from the Valid AP database.
- **Delete All**—Deletes all APs from the local Valid AP database. Managed APs must be reset to complete their removal from the Valid AP database.
- **Refresh**—Updates the page with the latest information.
- **Next**—Navigates to the next page in the Setup Wizard configuration. Any changes you made to the current page are saved before the next page is displayed. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click System > System Utilities > Save All Applied Changes.

Valid Access Point Configuration

From the **Valid Access Point Configuration** page, you can manually set the channel and RF signal transmit power level for an individual AP. You can also configure the AP mode and local authentication password, and you can specify which profile the AP uses.

If you use the local database for AP validation, the switch maintains the database of access points that you validate. When you add the MAC address of an AP to the database, you can specify whether the AP is a managed AP, standalone AP, or a Rogue. If the AP is to be managed by the switch, you can assign an AP profile to the device. When the switch collects and reports information from the RF scan, it can assign the appropriate status to an AP if it is in the database.

Note: Any configuration changes for a managed AP will not be applied until the AP is reset and re-authenticated. If you select a different profile from the menu, a pop-up message asks you to confirm the change. If the AP is managed, a second message asks if you would like to reset the AP. If you click OK, the AP is reset.

To open this page, click **Setup Wizard > Valid VAP**, then click an entry in the MAC Address field.

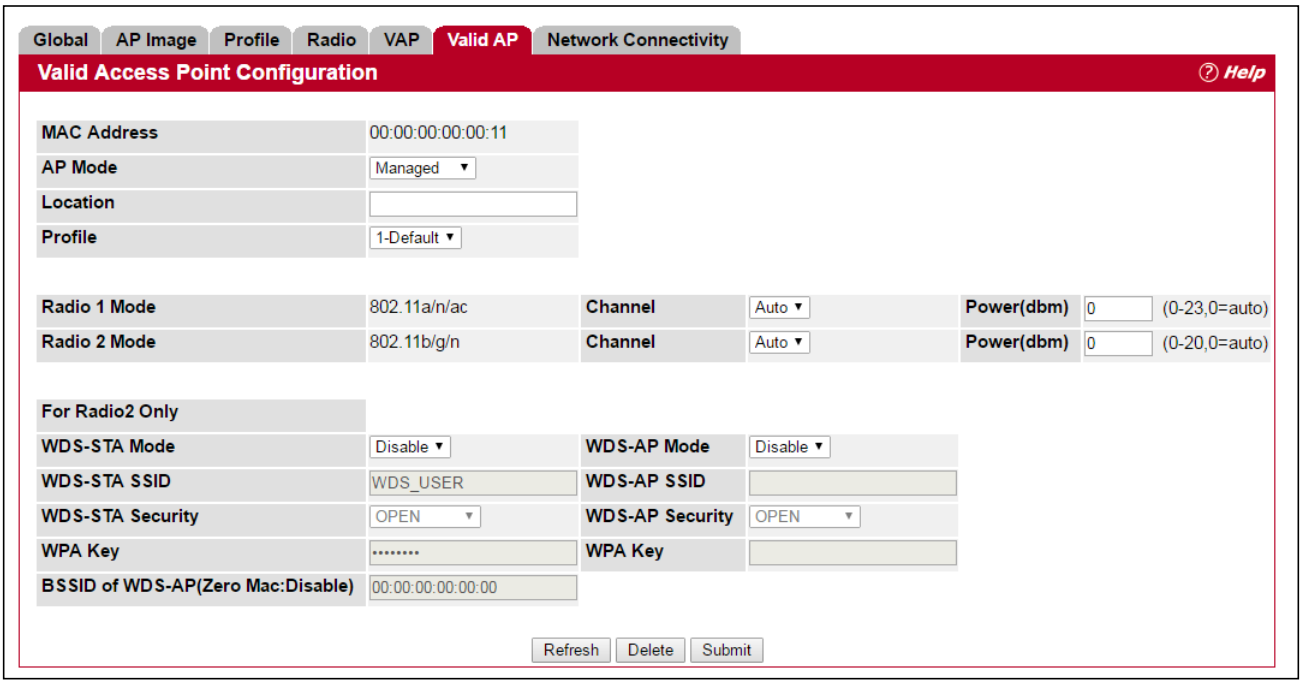


Figure 115: Configuring a Valid Access Point

The following table describes the fields available on the Valid Access Point Configuration page.

Table 104: Valid Access Point Configuration

Field	*Description*
MAC Address	This field shows the MAC address of the AP. To change this field, you must delete the entire Valid AP configuration and then enter the correct MAC address from the page that lists all Valid APs.
AP Mode	You can configure the AP to be in one of three modes: • **Standalone**: The AP acts as an individual access point in the network. You do not manage the AP by using the switch. Instead, you log on to the AP itself and manage it by using the Administrator Web User Interface (UI), CLI, or SNMP. If you select the Standalone mode, the screen refreshes and different fields appear. See the following table for the Standalone mode field descriptions. • **Managed**: The AP is part of the Unified Wireless Switch, and you manage it by using the UWS. If an AP is in Managed Mode, the Administrator Web UI and SNMP services on the AP are disabled. • **Rogue**: Select Rogue as the AP mode if you wish to be notified (through an SNMP trap, if enabled) when this AP is detected in the network. Additionally, when this AP is detected through an RF scan, the status is listed as Rogue. If you select the Rogue mode, the screen refreshes, and fields that do not apply to this mode are hidden.
Name	To help you identify the AP, you can enter a location. Enter a location to help identify the AP. This field is optional and accepts up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted.
Profile	If you configure multiple AP Profiles, you can select the profile to assign to this AP. For more information about configuring AP Profiles, see "AP Profiles" on page 239.

Table 104: Valid Access Point Configuration (Cont.)

Field	*Description*
Channel	The Channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface and the country in which the APs operate. In the United States, IEEE 802.11b, 802.11g, and 2.4 GHz 802.11n modes (802.11 b/g/n) support the use of channels 1 through 11 inclusive, while IEEE 802.11a and 5 GHz 802.11n modes supports a larger set of non-consecutive channels (36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165, 169, 173). Interference can occur when multiple access points within range of each other are broadcasting on the same or overlapping channels. The impact of this interference on network performance can intensify during busy times when a large amount of data and media traffic is competing for bandwidth. If you select auto, the AP scans the RF area for occupied channels and selects a channel from the available non-interfering, or clear channels. The AP selects the best channel whenever its radio or radios restart. If you specify a channel, make sure that the channel does not interfere with the channel that neighbor APs use. ***Note:*** The channel you set for an AP in the valid AP database is fixed and takes precedence over initial channel selection done by the AP and any automatic channel planning done by the switch. ***Note:*** For radios that use 802.11a and/or 5 GHz 802.11n mode, some countries have a regulatory domain that requires radar detection. For these countries (based on the country code setting), the radio automatically uses the 802.11h protocol for selecting the channel if radar is detected on the statically assigned channel.
Power	The power level affects how far an AP broadcasts its RF signal. If the power level is too low, wireless clients will not detect the signal or experience poor WLAN performance. If the power level is too high, the RF signal might interfere with other APs within range. The default value of 0 indicates that the AP uses the power level set in the AP profile. ***Note:*** The power level you set for an AP in the valid AP database is fixed and takes precedence over any automatic power adjustments done by the AP or the switch.
For Radio2 Only	***Note:*** The items in this section are obsolete and will be removed in future software releases.
WDS-STA Mode	The VAP operates as a client station in Wireless Distribution System (WDS) mode, which connects to an access point VAP in WDS-AP mode. The user needs to specify the BSSID of WDS-AP, the MAC address of the access point in WDS-AP mode to which it intends to connect.
WDS-STA SSID	The service set identifier for the VAP. The SSID is an alphanumeric key that uniquely identifies a wireless local area network. The SSID can be up to thirty-two characters in length, and there are no restrictions on the characters that may be used in an SSID.

Table 104: Valid Access Point Configuration (Cont.)

Field	*Description*
WDS-STA Security	The security options include: • OPEN—The VAP is configured by default as an "open system," which broadcasts a beacon signal including the configured SSID. Wireless clients with an SSID setting of "any" can read the SSID from the beacon and automatically set their SSID to allow immediate connection. • WPA2-PSK—Clients using WPA2 with a Pre-shared Key are accepted for authentication. WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.
WPA Key	The WPA Key is the shared secret key. Enter a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.
BSSID of WDS-AP (Zero Mac: Disable)	Basic Service Set Identifier advertised by the VAP in the beacon frames.
WDS-AP Mode	The VAP operates as an access point in Wireless Distribution System (WDS) mode, which accepts connections from APs in WDS-STA mode.
WDS-AP SSID	The service set identifier for the VAP. The SSID is an alphanumeric key that uniquely identifies a wireless local area network. The SSID can be up to thirty-two characters in length, and there are no restrictions on the characters that may be used in an SSID.
WDS-AP Security	The security options include: • OPEN—The VAP is configured by default as an "open system," which broadcasts a beacon signal including the configured SSID. Wireless clients with an SSID setting of "any" can read the SSID from the beacon and automatically set their SSID to allow immediate connection. • WPA2-PSK—Clients using WPA2 with a Pre-shared Key are accepted for authentication. WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.
WPA Key	The WPA Key is the shared secret key. Enter a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.

Standalone APs are managed individually, and not by using a Unified Wireless Switch. By including standalone APs in the Valid AP database and specifying their expected settings, you can help ensure that only legitimate APs are on your network. If any of the expected settings you configure for the standalone AP do not match the settings detected through the RF scan, and the *Standalone AP with unexpected configuration* test is enabled on the **WLAN** > **WLAN Configuration > WIDS Security** page, the standalone AP is listed as a Rogue on the **WLAN** > **Intrusion Detection> Rogue/RF Scan** page.

If you select Standalone from the AP Mode menu on the **Valid Access Point Configuration** page, the screen refreshes, and additional fields appear. The following table describes the additional information you can include about the standalone APs you add to the Valid AP database.

Table 105: Valid AP Configuration (Standalone Mode)

Field	*Description*
Expected SSID	Enter the SSID that identifies the wireless network on the standalone AP.
Expected Channel	Select the channel that the standalone AP uses. If the AP is configured to automatically select a channel, or if you do not want to specify a channel, select Any.
Expected WDS Mode	Standalone APs can use a Wireless Distribution System (WDS) link to communicate with each other without wires. The menu contains the following options: • **Bridge**: Select this option if the standalone AP you add to the Valid AP database is configured to use one or more WDS links. • **Normal**: Select this option if the standalone AP is not configured to use any WDS links. • **Any**: Select this option if the standalone AP might use a WDS link.
Expected Security Mode	Select the option to specify the type of security the AP uses: • **Any**—Any security mode • **Open**—No security • **WEP**—Static WEP or WEP 802.1X • **WPA/WAP2**—WPA and/or WPA2 (Personal or Enterprise)
Expected Wired Network Mode	If the standalone AP is allowed on the wired network, select Allowed. If the AP is not permitted on the wired network, select Not Allowed.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Delete**—Deletes the AP from the local Valid AP database. Managed APs must be reset to complete their removal from the Valid AP database.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).

Network Connectivity Configuration

From the **Network Connectivity Configuration** page you can change the IPv4 information. The network interface is the logical interface used for in-band management connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

You configure default Network Connectivity settings from the *System* **> Setup Wizard > Network Connectivity** tab, which the following figure shows.

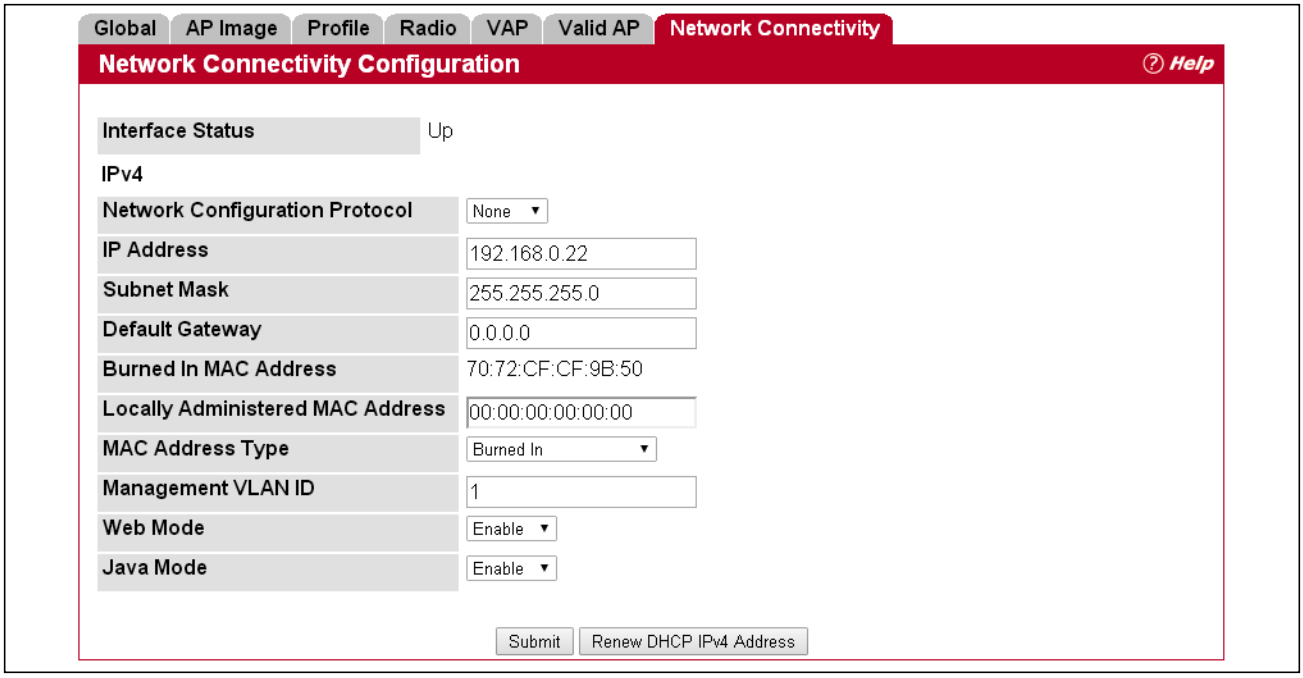


Figure 116: Network Connectivity Configuration for IPv4

Table 106: Network Connectivity Configuration for IPv4 Fields

Field	*Description*
Network Configuration Protocol	Specify what the switch should do following power-up. The factory default is None. The options are as follows: • **BOOTP:** Transmit a BOOTP request. • **DHCP:** Transmit a DHCP request. • **None:** Do not send any requests following power-up.
IP Address	The IP address of the network interface. The factory default value is 0.0.0.0 ***Note:*** Each part of the IP address must start with a number other than zero. For example, IP addresses 001.100.192.6 and 192.001.10.3 are not valid.
Subnet Mask	The IP subnet mask for the interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for the IP interface. The factory default value is 0.0.0.0.
Burned-in MAC Address	This read-only field displays the MAC address that is burned-in to the network card at the factory. This MAC address is used for in-band connectivity if you choose not to configure a locally administered address.

Table 106: Network Connectivity Configuration for IPv4 Fields (Cont.)

Field	*Description*
Locally Administered MAC Address	Specifies a locally administered MAC address for in-band connectivity instead of using the burned-in universally administered MAC address. In addition to entering an address in this field, you must also set the MAC address type to locally administered. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0, i.e. byte 0 must have a value between x'40' and x'7F'.
MAC Address Type	Specify whether the burned-in or a locally administered MAC address should be used for in-band connectivity. The factory default is to use the burned-in MAC address.
Management VLAN ID	Specifies the management VLAN ID of the switch. It may be configured to any value in the range of (1 to 4093). The management VLAN is used for management of the switch. The default management VLAN ID is 1.
Web Mode	Enables/Disables Web Mode on the switch.
Java Mode	Enables/Disables Java mode on the switch.

If you change any of the network connectivity parameters, click **Submit** to apply the changes to the system. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).

Click **Renew DHCP IPv4 Address** to force the interface to release the current DHCP-assigned information and submit a request for new information.

WLAN Configuration

From the **WLAN Configuration** folder, you can access the following pages:

- Wireless Global Configuration
- Wireless Discovery Configuration
- Known Client
- AP Image Availability List
- Configuring Networks
- AP Profiles
- Local Access Point Database
- Peer Switch
- WIDS Security
- Switch Provisioning
- Local OUI Database Summary

Wireless Global Configuration

This folder includes configuration settings for the UWS and AP profiles which apply to managed APs.

Wireless Global Configuration

The fields on the **Wireless Global Configuration** page are settings that apply to the UWS.

To access this page, click **WLAN** > **WLAN Configuration** > **Global**, and then click the **Global** tab.

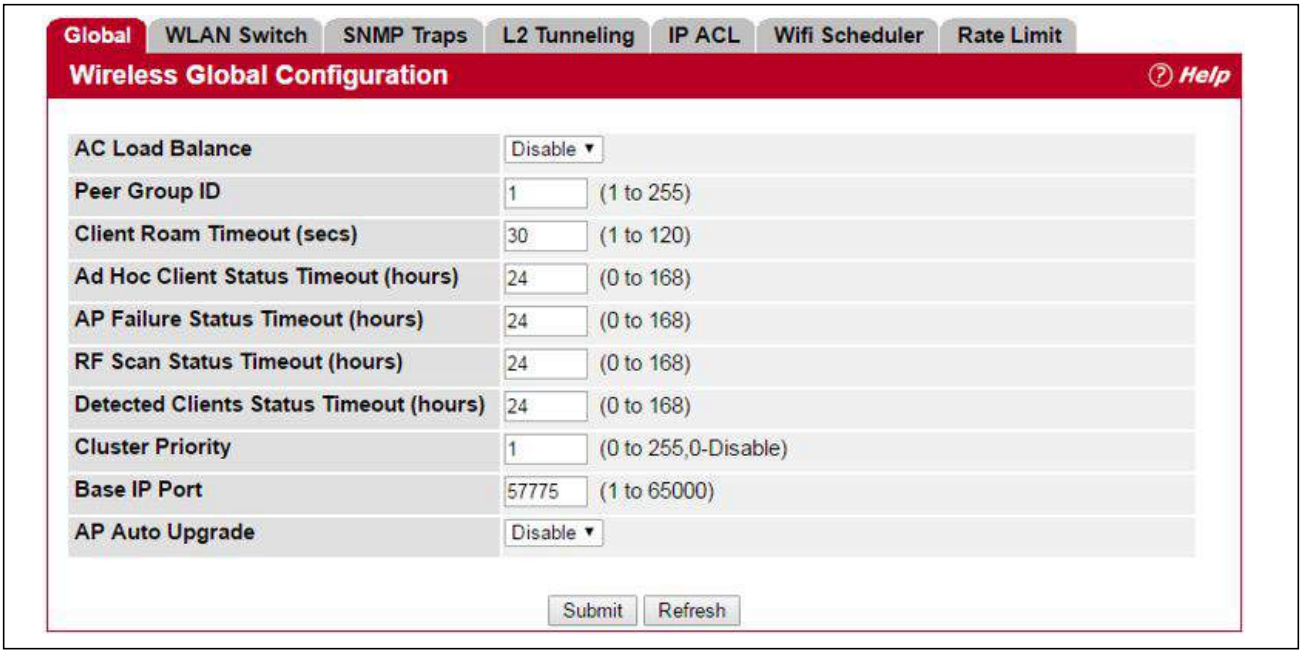


Figure 117: Wireless Global Configuration

Table 107 describes the fields on the **Wireless Global Configuration** page.

Table 107: General Global Configurations

Field	*Description*
AC Load Balance	When access controller (AC) switches are configured in a cluster, load balancing will ensure that each AC manages an even number of APs. In addition, the cluster supports redundancy between primary and secondary ACs. If the primary AC fails, the secondary AC will support the load until the primary AC recovers.
Peer Group ID	To support larger networks, you can configure wireless switches as peers, with up to 64 switches in a cluster (peer group). Peer switches share some information about APs and allow L3 roaming among them. Peers are grouped according to the Group ID.
Client Roam Timeout (secs)	This value determines how long to keep an entry in the Associated Client Status list after a client has disassociated. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted.
Ad Hoc Client Status Timeout (hours)	This value determines how long to keep an entry in the Ad Hoc Client Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted. A value of 0 means that the entry does not timeout.
AP Failure Status Timeout (hours)	This value determines how long to keep an entry in the AP Authentication Failure Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted. A value of 0 means that the entry does not timeout.
RF Scan Status Timeout (hours)	This value determines how long to keep an entry in the RF Scan Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted. A value of 0 means that the entry does not timeout.
Detected Clients Status Timeout (hours)	This value determines how long to keep an entry in the Detected Client Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted. A value of 0 means that the entry does not timeout.
Cluster Priority	Specify the priority of this switch for the Cluster Controller election. The switch with highest priority in a cluster becomes the Cluster Controller. If the priority is the same then the switch with lowest IP address becomes the Cluster Controller. A priority of 0 means that the switch cannot become the Cluster Controller. The highest possible priority is 255.
Base IP Port	Sets the first IP port number within the range that the wireless system uses to send and receive IP traffic. By default the Wireless system uses the IP ports 57775 to 57784. If you change the base IP port, the wireless feature is automatically disabled and re-enabled. The default Wireless IP port is not sent as part of the global switch configuration in the cluster configuration distribution command, so every switch in the cluster must be configured independently with the new IP port number. If the Wireless IP port number is changed from its default value on the switch, then it must also be changed on the Access Points. The port can be set on the AP via an AP administrative command, or DHCP option 43, sub-option 3. If the port is set via DHCP then the DHCP setting supersedes the configured setting.
AP Auto Upgrade	Automatically upgrades the current operational code on the AP when a more recent version exists on the access controller. See "AP Image Settings" on page 187.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).
- **Refresh**—Updates the page with the latest information.

WLAN Switch Configuration

For the UWS to be able to discover and manage access points, both the WLAN switch and its operational status must be enabled. However, before you enable the WLAN switch, set the correct country code for the switch so that the access points can operate only in the modes permitted in your country. The default country code is US for operation in the United States. To set the country code and enable switch operation by using the Web interface, be sure to set these parameters in the **WLAN > WLAN Configuration > Global** > **WLAN Switch** tab.

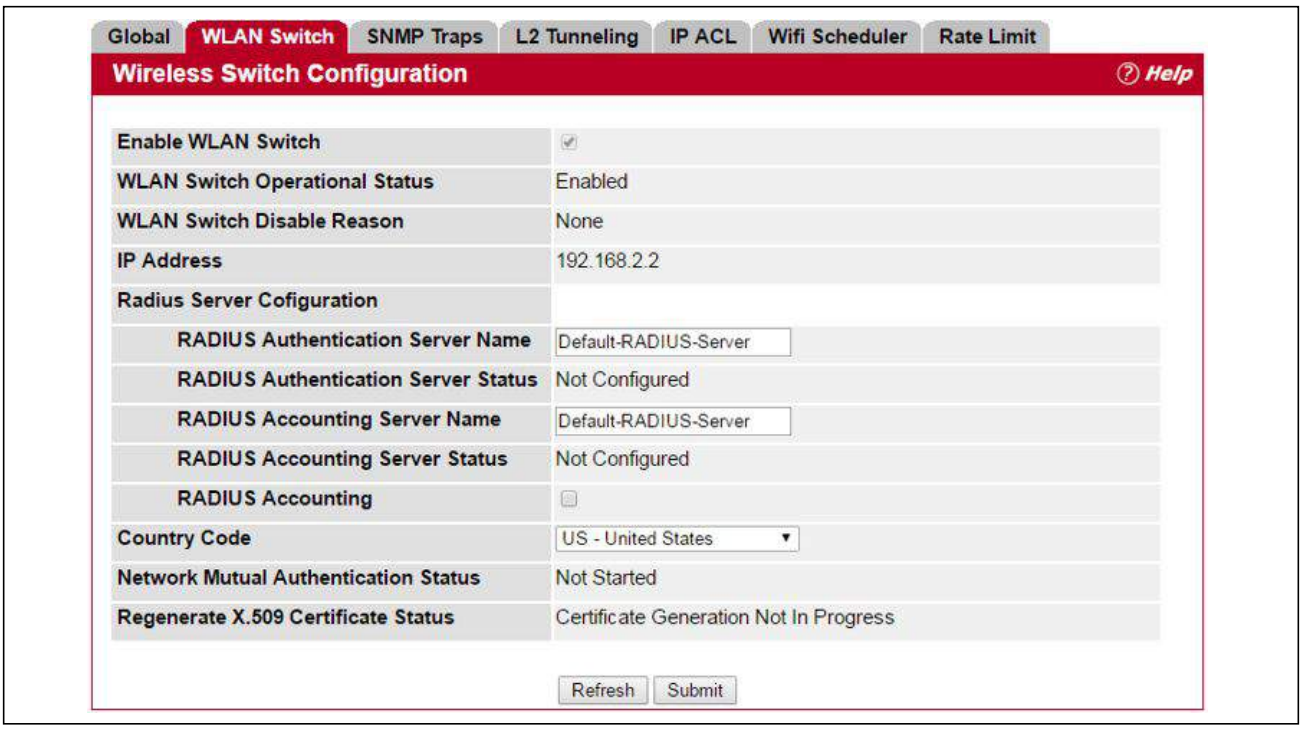


Figure 118: WLAN Switch Configuration

The following table describes the fields available on the Wireless Global Configuration page.

Table 108: Basic Wireless Global Configuration

Field	*Description*
Enable WLAN Switch	Select this option to enable WLAN switching functionality on the system. Clear the option to administratively disable the WLAN switch. If you clear the option, all peer switches and APs that are associated with this switch are disassociated. Disabling the WLAN switch does not affect non-WLAN features on the switch, such as VLAN or STP functionality.

Table 108: Basic Wireless Global Configuration (Cont.)

Field	*Description*
WLAN Switch Operational Status	Shows the operational status of the switch. The status can be one of the following values: • Enabled • Enable-Pending • Disabled • Disable-Pending If the status is pending, click **Refresh** to update the screen with the latest information.
WLAN Switch Disable Reason	If the status is disabled, this field appears and one of the following reasons is listed: • None: The cause for the disabled status is unknown. • Administrator disabled: The Enable WLAN Switch check box has been cleared. • No IP Address: The WLAN interface does not have an IP address. • No SSL Files: The UWS communicates with the APs it manages by using Secure Sockets Layer (SSL) connections. The first time you power on the UWS, it automatically generates a server certificate that will be used to set up the SSL connections. The SSL certificate and key generation typically completes within a few minutes. If routing is enabled on the switch, the operational status might be disabled due to one of the following reasons: • No Loopback Interface: The switch does not have a loopback interface. • Global Routing Disabled: Even if the routing mode is enabled on the WLAN switch interface, it must also be enabled globally for the operational status to be enabled.
IP Address	This field shows the IP address of the WLAN interface on the switch. If the switch does not have the Routing Package installed, or if routing is disabled, the IP address is the network interface. If the routing package is installed and enabled, this is the IP address of the routing or loopback interface you configure for the UWS features. If routing is enabled, it is strongly recommended that you define a loopback interface on the switch. By creating a loopback interface, you can control which routing interface the wireless function uses for its IP address when multiple routing interfaces exist. This can avoid discovery problems for the discovery modes where the AP knows the IP address of the UWS. With the loopback interface, the IP address of the wireless function is always the same. In this context, the loopback interface does not refer to the loopback interface with the 127.0.0.1 IP address. When you configure a loopback interface for the wireless interface on the switch, it is essentially a permanent logical interface and cannot have an IP address of 127.0.0.1. You must create a dedicated subnet for the loopback interface, and other devices on the network must be able to contact the IP address of the loopback interface.
RADIUS Authentication Server Name	Enter the name of the RADIUS server used for AP and client authentications when a network-level RADIUS server is not defined on the **Basic Setup > VAP > Wireless Network Configuration** page. The name can contain up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted. The switch acts as the RADIUS client and performs all RADIUS transactions on behalf of the APs and wireless clients.
RADIUS Authentication Server Status	Indicates whether the RADIUS authentication server is configured. To configure RADIUS server information, go to **Security > RADIUS > Server Configuration**.

Table 108: Basic Wireless Global Configuration (Cont.)

Field	*Description*
RADIUS Accounting Server Name	Enter the name of the RADIUS server used for reporting wireless client associations and disassociations when a network-level RADIUS accounting server is not defined on the **Basic Setup > VAP > Wireless Network Configuration** page. The name can contain up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted.
RADIUS Accounting Server Status	Indicates whether the RADIUS accounting server is configured. To configure RADIUS accounting server information, go to **Security > RADIUS > Accounting Server Configuration**.
RADIUS Accounting	Select this option to enable RADIUS accounting for wireless clients.
Country Code	Select the country code that represents the country where your switch and APs operate. When you click **Submit**, a pop-up message asks you to confirm the change. Wireless regulations vary from country to country. Make sure you select the correct country code so that your WLAN system complies with the regulations in your country. ***Note:*** Changing the country code disables and re-enables the switch. Channel and radio mode settings that are invalid for the regulatory domain are reset to the default values. The country code (IEEE 802.11d) is transmitted in beacons and probe responses from the access points.
Network Mutual Authentication Status	The mutual authentication feature allows authentication between switches and APs and between peer switches. Mutual authentication is accomplished by using X.509 certificate exchange. This field shows the status of the mutual authentication feature. The field has one of the following values: • Not Started • In Progress—Mutual authentication is in the process of being enabled or disabled. • Complete Without Errors—The mutual authentication process finished without any problems. • Complete With Errors —Mutual authentication finished, but problems were detected. This means that you may need to provision some switches or APs separately.
Regenerate X.509 Certificate Status	Status of the request to generate an X.509 certificate. To initiate X.509 certificate generation, go to the **Advanced Configuration > Switch Provisioning** page. The field has one of the following values: • Certificate Generation is not in progress • Start Certificate Generation • Certificate Generation is in progress.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click System > System Utilities > Save All Applied Changes.
- **Next**—Navigates to the next page in the Basic Setup configuration. Any changes you made to the current page are saved before the next page is displayed. To retain the new values across a power cycle, you must perform a

save on the WLAN switch (not the AP). To perform a save, click System > System Utilities > Save All Applied Changes.

Wireless SNMP Trap Configuration

If you use Simple Network Management Protocol (SNMP) to manage the UWS, you can configure the SNMP agent on the switch to send traps to the SNMP manager on your network from the **WLAN > WLAN Configuration > SNMP Traps** tab.

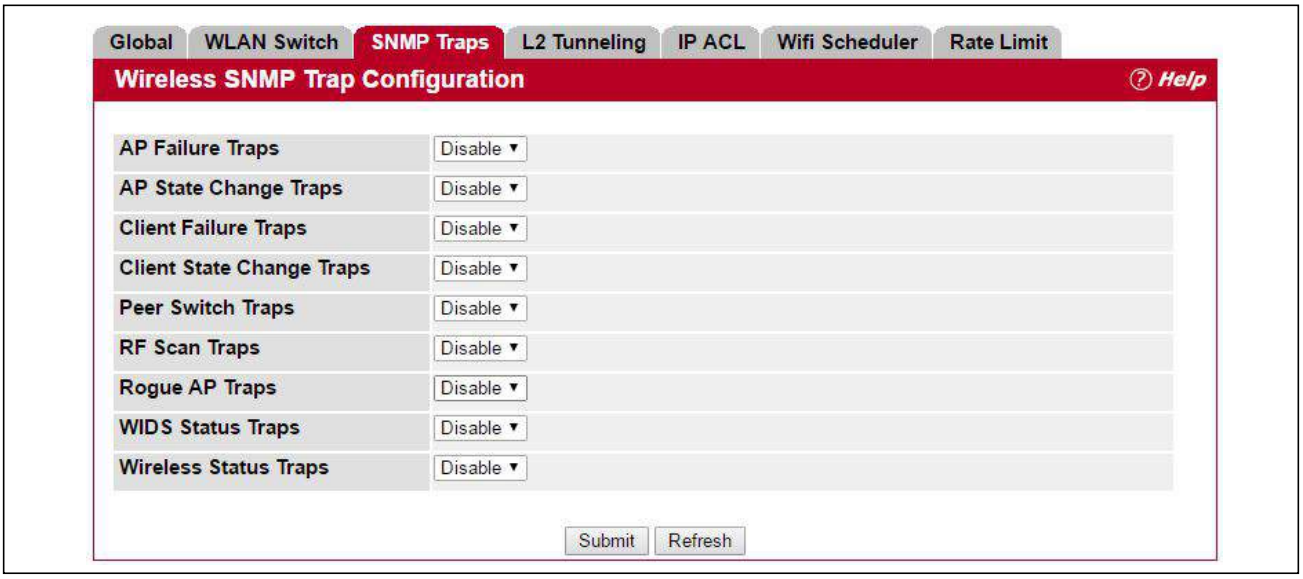


Figure 119: SNMP Trap Configuration

When an AP is managed by a switch, it does not send out any traps. The switch generates all SNMP traps based on its own events and the events it learns about through updates from the APs it manages.

All Wireless SNMP traps are disabled by default.

The following table describes the events that generate SNMP traps. All traps are disabled by default.

Table 109: Wireless SNMP Traps

Field	*Description*
AP Failure Traps	If you enable this field, the SNMP agent sends a trap if an AP fails to associate or authenticate with the switch.
AP State Change Traps	If you enable this field, the SNMP agent sends a trap for one of the following reasons: • Managed AP Discovered • Managed AP Failed • Managed AP Unknown Protocol Discovered • Managed AP Load Balancing Utilization Exceeded
Client Failure Traps	If you enable this field, the SNMP agent sends a trap if a wireless client fails to associate or authenticate with an AP that is managed by the switch.

Table 109: Wireless SNMP Traps (Cont.)

Field	*Description*
Client State Change Traps	If you enable this field, the SNMP agent sends a trap for one of the following reasons associated with the wireless client: • Client Association Detected • Client Disassociation Detected • Client Roam Detected
Peer Switch Traps	If you enable this field, the SNMP agent sends a trap for one of the following reasons associated with a peer switch • Peer Switch Discovered • Peer Switch Failed • Peer Switch Unknown Protocol Discovered
RF Scan Traps	If you enable this field, the SNMP agent sends a trap when the RF scan detects a new AP, wireless client, or ad-hoc client.
Rogue AP Traps	If you enable this field, the SNMP agent sends a trap when the switch discovers a rogue AP.
WIDS Status Traps	If you enable this field, the SNMP agent sends a trap when WIDS generates messages.
Wireless Status Traps	If you enable this field, the SNMP agent sends a trap if the operational status of the UWS changes or if any of the following databases or lists has reached the maximum number of entries: • Managed AP database • AP Neighbor List • Client Neighbor List • AP Authentication Failure List • RF Scan AP List • Client Association Database • Client Authentication Failure List Additionally, when this field is enabled and the switch supports both Independent and Integrated AP image download modes, the SNMP agent sends a trap if the switch cannot find the code image required to automatically update the AP.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).
- **Refresh**—Updates the page with the latest information.

Centralized L2 Tunnel Configuration

Sometimes it is desirable for wireless clients to be able to roam from an AP in one subnet to an AP in a different subnet without losing their own IP addresses. This mode of operation is particularly useful for IP phones, enabling a call to stay active even while roaming between APs in different subnets.

The centralized L2 tunneling feature extends the VLANs configured on the switch to the wireless clients. The Administrator configures which VLANs participate in the L2 tunnel. The switch establishes one L2 tunnel with every peer switch and every access point that it manages. The APs encapsulate all frames for participating VLANs, and

then send the data to the switch. At the switch, the encapsulation is removed and the frames are forwarded using L2 forwarding rules.

You can configure a list of up to 64 VLANs to participate in L2 tunneling. The list is passed to peer switches during the global configuration push and to APs as they join the switch. You can modify the list of VLANs at any time without disrupting traffic flow on the APs for VLANs that are not affected by the change.

To create a centralized L2 tunnel, click **WLAN** > **WLAN Configuration** > **Global**, and then select the **L2 Tunneling** tab.

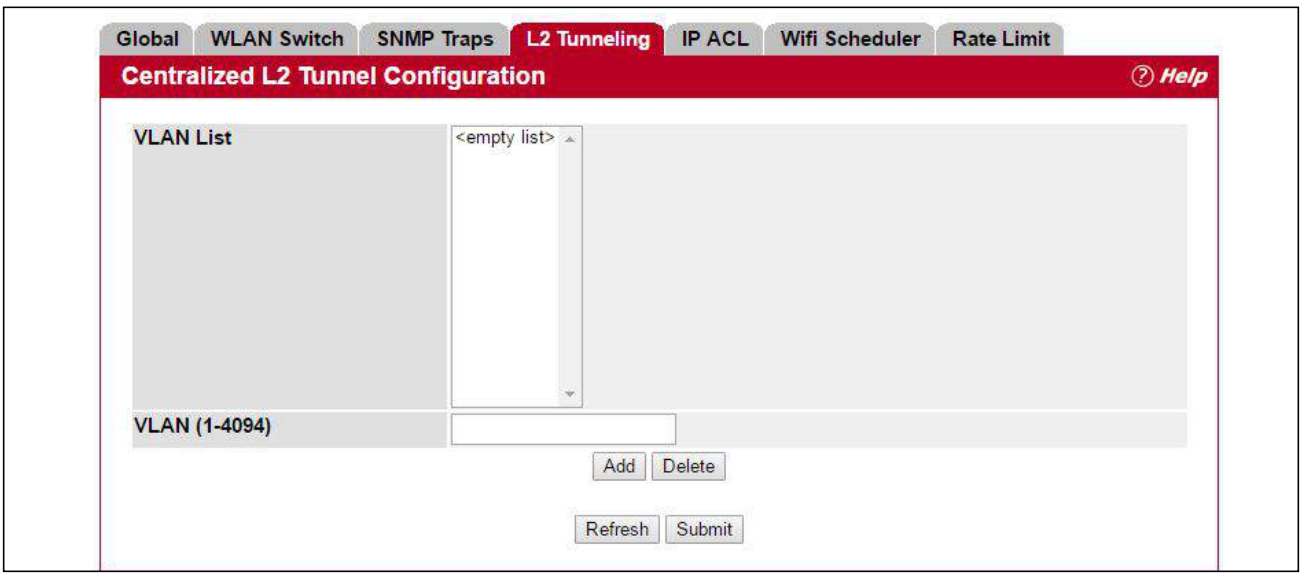


Figure 120: L2 Tunneling Configuration

Table 110: L2 Tunneling Configuration Fields

Field	*Description*
VLAN List	Displays the list of VLANs that have been added to the L2 tunnel.
VLAN (1-4094)	Enter a VLAN ID from 1–4094 and click Add to add a VLAN to the L2 tunnel.

Command Buttons

The page includes the following buttons:

- **Add**—Adds the VLAN to the L2 tunnel.
- **Delete**—Deletes the selected VLAN from the L2 tunnel.
- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter.

IP ACL Configuration

IP Access Control Lists (ACL) allow network managers to define classification actions and rules for specific ports. ACLs are composed of access control entries (ACE), or rules, that consist of filters that determine traffic classifications. These rules are matched sequentially against a packet. When packet meets the match criteria of a rule, the specific rule action (Permit/Deny) is taken, including dropping the packet or disabling the port, and the additional rules are not checked for a match. For example, a network administrator defines an ACL rule that says port number 20 can receive TCP packets. However, if a UDP packet is received the packet is dropped.

Use the IP ACL page to add or remove IP-based ACLs. On this menu rules for the IP ACL are specified/created.

To configure IP ACLs, click **WLAN** > **WLAN Configuration** > **Global**, and then select the **IP ACL** tab.

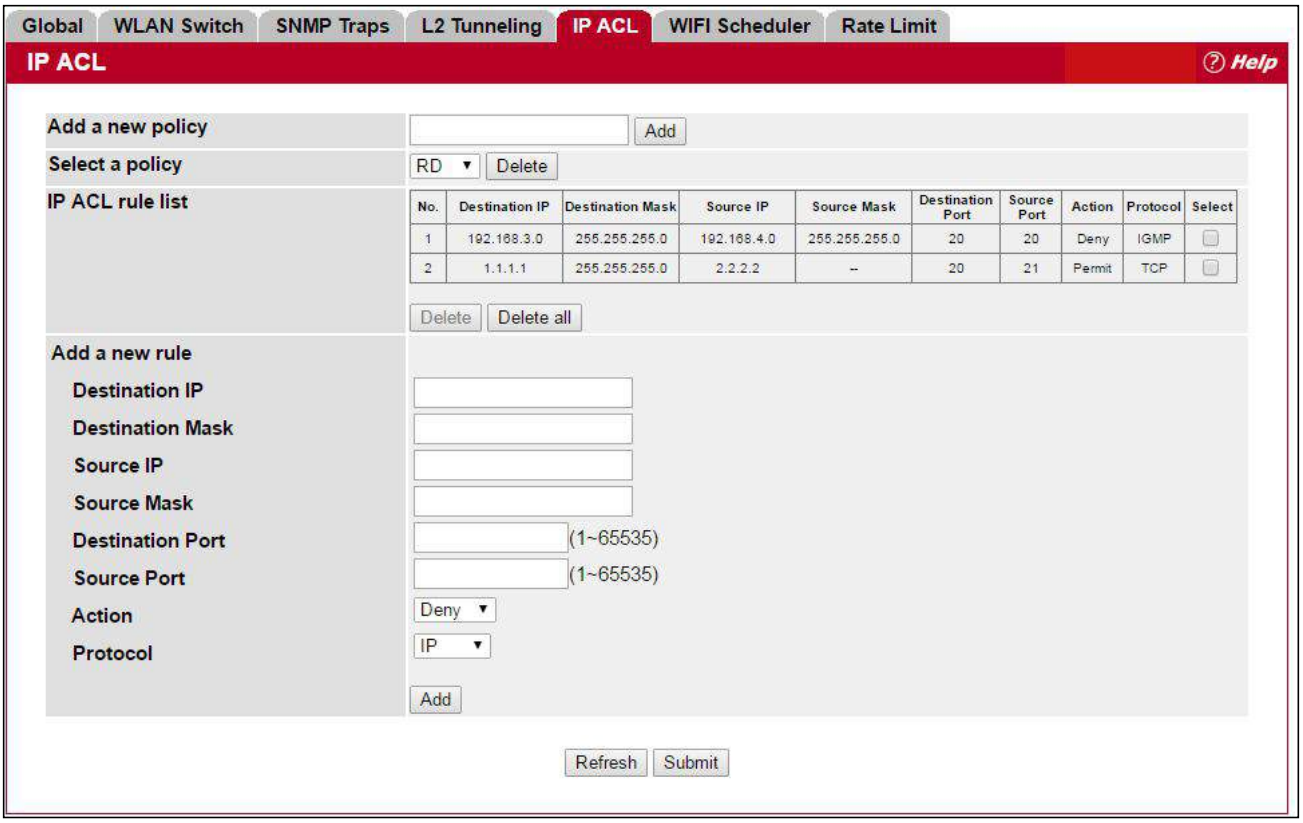


Figure 121: IP ACL Configuration

Table 111: IP ACL Configuration Fields

Field	*Description*
Add a new policy	Enter the name that identifies the ACL. The policy name can include 1 to 31 alphanumeric characters and the following special characters: hyphen, underscore, backslash and colon. Spaces are not allowed. Before you add or remove a rule, you must select the ID of the ACL from the menu.
Select a policy	Select the Policy to configure with the new rule. To delete a policy, select it from the list, and then click the **Delete** button.
IP ACL rule list	Shows the list of rules assigned to this policy.

Table 111: IP ACL Configuration Fields

Field	*Description*
Add a new rule	After enter a new ACL rule, click the **Add** button to add a new data in the list.
No.	The number that identifies the rule. A number is automatically assigned to a rule when it is created. Rules are added in the order that they are created and cannot be renumbered. Packets are checked against the rule criteria in order, from lowest numbered rule to highest. When the packet matches the criteria in a rule, it is handled according to the rule action and attributes. If no rule matches a packet it is discarded based on the implicit deny all rules, which is the final in every ACL.
Destination IP	The destination port IP address in the packet to compare to the IP address in the packet header.
Destination Mask	The destination IP wildcard mask (in the second field) to compare to the IP address in the packet header. Wild card masks determine which bits in the IP address are used and which bits are ignored. A wild card mask of 255.255.255.255 indicate that no bit is important. Wild card masking of ACLs operates differently from a subnet mask. A wild card is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address and zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has zeros (0's) in the bit positions that must be checked. A 1 in the bit position of the ACL mask indicates the corresponding bit can be ignored. The field is required when you configure a destination IP address.
Source IP	The source port IP address in the packet to compare to the IP address in the packet header.
Source Mask	The source IP wildcard mask (in the second field) to compare to the IP address in the packet header. Wild card masks determine which bits in the IP address are used and which bits are ignored. A wild card mask of 255.255.255.255 indicate that no bit is important. Wild card masking of ACLs operates differently from a subnet mask. A wild card is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address and zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has zeros (0's) in the bit positions that must be checked. A 1 in the bit position of the ACL mask indicates the corresponding bit can be ignored. The field is required when you configure a source IP address.
Destination Port	The TCP/UDP destination port to match in the packet header.
Source Port	The TCP/UDP source port to match in the packet header.
Action	The action to take when a packet or frame matches the criteria in the rule.
• **Permit**	When you select **Permit**, the rule allows all traffic that meets the rule criteria to enter or exit the AP (depending on the ACL direction you select). Traffic that does not meet the criteria is dropped.
• **Deny**	When you select **Deny**, the rule blocks all traffic that meets the rule criteria from entering or exiting the AP (depending on the ACL direction you select). Traffic that does not meet the criteria is forwarded unless this rule is the final rule. Because there is an implicit deny all rule at the end of every ACL, traffic that is not explicitly permitted is dropped
Protocol	Select the Protocol field to use an L3 or L4 protocol match condition based on the value of the IP Protocol field in IPv4 packets. You can specify one of the following keywords: IP, ICMP, IGMP, TCP, or UDP.

Use the following procedures to add a rate limit policy.

1. Specify the name of a policy in the **Add a new policy** field, and click **Add**.
2. Add the required match criteria under **Add a new rule**, and click **Add**.
3. Verify the rule settings under **IP ACL rule list**.
4. Click the **Select** field for those rules to add to the policy.
5. Cick **Submit**.
6. Apply the rate limit policy to one or more VAPs. See "Configuring the Default Network" on page 196.

Click **Refresh** to update the information on the screen.

WIFI Scheduler

The WIFI Scheduler allows you to configure a rule with a specific time interval for radios to be operational, thereby automating the enabling or disabling of the VAPs and Radios.

One of the ways you can use this feature is to schedule radios to operate only during the office working hours in order to achieve security and reduce power consumption. You can also use the Scheduler to allow access to VAPs for wireless clients only during specific times of day.

Each rule specifies the start time, end time and day (or days) of the week the radio or VAP can be operational. The rules are periodic in nature and are repeated every week.

A valid rule must contain all of the following parameters:

- Days of the Week
- Start Time (hour and minutes)
- End Time (hour and minutes)

Only valid rules are added to the profile. Up to 16 rules are grouped together to form a scheduling profile. Any two periodic rules time entries belonging to the same profile must not overlap. The time granularity for the schedules is one minute. The UAP supports up to 16 profiles.

To configure a time range during which the WLAN is enabled, click **WLAN** > **WLAN Configuration** > **Global**, and then click the **WIFI Scheduler** tab.

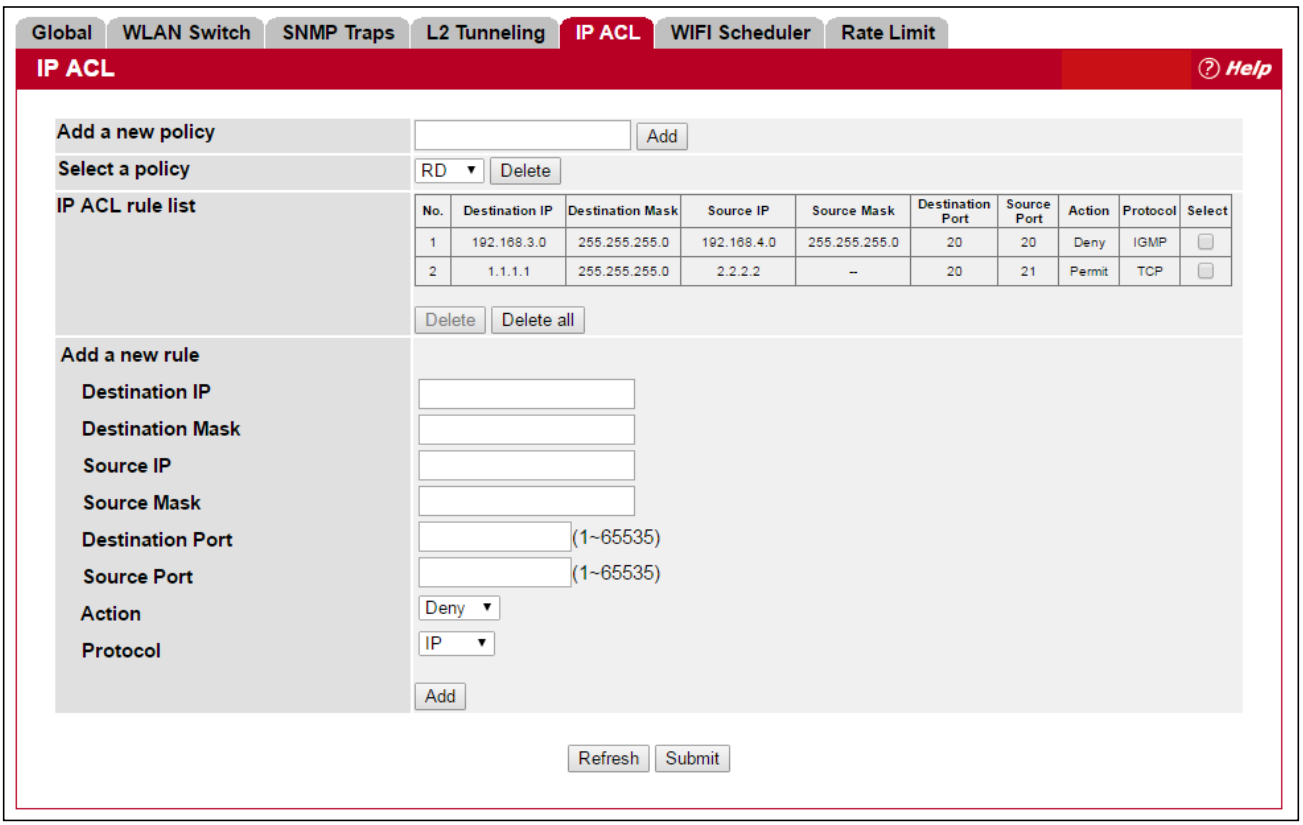


Figure 122: WIFI Scheduler Configuration

Table 112: WIFI Scheduler Configuration Fields

Field	*Description*
Scheduler Status	A global switch to enable or disable the scheduler feature. The default is Disable.
Add a new Scheduler Policy	The Scheduler policy defines the list of profiles names that can be associated to the VAP or Radio configuration. Rules are associated with a named scheduler profile. You can define up to 16 scheduler profile names. By default, no profiles are created. The profile name can be up to 32 alphanumeric characters. Click **Add** to add the policy name.
Scheduler Policy	Select a scheduler policy to display the assigned rules. To remove a policy from the menu, select the policy from the list, and then click **Delete**.
Schedule Rule List	Each scheduler policy may have up to 16 periodic rules. This table includes the settings you use to configure periodic rules. To remove a rule from a scheduler policy, select the rule from the list, and then click **Delete**. To remove all of the rules from a scheduler policy, click **Delete All**.
Add a Scheduler Rule	Select the time range for a new rule, enter the required fields, and click **Add.**
No.	A number that identifies a rule assigned to the scheduler policy. A number is automatically assigned to a rule when it is created. The policy is checked against the rule criteria in order, from lowest numbered rule to the highest.
Day In a Week	Options include the day of the week. Range is: **Daily**, **Weekday** (Monday to Friday), **Weekend** (Saturday and Sunday), **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, **Sunday**. The default is **Daily**.
Start Time	The time when the radio or VAP will be operationally enabled. The time is in HH:MM 24-hour format. The range is <00-23>:<00-59>. The default is 00:00.
End Time	The time when the radio or VAP will be operationally disabled. The time is in HH:MM 24-hour format. The range is <00-23>:<00-59>. The default is 00:00.

Use the following procedures to add a scheduler policy.

1. Specify the name of a policy in the **Add a new Scheduler Policy** field, and click **Add**.
2. Add the required match criteria under **Add a Scheduler Rule**, and click **Add**.
3. Verify the rule settings under **Scheduler Rule List**.
4. Click the **Select** field for those rules to add to the policy.
5. Cick **Submit**.
6. Apply the rate limit policy to one or more VAPs. See "Configuring the Default Network" on page 196.

The page includes the following buttons:

- **Add**: Adds the data in the scheduler policy or rules to the appropriate list.
- **Delete**: Deletes the selected entry from the scheduler policy or rules list.
- **Delete All**: Deletes all rules list.
- **Refresh**: Updates the page with the latest information.
- **Submit**: Assign all of the defined rules to a scheduler. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click **System** > **System Utilities** > **Save All Applied Changes**.

Rate Limit Configuration

Each rate limit policy is a set of up to 10 rules applied to traffic sent from a wireless client or to be received by a wireless client. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network. Rules can be based on various criteria and may apply to one ore more fields within a packet, such as the source or destination IP address, the source or destination L4 port, or the protocol carried in the packet.

To configure a rate limit on traffic passing through the WLAN, click **WLAN** > **WLAN Configuration** > **Global**, and then the **Rate Limit** tab.

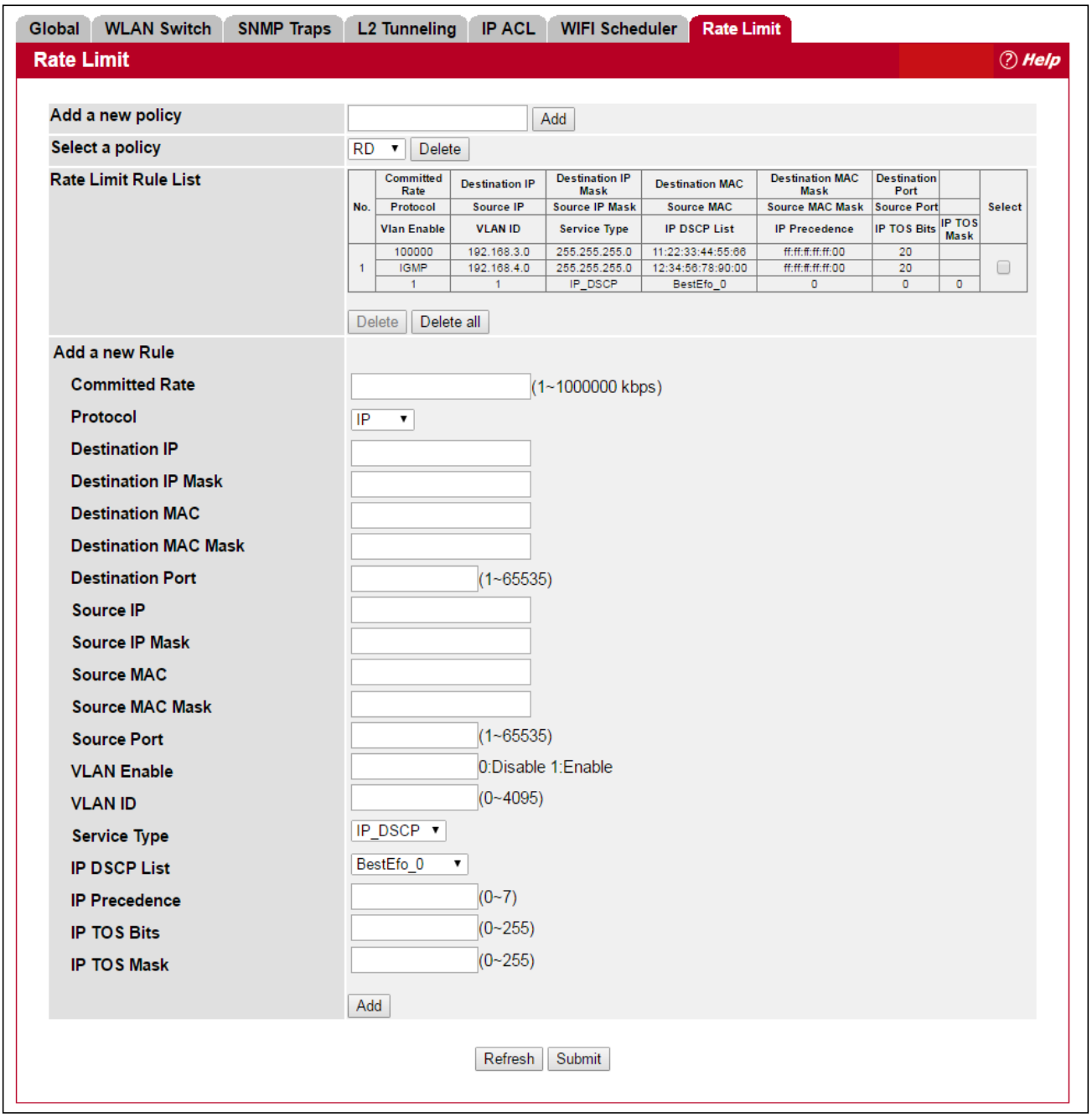


Figure 123: Rate Limit Configuration

Table 113: Rate Limit Configuration Fields

Field	*Description*
Add a new policy	The rate limit policy defines the list of rate limit rules that can be associated with a VAP or Radio configuration. Rules are associated with a named scheduler profile. You can define up to 32 scheduler profile names. By default, no profiles are created. The policy name can include 1 to 31 alphanumeric characters and the following special characters: hyphen, underscore, backslash and colon. If spaces are include, enclose them in double quotes. Click **Add** to add a new policy.
Select a policy	Select a rate limit policy to display the assigned rules. To remove a policy from the menu, select the policy from the list, and then click **Delete**.
Rate Limit Rule List	Each rate limit policy may have up to 32 rules. This table includes the settings you use to configure rate limit rules. To remove a rule from a scheduler policy, select the rule from the list, and then click **Delete**. To remove all of the rules from a scheduler policy, click **Delete All**.
Add a new Rule	Select the rate limit policy for a new rule, enter the required fields, and click **Add.**
No.	The number that identifies the rule. A number is automatically assigned to a rule when it is created. Rules are added in the order that they are created and cannot be renumbered. Packets are checked against the rule criteria in order, from lowest numbered rule to highest. When the packet matches the criteria in a rule, it is handled according to the rule attributes.
Committed Rate	Enter the maximum allowed transmission rate between the AP and the wireless client in Kbps. The valid range is 0-1363148800 bps. A non-zero configured value is rounded down to the nearest 64 Kbps value for use in the AP, but to no less than 64 Kbps. A value of 0 means that the bandwidth maximum limit is not enforced.
Protocol	The protocol type to match within the IP Protocol field in the IP packet header. You can specify one of the following keywords: IP, ICMP, IGMP, TCP, or UDP.
Destination IP	The destination port IP address in the packet to compare to the IP address in the packet header.
Destination IP Mask	The destination IP wildcard mask (in the second field) to compare to the IP address in the packet header. Wild card masks determine which bits in the IP address are used and which bits are ignored. A wild card mask of 255.255.255.255 indicate that no bit is important. Wild card masking of ACLs operates differently from a subnet mask. A wild card is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address and zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has zeros (0's) in the bit positions that must be checked. A 1 in the bit position of the ACL mask indicates the corresponding bit can be ignored. The field is required when you configure a destination IP address.
Destination MAC	The destination port MAC address in the packet to compare to the MAC address in Destination MAC field of the packet header.
Destination MAC Mask	Enter the destination MAC address mask specifying which bits in the destination MAC address to compare to the MAC address in the packet header. A 0 indicates that the address bit is significant, and an f indicates that the address bit is to be ignored. A MAC mask of 00:00:00:00:00:00 matches a single MAC address.
Destination Port	The TCP/UDP destination port to match in the packet header.
Source IP	The source port IP address in the packet to compare to the IP address in the Source MAC field of the packet header.

Table 113: Rate Limit Configuration Fields

Field	*Description*
Source IP Mask	The source IP wildcard mask (in the second field) to compare to the IP address in the packet header. Wild card masks determine which bits in the IP address are used and which bits are ignored. A wild card mask of 255.255.255.255 indicate that no bit is important. Wild card masking of ACLs operates differently from a subnet mask. A wild card is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address and zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has zeros (0's) in the bit positions that must be checked. A 1 in the bit position of the ACL mask indicates the corresponding bit can be ignored. The field is required when you configure a source IP address.
Source MAC	The source port MAC address in the packet to compare to the MAC address in Source MAC field of the packet header.
Source MAC Mask	Enter the source MAC address mask specifying which bits in the source MAC address to compare to the MAC address in the packet header. A 0 indicates that the address bit is significant, and an f indicates that the address bit is to be ignored. A MAC mask of 00:00:00:00:00:00 matches a single MAC address.
Source Port	The TCP/UDP source port to match in the packet header.
VLAN Enable	Enter "1" to compare the VLAN ID specified by this policy against an Ethernet frame. Enter "0" to disable this feature.
VLAN ID	Enter the VLAN ID to compare against an Ethernet frame. This field is located in the first/only 802.1Q VLAN tag.
Service Type	Select this field and enter an 802.1p user priority to compare against an Ethernet frame.
IP DSCP List	To use IP DSCP as a match criteria, select a DSCP keyword from the list.
IP Precedence	Enter the packet's IP Precedence value to match. The IP Precedence range is 0-7.
IP TOS Bits	Enter a value match against the packet's Type of Service bits in the IP header. The IP TOS field in a packet is defined as all eight bits of the Service Type octet in the IP header. The TOS Bits value is a two-digit hexadecimal number from 00 to ff. The high-order three bits represent the IP precedence value. The high-order six bits represent the IP Differentiated Services Code Point (DSCP) value.
IP TOS Mask	Enter an IP TOS mask value to identify the bit positions in the TOS Bits value that are used for comparison against the IP TOS field in a packet. The TOS Mask value is a two-digit hexadecimal number from 00 to ff, representing an inverted (i.e. wildcard) mask. The zero-valued bits in the TOS Mask denote the bit positions in the TOS Bits value that are used for comparison against the IP TOS field of a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a TOS Bits value of a0 and a TOS Mask of 00. This is an optional configuration.

Use the following procedures to add a rate limit policy.

1. Specify the name of a policy in the **Add a new policy** field, and click **Add**.
2. Add the required match criteria under **Add a new rule**, and click **Add**.
3. Verify the rule settings under **Scheduler Rule List**.
4. Click the **Select** field for those rules to add to the policy.

5. Click **Submit**.
6. Apply the rate limit policy to one or more VAPs. See "Configuring the Default Network" on page 196.

The page includes the following buttons:

- **Refresh**: Updates the page with the latest information.
- **Submit**: Updates the switch with the values you enter.

Wireless Discovery Configuration

The UWS can discover, validate, authenticate, or monitor the following system devices:

- Peer wireless switches
- APs
- Wireless clients
- Rogue APs
- Rogue wireless clients

The UWS can discover peer wireless switches and APs regardless of whether these devices are connected to each other, located in the same Layer 2 broadcast domain, or attached to different IP subnets.

You can enable discovery between the switch and peer switches or APs by using one of following four mechanisms:

1. Manually add the IP address of the switch to the AP when it is in Standalone mode.
2. Configure a DHCP server to include the switch IP address in the DHCP response to the AP DHCP client request.
3. Use VLANs to broadcast the Broadcom Wireless Device Discovery Protocol.
4. Manually add the IP address of the AP to the switch.

Note: With this method, multiple peer switches might find the same access point. The first association always takes precedence. The AP does not change its association unless the connectivity to the current wireless switch fails or the switch tells the AP to disassociate and associate with another switch.

To configure the switch to discover APs and other switches by using methods 3 and 4, click **WLAN** > **WLAN Configuration** > **Discovery**.

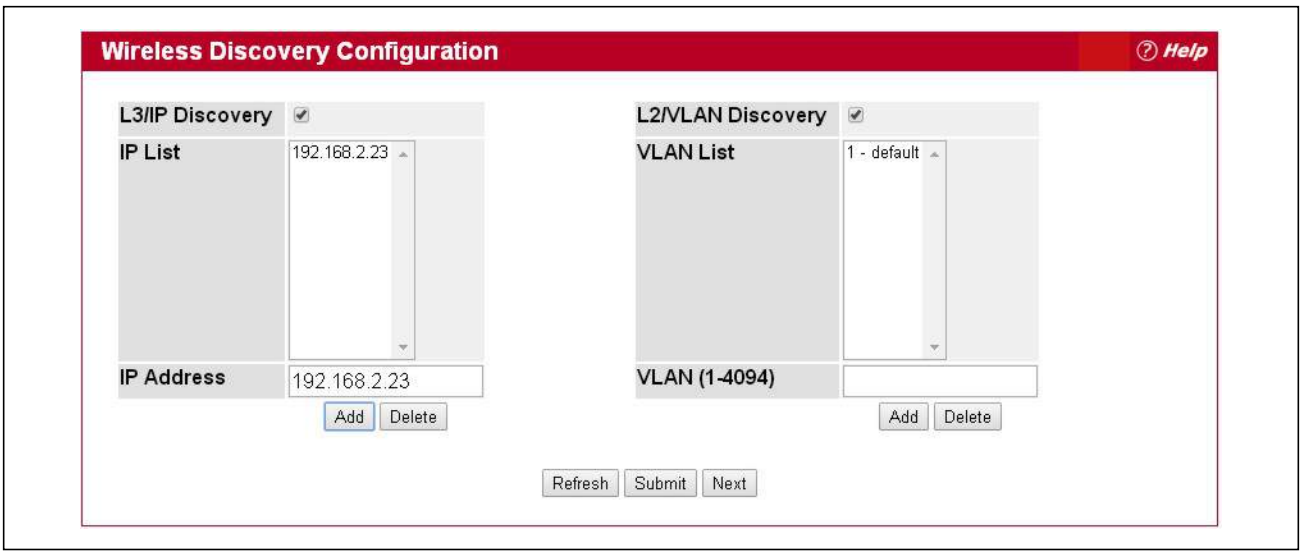


Figure 124: Wireless Discovery Configuration

For the UWS to discover other WLAN devices and establish communication with them, the devices must have their own IP address, must be able to find other WLAN devices, and must be compatible.

When the UWS discovers and validates APs, the switch takes over the management of the AP. If you configured the AP in Standalone mode, the existing AP configuration is replaced by the default AP Profile configuration on the switch.

L3/IP Discovery

You can configure up to 256 IP addresses in the UWS for potential peer switches and APs. The switch sends association invitations to all IP addresses in this list. If the device accepts the invitation and is successfully validated by the switch, the switch and the AP or peer switch are associated.

This discovery method mechanism is useful for peer switch discovery and AP discovery when the devices are in different IP subnets. In fact, for a switch to recognize a peer that is not on the same subnet, you must configure the IP addresses of each switch in the peer's L3 discovery list.

Note: The list of IP addresses is separate and independent from the list of valid managed APs. Devices discovered through this list might not be valid APs or switches.

Note: If an AP has already been discovered through another method, the UWS will not poll the IP address of the AP.

Table 114: L3 VLAN Discovery

Field	*Description*
L3/IP Discovery	Select or clear this option to enable or disable IP-based discovery of access points and peer wireless switches. When the L3/IP Discovery option is selected, IP polling is enabled and the switch will periodically poll each address in the configured IP List. By default, L3/IP Discovery is enabled.
IP List	Shows the list of IP addresses configured for discovery. To remove entries from the list, select one or more entries and click **Delete**. There are no default entries, and the maximum number of entries supported is 256.
IP Address	To add entries to the IP List, enter a valid IP address and click **Add**. Once all desired entries are added, click submit to save the list in the running configuration.

To view the IP discovery status of the devices you add to the IP List, such as whether the switch successfully polled the IP address you entered, navigate to the **WLAN > Status/Statistics > Global > IP Discovery tab.**

L2/VLAN Discovery

The Edge-Core Wireless Device Discovery Protocol is a good discovery method to use if the UWS and APs are located in the same Layer 2 multicast domain. The UWS periodically sends a multicast packet containing the discovery message on each VLAN enabled for discovery. You can enable the discovery protocol on up to 16 VLANs.

By default, VLAN 1 is enabled on the AP, and VLAN 1 is enabled for discovery on the UWS. If the switch and AP are in the same Layer 2 multicast domain, you might not need to take any action to enable AP-to-UWS discovery. The UWS also uses L2/VLAN discovery to find peer switches within the L2 multicast domain.

The APs process the discovery message only when it comes in on the management VLAN. The APs do not forward the L2 discovery messages onto the wireless media.

From the UWS, you can check the discovery status of APs and peer switches. To view information about whether the switch discovered any APs, navigate to the **WLAN > Status/Statistics > Managed AP** page. If you have not added the MAC address of the AP to the local or RADIUS Valid AP database, the AP appears in the **WLAN > Intrusion Detection > AP Authentication Failures** list, and the failure type is listed as No Database Entry.

To view information about whether the switch discovered any peer switches, navigate to the **WLAN > Status/ Statistics > Peer Switch page.**

Command Buttons

The page includes the following buttons:

- **Add**—Adds the data in the IP Address or VLAN field to the appropriate list.
- **Delete**—Deletes the selected entry from the IP or VLAN list.
- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click System > System Utilities > Save All Applied Changes.
- **Next**—Navigates to the next page in the Basic Setup configuration. Any changes you made to the current page are saved before the next page is displayed. To retain the new values across a power cycle, you must perform a

save on the WLAN switch (not the AP). To perform a save, click System > System Utilities > Save All Applied Changes.

Known Client

From the **Known Client Summary** folder, you can access the following pages:

- Known Client Summary
- Known Client Configuration

Known Client Summary

The Known Client Summary shows the wireless clients currently in the Known Client Database. The database contains wireless client MAC addresses and names. The database is used to retrieve client descriptive names from the RADIUS server as well as implement MAC Authentication.

To show the Known Client Summary page, click **WLAN** > **WLAN Configuration** > **Known Client**.

Figure 125: Known Client Summary

To view or configure information about an existing client, click the MAC address of the client.

The following table describes the fields on **Known Client Summary** page.

Table 115: Known Client Summary Fields

Field	*Description*
MAC Address	Shows the MAC address of the known client.
Name	Shows the descriptive name configured for the client when it was added to the Known Client database.

Table 115: Known Client Summary Fields (Cont.)

Field	*Description*
Authentication Action	When MAC authentication is enabled on the network, this field shows the action to take on a wireless client. The following options are available: • Grant—Allow the client with the specified MAC address to access the network. • Deny—Prohibit the client with the specified MAC address from accessing the network. • Global Action—Use the global white-list or black-list action configured on the Wireless Global Configuration page to determine how to handle the client.
Client Group	The name of a group of clients (VAP) to which the settings on this page apply. New clients are assigned to the 1-Default group by default.

Command Buttons

The page includes the following buttons:

- **Add**—Adds a client with the MAC address you enter in the field to the Known Client database.
- **Delete**—Removes the selected client from the Known Client database.
- **Delete All**—Removes all clients in the list from the Known Client database.
- **Refresh**—Updates the page with the latest information.

Known Client Configuration

When you add a client to the Known Client database or click the MAC address of a client from the Known Client Summary page, the **Known Client Configuration** page appears. On this page, you can add a descriptive name for the client and specify the authentication action to take on the client when it attempts to access the network.

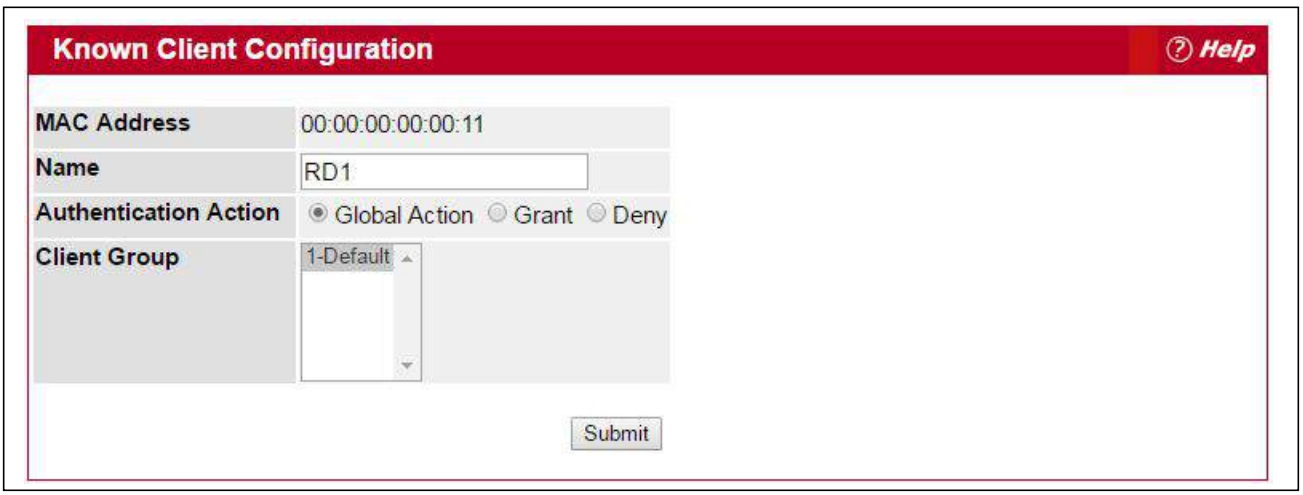


Figure 126: Known Client Configuration

The following table describes the fields on **Known Client Configuration** page.

Table 116: Known Client Configuration

Field	*Description*
MAC Address	Shows the MAC address of the client. To view or configure the name or authentication action for another client in the Known Client database, select its MAC address from the menu.
Name	Enter a descriptive name for the client, which can contain up to 32 characters, including alphanumeric and special characters. This field is optional.
Authentication Action	Specify the action to take on a wireless client when MAC authentication is enabled on the network. The following options are available: • Grant—Allow the client with the specified MAC address to access the network. • Deny—Prohibit the client with the specified MAC address from accessing the network. • Global Action—Use the global white-list or black-list action configured on the Advanced Global Configuration page to determine how to handle the client.
Client Group	The name of a group of clients (VAP) to which the settings on this page apply. Assign the known client to at least one Client Group. To assign a client to more than one group, press the Ctrl key and click each group. New clients are assigned to the 1-Default group by default.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).

AP Image Availability List

The **WLAN** > **WLAN Configuration > AP Image Availability List** page displays the AP images that have been stored on the switch. AP images can be uploaded to the switch using the System > System Utilities > Upload File to Switch page.

Figure 127: AP Image Availability List

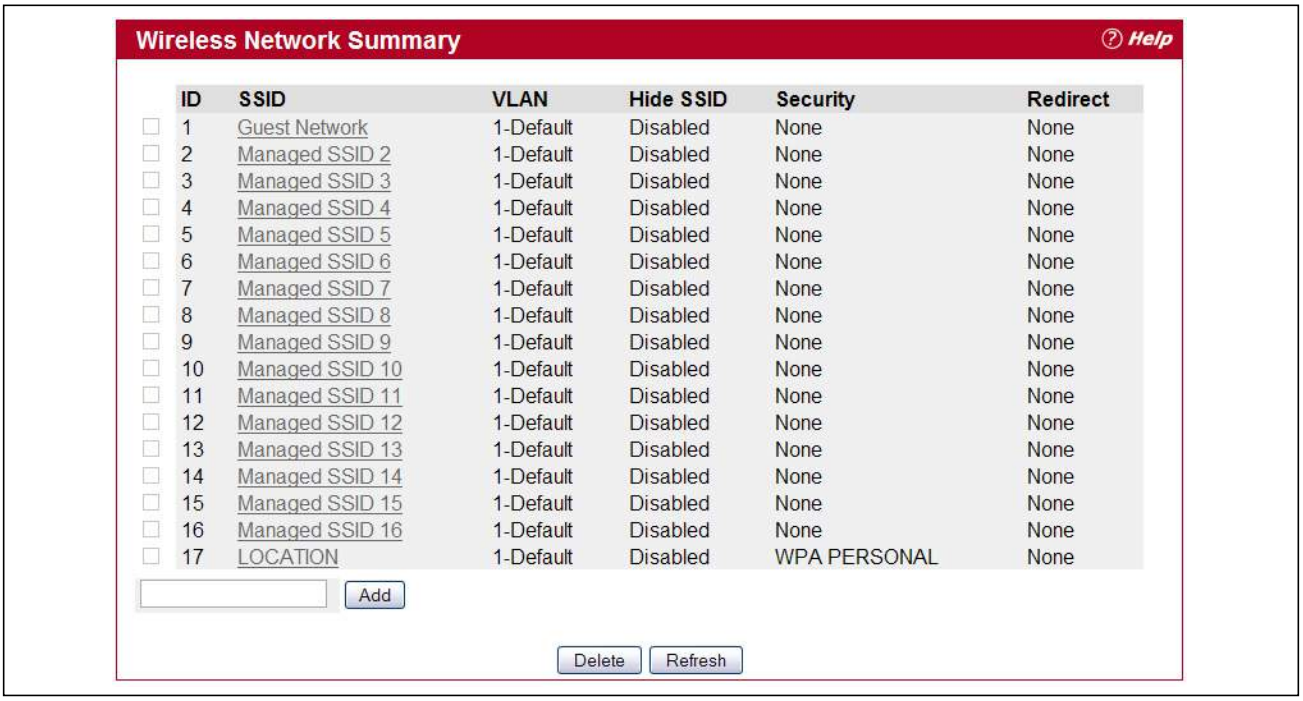
Configuring Networks

The **WLAN** > **WLAN Configuration > Networks** page displays the **Wireless Network Summary** page. Any of the networks displayed configured by clicking on an entry under the SSID field.

Wireless Network Summary

The wireless network summary shows all the wireless networks configured on the switch. The first 16 networks are created by default. You can modify the default networks, but you cannot delete them. You can add and configure up to 240 additional networks for a total of 256 wireless networks. Multiple networks can have the same SSID.

To show the wireless network summary, click **WLAN** > **WLAN Configuration** > **Networks**.



ID	SSID	VLAN	Hide SSID	Security	Redirect
1	Guest Network	1-Default	Disabled	None	None
2	Managed SSID 2	1-Default	Disabled	None	None
3	Managed SSID 3	1-Default	Disabled	None	None
4	Managed SSID 4	1-Default	Disabled	None	None
5	Managed SSID 5	1-Default	Disabled	None	None
6	Managed SSID 6	1-Default	Disabled	None	None
7	Managed SSID 7	1-Default	Disabled	None	None
8	Managed SSID 8	1-Default	Disabled	None	None
9	Managed SSID 9	1-Default	Disabled	None	None
10	Managed SSID 10	1-Default	Disabled	None	None
11	Managed SSID 11	1-Default	Disabled	None	None
12	Managed SSID 12	1-Default	Disabled	None	None
13	Managed SSID 13	1-Default	Disabled	None	None
14	Managed SSID 14	1-Default	Disabled	None	None
15	Managed SSID 15	1-Default	Disabled	None	None
16	Managed SSID 16	1-Default	Disabled	None	None
17	LOCATION	1-Default	Disabled	WPA PERSONAL	None

Figure 128: Wireless Network Summary

Table 117: Wireless Network Summary

Field	*Description*
ID	Shows the ID associated with the network. Sixteen networks are created by default. The switch supports up to 256 networks.
SSID	Identifies the name of the network. The SSID is a hyperlink to the Wireless Network Configuration page for the network.
VLAN	Shows the VLAN ID the wireless network uses.
Hide SSID	Shows whether the network broadcasts the SSID. If enabled, the SSID for this network is not included in AP beacons. To change this setting, click **Edit**.
Security	Shows the current security settings for the network.

Table 117: Wireless Network Summary (Cont.)

Field	*Description*
Redirect	Shows whether HTTP redirect is enabled. The possible values for the field are as follows: • HTTP: HTTP Redirect is enabled • None: HTTP Redirect is disabled

Command Buttons

The page includes the following buttons:

- **Add**—Adds a new network with the SSID you enter in the associated field. The Wireless Network Configuration page for the new network appears after you click **Add**.
- **Delete**—Removes the selected network. You cannot delete networks 1–16.
- **Refresh**—Updates the page with the latest information.

Wireless Network Configuration

Each network is identified by its Service Set Identifier (SSID), which is an alphanumeric key that identifies a wireless local area network. You can configure up to 256 different networks on the UWS. Each network can have a unique SSID, or you can configure multiple networks with the same SSID.

Click **Edit** for one of the networks to open the Wireless Network Configuration page, as the following figure shows.

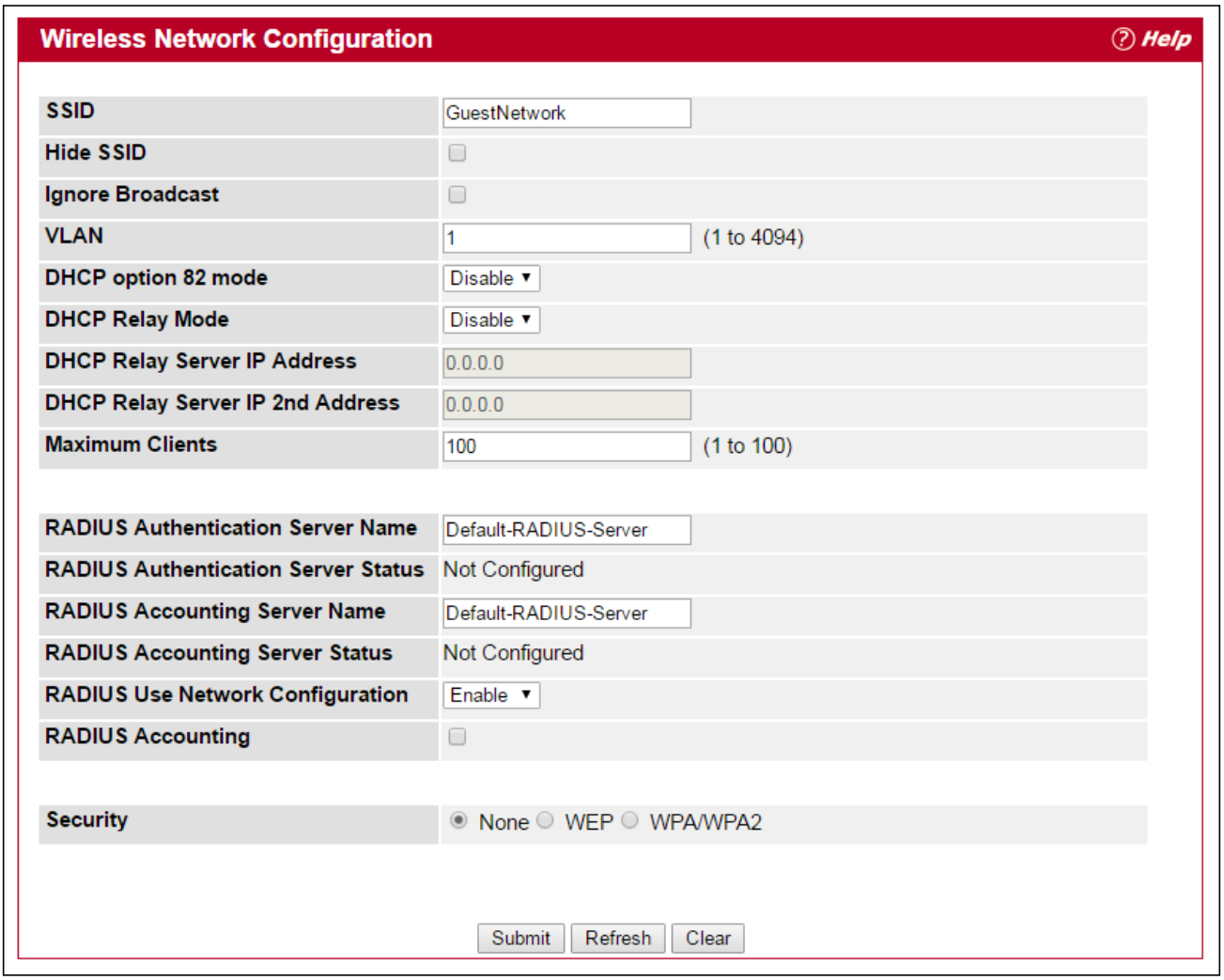


Figure 129: Configuring Network Settings

The following table describes the fields on the Wireless Network Configuration page. After you change the wireless network settings, click **Submit** to save the changes.

Table 118: Wireless Network Configuration

Field	*Description*
SSID	Wireless clients identify a wireless network by the SSID, which is an alphanumeric key that uniquely identifies a wireless local area network. The SSID can be up to thirty-two characters in length, and there are no restrictions on the characters that may be used in an SSID.
Hide SSID	You can hide the SSID broadcast to discourage stations from automatically discovering your access point. When the broadcast SSID of the AP is hidden, the network name is not displayed in the list of available networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it is able to connect. Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect, or monitor unencrypted traffic. Hiding the SSID offers a very minimal level of protection on an otherwise exposed network (such as a guest network) where the priority is making it easy for clients to get a connection and where no sensitive information is available.
Ignore Broadcast	If a wireless client broadcasts probe requests to all available SSIDs, this option controls whether the AP will respond to the probe request. • Select this option to prohibit the AP from responding to client probe requests • Clear this option to allow the AP to respond to client probe requests.
VLAN	A virtual LAN (VLAN) is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be. The nodes in a VLAN share resources and bandwidth and are isolated on that network. The Unified Wireless Switch supports the configuration of a wireless VLAN. You can configure each VAP to be on a unique VLAN or on the same VLAN as other VAPs. When a wireless client connects to the AP by using this network (SSID), the AP tags the client's traffic with the VLAN ID you configure in this field. By default, all networks use VLAN 1, which is also untagged by default. ***Note:*** The VLAN ID you configure in this field can be overwritten by the VLAN ID configured for the AP in the RADIUS server. In other words, if your network uses a RADIUS server to assign wireless clients to VLANs, the wireless client uses the VLAN ID from the RADIUS server and ignores the VLAN ID configured on the VAP.
DHCP Option 82 Mode	When DHCP Option82 is enabled, the UWS sends information about its DHCP clients to the DHCP server. When enabled, the client will get an IP address from the DHCP server according to its VLAN ID.
DHCP Relay Mode	Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients that broadcast a request. To receive the broadcast request, the DHCP server would normally have to be on the same subnet as the client. However, when the DHCP relay agent is enabled, received client requests can be forwarded directly to a known DHCP server on another subnet. Responses from the DHCP server are returned to the switch, which then broadcasts them back to clients.
DHCP Relay Server IP Address	The IP address of the DHCP relay server.
DHCP Relay Server IP 2nd Address	The IP address of a secondary DHCP server to be used if the first DHCP server does not repond.

Table 118: Wireless Network Configuration (Cont.)

Field	*Description*
Maximum Clients	Specifies the maximum number of stations allowed to associate with this access point at any one time. You can enter a value between 0 and 100.
RADIUS Authentication Server Name	Enter the name of the RADIUS server that the VAP uses for AP and client authentications. The name can contain up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted. Any RADIUS information you configure for the wireless network overrides the global RADIUS information configured on the **Wireless Global Configuration** page. The switch acts as the RADIUS client and performs all RADIUS transactions on behalf of the APs and wireless clients.
RADIUS Authentication Server Status	Indicates whether the RADIUS authentication server is configured for the VAP. To configure RADIUS server information, go to the **Security > RADIUS > Server Configuration** page.
RADIUS Accounting Server Name	Enter the name of the RADIUS server that the VAP uses for reporting wireless client associations and disassociations. The name can contain up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted. Any RADIUS information you configure for the wireless network overrides the global RADIUS information configured on the **Wireless Global Configuration** page.
RADIUS Accounting Server Status	Indicates whether the RADIUS accounting server is configured. To configure RADIUS accounting server information, go to **Security > RADIUS > Accounting Server Configuration**.
RADIUS Use Network Configuration	This field controls whether the VAP uses the network RADIUS settings or the global RADIUS settings. • Enable: Use RADIUS Servers defined on the Wireless Network Configuration page. • Disable: Use RADIUS servers defined on the Wireless Global Configuration page.
RADIUS Accounting	Select this option to enable RADIUS accounting for wireless clients.
Security	The default AP profile does not use any security mechanism by default. To protect your network, Edge-Core strongly recommends that you select a security mechanism so that unauthorized wireless clients cannot gain access to your network. The following WLAN network security options are available: • None • WEP • WPA/WPA2 If you select WEP or WPA/WPA2 as your security mechanism, additional fields appear. "Configuring AP Security" on page 199 describes the security mechanisms and the additional fields you can configure if you select WEP or WPA/WPA2.

For information on the Security settings, see "Configuring AP Security" on page 199.

AP Profiles

From the **AP Profiles** folder, you can access the following pages:

- Access Point Profile List
- Access Point Profile Global Configuration
- Access Point Profile Radio Configuration
- Access Point Profile VAP Configuration
- Access Point Profile QoS Configuration
- Wireless Network Configuration

Access Point Profile List

The switch can support APs that have different hardware capabilities, such as the supported number of radios and the supported IEEE 802.11 modes. APs that use the same profile should have the same hardware capabilities so that the settings you configure in the profile are valid for all APs within the profile. Different hardware platforms might also require different software images.

Access point configuration profiles are a useful feature for large wireless networks with APs that serve a variety of different users. You can create multiple AP profiles on the UWS to customize APs based on location, function, or other criteria. Profiles are like templates, and once you create an AP profile, you can apply that profile to any AP that the UWS manages.

For each AP profile, you can configure the following features:

- Profile settings (Name, Hardware Type ID, Wired Network Discovery VLAN ID)
- Radio settings
- VAP settings
- QoS configuration

Figure 130 on page 239 shows ten APs that are managed by a UWS in a campus network. Each building has multiple APs, and the users in one building have different network requirements than the users in other buildings. The administrator of this WLAN has created two AP profiles on the switch in addition to the default profile.

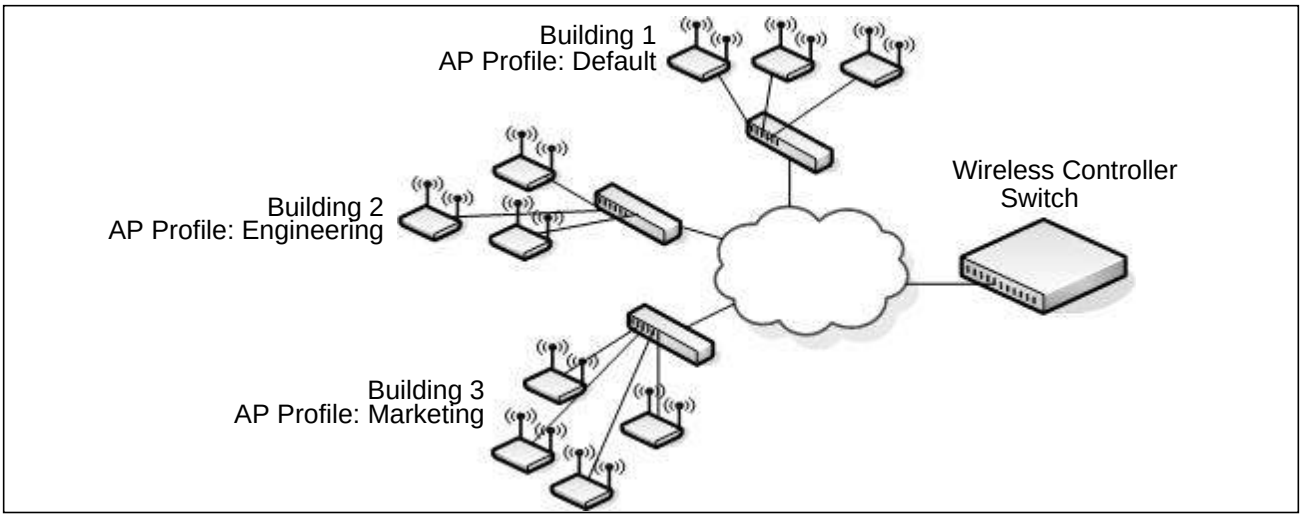


Figure 130: Multiple AP Profiles

Building 1 contains the main lobby and several conference rooms. The WLAN users in this location are primarily non-employees and guests. The APs in Building 1 uses the default AP profile with no additional networks and no security.

Building 2 is the engineering building. The Building 2 APs use a profile called “Engineering.” The Engineering profile has three different VAPs that each have a unique SSID: Hardware, Software and Test. Building 3 is the Sales and Marketing building. The Building 3 AP uses a profile called “Marketing.” The Marketing AP Profile has three VAPs. The SSIDs for the VAPs are: Sales, Marketing, and Program Management. If the network administrator adds another AP to Building 2, she assigns the Engineering profile to the AP during the AP validation process.

Creating, Copying, and Deleting AP Profiles

From the **Access Point Profile List** page, you can create, copy, or delete AP profiles. You can create up to 16 AP profiles on the UWS. To create a new profile, enter the name of the profile in the **Profile** field, and then click **Add**. The profile name can contain up to 32 alphanumeric characters as well as spaces, dashes and underscores.

To configure AP profiles, click **WLAN** > **WLAN Configuration** > **AP Profiles**.

Figure 131: Adding a Profile

After you add the profile, the **Access Point Profile Global Configuration** page for the profile appears. Click the Global, Radio, VAP, or QoS tabs to configure features for the profile.

The following table shows the fields on the page.

Table 119: Access Point Profile List

Field	*Description*
Profile	Identifies the name of the configured profile.

Table 119: Access Point Profile List

Field	*Description*
Profile Status	Indicates whether a profile is applied to one or more managed APs and shows the status for a request to re-apply the profile to its associated managed APs. The status is one of the following: • **Associated**: The profile is configured, and one or more APs managed by the switch are associated with this profile. • **Associated-Modified**: The profile has been modified since it was applied to one or more associated APs; the profile must be re-applied for the changes to take effect. • **Apply Requested**: After you select a profile and click **Apply**, the screen refreshes and shows that an apply has been requested. • **Apply In Progress**: The profile is being applied to all APs that use this profile. During this process the APs reset, and all wireless clients are disassociated from the AP. • **Configured**: The profile is configured, but no APs managed by the switch currently use this profile.

Command Buttons

The page includes the following buttons:

- **Add**—Adds a profile with the name you enter in the associated field. The Access Point Profile Global Configuration page for the new profile appears after you click **Add**.
- **Copy**—Copies the selected profile and adds it with the name you enter in the associated field.
- **Delete**—Removes the selected profile. You can rename the default profile, but you cannot delete it.
- **Apply**—Applies the profile changes to all access points that use a profile.
- **Refresh**—Updates the page with the latest information.

To copy an existing profile and all of its configurations to a new profile, select the profile with the configuration to copy, enter a name for the new profile, and click **Copy**.

To delete a profile, select the profile and click **Delete**.

To access an existing profile, click the name of the profile. When you add a new profile, it has the default AP settings. When you copy a profile, it has the AP settings configured in the original profile.

To modify any settings within a profile, click the Global, Radio, VAP or QoS settings for the profile you select and update the appropriate fields.

Applying an AP Profile

After you update an AP Profile on the UWS, the changes are not applied to the access points that use that profile until you explicitly apply the profile on the **Access Point Profile List** page or reset the APs that use the profile.

Note: When you change the VLAN ID for a wireless network, the AP might temporary lose its DHCP-assigned IP address when you apply the updated profile. If this occurs, the AP goes into Standalone mode. As soon as the AP regains its IP address from the DHCP server on your network, it resumes normal operation as a managed AP. You might also see this behavior when you enable or disable a VAP (SSID) and re-apply the AP profile.

To apply the profile changes to all access points that use the profile, select the profile and click **Apply**, as the following figure shows.

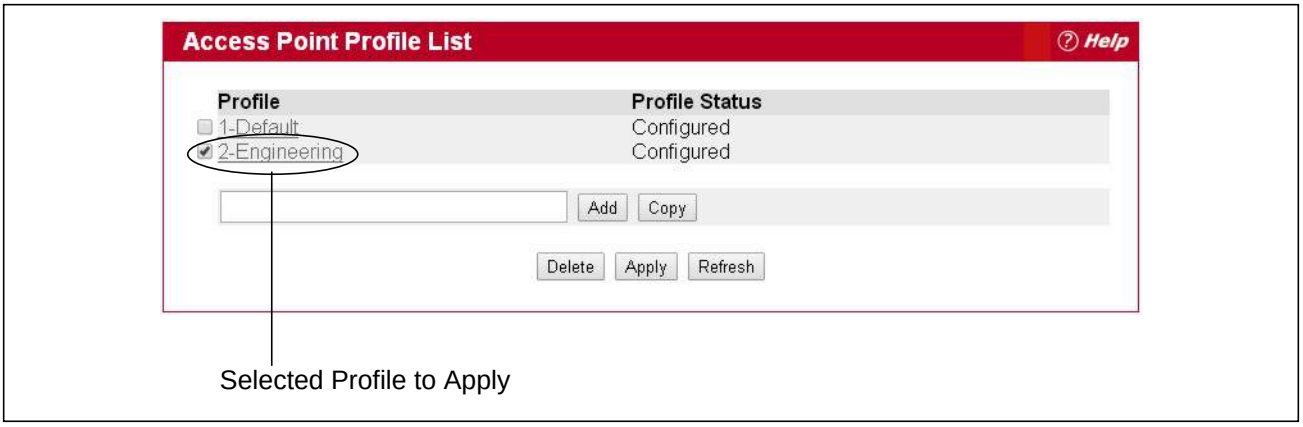


Figure 132: Applying the AP Profile

Note: When you apply new AP Profile settings to an AP, the access point stops and restarts system processes. If this happens, wireless clients will temporarily lose connectivity. It is therefore advisable to change access point settings when WLAN traffic is low.

Note: You associate a profile with an AP in the Valid AP database.

Access Point Profile Global Configuration

Use the **Access Point Profile Global Configuration** page to configure a variety of global settings for a new or existing AP profile. When you add a new profile, this page automatically appears and is populated with the default AP settings.

The switch can support APs that have different hardware capabilities, such as the supported number of radios and the supported IEEE 802.11 modes. APs that use the same profile should have the same hardware capabilities so that the settings you configure in the profile are valid for all APs within the profile. Different hardware platforms might also require different software images.

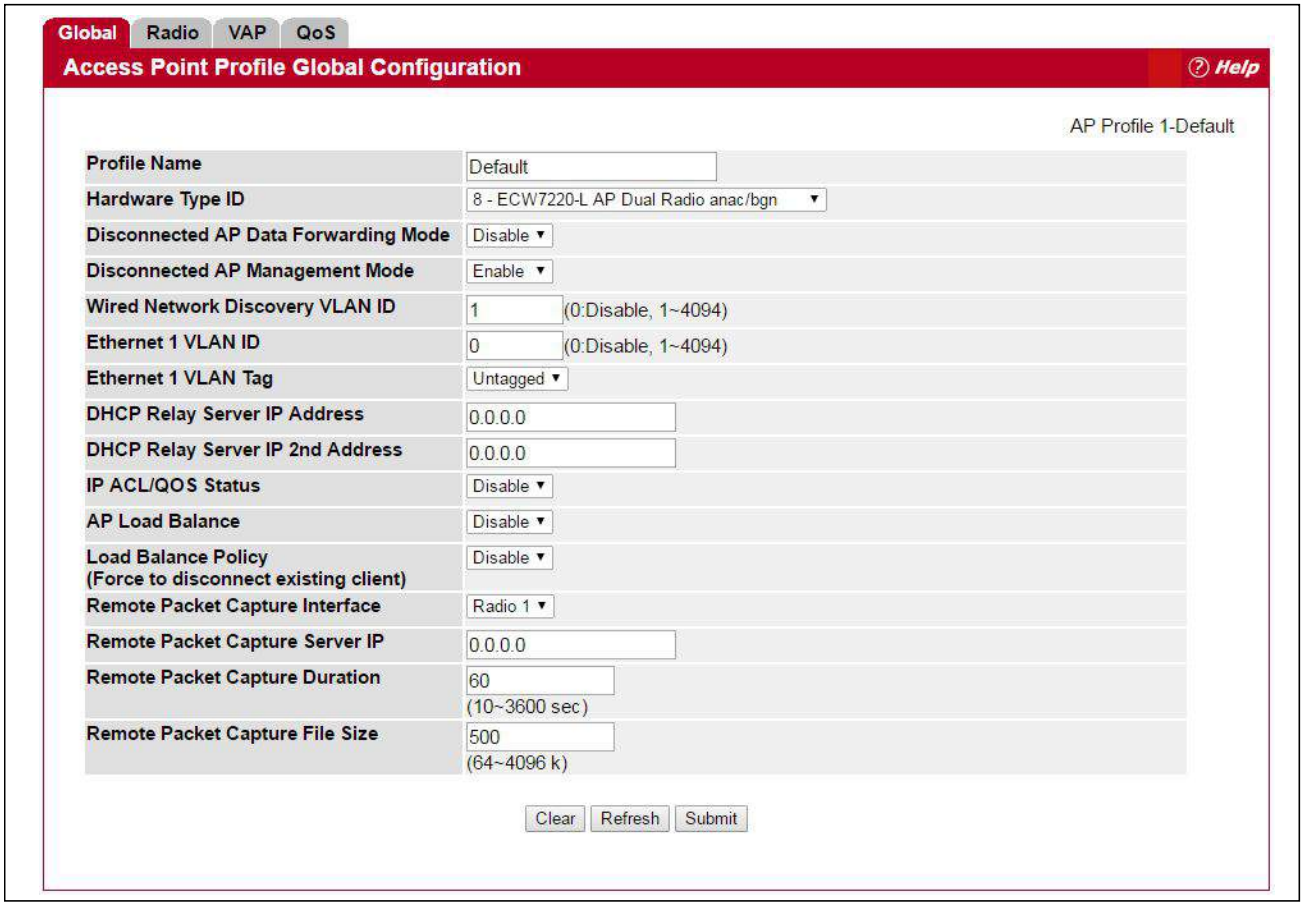


Figure 133: AP Profile Configuration

Table 120 describes the fields available on the AP Profile Global Configuration page.

Table 120: Access Point Profile Global Configuration

Field	*Description*
Profile Name	Displays the name of the selected profile. To rename the profile, enter the new name in the field and click **Submit**.

Table 120: Access Point Profile Global Configuration (Cont.)

Field	*Description*
Hardware Type ID	Select the hardware type for the APs that use this profile. The hardware type is determined, in part, by the number of radios the AP supports (single or dual) and the IEEE 802.11 modes that the radio supports (a/b/g or a/b/g/n). The options available in the Hardware Type ID are as follows: • Any • MJ Dual Radio a/b/g • MJ Single Radio a/b/g • MJ Dual Radio a/b/g/n • MJ Single Radio a/b/g/n • Enterprise Dual Radio a/b/g/n • Enterprise Single Radio a/b/g/n • AP-64 Dual Radio a/b/g/n • ECW7220-L AP Dual Radio anac/bgn • ECWO7220-L OAP Dual Radio anac/bgn • EAP7151A Single Radio b/g/n • EAP7011CA Single Radio b/g/n • EAP9012CA Dual Radio a/b/g/n • EAP7015A Single Radio b/g/n • EAP7315A Single Radio b/g/n • EAP7311A Single Radio b/g/n • EAP9012A Dual Radio a/b/g/n
Disconnected AP Data Forwarding Mode	Specifies whether the managed AP should allow clients that are already associated to continue forwarding traffic when the AP loses connection with the wireless switch. When disabled, the managed AP will not allow clients that are already associated to continue forwarding traffic if the AP loses connection with the wireless switch.
Disconnected AP Management Mode	Specifies whether the managed AP should enable stand-alone management functionality when it loses connection with the wireless switch. When disabled, the AP will not allow CLI, web, or SNMP access to the stand-alone management interface.
Wired Network Discovery VLAN ID	Enter the VLAN ID that the AP uses to send tracer packets in order to detect APs connected to the wired network. The tracer packets help APs identify unauthorized APs that do not belong to the Unified Wireless Switch but are connected to the wired network.
Ethernet 1 VLAN ID	The VLAN ID for this interface. The range is 1-4094, or 0 to disable.
Ethernet 1 VLAN Tag	This interface accepts either tagged or untagged frames. The default is untagged.
DHCP Relay Server IP Address	IP address of a DHCP relay server.
DHCP Relay Server IP 2nd Address	IP address of second DHCP relay server.
IP ACL/QoS Status	Enables IP address filtering for the profile.

Table 120: Access Point Profile Global Configuration (Cont.)

Field	*Description*
AP Load Balance	The AC implements load balancing between neighboring APs based on the number of associated clients or traffic loading. • Association Number: When an AP's number of associated clients exceeds that of its neighbors, the response to new client associations is failure. • Traffic Loading: When an AP's traffic load is over a threshold and more than twice that of neighbor APs, the response to new client associations is failure.
Load Balance Policy (Force to disconnect existing client)	If enabled, the AC will disconnect an existing client in order to balance the loading between neighboring APs.
Remote Packet Capture Interface	Selects the AP radio interface targeted for packet capture.
Remote Packet Capture Server IP	Set the server ip to save the remote capture packets.
Remote Packet Capture Duration	Set the duration to capture the packet. The range of duration is 10-3600 seconds. The default duration is 30 seconds.
Remote Packet Capture File Size	Set the file size of the remote capture packets. The range is 1~ 4096 KB. The default file size is 512 KB.

Command Buttons

The page includes the following buttons:

- **Clear**—Resets the profile configuration settings to the default values. The Profile Name is not cleared.
- **Delete**—Deletes the profile. This button is not available on the Default profile because. You can rename the Default profile, but you cannot delete it.
- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).

Access Point Profile Radio Configuration

To accommodate a broad range of wireless clients and wireless network requirements, the AP can support up to two radios. By default, Radio 1 operates in the IEEE 802.11b/g/n mode, and Radio 2 operates in the IEEE 802.11a/n mode. The difference between these modes is the frequency in which they operate. IEEE 802.11b/g/n operates in the 2.4 GHz frequency, and IEEE 802.11a/n operates in the 5 GHz frequency of the radio spectrum.

To open the **Radio** page, click **WLAN** > **WLAN Configuration** > **AP Profiles**, click one of the profiles, and then click the **Radio** tab.

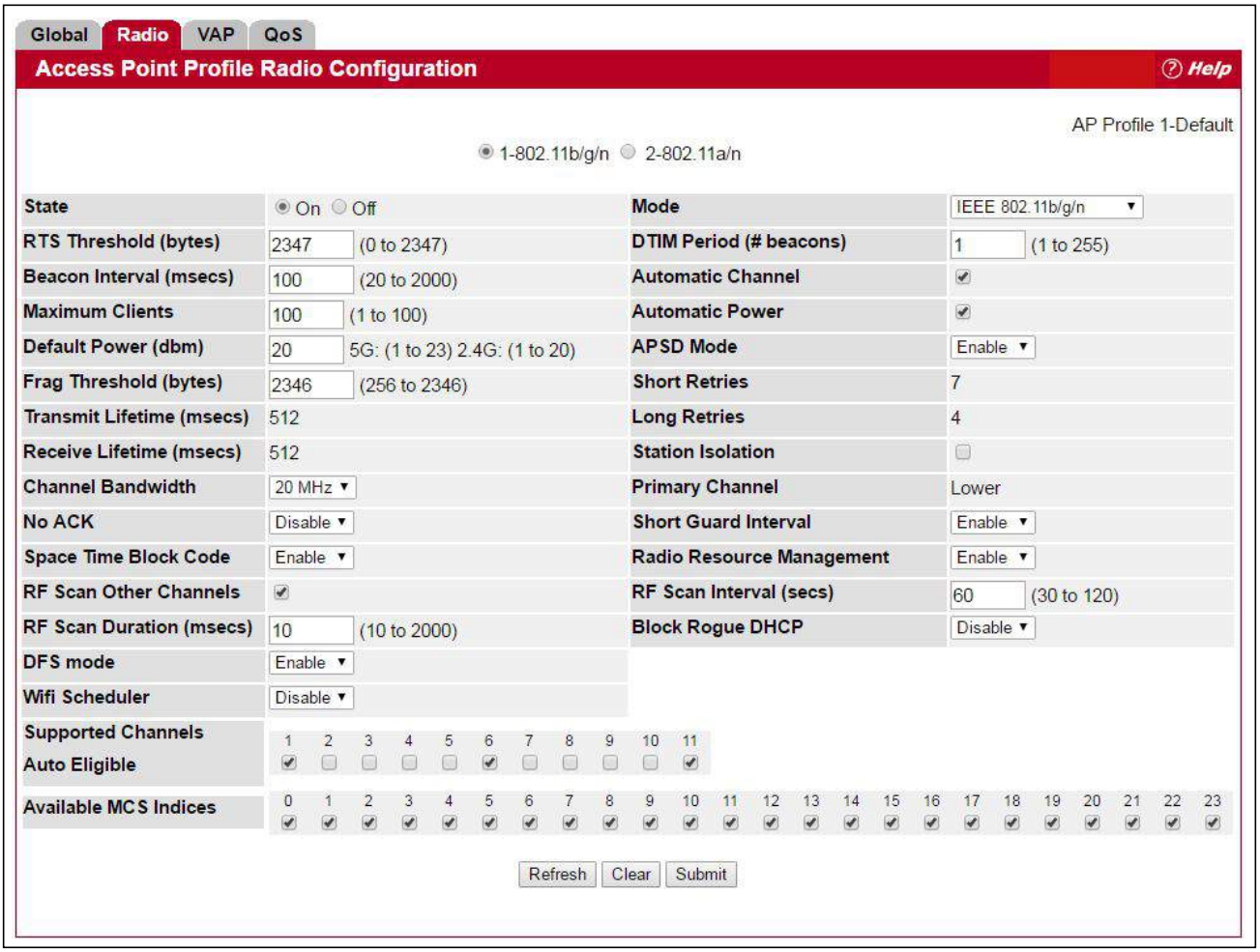


Figure 134: AP Profile Radio Settings

To change the settings for a radio, you must first select the radio you want to configure (1 or 2). After you change the settings, click **Submit** to apply the settings. Changes to the settings apply only to the selected radio.

Table 121: Radio Settings

Field	*Description*
1-802.11b/g/n **2-802.11a/n**	From this field, you can select the radio that you want to configure. By default, Radio 1 operates in IEEE 802.11b/g/n mode, and Radio 2 operates in IEEE 802.11a/n mode. If you change the mode, the labels for the radios change accordingly. Changes to the settings apply only to the selected radio.
State	Specify whether you want the radio on or off by clicking **On** or **Off**. If you turn off a radio, the AP sends disassociation frames to all the wireless clients it is currently supporting so that the radio can be gracefully shutdown and the clients can start the association process with other available APs.
RTS Threshold	Specify a Request to Send (RTS) Threshold value between 0 and 2347. The RTS threshold indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed. Changing the RTS threshold can help control traffic flow through the AP, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.
Beacon Interval	Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second). The Beacon Interval value is set in milliseconds. Enter a value from 20 to 2000.
Maximum Clients	Specify the maximum number of stations allowed to associate with this access point at any one time. You can enter a value between 0 and 200.
Default Power (dbm)	The automatic power algorithm will not reduce the power below the number you set in the default power field. By default, the power level is 20 dBm. Therefore, even if you enable automatic power, the power of the RF signal will not decrease. The power level is the maximum transmission power for the RF signal.
Frag Threshold (bytes)	The fragmentation threshold limits the size of packets transmitted over the network. Acceptable values are *even* numbers from 256-2345. Packets that are under the configured size are not fragmented. A value of 2346 means that packets are not fragmented.
Transmit Lifetime	Shows the number of milliseconds to wait before terminating attempts to transmit the MSDU after the initial transmission.
Receive Lifetime	Shows the number of milliseconds to wait before terminating attempts to reassemble the MMPDU or MSDU after the initial reception of a fragmented MMPDU or MSDU.
Channel Bandwidth	The 802.11n specification allows the use of a 40-MHz-wide channel in addition to the legacy 20-MHz channel available with other modes. The 40-MHz channel enables higher data rates but leaves fewer channels available for use by other 2.4 GHz and 5 GHz devices. The 40-MHz option is enabled by default for 802.11a/n modes and 20 MHz for 802.11b/g/n modes. You can use this setting to restrict the use of the channel bandwidth to a 20-MHz channel.
No ACK	Select Enable to specify that the AP should not acknowledge frames with QosNoAck as the service class value.

Table 121: Radio Settings (Cont.)

Field	*Description*
Space Time Block Code	Space Time Block Coding (STBC) is an 802.11n technique intended to improve the reliability of data transmissions. The data stream is transmitted on multiple antennas so the receiving system has a better chance of detecting at least one of the data streams. Select one of the following options: • Enable — The AP transmits the same data stream on multiple antennas at the same time. • Disable — The AP does not transmits the same data on multiple antennas.
RF Scan Other Channels	The access point can perform RF scans to collect information about other wireless devices within range and then report this information to the UWS. If enabled, the radio periodically moves away from the operational channel to scan other channels. Enabling this mode causes the radio to interrupt user traffic, which may be noticeable with voice connections. When disabled, the AP only scans the operating channel.
RF Scan Duration	This field controls the amount of time the radio spends scanning one of the other channels during an RF scan.
DFS Mode	DFS (Dynamic Frequency Selection) is a mechanism that requires wireless devices to share spectrum and avoid co-channel operation with radar systems in the 5 GHz band. DFS requirements vary based on the regulatory domain, which is determined by the country code setting of the AP. For radios in the 5 GHz band, when DFS support is on and the regulatory domain requires radar detection on the channel, DFS and Transmit Power Control (TPC) features of 802.11h are activated.
WIFI Scheduler	Selects an ACL policy which imposes a limitation on the time range during which the WLAN is enabled. See "WIFI Scheduler" on page 223.
Supported Channels	This field displays the channels that are supported for the radio mode currently selected on the page and for the country configured on the **Global Wireless Settings** page.
Auto Eligible	Select the **Auto Eligible** option beneath each channel to include the channel in the automatic channel assignment process.
Available MCS Indices	This field shows the Modulation and Coding Scheme (MCS) index values supported by the radio. Each index can be enabled and disabled independently.

Table 121: Radio Settings (Cont.)

Field	*Description*
Mode	The Mode defines the Physical Layer (PHY) standard the radio uses. Select one of the following modes for each radio interface: • **IEEE 802.11a** is a PHY standard that specifies operating in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 6 to 54 Mbps. • **IEEE 802.11a/n/ac** operates in the 5 GHz ISM band and includes support for 802.11a, 802.11n, and 802.11ac devices. IEEE 802.11n is an extension of the 802.11 standard that includes multiple-input multiple-output (MIMO) technology. IEEE 802.11n supports data ranges of up to 248 Mbps and nearly twice the indoor range of 802.11 b, 802.11g, and 802.11a. IEEE 802.11ac has expected multi-station WLAN throughput of at least 1 Gigabit per second and a single link throughput of at least 500 megabits per second (500 Mbit/s). This is accomplished by using wider RF bandwidth (up to 160 MHz), more MIMO spatial streams (up to eight), downlink multi-user MIMO (up to four clients), and high-density modulation (up to 256-QAM). • **5 GHz IEEE 802.11n/ac** is the recommended mode for networks with 802.11n or 802.11ac devices that operate in the 5 GHz frequency that do not need to support 802.11a or 802.11b/g devices. IEEE 802.11n/ac can achieve a higher throughput when it does not need to be compatible with legacy devices (802.11b/g or 802.11a).
DTIM Period (# beacons)	The Delivery Traffic Information Map (DTIM) message is an element included in some Beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the access point awaiting pick-up. The DTIM period you specify indicates how often the clients served by this access point should check for buffered data still on the AP awaiting pickup. Specify a DTIM period within the given range (1–255). The measurement is in beacons. For example, if you set this field to 1, clients will check for buffered data on the AP at every beacon. If you set this field to 10, clients will check on every 10th beacon.
Automatic Channel	The channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface. When the AP boots, the AP scans the RF area for occupied channels and selects a channel from the available non-interfering or clear channels. However, channel conditions can change during operation. Enabling the **Automatic Channel** makes APs assigned to this profile eligible for auto-channel selection. You can automatically or manually run the auto-channel selection algorithm to allow the UWS to adjust the channel on APs as WLAN conditions change. By default, the global auto-channel mode is set to manual. To enable the automatic channel selection mode, go to the **AP Management > RF Management** page and select Fixed or Interval for the Channel Plan mode. You can also run the automatic channel selection algorithm manually from the **Manual Channel Plan** page. ***Note:*** If you assign a static channel to an AP in the Valid AP database or on the Advanced AP Management page, the AP will not participate in the auto-channel selection.

Table 121: Radio Settings (Cont.)

Field	*Description*
Automatic Power	The power level affects how far an AP broadcasts its RF signal. If the power level is too low, wireless clients will not detect the signal or experience poor WLAN performance. If the power level is too high, the RF signal might interfere with other APs within range. Automatic power uses a proprietary algorithm to automatically adjust the RF signal to broadcast far enough to reach wireless clients, but not so far that it interferes with RF signals broadcast by other APs. The power level algorithm increases or decreases the power level in 10% increments based on presence or absence of packet retransmission errors.
APSD Mode	Select Enable to enable Automatic Power Save Delivery (APSD), which is a power management method. APSD is recommended if VoIP phones access the network through the AP.
Short Retries	The value in this field indicates the maximum number of transmission attempts on frame sizes less than or equal to the RTS Threshold. The range is 1-255.
Long Retries	The value in this field indicates the maximum number of transmission attempts on frame sizes greater than the RTS Threshold. The range is 1-255.
Station Isolation	When this option is selected, the AP blocks communication between wireless clients. It still allows data traffic between its wireless clients and wired devices on the network, but not among wireless clients. This feature is disabled by default. • To enable Multicast and Broadcast Rate Limiting, click Enabled. • To disable Multicast and Broadcast Rate Disabled, click Disabled.
Primary Channel	This setting is editable only when a channel is selected and the channel bandwidth is set to 40 MHz. A 40-MHz channel can be considered to consist of two 20-MHz channels that are contiguous in the frequency domain. These two 20-MHz channels are often referred to as the Primary and Secondary channels. The Primary Channel is used for 802.11n clients that support only a 20-MHz channel bandwidth and for legacy clients. Use this setting to set the Primary Channel as the upper or lower 20-MHz channel in the 40-MHz band.
Short Guard Interval	The guard interval is the dead time, in nanoseconds, between OFDM symbols. The guard interval prevents Inter-Symbol and Inter-Carrier Interference (ISI, ICI). The 802.11n mode allows for a reduction in this guard interval from the a and g definition of 800 nanoseconds to 400 nanoseconds. Reducing the guard interval can yield a 10% improvement in data throughput. Select one of the following options: • Enable — The AP transmits data using a 400 ns guard Interval when communicating with clients that also support the 400 ns guard interval. • Disable — The AP transmits data using an 800 ns guard interval.
Radio Resource Management	Radio Resource Measurement (RRM) mode requires the Wireless System to send additional information in beacons, probe responses, and association responses. Enable or disable the support for radio resource measurement feature in the AP profile. The feature is set independently for each radio and is enabled by default.
RF Scan Interval	This field controls the length of time between channel changes during the RF Scan.
Block Rogue DHCP	A DHCP server classified as a threat by one of the threat detection algorithms can be blocked from accessing the network using this option. (Default: Disabled)

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Clear**—Resets the settings on the page to the default values.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).

Access Point Profile VAP Configuration

The **Access Point Profile VAP Configuration** page displays the virtual access point (VAP) settings associated with the selected AP profile. Each VAP is identified by its network number and Service Set Identifier (SSID). You can configure and enable up to 16 VAPs per radio on each physical access point.

To open the **VAP** page, click **WLAN** > **WLAN Configuration** > **AP Profiles**, click one of the profiles, and then click the **VAP** tab.

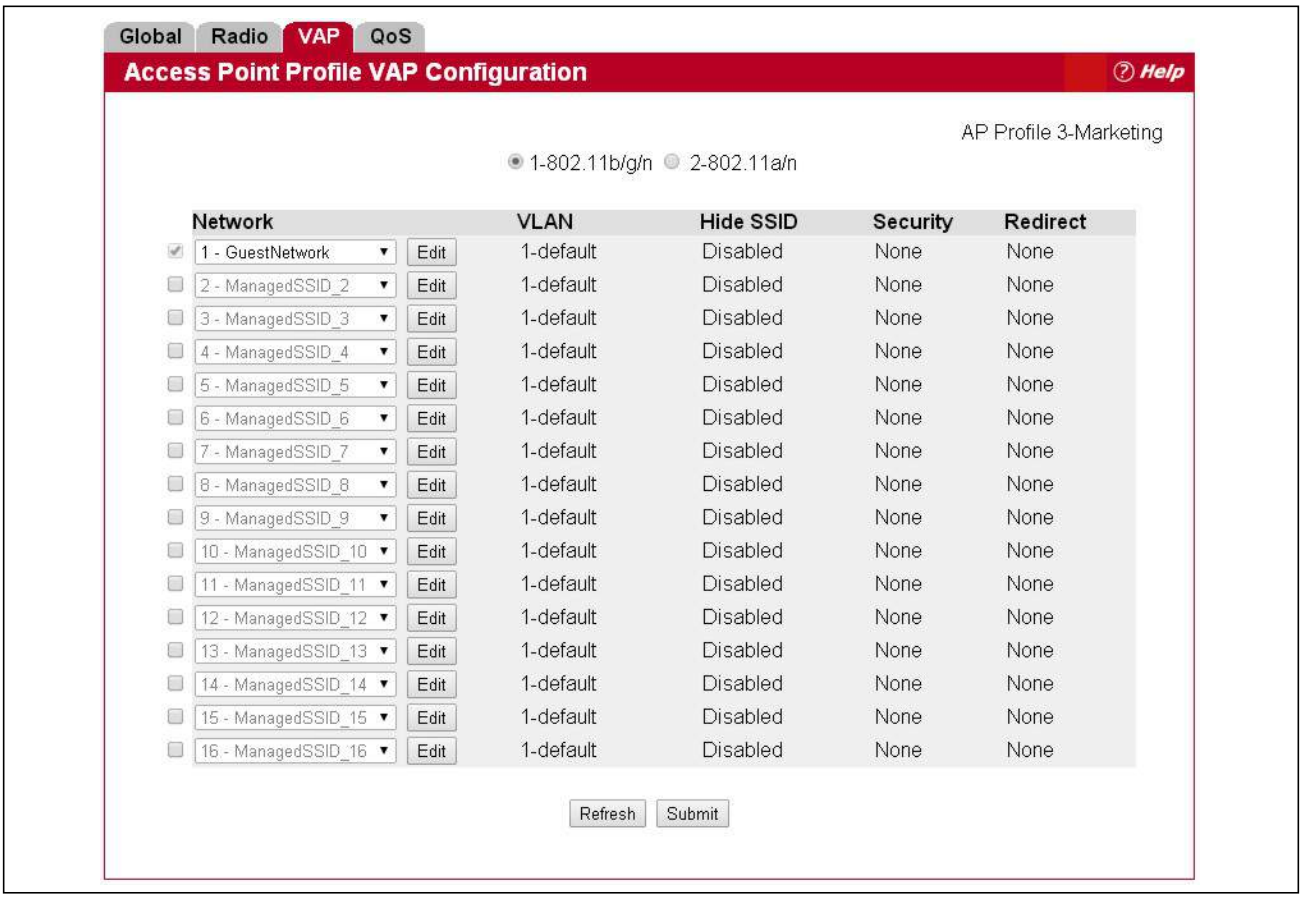


Figure 135: AP Profile VAP Configuration

The following table describes the fields on the **Access Point Profile VAP Configuration** page.

Table 122: Default VAP Configuration

Field	*Description*
Radio 1 **Radio 2**	You configure the VAPs for Radio 1 and Radio 2 separately. Select the radio to configure the settings for before you enable the VAP.
Network	Use the option to the left of the network to enable or disable the corresponding VAP on the selected radio. When enabled, click **Edit** and use the menu to select a network to assign to the VAP. You can configure up to 64 separate networks on the switch and apply them across multiple radio and VAP interfaces. By default, 16 networks are pre-configured and applied in order to the VAPs on each radio. Enabling a VAP on one radio does not automatically enable it on the other radio. ***Note:*** You cannot disable the default VAP, VAP0. To configure additional networks, click **WLAN > WLAN Configuration > Networks**.
Edit	Click **Edit** to modify settings for the corresponding network. When you click **Edit**, the Wireless Network Configuration page appears.
VLAN	Shows the VLAN ID of the VAP. To change this setting, click **Edit**.
Hide SSID	Shows whether the VAP broadcasts the SSID. If enabled, the SSID for this network is not included in AP beacons. To change this setting, click **Edit**.
Security	Shows the current security settings for the VAP. To change this setting, click **Edit**.
Redirect	Shows whether HTTP redirect is enabled. The possible values for the field are as follows: • HTTP: HTTP Redirect is enabled • None: HTTP Redirect is disabled

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).

Access Point Profile QoS Configuration

Quality of Service (QoS) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like Voice-over-IP (VoIP), other types of audio, video, and streaming media as well as traditional IP data over the Unified Wireless Switch.

To display the QoS Configuration page for an AP profile, click **WLAN > WLAN Configuration > AP Profiles**, click on the corresponding profile, and click the **QoS** tab. Click the radio button corresponding to the radio interface you want to configure (QoS is configured per radio interface).

To open the **QoS** page, click **WLAN** > **WLAN Configuration** > **AP Profiles**, click one of the profiles, and then click the **QoS** tab.

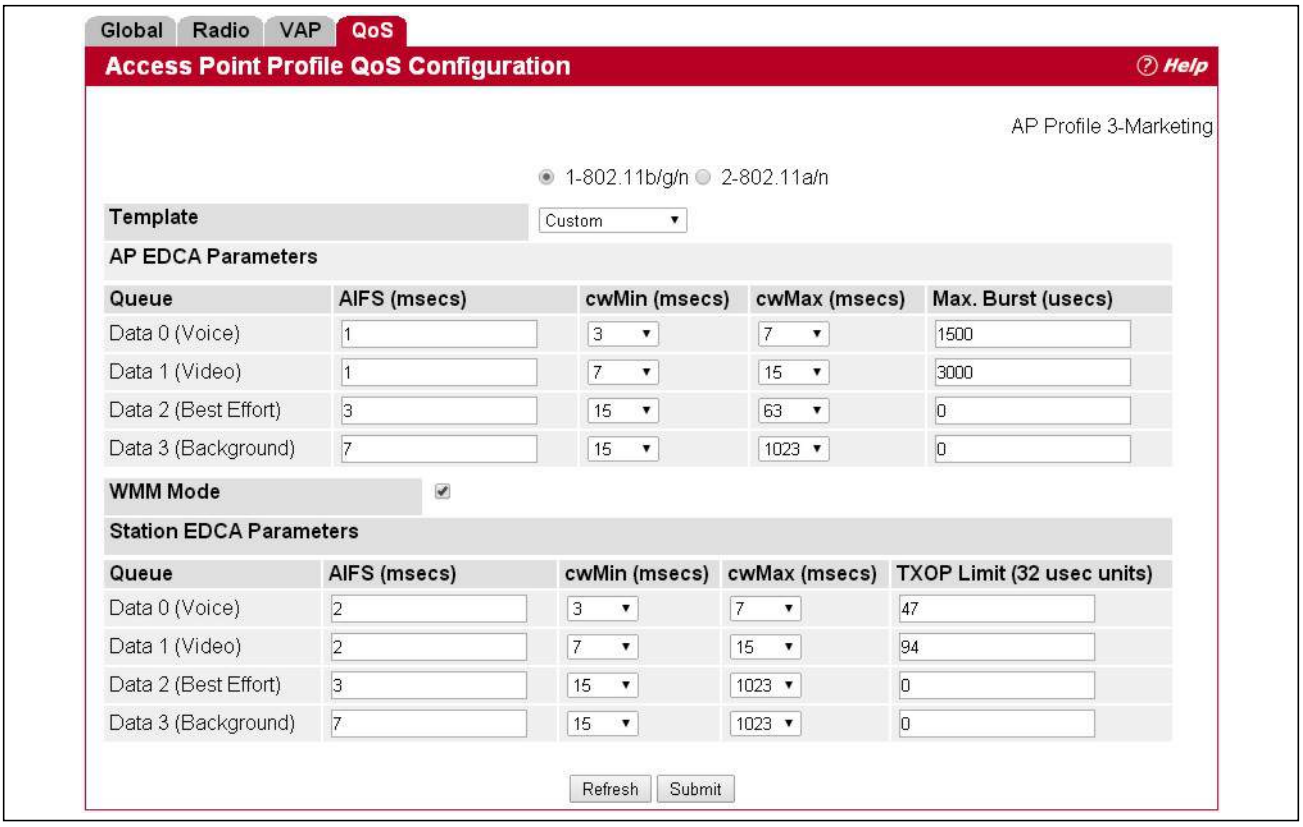


Figure 136: QoS Configuration

Configuring Quality of Service (QoS) on the Unified Wireless Switch consists of setting parameters on existing queues for different types of wireless traffic, and effectively specifying minimum and maximum wait times (through Contention Windows) for transmission. The settings described here apply to data transmission behavior on the access point only, not to that of the client stations.

AP Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the access point to the client station. Station Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the client station to the access point.

You can specify custom QoS settings, or you can select a template that configures the AP profile with pre-defined settings that are optimized for data traffic or voice traffic.

Table 123 describes the QoS settings you can configure.

Table 123: QoS Settings

Field	*Description*
Template	Select the QoS template to apply to the AP profile. If you select Custom, you can change the AP and station parameters. If you select Voice or Factory Defaults, the switch will use the pre-defined settings for the template you select.
AP EDCA Parameters	
Queue	Queues are defined for different types of data transmitted from AP-to-station: • Data 0 (Voice)—High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. • Data 1(Video)—High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. • Data 2 (best effort)—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. • Data 3 (Background)—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AIFS (Inter-Frame Space)	The **Arbitration Inter-Frame Spacing (AIFS)** specifies a wait time for data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 255.
cwMin (Minimum Contention Window)	This parameter is input to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission. The value specified here in the **Minimum Contention Window** is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window. Valid values for the cwmin are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for cwmin must be lower than the value for cwmax.
cwMax (Maximum Contention Window)	The value specified here in the **Maximum Contention Window** is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the cwmax are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for cwmax must be higher than the value for cwmin.
Max. Burst	**AP EDCA Parameter Only** (The Max. Burst Length applies only to traffic flowing from the access point to the client station.) This value specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A *packet burst* is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance. Valid values for maximum burst length are 0.0 through 999.

Table 123: QoS Settings (Cont.)

Field	*Description*
General Parameters	
WMM Mode	**WI-FI MultiMedia** (WMM) is enabled by default. With WMM enabled, QoS prioritization and coordination of wireless medium access is on. With WMM enabled, QoS settings on the Unified Wireless Switch control *downstream* traffic flowing from the access point to client station (AP EDCA parameters) and the *upstream* traffic flowing from the station to the access point (station EDCA parameters). Disabling WMM deactivates QoS control of station EDCA parameters on *upstream* traffic flowing from the station to the access point With WMM disabled, you can still set some parameters on the downstream traffic flowing from the access point to the client station (AP EDCA parameters). To disable WMM extensions, click **Disabled**. To enable WMM extensions, click **Enabled**.
Station EDCA Parameters	
Queue	Queues are defined for different types of data transmitted from station-to-AP: • Data 0 (Voice)—Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. • Data 1(Video)—Highest priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. • Data 2 (best effort)—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. • Data 3 (Background)—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AIFS (Inter-Frame Space)	The **Arbitration Inter-Frame Spacing (AIFS)** specifies a wait time for data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 255.
cwMin (Minimum Contention Window)	This parameter is used by the algorithm that determines the initial random backoff wait time (window) for data transmission during a period of contention for The value specified in the **Minimum Contention Window** is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated will be a number between 0 and the number specified here. If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window.
cwMax (Maximum Contention Window)	The value specified in the **Maximum Contention Window** is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached.

Table 123: QoS Settings (Cont.)

Field	*Description*
TXOP Limit	**Station EDCA Parameter Only** (The TXOP Limit applies only to traffic flowing from the client station to the access point.) The Transmission Opportunity (TXOP) is an interval of time when a WME client station has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for client stations; that is, the interval of time when a WMM client station has the right to initiate transmissions on the wireless network.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).
- **Refresh**—Updates the page with the latest information.

Wireless Network Configuration

The **Wireless Network Configuration** page displays the virtual access point (VAP) settings associated with the selected AP profile. Each VAP has an associated network, which is identified by its network number and Service Set Identifier (SSID). You can configure and enable up to 16 VAPs per radio on each physical access point.

VAPs segment the wireless LAN into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. To a wireless client, each VAP appears to be a single physical access point. However, since the VAPs use the same channel, there is no risk of RF interference among the networks that are on a single AP.

VAPs can help you maintain better control over broadcast and multicast traffic, which affects network performance. You can also configure different security mechanisms for each VAP.

A VAP is a physical entity. Each VAP maps directly to a MAC address. A network is a logical entity that you apply to a VAP. Networks are identified by a network number and an associated SSID. The SSID does not need to be unique for each network. You can create and modify a network in one place and apply the network to one or more VAPs as needed. This allows you to mix networks within different profiles without having to reconfigure everything. When you edit a network configuration that is applied to more than one VAP, you edit it for every VAP that uses the network.

Configuring Basic Settings for a Wireless Network

Each network is identified by its Service Set Identifier (SSID), which is an alphanumeric key that identifies a wireless local area network. You can configure up to 64 different networks on the UWS. Each network can have a unique SSID, or you can configure multiple networks with the same SSID.

The Default AP profile has one VAP on each radio enabled by default. The default VAP uses the Guest Network SSID, and there is no security to prevent wireless clients from associating with the VAP. To edit the settings for a configured VAP, under the **WLAN** > **WLAN Configuration** > **AP Profiles** > **VAP** tab, select the check box next to the VAP. Once you enable a VAP, you can select the network (SSID) to use from the drop-down menu. To change Network settings, click **Edit**.

When you click **Edit** for one of the networks that display on the VAP page, the Wireless Network Configuration page appears. Refer to "Configuring the Default Network" on page 196 for information about the fields listed on this page.

Local Access Point Database

The **Local Access Point Database** page contains information about APs configured in the local database. If RADIUS servers are configured on the WLAN > WLAN Configuration > Networks > Wireless Network Configuration page, information about the APs to be managed by the switch must be added to the external RADIUS database.

Adding a Valid Access Point

You can add an AP into the local list of Valid APs from the **WLAN > WLAN Configuration > Local AP Database** page, as the following figure shows, or you can add an AP from the AP Authentication Failures or Rogue RF Scan lists.

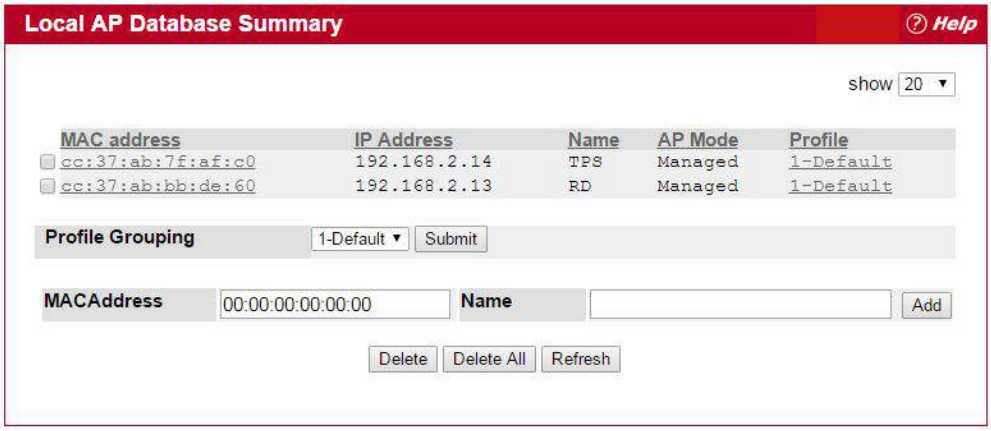


Figure 137: Adding a Valid AP

Table 124: Local Access Point Database

Field	*Description*
MAC Address	Enter the MAC address of the AP in this field. When you add the MAC address, you add the AP to the local database on the switch.
IP Address	This field displays the IP address of the AP.
Name	Enter a name to help identify the AP. This field is optional and accepts up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted.
AP Mode	This field displays the current mode of the AP, which can be one of the following: • Managed • Standalone • Rogue To configure a different mode, click the MAC address of the AP to go to the Valid Access Point Configuration page.

Table 124: Local Access Point Database

Field	*Description*
Profile	This field displays the AP profile assigned to the AP. To assign a different profile to the AP, click the MAC address of the AP to go to the Valid Access Point Configuration page. Click the profile name to access the configuration pages for the profile.
Profile Grouping	Assigns a profile to the selected MAC address entries.

After you enter the MAC address and name of the AP to add to the list, click **Add** to add the AP to the database and to access the configuration page for the AP. For an AP that is already in the database, click the MAC address of the AP to access its configuration page.

Command Buttons

The page includes the following buttons:

- **Add**—Adds the AP MAC Address and Name information to the local Valid AP database.
- **Delete**—Deletes any selected APs from the local Valid AP database. This button is available if the check box next to at least one AP MAC address is selected. Managed APs must be reset to complete their removal from the Valid AP database.
- **Delete All**—Deletes all APs from the local Valid AP database. Managed APs must be reset to complete their removal from the Valid AP database.
- **Refresh**—Updates the page with the latest information.

Valid Access Point Configuration

From the **Valid Access Point Configuration** page, you can manually set the channel and RF signal transmit power level for an individual AP. You can also configure the AP mode and local authentication password, and you can specify which profile the AP uses.

If you use the local AP database for AP validation, the switch maintains the database of access points that you validate. When you add the MAC address of an AP to the database, you can specify whether the AP is a managed AP, standalone AP, or Rogue. If the AP is to be managed by the switch, you can assign an AP profile to the device. When the switch collects and reports information from the RF scan, it can assign the appropriate status to an AP if it is in the database.

Refer to “Valid Access Point Configuration” on page 205 for information about the items listed on the following page.

Note: Any configuration changes for a managed AP will not be applied until the AP is reset and re-authenticated. If you select a different profile from the menu, a pop-up message asks you to confirm the change. If the AP is managed, a second message asks if you would like to reset the AP. If you click OK, the AP is reset.

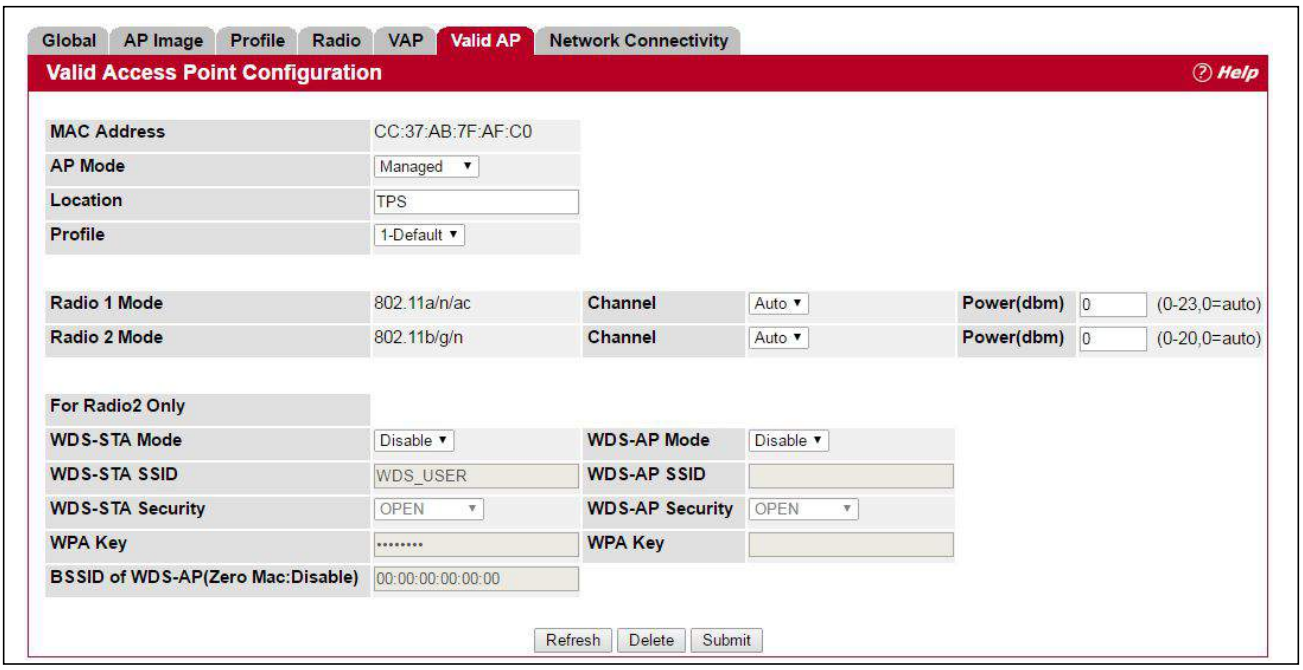


Figure 138: Configuring a Valid Access Point

For information about the fields available on this page refer to Table 104: "Valid Access Point Configuration," on page 206.

Standalone APs are managed individually, and not by using a UWS (Unified Wireless Switch). By including standalone APs in the Valid AP database and specifying their expected settings, you can help ensure that only legitimate APs are on your network. If any of the expected settings you configure for the standalone AP do not match the settings detected through the RF scan, and the *Standalone AP with unexpected configuration* test is enabled on the **WLAN > WLAN Configuration > WIDS Security** page, the standalone AP is listed as a Rogue on the **Intrusion Detection > Rogue/RF Scan** page.

If you select Standalone from the Managed Mode menu on the **Valid Access Point Configuration** page, the screen refreshes, and additional fields appear. The following table describes the additional information you can include about the standalone APs you add to the Valid AP database.

Table 125: Valid AP Configuration (Standalone Mode)

Field	*Description*
Expected SSID	Enter the SSID that identifies the wireless network on the standalone AP.
Expected Channel	Select the channel that the standalone AP uses. If the AP is configured to automatically select a channel, or if you do not want to specify a channel, select Any.
Expected WDS Mode	Standalone APs can use a Wireless Distribution System (WDS) link to communicate with each other without wires. The menu contains the following options: • **Bridge**: Select this option if the standalone AP you add to the Valid AP database is configured to use one or more WDS links. • **Normal**: Select this option if the standalone AP is not configured to use any WDS links. • **Any**: Select this option if the standalone AP might use a WDS link.

Table 125: Valid AP Configuration (Standalone Mode) (Cont.)

Field	*Description*
Expected Security Mode	Select the option to specify the type of security the AP uses: • **Any**—Any security mode • **Open**—No security • **WEP**—Static WEP or WEP 802.1X • **WPA/WAP2**—WPA and/or WPA2 (Personal or Enterprise)
Expected Wired Network Mode	If the standalone AP is allowed on the wired network, select Allowed. If the AP is not permitted on the wired network, select Not Allowed.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Delete**—Deletes the AP from the local Valid AP database. Managed APs must be reset to complete their removal from the Valid AP database.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).

Peer Switch

Peer Switch Configuration Request Status

The Peer Switch Configuration feature allows you to send a variety of configuration information from one switch to all other switches. In addition to keeping the switches synchronized, this function allows you to manage all wireless switches in the cluster from one switch. The **Peer Switch Configuration Request Status** page provides information about the status of the configuration upgrade on the switches in the cluster.

To open the **Peer Switch Configuration Request Status** page, click **WLAN** > **WLAN Configuration** > **Peer Switch**.

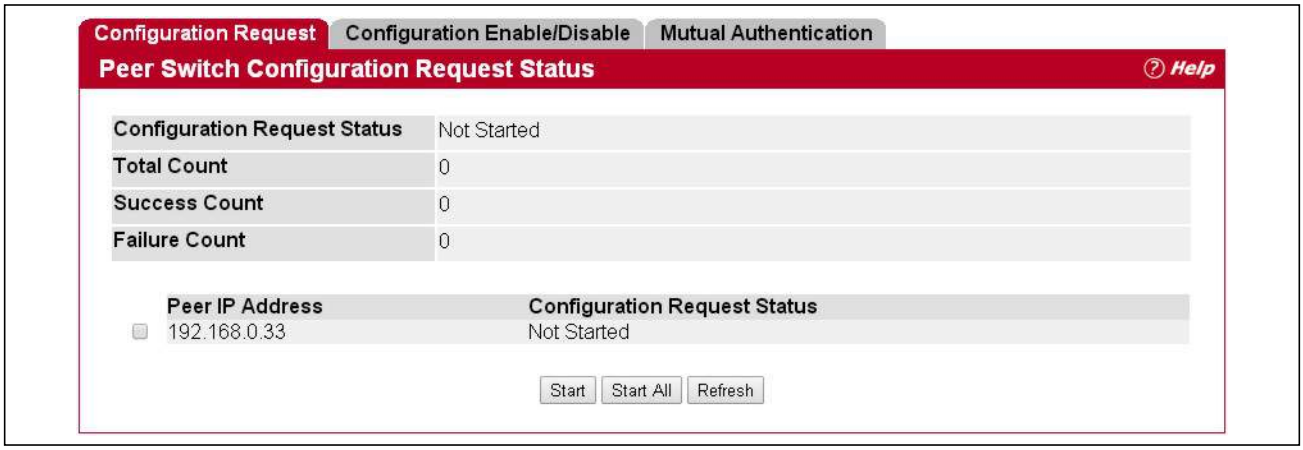


Figure 139: Peer Switch Configuration Request Status

The following table describes the fields on the **Peer Switch Configuration Request Status** page.

Table 126: Peer Switch Configuration Request Status

Field	*Description*
Configuration Request Status	Indicates the global status for a configuration push operation to one or more peer switches. The status can be one of the following: • Not Started • Receiving Configuration • Saving Configuration • Success • Failure—Invalid Code Version • Failure—Invalid Hardware Version • Failure—Invalid Configuration
Total Count	Indicates the number of peer switches included at the time a configuration download request is started, the value is 1 if a download request is for a single switch.
Success Count	Indicates the total number of peer switches that have successfully completed a configuration download.
Failure Count	Indicates the total number of peer switches that have failed to complete a configuration download.
Peer IP Address	Lists the IP address of each switch in the cluster and indicates the configuration request status of that switch.

Command Buttons

The page includes the following buttons:

- **Start**—Initiate a configuration update on the selected peer switch.
- **Start All**—Initiate a configuration update on the selected peer switch
- **Refresh**—Updates the page with the latest information.

Peer Switch Configuration Enable/Disable

You can copy portions of the switch configuration from one switch to another switch in the cluster. The **Peer Switch Configuration Enable/Disable** page allows you to select which parts of the configuration to copy to one or more peer switches in the group.

To open the **Peer Switch Configuration Enable/Disable** page, click the **WLAN** > **WLAN Configuration** > **Peer Switch** > **Configuration Enable/Disable** tab.

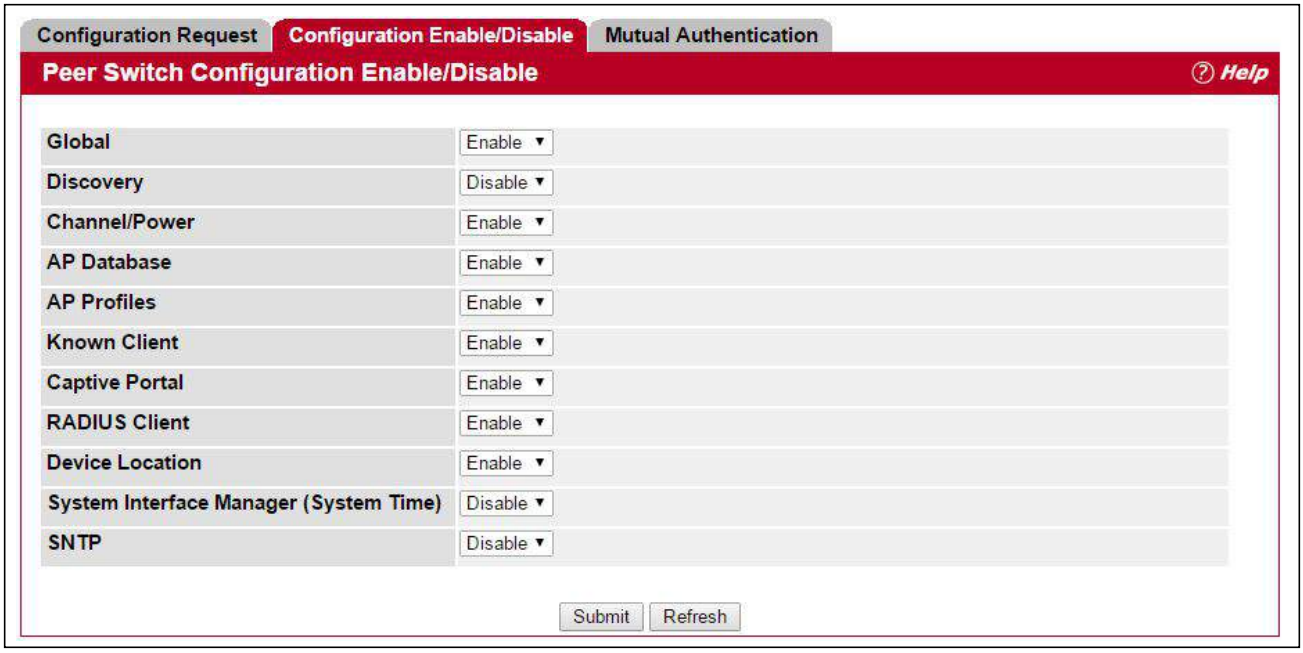


Figure 140: Peer Switch Configuration Enable/Disable

You can make changes to a configuration that has been sent to one or more peer switches, and you can make changes to a configuration received from a peer switch. No changes automatically propagate from one switch to the cluster; you must manually initiate a request on one switch in order to copy any configuration to its peers.

The following table shows the fields on the detail page for **Peer Switch Configuration Enable/Disable** page.

Table 127: Peer Switch Configuration Enable/Disable

Field	*Description*
Global	Enable this field to include the basic and global settings in the configuration that the switch pushes to its peers. The configuration does not include the switch IP address since that is a unique setting. To view current basic global settings, click the **WLAN > WLAN Configuration > Global** > **WLAN Switch** tab.

Table 127: Peer Switch Configuration Enable/Disable

Field	*Description*
Discovery	Enable this field to include the L2 and L3 discovery information, including the VLAN list and IP list, in the configuration that the switch pushes to its peers. **Caution:** Before pushing the IP discovery list from one switch to another, make sure that the list contains IP addresses of all switches, including the switch that is pushing the configuration. To view the discovery settings on the local switch, click the **WLAN > WLAN Configuration > Discovery** tab.
Channel/Power	Enable this field to include the RF management information in the configuration that the switch pushes to its peers. To view the channel and power settings on the local switch, click the **WLAN > AP Management > RF Management** tab.
AP Database	Enable this field to include the AP Database in the configuration that the switch pushes to its peers. To view the contents of the local AP Database, click the **WLAN > WLAN Configuration > Local AP Database > Valid AP** tab.
AP Profiles	Enable this field to include all AP profiles in the configuration that the switch pushes to its peers. The AP profile includes the global AP settings, such as the hardware type, Radio settings, VAP, Wireless Network settings, and QoS settings. To view the local AP Profile settings, click the tabs available under **WLAN > WLAN Configuration > AP Profiles**.
Known Client	Enable this field to include the Known Client Database in the configuration that the switch pushes to its peers. To view the contents of the Known Client Database, click the **WLAN > WLAN Configuration > Known Client** page.
Captive Portal	Enable this field to include Captive Portal information in the configuration that the switch pushes to its peers. To view the Captive Portal settings on the local switch, click the pages available in the **Security > Captive Portal** folder.
RADIUS Client	Enable this field to include the Client RADIUS information in the configuration that the switch pushes to its peers. To view the Client RADIUS settings on the local switch, click on the **WLAN > WLAN Configuration > Global** > **WLAN Switch** tab.
Device Name	Enable this field to include AP and Client location information in the configuration that the switch pushes to its peers.
System Interface Manager (System Time)	Enable this field to include system time information in the configuration that the switch pushes to its peers. Although there are other attributes in the System Interface Manager, for now, the only attribute that has been pushed to its peers from the switch is the system time on the switch.
SNTP	Enable this field to include SNTP information in the configuration that the switch pushes to its peers. To view the SNTP settings on the local switch, open the **System > SNTP** tab.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).
- **Refresh**—Updates the page with the latest information.

Mutual Authentication

Mutual Authentication provides security when adding switches and APs to the wireless network. If Mutual Authentication mode is enabled, the APs and switches perform X.509 Mutual Certificate exchanges. Each device compares the certificate received from the remote end-point with the local copy of the remote device's certificate. If the certificates don't match then the Transport Layer Security (TLS) connection is dropped.

To open the **Mutual Authentication** page, click the **WLAN** > **WLAN Configuration** > **Peer Switch** > **Mutual Authentication** tab.

Figure 141: Mutual Authentication

The following table shows the fields on the **Mutual Authentication** page.

Table 128: Mutual Authentication

Field	*Description*
Switch Provisioning Mode	When this field is enabled, switches can send and receive provisioning messages. As a security feature, you can disable switch provisioning. When switch provisioning mode is disabled the switch does not accept provisioning messages.
Network Mutual Authentication Mode	Select **Enable** to require mutual authentication on the wireless network. When **Disable** is selected, mutual authentication is not required. Changing this parameter on one switch automatically updates the configuration on all other switches in the cluster and all managed APs in the cluster. When this field is enabled, switch provisioning must be enabled in order for new switches to be added to the cluster. If switch provisioning is disabled, the cluster will not accept certificates from a new switch.

Table 128: Mutual Authentication

Field	*Description*
Unmanaged AP Reprovisioning Mode	When this field is enabled, the AP can be re-provisioned when it is not managed. Changing this parameter on one switch automatically updates the configuration on all other switches. This parameter is only applicable if mutual authentication is enabled.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).
- **Refresh**—Updates the page with the latest information.

WIDS Security

The Unified Wireless Switch Wireless Intrusion Detection System (WIDS) can help detect intrusion attempts into the wireless network and take automatic actions to protect the network.

WIDS AP Configuration

The **WIDS AP Configuration** page allows you to activate or deactivate various threat detection tests and set threat detection thresholds in order to help detect rogue APs on the wireless network. These changes can be done without disrupting network connectivity. Since some of the work is done by access points, the switch needs to send messages to the APs to modify its WIDS operational properties.

Note: The classification settings on the **WIDS AP Configuration** page are part of the global configuration on the switch and must be manually pushed to other switches in order to synchronize that configuration.

Many of the tests are focused on identifying APs that are advertising managed SSIDs, but are not in fact managed APs. Detecting such an AP means that a network is either misconfigured or that a hacker has set up a honeypot AP in an attempt to collect passwords or other secure information.

Although operational mode radios can detect most threats, the sentry radios detect the threats faster, especially when a potential rogue is operating on a different channel from any of the managed AP radios. The number of deployed sentry radios should be sufficient to provide coverage by one sentry radio in every geographical location within the network. A denser sentry deployment may be desirable in order to improve rogue or interferer signal triangulation.

To open the **WIDS AP Configuration** page, click **WLAN** > **WLAN Configuration** > **WIDS Security**.

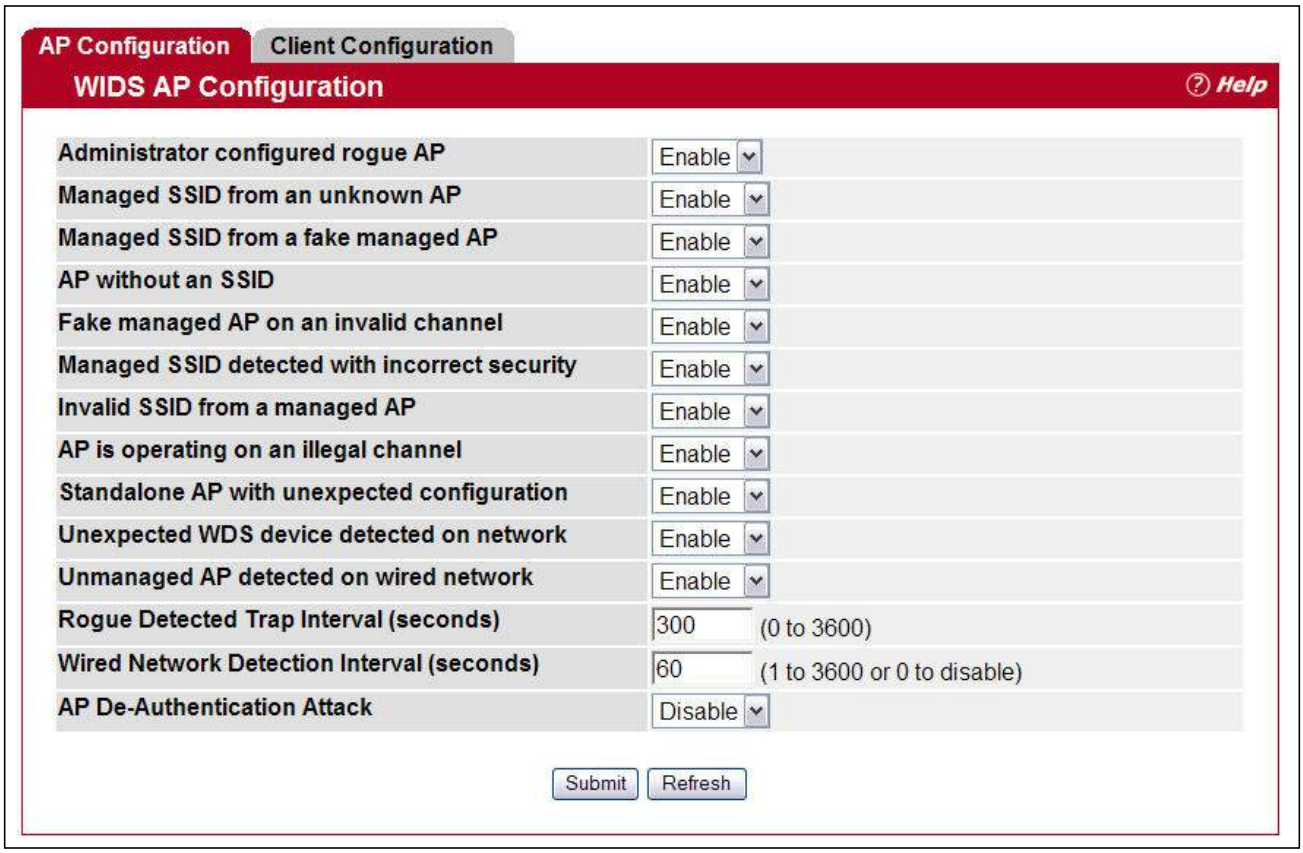


Figure 142: WIDS AP Configuration

The following table shows the fields on the WIDS Security AP Configuration page.

Table 129: WIDS AP Configuration

Field	*Description*
Administrator configured rogue AP	If the source MAC address is in the valid-AP database on the switch or on the RADIUS server and the AP type is marked as *Rogue*, then the AP state is Rogue.
Managed SSID from an unknown AP	This test checks whether an unknown AP is using the managed network SSID. A hacker may set up an AP with managed SSID to fool users into associating with the AP and revealing password and other secure information. Administrators with large networks who are using multiple clusters should either use different network names in each cluster or disable this test. Otherwise, if an AP in the first cluster detects APs in the second cluster transmitting the same SSID as APs in the first cluster then these APs are reported as rogues.
Managed SSID from a fake managed AP	A hacker may set up an AP with the same MAC address as one of the managed APs and configure it to send one of the managed SSIDs. This test checks for a vendor field in the beacons which is always transmitted by managed APs. If the vendor field is not present, then the AP is identified as a fake AP.

Table 129: WIDS AP Configuration (Cont.)

Field	*Description*
AP without an SSID	SSID is an optional field in beacon frames. To avoid detection a hacker may set up an AP with the managed network SSID, but disable SSID transmission in the beacon frames. The AP would still send probe responses to clients that send probe requests for the managed SSID fooling the clients into associating with the hacker's AP. This test detects and flags APs that transmit beacons without the SSID field. The test is automatically disabled if any of the radios in the profiles are configured not to send SSID field, which is not recommended because it does not provide any real security and disables this test.
Fake managed AP on an invalid channel	This test detects rogue APs that transmit beacons from the source MAC address of one of the managed APs, but on different channel from which the AP is supposed to be operating.
Managed SSID detected with incorrect security	During RF Scan the AP examines beacon frames received from other APs and determines whether the detected AP is advertising an open network, WEP, or WPA. If the SSID reported in the RF Scan is one of the managed networks and its configured security not match the detected security then this test marks the AP as rogue.
Invalid SSID from a managed AP	This test checks whether a known managed AP is sending an unexpected SSID. The SSID reported in the RF Scan is compared to the list of all configured SSIDs that are used by the profile assigned to the managed AP. If the detected SSID doesn't match any configured SSID then the AP is marked as rogue.
AP is operating on an illegal channel	The purpose of this test is to detect hackers or incorrectly configured devices that are operating on channels that are not legal in the country where the wireless system is set up. ***Note:*** For the wireless system to detect this threat, the wireless network must contain one or more radios that operate in sentry mode.
Standalone AP with unexpected configuration	If the AP is classified as a known standalone AP, then the switch checks whether the AP is operating with the expected configuration parameters. You configure the expected parameters for the standalone AP in the local or RADIUS Valid AP database. This test may detect network misconfiguration as well as potential intrusion attempts.The following parameters are checked: • Channel Number • SSID • Security Mode • WDS Mode. • Presence on a wired network.
Unexpected WDS device detected on network	If the AP is classified as a Managed or Unknown AP and wireless distribution system (WDS) traffic is detected on the AP, then the AP is considered to be Rogue. Only stand-alone APs that are explicitly allowed to operate in WDS mode are not reported as rogues by this test.

Table 129: WIDS AP Configuration (Cont.)

Field	*Description*
Unmanaged AP detected on wired network	This test checks whether the AP is detected on the wired network. If the AP state is Unknown, then the test changes the AP state to Rogue. The flag indicating whether AP is detected on the wired network is reported as part of the RF Scan report. If AP is managed and is detected on the network then the switch simply reports this fact and doesn't change the AP state to Rogue. In order for the wireless system to detect this threat, the wireless network must contain one or more radios that operate in sentry mode.
Rogue Detected Trap Interval	Specify the interval, in seconds, between transmissions of the SNMP trap telling the administrator that rogue APs are present in the RF Scan database. If you set the value to 0, the trap is never sent.
Wired Network Detection Interval	Specify the number of seconds that the AP waits before starting a new wired network detection cycle. If you set the value to 0, wired network detection is disabled.
AP De-Authentication Attack	Enable or disable the AP de-authentication attack. The wireless switch can protect against rogue APs by sending de-authentication messages to the rouge AP. The de-authentication attack feature must be globally enabled in order for the wireless system to do this function. Make sure that no legitimate APs are classified as rogues before enabling the attack feature. This feature is disabled by default.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).
- **Refresh**—Updates the page with the latest information.

WIDS Client Configuration

The Unified Wireless Switch Wireless Intrusion Detection System (WIDS) can help detect intrusion attempts into the wireless network and take automatic actions to protect the network. The settings you configure on the **WIDS Client Configuration** page help determine whether a detected client is classified as a rogue. Clients classified as rogues are considered to be a threat to network security.

Note: The classification settings on the **WIDS Client Configuration** page are part of the global configuration on the switch and must be manually pushed to other switches in order to synchronize that configuration.

As part of the general association and authentication process, wireless clients send 802.11 management messages to APs. The WIDS feature tracks the following types of management messages that each detected client sends:

- Probe Requests
- 802.11 Authentication Requests.
- 802.11 De-Authentication Requests.

To help determine whether a client is posing a threat to the network by flooding the network with management traffic, the system keeps track of the number of times the AP received each message type and the highest message rate detected in a single RF Scan report. On the **WIDS Client Configuration** page, you can set thresholds for each type of message sent, and the APs monitor whether any clients exceed those thresholds. or tests.

To open the **WIDS Client Configuration** page, click the **WLAN** > **WLAN Configuration** > **WIDS Security > Client Configuration** tab.

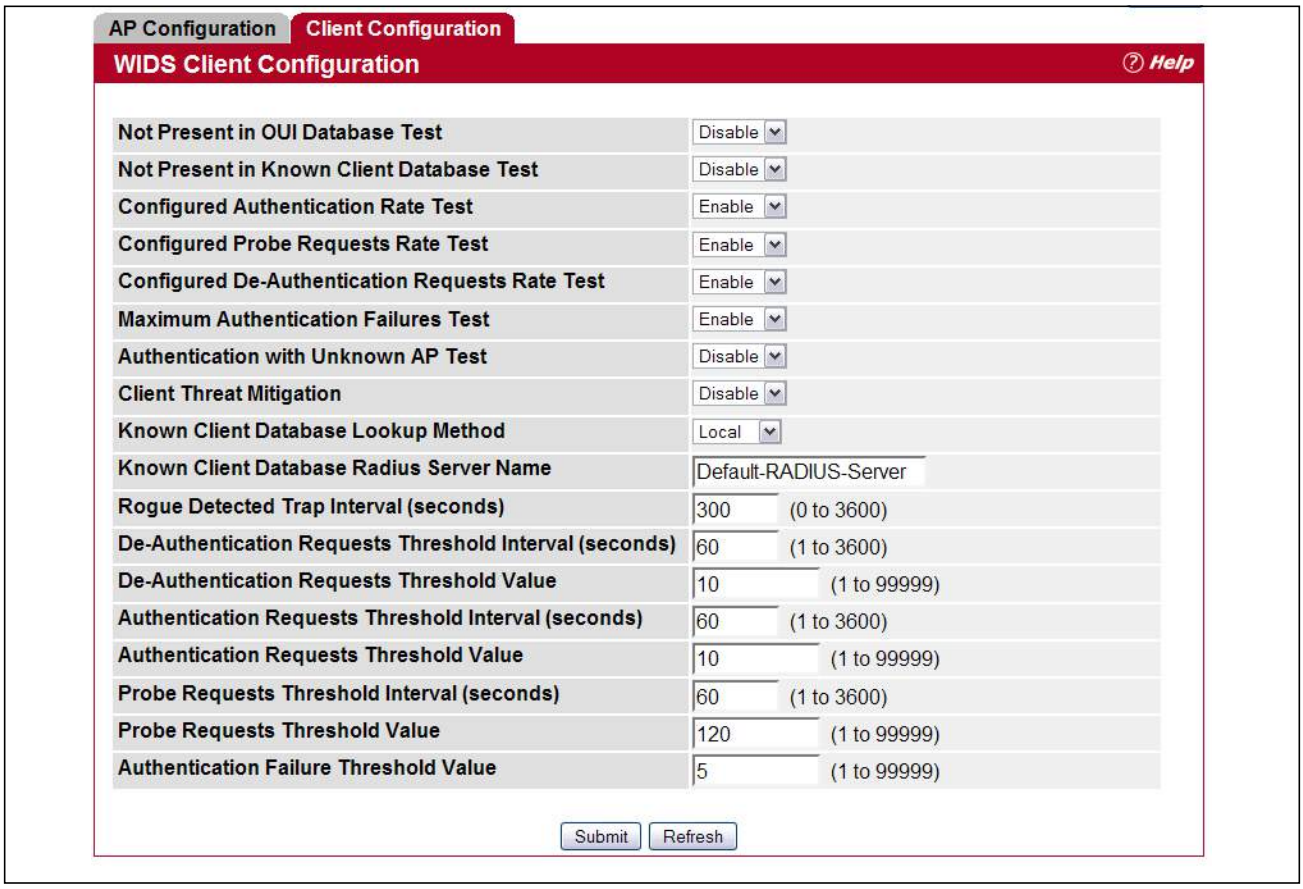


Figure 143: WIDS Client Configuration

The following table describes the fields on the **WIDS Client Configuration** page.

Table 130: WIDS Client Configuration

Field	*Description*
Not Present in OUI Database Test	This test checks whether the MAC address of the client is from a registered manufacturer identified in the OUI database.
Known Client Database Test	This test checks whether the client, which is identified by its MAC address, is listed in the Known Client Database and is allowed access to the AP either through the Authentication Action of Grant or through the White List global action. If the client is in the Known Client Database and has an action of Deny, or if the action is Global Action and it is globally set to Black List, the client fails this test.

Table 130: WIDS Client Configuration (Cont.)

Field	*Description*
Configured Authentication Rate Test	This test checks whether the client has exceeded the configured rate for transmitting 802.11 authentication requests.
Configured Probe Requests Rate Test	This test checks whether the client has exceeded the configured rate for transmitting probe requests.
Configured De-Authentication Requests Rate Test	This test checks whether the client has exceeded the configured rate for transmitting de-authentication requests.
Maximum Authentication Failures Test	This test checks whether the client has exceeded the maximum number of failed authentications.
Authentication with Unknown AP Test	This test checks whether a client in the Known Client database is authenticated with an unknown AP.
Client Threat Mitigation	Select enable to send de-authentication messages to clients that are in the Known Clients database but are associated with unknown APs. The Authentication with Unknown AP Test must also be enabled in order for the mitigation to take place. Select disable to allow clients in the Known Clients database to remain authenticated with an unknown AP.
Known Client Database Lookup Method	When the switch detects a client on the network it performs a lookup in the Known Client database. Specify whether the switch should use the local or RADIUS database for these lookups.
Known Client Database RADIUS Server Name	If the known client database lookup method is RADIUS then this field specifies the RADIUS server name.
Rogue Detected Trap Interval	Specify the interval, in seconds, between transmissions of the SNMP trap telling the administrator that rogue APs are present in the RF Scan database. If you set the value to 0, the trap is never sent.
De-Authentication Requests Threshold Interval	Specify the number of seconds an AP should spend counting the de-authentication messages sent by wireless clients.
De-Authentication Requests Threshold Value	If switch receives more than specified messages during the threshold interval the test triggers.
Authentication Requests Threshold Interval	Specify the number of seconds an AP should spend counting the authentication messages sent by wireless clients.
Authentication Requests Threshold Value	If switch receives more than specified messages during the threshold interval the test triggers.
Probe Requests Threshold Interval	Specify the number of seconds an AP should spend counting the probe messages sent by wireless clients.
Probe Requests Threshold Value	Specify the number of probe requests a wireless client is allowed to send during the threshold interval before the event is reported as a threat.
Authentication Failure Threshold Value	Specify the number of 802.1X authentication failures a client is allowed to have before the event is reported as a threat.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).

- **Refresh**—Updates the page with the latest information.

Switch Provisioning

Switch Certificate Request

Use the **Switch Certificate Request** page to request a X.509 certificate from the cluster controller. The X.509 mutual certificate exchange is the only mechanism for peer switches to authenticate with each other because switches do not support pass-phrase authentication.

The X.509 certificate is automatically generated by the switch, so it does not communicate with any trusted certificate authority, and there are no certificate maintenance fees.

To open the **Switch Certificate Request** page, click **WLAN** > **WLAN Configuration** > **Switch Provisioning**.

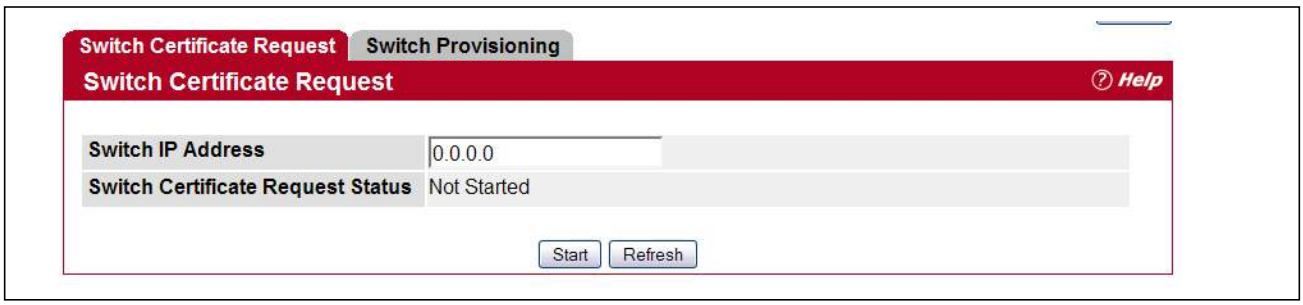


Figure 144: Switch Certificate Request

The following table shows the fields available on the **Switch Certificate Request** page.

Table 131: Switch Certificate Request

Field	*Description*
Switch IP Address	Enter the IP address of the wireless switch from which this switch requests an X.509 certificate.
Switch Certificate Request Status	Shows the status of the request, which is one of the following: • Not Started—Certificate exchange has not started. • Invalid IP address—IP address specified in the Switch IP Address field is not valid. • In Progress—Certificate request is in progress. • Success—Certificate has been obtained and added to the certificate file. • Timed Out—Certificate request timed out without getting a certificate.

Command Buttons

The page includes the following buttons:

- **Start**—Initiates the X.509 certificate request.
- **Refresh**—Updates the page with the latest information.

Switch Provisioning

Use the **Switch Provisioning** page to request provisioning information from a switch in the cluster. After the new switch receives the provisioning information, it can join the cluster.

To open the **Switch Provisioning** page, click the **WLAN** > **WLAN Configuration** > **Switch Provisioning** > **Switch Provisioning** tab.

Figure 145: Switch Provisioning

The following table shows the fields available on the **Switch Provisioning** page.

Table 132: Switch Provisioning

Field	*Description*
Switch IP Address	Enter the IP address of the switch in a cluster to which a new switch establishes a connection to obtain provisioning information. The provisioning information enables the new switch to join the cluster.
Switch Provisioning Status	Shows the status of the provisioning, which is one of the following: • Not Started • Success—The provisioning sequence completed successfully. • Connection Failed—Can't establish TLS connection with the cluster switch. • Provisioning Failed—The switch in the cluster did not respond with expected messages. This can happen if the switch is running code that does not support switch provisioning or the switch provisioning mode is disabled on the switch in the cluster.

Command Buttons

The page includes the following buttons:

- **Start**—Initiates the provisioning request for the switch.
- **Refresh**—Updates the page with the latest information.

Local OUI Database Summary

To help identify AP and Wireless Client adapter manufacturers detected in the wireless network, the wireless switch contains a database of registered Organizationally Unique Identifiers (OUIs). This is a read-only list with over 10,000 registrations. From the **Local OUI Database Summary** page, you can enter up to 64 user-defined OUIs. The local list is searched first, so the same OUI can be located in the local list as well as the read-only list.

To open the **Local OUI Database Summary** page, click **WLAN** > **WLAN Configuration** > **OUI**.

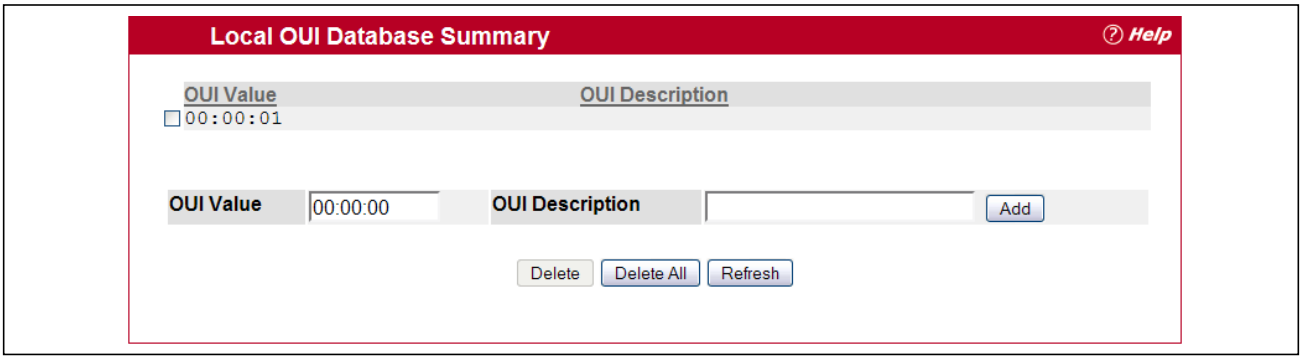


Figure 146: Local OUI Database Summary

Table 133: Local OUI Database Summary

Field	*Description*
OUI Value	Enter the OUI that represents the company ID in the format XX:XX:XX where XX is a hexadecimal number between 00 and FF. The first three bytes of the MAC address represents the company ID assignment. ***Note:*** The first byte of the OUI must have the least significant bit set to 0. For example 02:FF:FF is a valid OUI, but 03:FF:FF is not.
OUI Description	Enter the organization name associated with the OUI. The name can be up to 32 characters, including alphanumeric and spaces.

Command Buttons

The page includes the following buttons:

- **Add**—Adds the OUI value and description information to the local OUI database.
- **Delete**—Deletes any selected OUI entries from the local OUI database. This button is available if the check box next to at least one OUI entry is selected.
- **Delete All**—Deletes all manually-added entries from the local OUI database.
- **Refresh**—Updates the page with the latest information.

AP Management

The AP Management folder contains links to the following pages that help you manage and maintain the APs on your Unified Wireless Switch network:

- Reset
- RF Management
- License Management
- Managed AP Advanced Settings
- Remote Packet Capture

Reset

You can manually reset one or all APs from the UWS. When you issue the command to reset an AP, the AP closes the SSL connection to the switch before resetting the hardware.

To reset one or more APs, click **AP Management** > **Reset**.

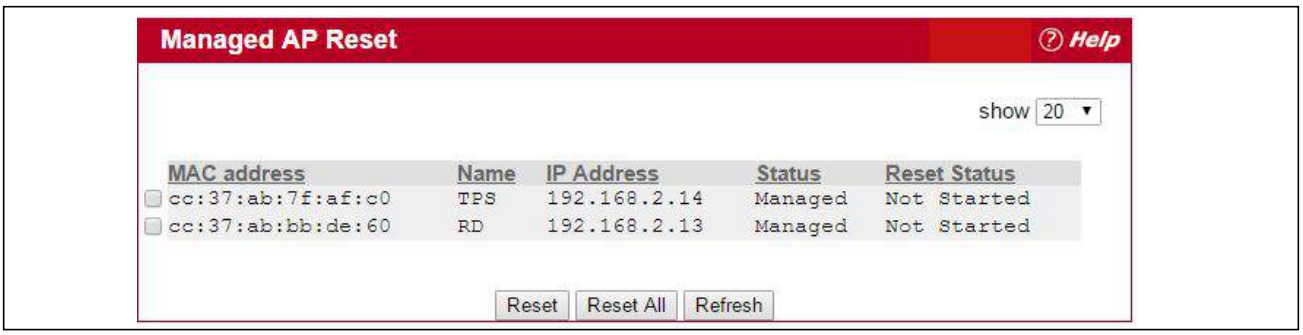


Figure 147: Access Point Reset

Table 134: Reset Fields

Field	*Description*
MAC Address	The MAC address of the AP
Name	The name of the AP, as specified in the Valid AP or RADIUS database
IP Address	The IP address of the AP
Status	Displays “Managed” to indicate that the AP is managed by the switch.
Reset Status	The status of the reset

Command Buttons

The page includes the following buttons:

- **Reset**—Resets the selected APs. To select an AP, click the check box next to the MAC address.
- **Reset All**—Resets all managed APs listed on the page.
- **Refresh**—Updates the page with the latest information.

The APs might take several minutes to reset and re-establish communication with the switch. While the AP is resetting, the status changes to failed, and then back to managed once the AP is back online.

RF Management

The radio frequency (RF) broadcast channel defines the portion of the radio spectrum that the radio on the access point uses for transmitting and receiving. The range of available channels for an access point is determined by the IEEE 802.11 mode (also referred to as band) of the access point.

Each AP is a dual-band system capable of operating in multiple modes. IEEE 802.11b and 802.11g modes (802.11b/g) operate in the 2.4-GHz RF frequency and support use of channels 1 through 11. IEEE 802.11a mode operates in the 5 GHz frequency and supports a larger set of non-consecutive channels (36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165, 169, 173). IEEE 802.11n mode can operate in either the 2.4 GHz or 5 GHz frequency.

Note: The available channels depends on the country in which the APs operate. The channels described in this section are valid for the United States.

Interference can occur when multiple access points within range of each other are broadcasting on the same or overlapping channels. The impact of this interference on network performance can intensify during busy times when a large amount of data and media traffic is competing for bandwidth. For the *b/g* radio band, the classical set of non-interfering channels is 1, 6, 11. Channels 1, 4, 8, 11 produce minimal overlap. A similar set of non-interfering channels is used for the *a* radio band, which includes all channels for that mode since they are not overlapping.

Configuring Channel Plan and Power Settings

The UWS software contains a channel plan algorithm that automatically determines which RF channels each AP should use to minimize RF interference. When you enable the channel plan algorithm, the switch periodically evaluates the operational channel on every AP it manages and changes the channel if the current channel is noisy.

Note: The regulation of radio frequencies and channel assignments varies from country to country. In countries that do not support channels 1, 6, and 11 on the 802.11b/g/n radio, the channel plan algorithm is inactive. For the 5-GHz radio, the algorithm is inactive in countries that require 802.11h radar detection, which includes European countries and Japan.

The automatic channel selection algorithm does not affect APs that meet any of the following conditions:

- The channel is statically assigned to the AP in the RADIUS or local AP database.
- The channel has been statically assigned to the AP from the **AP Management** > **Advanced Settings** page.
- The AP uses a profile that has the Automatic Channel field disabled (WLAN > WLAN Configuration > AP Profiles > Radio configuration setting).

Note: If the AP is not assigned a fixed channel or is not assigned a specific channel by the automatic channel selection algorithm, the AP channel selection mode is set to best. This means that the AP selects the best channel whenever the radio restarts or if the AP detects a radar signal.

The RF transmission power level affects how far an AP broadcasts its signal. If the power level is too low, wireless clients will not detect the signal or experience poor WLAN performance. If the power level is too high, the RF signal might interfere with other APs within range or broadcast the signal beyond the desired physical boundaries, which can create a security risk.

Automatic power uses a proprietary algorithm to automatically adjust the RF signal to broadcast far enough to reach wireless clients, but not so far that it interferes with RF signals broadcast by other APs.

To configure Channel Plan and Power Adjustment settings, click **WLAN** > **WLAN Configuration** > **AP Management** > **RF Management**.

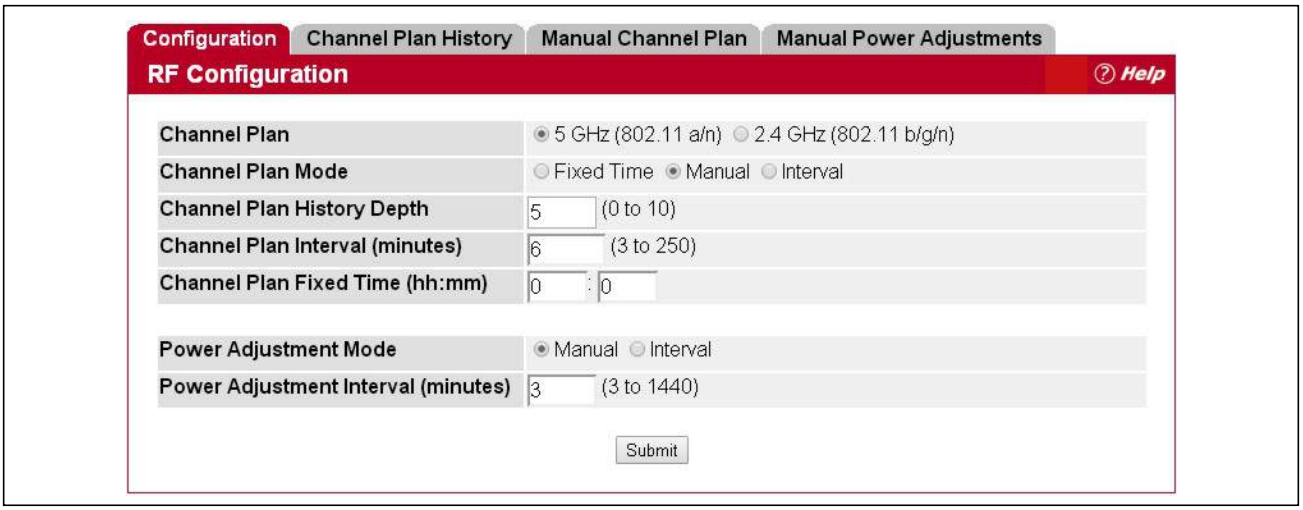


Figure 148: RF Channel Plan and Power Configuration

Table 135 describes the RF Channel Plan and Power Adjustment fields you can configure.

Note: When the AP changes its channel, all associated wireless clients temporarily lose their connection to the AP and must re-associate. The re-association can take several seconds, which can affect time-sensitive traffic such as voice and video.

Table 135: RF Channel Plan and Power Adjustment

Field	*Description*
Channel Plan	Each AP is dual-band capable of operating in the 2.4 GHz and 5 GHz frequencies. The 802.11a/n and 802.11b/g/n modes use different channel plans. Before you configure channel plan settings, select the mode to configure.

Table 135: RF Channel Plan and Power Adjustment (Cont.)

Field	*Description*
Channel Plan Mode	This field indicates the channel assignment mode. The mode of channel plan assignment can be one of the following: • **Fixed Time**: If you select the fixed time channel plan mode, you specify the time for the channel plan and channel assignment. In this mode the plan is applied once every 24 hours at the specified time. • **Manual**: With the manual channel plan mode, you control and initiate the calculation and assignment of the channel plan. You must manually run the channel plan algorithm and apply the channel plan to the APs. • **Interval**: In the interval channel plan mode, the switch periodically calculates and applies the channel plan. You can configure the interval to be from every 6 to every 24 hours. The interval period begins when you click **Submit**.
Channel Plan History Depth	The channel plan history lists the channels the switch assigns each of the APs it manages after a channel plan is applied. Entries are added to the history regardless of interval, time, or channel plan mode. The number you specify in this field controls the number of iterations of the channel assignment. ***Note:*** The APs changed in previous iterations cannot be assigned new channels in the next iteration. This history prevents the same APs from being changed time after time.
Channel Plan Interval	If you select the **Interval** channel plan mode, you can specify the frequency at which the channel plan calculation and assignment occurs. The interval time is in hours, and you can specify an interval that ranges between every 6 hours to every 24 hours.
Channel Plan Fixed Time	If you select the **Fixed Time** channel plan mode, you can specify the time at which the channel plan calculation and assignment occurs. The channel plan calculation will occur once every 24 hours at the time you specify.
Power Adjustment Mode	You can set the power of the AP radio frequency transmission in the AP profile, the local database or in the RADIUS server. The power level in the AP profile is the default level for the AP, and the power will not be adjusted below the value in the AP profile. The settings in the local database and RADIUS server always override power set in the profile setting. If you manually set the power, the level is fixed and the AP will not use the automatic power adjustment algorithm. You can configure the power as a percentage of maximum power, where the maximum power is the minimum of power level allowed for the channel by the regulatory domain or the hardware capability. • **Manual**: In this mode, you run the proposed power adjustments manually from the **Manual Power Adjustments** page. • **Interval**: In this mode, the switch periodically calculates the power adjustments and applies the power for all APs. The interval period begins when you click **Submit**. ***Note:*** If you set the power level in the local or RADIUS database, the settings override the power level set in the AP profile. For more information about manually setting the power level, see "Radio Configuration" on page 190 and "Local Access Point Database" on page 257.
Power Adjustment Interval	This field determines how often the switch runs the power adjustment algorithm. The algorithm runs automatically only if you set the power adjustment mode to **Interval**.

Command Buttons

The page includes the following button:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (System > System Utilities > Save All Applied Changes).

Viewing the Channel Plan History

The UWS stores channel assignment information for the APs it manages. To access the Channel Plan History information, click the **AP Management > RF Management > Channel Plan History** tab.

The Cluster Controller switch that controls the cluster maintains the channel history information for all switches in the cluster. On the Cluster Controller, the page shows information about the radios on all APs managed by switches in the cluster that are eligible for channel assignment and were successfully assigned a new channel.

Figure 149: Channel Plan History

Table 136 describes the Channel Plan History fields.

Table 136: Channel Plan History

Field	*Description*
5 GHz (802.11a/n) **2.4 GHz (802.11b/g/n)**	The 5 GHz and 2.4 GHz radios use different channel plans, so the switch tracks the channel history separately for each radio. The channel information that displays on the page is only for the radio you select.
Operational Status	This field shows whether the switch is using the automatic channel adjustment algorithm on the AP radios.
Last Iteration	The number in this field indicates the most recent iteration of channel plan adjustments. The APs that received a channel adjustment in previous iterations cannot be assigned new channels in the next iteration to prevent the same APs from being changed time after time. On the **AP Management > RF Management > Configuration** tab, you can set the history depth to control the maximum number of iterations stored and displayed in the channel plan history.
Last Algorithm Time	Shows the date and time when the channel plan algorithm last ran. ***Note:*** To set the system time on the switch, you must use SNTP, which is disabled by default. From the Web interface, you configure the SNTP client and server information from the pages in the **System > SNTP** folder. From the CLI, use the `sntp` commands in Global Config mode.

Table 136: Channel Plan History (Cont.)

Field	*Description*
AP MAC Address	The AP to which the channel plan is assigned.
Name	The name of the AP.
Radio	The radio functioning on the AP (5GHz or 2.4GHz).
Iteration	The current iteration executed by the channel plan.
Channel	The current operating channel for the AP that the algorithm recommends for new channel assignments.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Initiating Manual Channel Plan Assignments

If you specify Manual as the Channel Plan Mode on the Configuration tab, the **Manual Channel Plan** page allows you to initiate the channel plan algorithm.

To manually run the channel plan adjustment feature, select the radio to update the channels on (5 GHz or 2.4 GHz) and click **Start**.

Figure 150: Manual Channel Plan

The fields in Table 137 when click the **WLAN > AP Management > RF Management > Manual Channel Plage**.

Table 137: Manual Channel Plan

Field	*Description*
Current Status	Shows the Current Status of the plan, which is one of the following states: • None: The channel plan algorithm has not been manually run since the last switch reboot. • Algorithm In Progress: The channel plan algorithm is running. • Algorithm Complete: The channel plan algorithm has finished running. A table displays to indicate proposed channel assignments. Each entry shows the AP along with the current and new channel. To accept the proposed channel change, click **Apply**. You must manually apply the channel plan for the proposed assignments to be applied. • Apply In Progress: The switch is applying the proposed channel plan and adjusting the channel on the APs listed in the table. • Apply Complete: The algorithm and channel adjustment are complete.
Proposed Channel Plan Entries ***Note:*** If no APs appear in the table after the algorithm is complete, the algorithm does not recommend any channel changes.	
Current Channel	Shows the current operating channel for the AP that the algorithm recommends for new channel assignments.
New Channel	Shows the proposed operating channel for the AP.

To apply the new channels, click **Apply**.

It is possible for the network configuration to change between the time the automatic channel selection runs and the time you attempt to apply the proposed channel assignments.

The channel will fail to be applied to an AP if one of the following conditions exist:

- The AP has failed.
- The radio on the AP has been disabled through a profile update.
- The channel is not valid for the radio mode.
- The AP has been rebooted since the channel plan was computed and acquires a static channel that has been set statically via local database.
- The channel has been set manually through the advanced page.
- The auto-channel mode has been disabled in the profile for this AP.

Command Buttons

The page includes the following buttons:

- **Apply**—Apply the proposed channel change to the AP and change the current channel to the new channel.
- **Clear**—Clear the proposed channel plan information.
- **Refresh**—Updates the page with the latest information.
- **Start**—Initiate the channel plan algorithm.

Initiating Manual Power Adjustments

If you select Manual as the Power Adjustment Mode on the Configuration tab, you can manually initiate the power adjustment algorithm on the **Manual Power Adjustments** page.

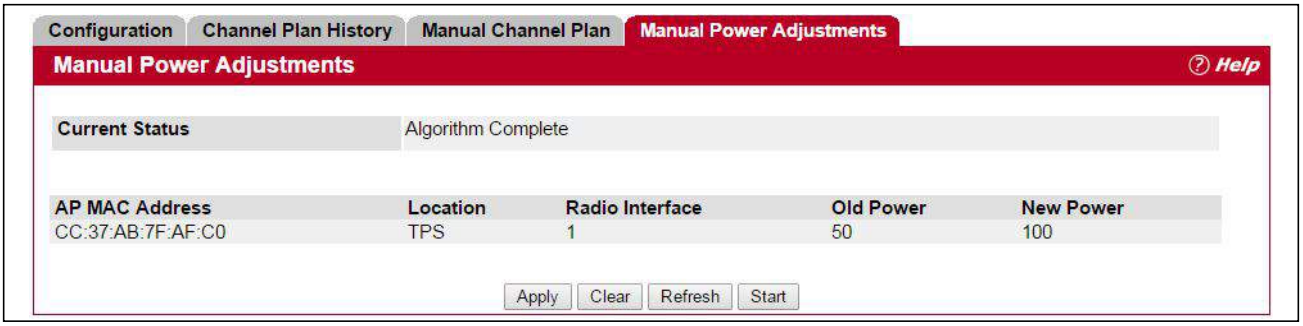


Figure 151: Manual Power Adjustments

Table 138: Manual Power Adjustments

Field	*Description*
Status	Shows the Current Status of the plan, which is one of the following states: • None: The power adjustment algorithm has not been manually run since the last switch reboot. • Algorithm In Progress: The power adjustment algorithm is running. • Algorithm Complete: The power adjustment algorithm has finished running. • A table displays to indicate proposed power adjustments. Each entry shows the AP along with the current and new power levels. To accept the proposed change, click Apply. You must manually apply the power adjustment for the proposed assignments to be applied. • Apply In Progress: The switch is adjusting the power levels that the APs use. • Apply Complete: The algorithm and power adjustment are complete.
AP MAC Address	Identifies the AP MAC address.
Name	The name of the AP, which is set in the Valid AP database.
Radio Interface	Identifies the radio.
Old Power	Shows the previous power level for the AP.
New Power	Shows the new power level for the AP.

Command Buttons

The page includes the following buttons:

- **Apply**—Apply the proposed power adjustment to the AP and change the current power level to the new power.
- **Clear**—Clear the proposed power adjustment information.
- **Refresh**—Updates the page with the latest information.
- **Start**—Initiate the power adjustment algorithm.

License Management

The supported number of APs and wireless clients is based on the access controller license certificate downloaded to the switch. For more information on access controller licenses, see "UWS Licenses" on page 178.

License information is displayed on the **WLAN** > **AP Management** > **License Management** page.

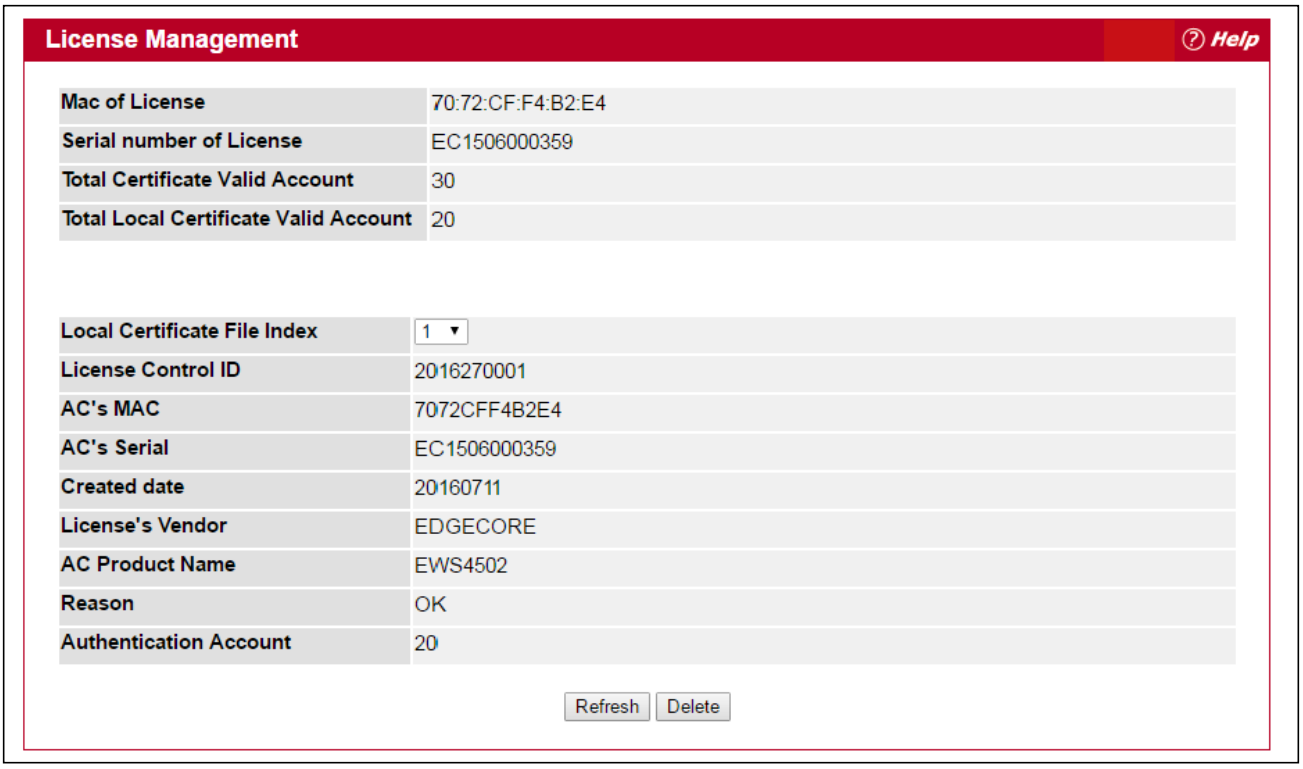


Figure 152: *License* Management

The UWS can upload up to 2000 licenses. The information displayed on the License Management page is displayed below.

Table 139: License Management

Field	*Description*
MAC of License	MAC address for the switch controller.
Serial Number of License	Serial number of the license.
Total Certificate Valid Account	This value is 6 (default provided by UWS) + Total Local Certificate Valid Account.
Total Local Certificate Valid Account	The number of manageable APs provided by all license files on this UWS.
Local Certificate File Index	The index to a local license certificate.
AC's MAC	The AC's MAC address for this certificate.
AC's Serial	The AC's serial number for this certificate.

Table 139: License Management (Cont.)

Field	*Description*
Created date	The date this certificate was created.
License's Vendor	The name of the license vendor.
AC Product Name	The AC product name for this certificate.
Reason	Specifies the authenticated result of license file after SSL verification: • OK: No error. • Invalid Certificate: There is no license file or file format is invalid. • Invalid MAC Length: The length of MAC address is invalid. • Invalid Serial Length: The length of serial number is invalid. • Invalid Product Length: The length of product name is invalid. • Invalid MAC: The format of MAC address is invalid. • Invalid Serial: The format of serial number is invalid. • Invalid Licence-ID Repeat: The file owns duplicated License Control ID.
Authentication Account	Identifies the number of manageable AP for license file.

The PEM file for license management uses the license information “MAC of License” and “Serial Number of License” as shown on this web page. When applying for a license, provide the “Serial Number” and “Burned In MAC Address” shown on the System > System Inventory page, as well as the number of APs and wireless clients to be supported.

Note that the “MAC of License” will be different from the “Burned in MAC Address” shown on the System Inventory Information page. The burned in MAC address is the “MAC of License” + 2.

Managed AP Advanced Settings

When the AP is in Managed mode, remote access to the AP is disabled. However, you can enable Telnet access by enabling the Debug feature on the **AP Management > Advanced Settings** page. From the **Managed AP Advanced Settings** page, you can also manually change the RF channel and power for each radio on an AP. The manual power and channel changes override the settings configured in the AP profile (including automatic channel selection) and take effect immediately. The manual channel and power assignments are not retained when the AP is reset or if the profile is reapplied to the AP, such as when the AP disassociates and reassociates with the switch.

To open this page, click **WLAN** > **WLAN Configuration** > **AP Management** > **Advanced Settings**.

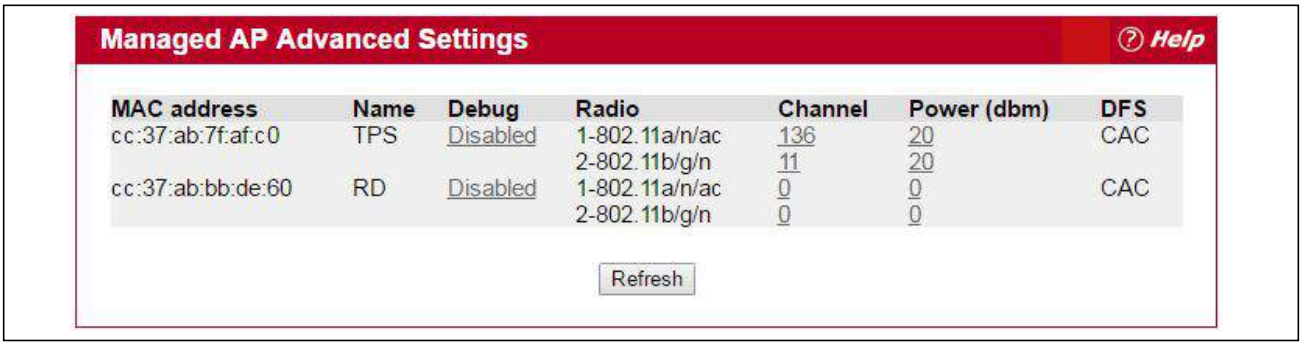


Figure 153: Advanced AP Management

Each AP managed by the UWS is listed by its MAC address and location. The location is based on the value in the RADIUS or local Valid AP database. Table 140 describes the Advanced features you can configure for the AP.

Table 140: Advanced AP Management

Field	*Description*
MAC Address	Shows the MAC address of the AP.
Name	Shows the AP name, which is based on the value configured in the RADIUS or local Valid AP database.
Debug	To help you troubleshoot, you can enable Telnet access to the AP so that you can debug the device from the CLI. The Debug field shows the debug status and can be one of the following: • Disabled • Set Requested • Set in Progress • Enabled To change the status, click the **Debug** status link. The Managed AP Debug page appears. Table 141 on page 285 describes the fields on the new page.
Radio	Identifies the radio to which the channel and power settings apply.
Channel	Click the **Channel** link to access the Managed AP Channel/Power Adjust page. From that page, you can set a new channel for Radio 1 or Radio 2. The available channels depend on the radio mode and country in which the APs operate. The manual channel change overrides the channel configured in the AP profile and is not retained when the AP reboots or when the AP profile is reapplied. Table 142 on page 287 describes the fields on the new page.
Power	Click the **Power** link to access the Managed AP Channel/Power Adjust page. From that page, you can set a new power level for the AP. The manual power change overrides the power setting configured in the AP profile and is not retained when the AP reboots or when the AP profile is reapplied. Table 142 on page 287 describes the fields on the new page.
DFS	DFS (Dynamic Frequency Selection) is a mechanism that requires wireless devices to share spectrum and avoid co-channel operation with radar systems in the 5 GHz band. DFS requirements vary based on the regulatory domain, which is determined by the country code setting of the AP. For radios in the 5 GHz band, when DFS support is on and the regulatory domain requires radar detection on the channel, DFS and Transmit Power Control (TPC) features of 802.11h are activated. The values displayed in this field include: • CAC - Channel Availability Check - The time a system monitors a channel for presence of radar prior to initiating a communication link on that channel; conventionally it is a default at 60 seconds so that during this period of time, 5GHz radio is inactive for wireless service. If no radar is detected during the CAC time, it will eventually switch to ISM mode. • ISM - In Service Monitor - The radio is operational in that channel and is prepared to move to another frequency in the presence of radar detection. • IDLE - AP is operating on the non-DFS channel so there is no need to detect radar.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Debugging the AP

You can enable debugging on an AP to allow Telnet access to the access point. Once you Telnet to the AP, you can issue commands from the CLI to help you troubleshoot.

To open this page, click **WLAN** > **WLAN Configuration** > **AP Management** > **Advanced Settings** > **Debug** link.

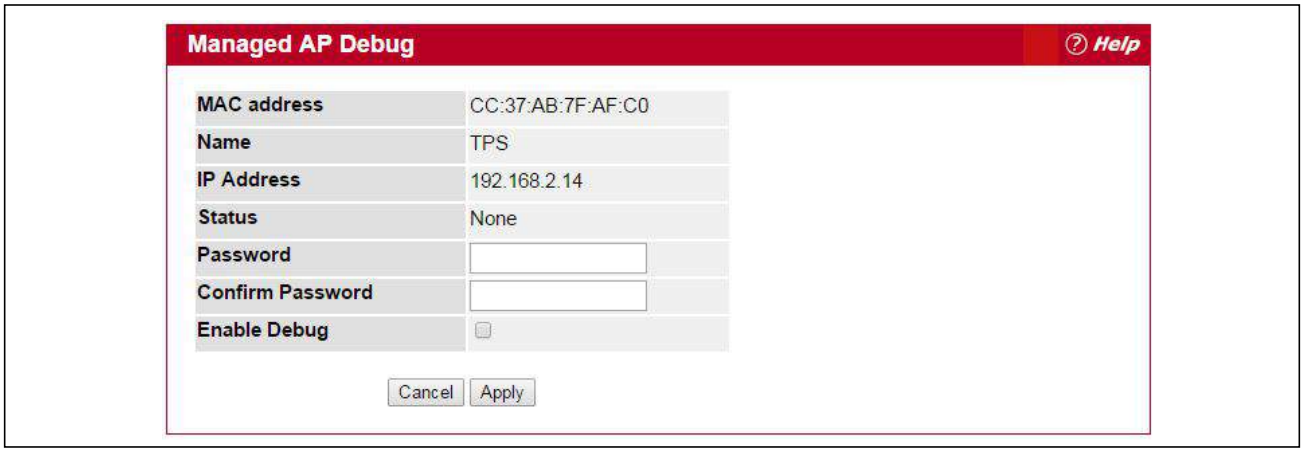


Figure 154: Managed AP Debug

The fields in Table 141 appear when you click the Debug link for a managed AP on the **Managed AP Advanced Settings** page.

Table 141: Managed AP Debug

Field	*Description*
MAC Address	Shows the MAC address of the access point.
Name	Shows the name of the access point, as configured in the Valid AP database.
IP Address	Shows the IP address of the AP.
Status	Shows the debug status, which can be one of the following: • None: Debugging has not been enabled or disabled. • Set Requested: A request has been made to change the debug status. • Set Complete: Debugging has been enabled or disabled.
Password	Enter the **admin** password for the AP (the default is **admin**).
Confirm Password	Since the password is encrypted, you must retype the password to confirm the password.

Table 141: Managed AP Debug (Cont.)

Field	*Description*
Enable Debug	Select or clear the **Enable** check box to enable or disable debugging. Once you Telnet to the AP, you get an AP interface login prompt. The user name is admin. Enter the password you set in the previous field. The default password is admin if you did not specify a new password. From the AP CLI, you can also access the standard Linux prompt by typing the '!' character. You can issue the following debug commands at the Linux OS prompt: • `get management`: Display management interface information • `get managed-ap`: Display managed AP information You can issue the following debug commands at the Linux OS prompt: • `ifconfig`: display all interfaces. • `cat /proc/meminfo`: View memory utilization

Command Buttons

The page includes the following buttons:

- **Cancel**—Cancels any actions and returns to the previous page.
- **Apply**—Applies the settings to the AP.

Adjusting the Channel and Power

Changes you make to the channel and power are runtime changes only. If you change the channel or power settings, the new settings are lost if the AP or switch is reset.

To open this page, click **WLAN** > **AP Management** > **Advanced Settings** > **Channel** or **Power** link.

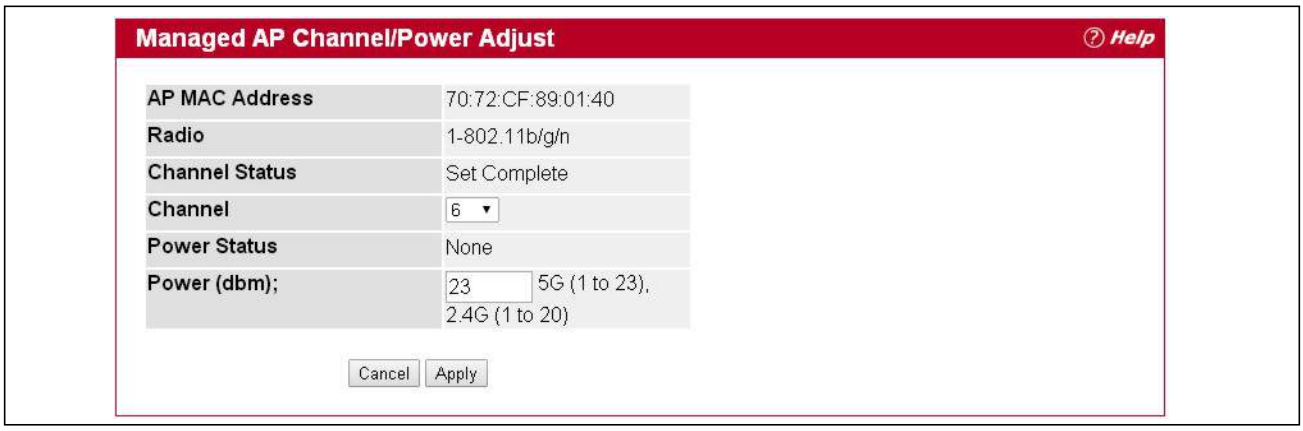


Figure 155: Managed AP Channel/Power Adjust

The fields in Table 142 appear when you click the current channel or power setting for an AP on the **Managed AP Advanced Settings** page.

Table 142: Managed AP Channel/Power Adjust

Field	*Description*
AP MAC Address	Shows the MAC address of the access point.
Radio	Displays the radio and its mode. The changes apply only to this radio.
Channel Status	The status is one of the following: • None • Set Requested • Set Complete
Channel	The Channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface. In the United States, IEEE 802.11b, 802.11g, and 2.4 GHz 802.11n modes (802.11 b/g/n) support the use of channels 1 through 11 inclusive, while IEEE 802.11a and 5-GHz 802.11n modes supports a larger set of non-consecutive channels (36,40,44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165, 169, 173). ***Note:*** The available channels depends on the country in which the APs operate. ***Note:*** For radios that use 5 GHz modes, some countries have a regulatory domain that requires radar detection. For these countries (based on the country code setting), the radio automatically uses the 802.11h protocol for selecting the channel if radar is detected on the statically assigned channel. Interference can occur when multiple access points within range of each other are broadcasting on the same or overlapping channels. The impact of this interference on network performance can intensify during busy times when a large amount of data and media traffic is competing for bandwidth. If you select auto, the AP scans the RF area for occupied channels and selects a channel from the available non-interfering, or clear channels. If you specify a channel, make sure that the channel does not interfere with the channel that neighbor APs use.
Power Status	The status is one of the following: • None • Set Requested • Set Complete
Power (dbm)	The power level affects how far an AP broadcasts its RF signal. If the power level is too low, wireless clients will not detect the signal or experience poor WLAN performance. If the power level is too high, the RF signal might interfere with other APs within range.

Command Buttons

The page includes the following buttons:

- **Cancel**—Cancels any actions and returns to the previous page.
- **Apply**—Applies the settings to the AP.

Remote Packet Capture

Packet capture is used to monitor data flows within a network. Packet capture allows you to discern each individual packet and analyze its content. Packet sniffing provides very detailed network monitoring and bandwidth usage analysis.

To capture packets passing through an remote access point, click **WLAN > AP Management > Remote Packet Capture**.

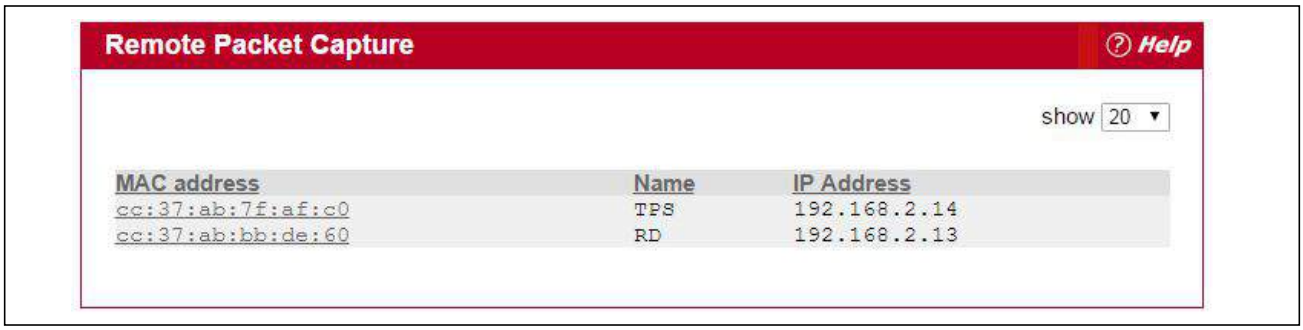


Figure 156: Remote Packet Capture

Table 143: Remote Packet Capture

Field	*Description*
MAC Address	Shows the MAC address of an access point.
Name	A name for the AP. This is the value configured in the valid AP database (either locally or on the RADIUS server).
IP Address	The network IP address of the managed AP.

Click on an entry under the MAC Address field to open the **Remote Packet Capture Action** page.

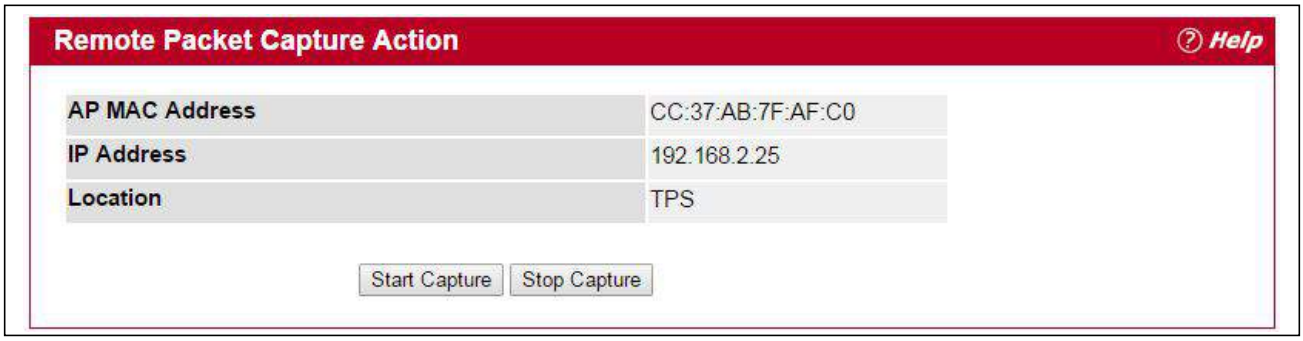


Figure 157: Remote Packet Capture Action

Table 144: Remote Packet Capture Action

Field	*Description*
AP MAC Address	Shows the MAC address of an access point.
IP Address	The network IP address of the managed AP.
Name	The name of the AP. This is the value configured in the valid AP database (either locally or on the RADIUS server).

Command Buttons

The page includes the following buttons:

- **Start Capture** — Start capturing packets passing through the remote AP.
- **Stop Capture** — Stop capturing packets passing through the remote AP.

To capture packets traversing a remote access point:

1. On an AP profile, enter the following information on AP profile > (Default profile, for an example) > Global.
   - Remote Packet Capture Interface: Select “Radio 1” if capturing 5GHz packets or “Radio 2” if capturing 2.4 GHz packets.
   - Remote Packet Capture Server IP: Enter the address of the TFTP server to which captured packets are sent.
   - Remote Packet Capture Duration: Enter the maximum time of the capture duration in seconds.
   - Remote Packet Capture File Size: Enter the maximum file size of the capture.
2. On the TFTP server, click Browse to navigate to the file location.
3. On the TFTP server, select the file to upload and click **Start File Transfer**.
4. On the Remote Packet Capture page, click on one of the managed AP's MAC address.
5. Click on **Start Capture** to start capturing packets and **Stop Capture** to stop.
6. Verify that you received the captured wireless packets on the TFTP server.
7. The packets will be in .pcap format, and can be viewed by wireshark for example or any software that can interpret .pcap format.

Monitoring Status and Statistics

The Status/Statistics folder contains links to the following pages that help you monitor the status and statistics for your Unified Wireless Switch network:

- Wireless Global Status/Statistics
- Managed AP Status
- Associated Client Status/Statistics
- Peer Switch Status

Wireless Global Status/Statistics

The UWS periodically collects information from the APs it manages and from associated peer switches. The information on the Global page shows status and statistics about the switch and all of the objects associated with it. You can access the global WLAN statistics by clicking **WLAN** > **Status/Statistics** > **Global**.

Global | Switch Status | IP Discovery | Configuration Received | AP Hardware Capability | AP Image Availability

Wireless Global Status/Statistics Help

WLAN Switch Operational Status	Enabled	IP Address	192.168.0.22
Peer Switches	1		
Cluster Controller	Yes	Cluster Controller IP Address	192.168.0.22
Total Access Points	2	Total Clients	0
Managed Access Points	2	Authenticated Clients	0
Discovered Access Points	0	Maximum Associated Clients	45000
Connection Failed Access Points	0	Rogue AP Mitigation Count	0
Maximum Managed APs in Peer Group	506	Rogue AP Mitigation Limit	16
Rogue Access Points	21	Detected Clients	456
Standalone Access Points	0	Maximum Detected Clients	90000
Unknown Access Points	75	WLAN Utilization	0 %
Maximum Pre-authentication History Entries	500	Total Pre-authentication History Entries	0
Maximum Roam History Entries	500	Total Roam History Entries	4
AP Provisioning Count	2	Maximum AP Provisioning Entries	1012
RRM Channel Load History Entries	0	Maximum Channel Load History Entries	100
WLAN Bytes Transmitted	6807387	WLAN Packets Transmitted	319623
WLAN Bytes Received	24288683	WLAN Packets Received	1094556
WLAN Bytes Transmit Dropped	0	WLAN Packets Transmit Dropped	0
WLAN Bytes Receive Dropped	0	WLAN Packets Receive Dropped	0
Distributed Tunnel Packets Transmitted	0	Distributed Tunnel Roamed Clients	0
Distributed Tunnel Clients	0	Distributed Tunnel Client Denials	0
Total Voice Traffic Streams	0	Total Traffic Stream Clients	0
Total Video Traffic Streams	0	Total Traffic Stream Roaming Clients	0

TSPEC Statistics

Access Category	Voice	Video
Total TSPEC Packets Received	0	0
Total TSPEC Packets Transmitted	0	0
Total TSPEC Bytes Received	0	0
Total TSPEC Bytes Transmitted	0	0
Total TSPECs Accepted	0	0
Total TSPECs Rejected	0	0
Total Roaming TSPECs Accepted	0	0
Total Roaming TSPECs Rejected	0	0

Refresh | Clear Statistics

Figure 158: Global WLAN Status/Statistics

Table 145 describes the fields on the **Wireless Global Status/Statistics** page.

Table 145: Global WLAN Status/Statistics

Field	*Description*
WLAN Switch Operation Status	This status field displays the operational status of the WLAN Switch. The WLAN Switch may be configured as enabled, but is operationally disabled due to configuration dependencies. If the operational status is disabled, the reason will be displayed in the following status field. The WLAN Switch is composed of multiple components, and each component in the system must acknowledge an enable or disable of the WLAN Switch. During a transition the operational status might temporarily show a pending status.
WLAN Switch Disable Reason	If the status is disabled, this field appears and one of the following reasons is listed: • None: The cause for the disabled status is unknown. • Administrator disabled: The Enable WLAN Switch option on the global configuration page has been cleared. • No IP Address: The WLAN interface does not have an IP address. • No SSL Files: The UWS communicates with the APs it manages by using Secure Sockets Layer (SSL) connections. The first time you power on the UWS, it automatically generates a server certificate that will be used to set up the SSL connections. The SSL certificate and key generation typically completes in a few minutes. If routing is enabled on the switch, the operational status might be disabled due to one of the following reasons: • No Loopback Interface: The switch does not have a loopback interface. • Global Routing Disabled: Even if the routing mode is enabled on the WLAN switch interface, it must also be enabled globally for the operational status to be enabled.
IP Address	IP address of the switch.
Peer Switches	Number of peer WLAN switches detected on the network.
Cluster Controller	Indicates whether this switch is the Cluster Controller for the cluster. Among a group of peer switches, one of the switches is automatically elected or configured to be the Cluster Controller. The Cluster Controller gathers status and statistics about all APs and clients in the peer group. ***Note:*** Only the Cluster Controller switch can display managed APs, clients, statistics, and RF Scan databases for the whole cluster. The switches that are not Cluster Controllers can display information only about locally attached devices.
Cluster Controller IP Address	The IP address of the peer switch that is the Cluster Controller.
Total Access Points	Total number of Managed APs in the database. This value is always equal to the sum of Managed Access Points, Connection Failed Access Points, and Discovered Access Points.
Managed Access Points	Number of APs in the managed AP database that are authenticated, configured, and have an active connection with the wireless switch.
Discovered Access Points	APs that have a connection with the switch, but haven't been completely configured. This value includes all managed APs with a Discovered or Authenticated status.
Connection Failed Access Points	Number of APs that were previously authenticated and managed, but currently don't have connection with the wireless switch.
Maximum Managed APs in Peer Group	Maximum number of access points that can be managed by the cluster.

Table 145: Global WLAN Status/Statistics (Cont.)

Field	*Description*
Rogue Access Points	Number of Rogue APs currently detected on the WLAN. When an AP performs an RF scan, it might detect access points that have not been validated. It reports these APs as rogues.
Standalone Access Points	Number of trusted APs in Standalone mode. APs in Standalone mode are not managed by a switch.
Unknown Access Points	Number of Unknown APs currently detected on the WLAN. If an AP configured to be managed by the wireless switch is detected through an RF scan at any time that it is not actively managed it is classified as an Unknown AP.
Maximum Pre-authentication History Entries	Maximum number of Client Pre-Authentication events that can be recorded by the system.
Maximum Roam History Entries	Maximum number of entries that can be recorded in the roam history for all detected clients.
AP Provisioning Count	Current number of APs in the provisioning database.
RRM Channel Load History Events	Current number of entries in the RRM Channel Load History table. If a new entry is added when the list reaches the number of entries indicated in the **Channel Load History Entries** field**,** the oldest entry is purged.
Total Clients	Total number of clients in the database. This total includes clients with an Associated, Authenticated, or Disassociated status.
Authenticated Clients	Total number of clients in the associated client database with an Authenticated status.
Maximum Associated Clients	Maximum number of clients that can associate with the wireless system. This is the maximum number of entries allowed in the Associated Client database.
Rogue AP Mitigation Count	Number of APs to which the wireless system is currently sending de-authentication messages to mitigate against rogue APs. A value of 0 indicates that mitigation is not in progress.
Rough AP Mitigation Limit	Maximum number of APs for which the system can send de-authentication frames.
Detected Clients	Number of wireless clients detected in the WLAN.
Maximum Detected Clients	Maximum number of clients that can be detected by the switch. The number is limited by the size of the Detected Client Database.
WLAN Utilization	Total network utilization across all APs managed by this switch. This is based on global statistics.
Total Pre-authentication History Entries	Current number of pre-authentication history entries in use by the system.
Total Roam History Entries	Current number of roam history entries in use by the system.
Maximum AP Provisioning Entries	Number of AP provisioning entries that can be stored by the system.
Maximum Channel Load History Entries	Number of channel load history entries that can be stored by the system.
WLAN Bytes Transmitted	Total bytes transmitted across all APs managed by the switch.
WLAN Bytes Received	Total bytes received across all APs managed by the switch.

Table 145: Global WLAN Status/Statistics (Cont.)

Field	*Description*
WLAN Packets Transmitted	Total packets transmitted across all APs managed by the switch.
WLAN Packets Received	Total packets received across all APs managed by the switch.
WLAN Bytes Transmit Dropped	Total bytes transmitted across all APs managed by the switch that were dropped.
WLAN Bytes Received Dropped	Total bytes received across all APs managed by the switch that were dropped.
WLAN Packets Transmit Dropped	Total packets transmitted across all APs managed by the switch that were dropped.
WLAN Packets Receive Dropped	Total packets received across all APs managed by the switch that were dropped.
Distributed Tunnel Packets Transmitted	Total number of packets sent by all APs via distributed tunnels.
Distributed Tunnel Clients	Total number of clients that are associated with an AP that are using distributed tunneling.
Distributed Tunnel Roamed Clients	Total number of clients that successfully roamed away from Home AP using distributed tunneling.
Distributed Tunnel Client Denials	Total number of clients for which the system was unable to set up a distributed tunnel when client roamed.
Total Voice Traffic Streams	Shows the number of voice traffic streams being transmitted by wireless clients that are connected to the network through APs managed by this switch. ***Note:*** A traffic stream is a collection of data packets identified by the AP as belonging to a particular user priority.
Total Video Traffic Streams	Shows the number of video traffic streams being transmitted by wireless clients that are connected to the network through APs managed by this switch.
Total Traffic Stream Clients	Shows the number of wireless clients currently transmitting traffic streams.
Total Traffic Stream Roaming Clients	Shows the number of wireless clients with a roaming status that are currently transmitting traffic streams.
TSPEC Statistics (Voice and Video)	
Total TSPEC Packets Received	The number of TSPEC packets sent from the wireless client to the AP. The number is a total for all APs managed by the switch.
Total TSPEC Packets Transmitted	The number of TSPEC packets sent from the AP to the wireless client. The number is a total for all APs managed by the switch.
Total TSPEC Bytes Received	The number of TSPEC bytes sent from the wireless client to the AP. The number is a total for all APs managed by the switch.
Total TSPEC Bytes Transmitted	The number of TSPEC bytes sent from the AP to the wireless client. The number is a total for all APs managed by the switch.
Total TSPECs Accepted	The number of TSPEC packets that were accepted by all APs that the switch manages.
Total TSPECs Rejected	The number of TSPEC packets that were rejected by all APs that the switch manages.
Total Roaming TSPECs Accepted	The total number of TSPEC packets transmitted by roaming clients that were accepted by all APs that the switch manages.

Table 145: Global WLAN Status/Statistics (Cont.)

Field	*Description*
Total Roaming TSPECs Rejected	The total number of TSPEC packets transmitted by roaming clients that were rejected by all APs that the switch manages.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Clear Statistics**—Reset all counters on the page to zero.

Viewing Switch Status and Statistics Information

The **Switch Status/Statistics** page for each switch provides information about the access points it manages and their associated clients. If the switch is the Cluster Controller, it provides the switch status and statics information about each switch in its group.

Note: Only the Cluster Controller switch can display managed APs, clients, statistics, and RF Scan database information for the whole cluster. The switches that are not Cluster Controllers can display information about locally attached devices.

Use the drop-down menu to select the switch with the information to display. If the local switch is the only available option, then it is the only switch in the cluster, or it is not a Cluster Controller.

To open this page, click the **WLAN** > **Status/Statistics** > **Switch Status** tab.

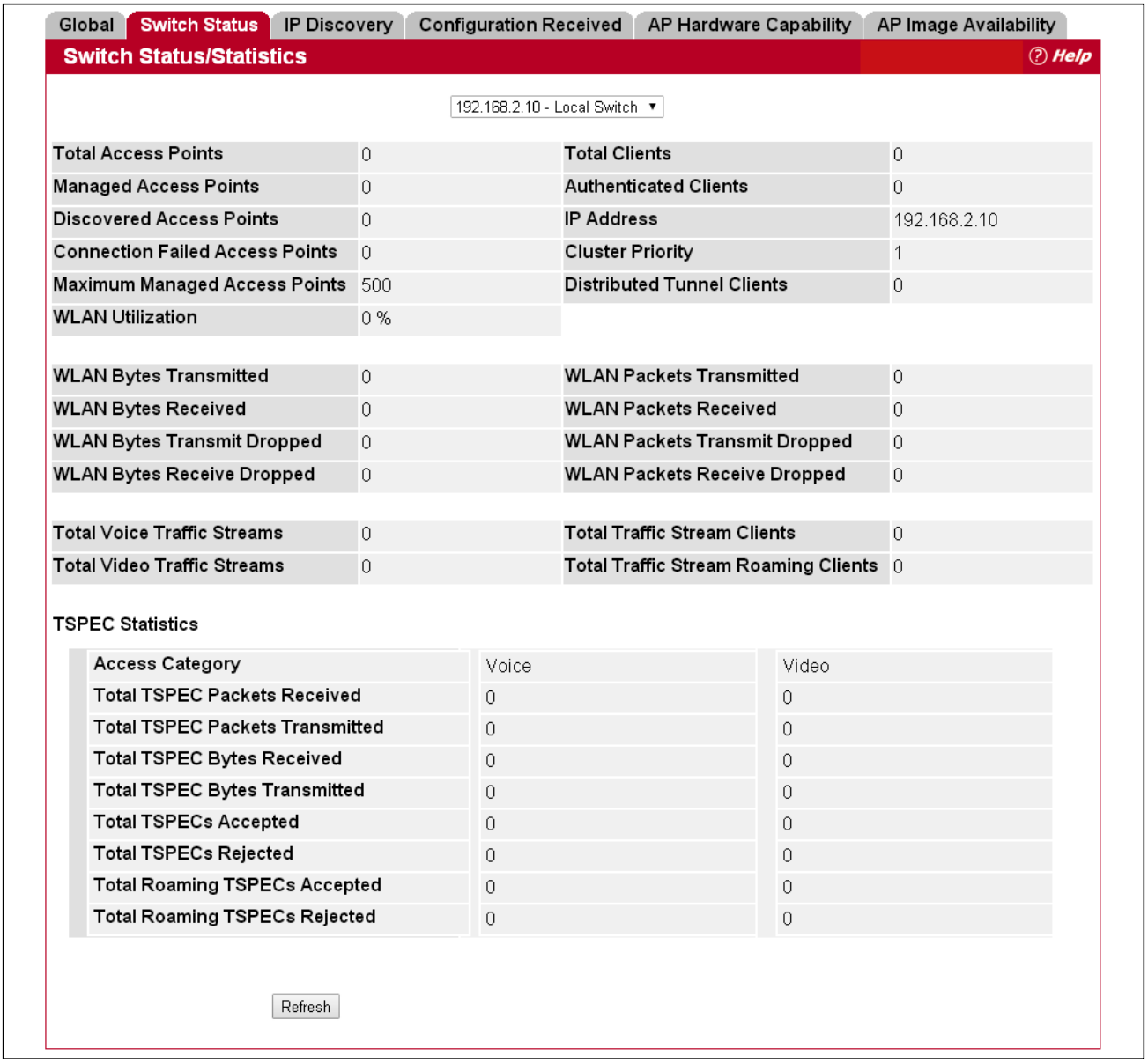


Figure 159: Switch Status/Statistics

Table 146 describes the fields on the **Switch Status/Statistics** page.

Table 146: Switch Status/Statistics

Field	*Description*
Total Access Points	Total number of Managed APs in the database. This value is always equal to the sum of Managed Access Points, Connection Failed Access Points, and Discovered Access Points.
Managed Access Points	Number of APs in the managed AP database that are authenticated, configured, and have an active connection with the wireless switch.
Discovered Access Points	APs that have a connection with the switch, but haven't been completely configured. This value includes all managed APs with a Discovered or Authenticated status.
Connection Failed Access Points	Number of APs that were previously authenticated and managed, but currently don't have connection with the wireless switch.
Maximum Managed Access Points	Maximum number of access points that can be managed by the switch.
WLAN Utilization	Total network utilization across all APs managed by this switch. This is based on global statistics.
Total Clients	Total number of clients in the database. This total includes clients with an Associated, Authenticated, or Disassociated status.
Authenticated Clients	Total number of clients in the associated client database with an Authenticated status.
IP Address	IP address of the switch.
Cluster Priority	Cluster priority value of the switch. The switch with highest priority in a cluster becomes the Cluster Controller. If the priority is the same then the switch with lowest IP address becomes the Cluster Controller. A priority of 0 means that the switch cannot become the Cluster Controller.
Distributed Tunnel Clients	Total number of clients that are associated with an AP that are using distributed tunneling.
WLAN Bytes Transmitted	Total bytes transmitted across all APs managed by the switch.
WLAN Bytes Received	Total bytes received across all APs managed by the switch.
WLAN Bytes Transmit Dropped	Total bytes transmitted across all APs managed by the switch that were dropped.
WLAN Bytes Received Dropped	Total bytes received across all APs managed by the switch that were dropped.
WLAN Packets Transmitted	Total packets transmitted across all APs managed by the switch.
WLAN Packets Received	Total packets received across all APs managed by the switch.
WLAN Packets Transmit Dropped	Total packets transmitted across all APs managed by the switch that were dropped.
WLAN Packets Receive Dropped	Total packets received across all APs managed by the switch that were dropped.
Total Voice Traffic Streams	Shows the number of voice traffic streams being transmitted by wireless clients that are connected to the network through APs managed by this switch. ***Note:*** A traffic stream is a collection of data packets identified by the AP as belonging to a particular user priority.

Table 146: Switch Status/Statistics (Cont.)

Field	*Description*
Total Video Traffic Streams	Shows the number of video traffic streams being transmitted by wireless clients that are connected to the network through APs managed by this switch.
Total Traffic Stream Clients	Shows the number of wireless clients currently transmitting traffic streams.
Total Traffic Stream Roaming Clients	Shows the number of wireless clients with a roaming status that are currently transmitting traffic streams.
TSPEC Statistics	
Access Category	Indicates whether the TSPEC data is for voice traffic or video traffic. The wireless system maintains separate counters for the voice and video categories.
Total TSPEC Packets Received	The number of TSPEC packets sent from the wireless client to the AP. The number is a total for all APs managed by the switch.
Total TSPEC Packets Transmitted	The number of TSPEC packets sent from the AP to the wireless client. The number is a total for all APs managed by the switch.
Total TSPEC Bytes Received	The number of TSPEC bytes sent from the wireless client to the AP. The number is a total for all APs managed by the switch.
Total TSPEC Bytes Transmitted	The number of TSPEC bytes sent from the AP to the wireless client. The number is a total for all APs managed by the switch.
Total TSPECs Accepted	The number of TSPEC packets that were accepted by all APs that the switch manages.
Total TSPECs Rejected	The number of TSPEC packets that were rejected by all APs that the switch manages.
Total Roaming TSPECs Accepted	The total number of TSPEC packets transmitted by roaming clients that were accepted by all APs that the switch manages.
Total Roaming TSPECs Rejected	The total number of TSPEC packets transmitted by roaming clients that were rejected by all APs that the switch manages.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing IP Discovery Status

From the **WLAN > Status/Statistics** > **IP Discovery** tab, you can view information about communication with the devices in the IP discovery list on the **Wireless Discovery Status** page.

The IP Discovery list can contain the IP addresses of peer switches and APs for the UWS to discover and associate with as part of the WLAN.

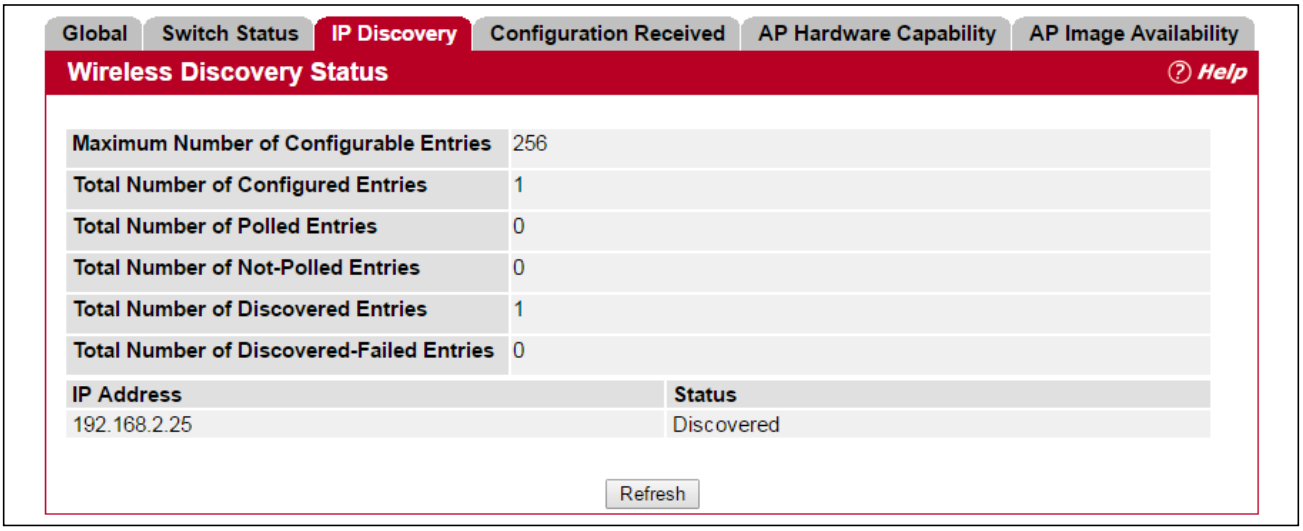


Figure 160: Wireless Discovery Status

Table 147: AP Hardware Capability Radio Detail

Field	*Description*
Maximum Number of Configurable Entries	Shows the maximum number of IP addresses that can be configured in the IP Discovery list.
Total Number of Configured Entries	Shows the number of IP addresses that have been configured in the IP Discovery list.
Total Number of Polled Entries	Identifies how many of the IP addresses in the IP Discovery list the switch has attempted to contact.
Total Number of Not-Polled Entries	Identifies how many of the IP addresses in the IP Discovery list the switch has not attempted to contact.
Total Number of Discovered Entries	Identifies how many devices (peer switches or APs) the switch has successfully discovered, authenticated, and validated by polling the IP address configured in the IP Discovery list.
Total Number of Discovered-Failed Entries	Identifies how many devices that have an IP address configured in the IP Discovery list that the switch has attempted to contact and failed to authenticate or validate.

Table 147: AP Hardware Capability Radio Detail (Cont.)

Field	*Description*
IP Address	Shows the IP address of the device configured in the IP Discovery list.
Status	The status is in one of the following states: • **Not Polled**: The switch has not attempted to contact the IP address in the L3/IP Discovery list. • **Polled**: The switch has attempted to contact the IP address. • **Discovered**: The switch contacted the peer switch or the AP in the L3/IP Discovery list and has authenticated or validated the device. • **Discovered - Failed**: The switch contacted the peer switch or the AP with IP address in the L3/IP Discovery list and was unable to authenticate or validate the device. If the device is an access point, an entry appears in the AP failure list with a failure reason.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing the Peer Switch Configuration Received Status

The Peer Switch Configuration feature allows you to send the critical wireless configuration from one switch to all other switches. In addition to keeping the switches synchronized, this function enables the administrator to manage all wireless switches in the cluster from one switch. The **Peer Switch Configuration Receive Status** page provides information about the configuration a switch has received from one of its peers.

To open the following page, click the **WLAN** > **Status/Statistics** > **Configuration Received** tab**.**

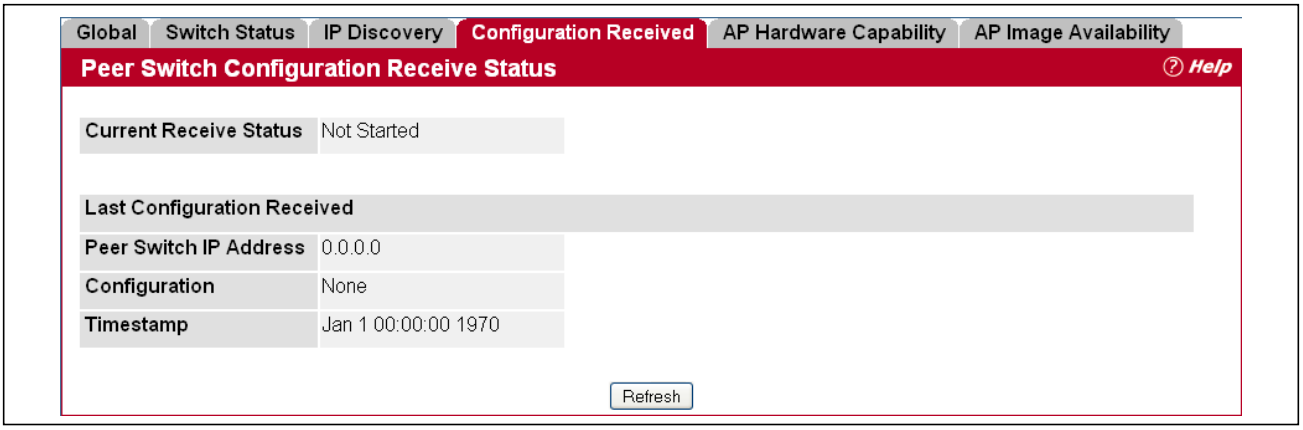


Figure 161: Configuration Received

Table 148 describes the fields on the **Peer Switch Configuration Received Status** page.

Table 148: Peer Switch Configuration

Field	*Description*
Current Receive Status	Indicates the global status when wireless configuration is received from a peer switch. The possible status values are as follows: • Not Started • Receiving Configuration • Saving Configuration, • Applying AP Profile Configuration • Success • Failure - Invalid Code Version • Failure - Invalid Hardware Version • Failure - Invalid Configuration
Last Configuration Received	
Peer Switch IP Address	Indicates the last switch from which this switch received any wireless configuration data.
Configuration	Indicates which portions of configuration were last received from a peer switch, which can be one or more of the following: • None • Global • Discovery • Channel/Power • AP Database • AP Profiles • Known Client • Captive Portal • RADIUS Client • QoS ACL • QoS DiffServ If the switch has not received any configuration for another switch, the value is None.
Timestamp	Indicates the last time this switch received any configuration data from a peer switch.

Command Buttons

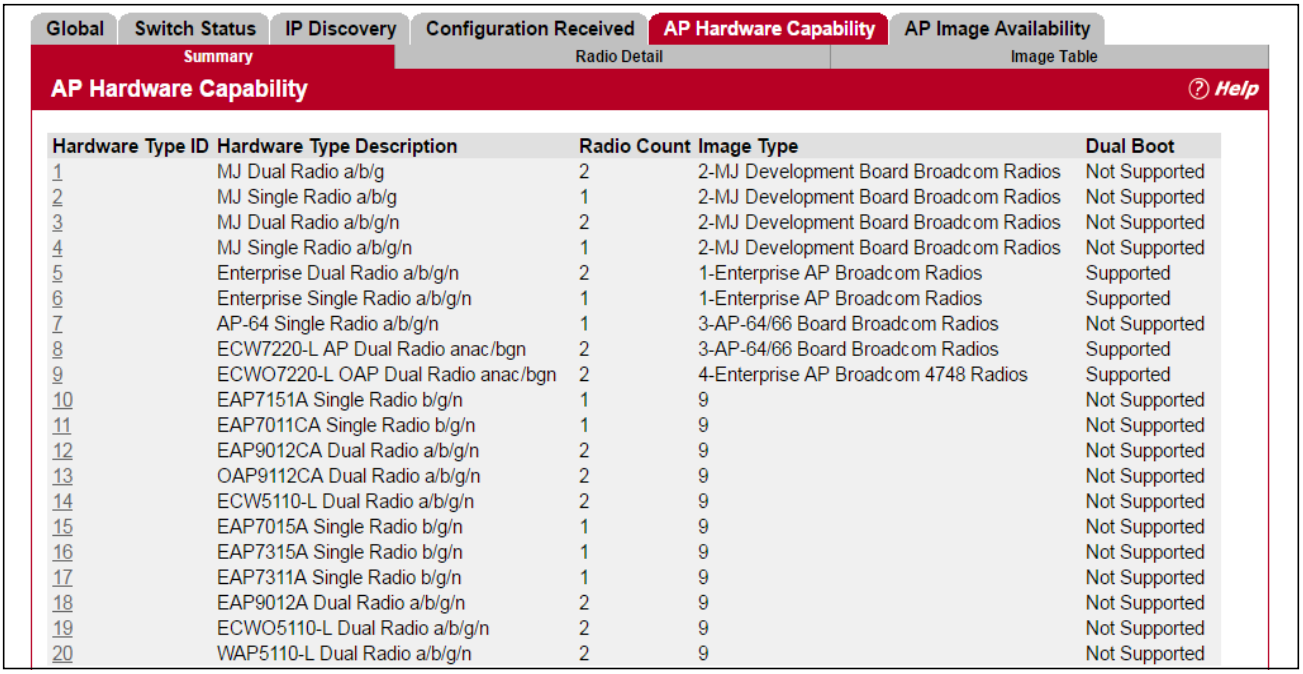
The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing the AP Hardware Capability List

The switch can support APs that have different hardware capabilities, such as the supported number of radios, the supported IEEE 802.11 modes, and the software image required by the AP. From the AP Hardware Capability tab, you can access summary information about the AP Hardware support, the radios and IEEE modes supported by the hardware, and the software images that are available for download to the APs.

To open the following page, click the **WLAN Status/Statistics** > **AP Hardware Capability** > **Summary** tab**.**



Hardware Type ID	Hardware Type Description	Radio Count	Image Type	Dual Boot
1	MJ Dual Radio a/b/g	2	2-MJ Development Board Broadcom Radios	Not Supported
2	MJ Single Radio a/b/g	1	2-MJ Development Board Broadcom Radios	Not Supported
3	MJ Dual Radio a/b/g/n	2	2-MJ Development Board Broadcom Radios	Not Supported
4	MJ Single Radio a/b/g/n	1	2-MJ Development Board Broadcom Radios	Not Supported
5	Enterprise Dual Radio a/b/g/n	2	1-Enterprise AP Broadcom Radios	Supported
6	Enterprise Single Radio a/b/g/n	1	1-Enterprise AP Broadcom Radios	Supported
7	AP-64 Single Radio a/b/g/n	1	3-AP-64/66 Board Broadcom Radios	Not Supported
8	ECW7220-L AP Dual Radio anac/bgn	2	3-AP-64/66 Board Broadcom Radios	Supported
9	ECWO7220-L OAP Dual Radio anac/bgn	2	4-Enterprise AP Broadcom 4748 Radios	Supported
10	EAP7151A Single Radio b/g/n	1	9	Not Supported
11	EAP7011CA Single Radio b/g/n	1	9	Not Supported
12	EAP9012CA Dual Radio a/b/g/n	2	9	Not Supported
13	OAP9112CA Dual Radio a/b/g/n	2	9	Not Supported
14	ECW5110-L Dual Radio a/b/g/n	2	9	Not Supported
15	EAP7015A Single Radio b/g/n	1	9	Not Supported
16	EAP7315A Single Radio b/g/n	1	9	Not Supported
17	EAP7311A Single Radio b/g/n	1	9	Not Supported
18	EAP9012A Dual Radio a/b/g/n	2	9	Not Supported
19	ECWO5110-L Dual Radio a/b/g/n	2	9	Not Supported
20	WAP5110-L Dual Radio a/b/g/n	2	9	Not Supported

Figure 162: AP Hardware Capability Summary Information

Table 149 describes the fields available on the **AP Hardware Capability Summary** page.

Table 149: AP Hardware Capability Summary

Field	*Description*
Hardware Type ID	Identifies the ID number assigned to each AP hardware type. The switch supports up to six different AP hardware types.
Hardware Type Description	Includes a description of the platform and the supported IEEE 802.11 modes.
Radio Count	Specifies whether the hardware supports one radio or two radios.
Image Type	Specifies the type of software the hardware requires.
Dual Boot	Indicates whether this AP hardware type supports dual boot. On dual boot APs, if the AP code is corrupted during the code upgrade process due to a power failure or unexpected AP reset while the AP is writing to NVRAM then the AP is able to come up using the old image.

Click the Hardware Type ID to view the AP hardware radio capability information for that hardware type.

AP Hardware Radio Capability

Use the menu to select the hardware type, and then select the radio to view radio details. If the selected hardware only supports one radio, Radio 2 displays a message indicating that the radio is invalid for the selected hardware type. To open the this page, click the **WLAN > Status/Statistics** > **AP Hardware Capability** > **Radio Detail** tab**.**

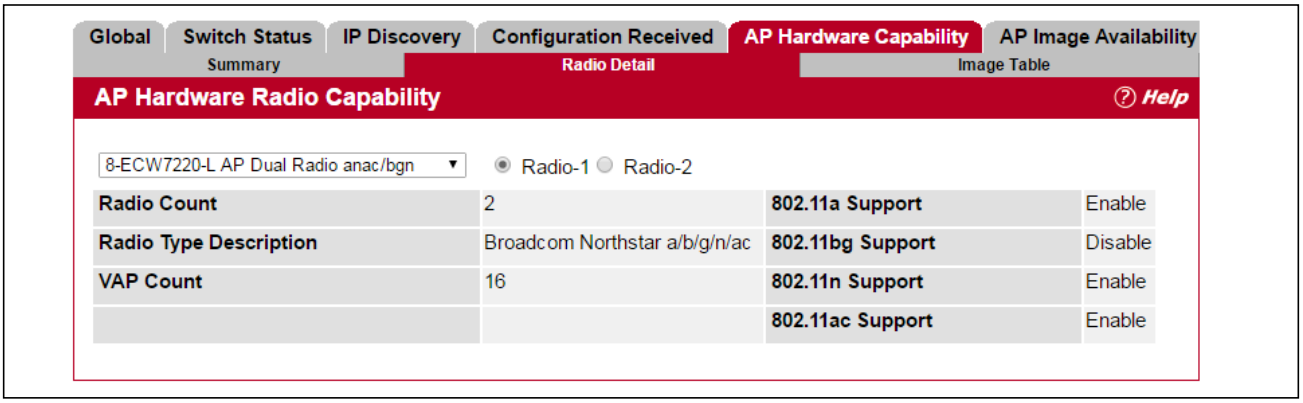


Figure 163: AP Hardware Capability Radio Detail

Table 150 describes the fields available on the **AP Hardware Radio Capability Radio Detail** page.

Table 150: AP Hardware Capability Radio Detail

Field	*Description*
Radio Count	Displays the number of radios supported on the hardware platform, which is either 1 or 2.
Radio Type Description	Displays the type of radio, which might contain information such as the manufacturer name and supported IEEE 802.11 modes.
VAP Count	Displays the number of VAPs the radio supports.
802.11a Support	Shows whether support for IEEE 802.11a mode is enabled.
802.11bg Support	Shows whether support for IEEE 802.11bg mode is enabled.
802.11n Support	Shows whether support for IEEE 802.11n mode is enabled.
802.11ac Support	Shows whether support for IEEE 802.11ac mode is enabled.

AP Image Capability

The switch is able to update software on the access points that it manages. To update the AP with the correct software, the UWS can store up to three AP software images to support different AP hardware types. The Image Table displays the image ID-to-hardware type mapping. To open this page, click the **WLAN >** > **Status/Statistics** > **AP Hardware Capability** > **Image Table** tab.

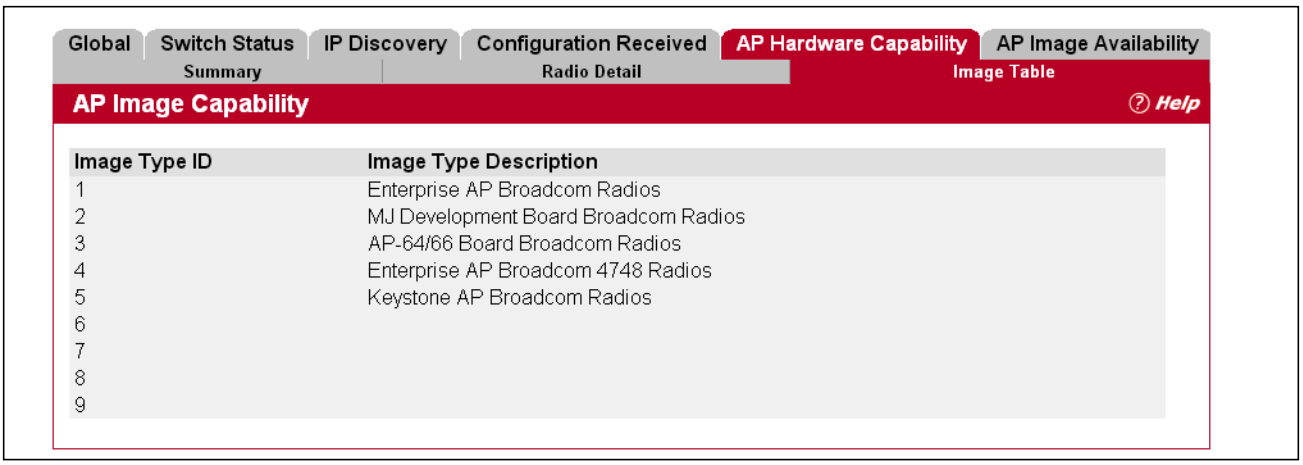


Figure 164: AP Hardware Capability Image Table

Table 151 describes the fields available on the **AP Hardware Capability Image Table** page.

Table 151: AP Image Capability

Field	*Description*
Image Type ID	Shows the ID number assigned to the image.
Image Type Description	Provides a basic description of the image.

Integrated AP Image Availability

The **AP Image Availability** page is available on switches that support the integrated mode for upgrading code on managed APs (Broadcom AP). In the Integrated AP Image mode, the switch that manages the AP automatically loads the code image for the AP stored on the switch. The new code is loaded whenever the AP code does not match the version stored on the switch, so the AP may be upgraded or downgraded.

The Integrated AP Image Availability table shows all code image types available on the switch for the APs and the version number of each image. To open this page, click the **WLAN** > **Status/Statistics** > **AP Image Availability** tab.

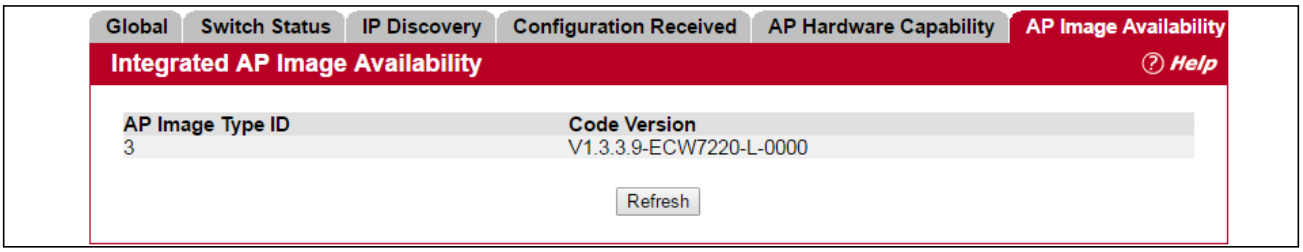


Figure 165: Integrated AP Image Availability

Table 152 describes the fields available on the AP Image Availability page.

Table 152: Integrated AP Image Availability

Field	*Description*
AP Image Type ID	Shows the ID number assigned to the image.
Code Version	Identifies the code version number.

Managed AP Status

From the **Managed Access Point Status** page, you can access a variety of information about each AP that the switch manages. The pages you access from the **Status** tab provide configuration and association information about managed APs and their neighbors. The pages you access from the **Statistics** tab display information about the number of packets and bytes transmitted and received on various interfaces.

Monitoring AP Status

To open this page click **WLAN** > **Status/Statistics** > **Managed AP** > **Status**. The following figure shows the **Managed Access Point Status** page with one managed AP.

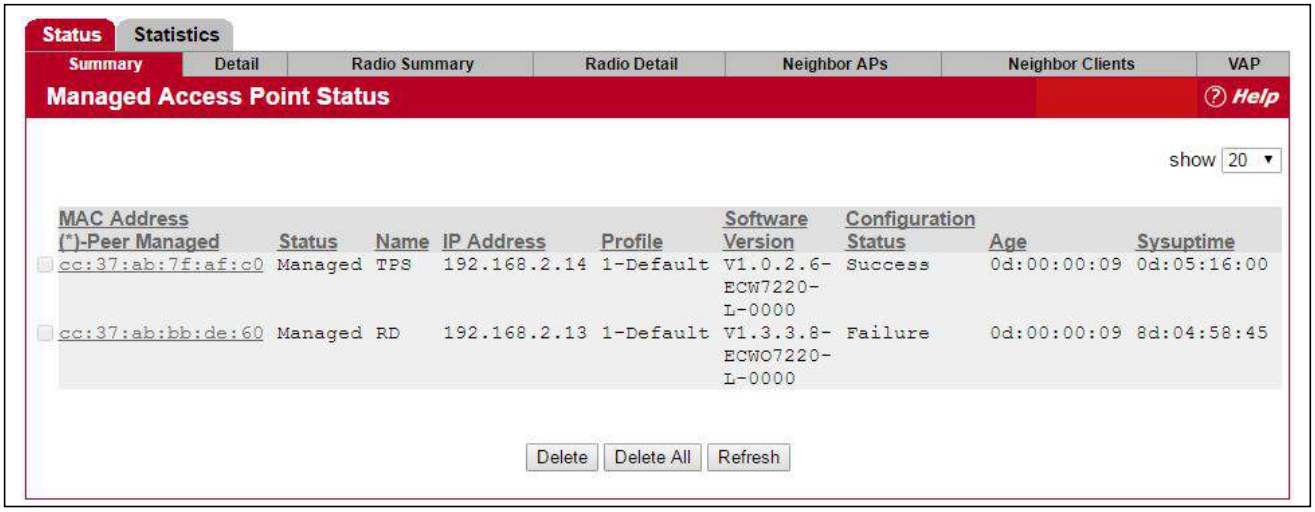


Figure 166: Managed Access Point Status

The following tabs are available from the **Managed Access Point Status** page:

Tab	*Description*
Summary	Lists the APs managed by the switch and provides summary information about them.
Detail	Shows detailed status information collected from the AP
Radio Summary	Shows the channel, transmit power, and number of associated wireless clients for all managed APs.
Radio Detail	Shows detailed status for a radio interface. Use the radio button to navigate between the two radio interfaces.

Tab	*Description*
Neighbor APs	Shows the neighbor APs that the specified AP has discovered through periodic RF scans on the selected radio interface.
Neighbor Clients	Shows information about wireless clients associated with an AP or detected by the AP radio.
VAP	Shows summary information about the virtual access points (VAPs) for the selected AP and radio interface on the APs that the switch manages.

The following table provides summary information about the APs that the switch manages. If the switch is the Cluster Controller, the page provides information about the APs managed by all switches in the cluster.

Table 153: Managed Access Point Status

Field	*Description*
MAC Address	The Ethernet address of the UWS-managed AP. If the MAC address of the AP is preceded by an asterisk (*), it is managed by a peer switch.
Status	The current managed state of the AP. The possible values are: • Discovered: The AP is discovered and by the switch, but is not yet authenticated. • Authenticated: The AP has been validated and authenticated (if authentication is enabled), but it is not configured. • Upgrading: The AP is in the process of receiving or activating a new image. This status is applicable only when the wireless switch supports the Integrated AP Image Download mode. • Managed: The AP profile configuration has been applied to the AP and it's operating in managed mode. • Failed: The UWS lost contact with the AP, a failed entry will remain in the managed AP database unless you remove it. Note that a managed AP will temporarily show a failed status during a reset.
Name	A name for the AP. This is the value configured in the valid AP database (either locally or on the RADIUS server).
IP Address	The network IP address of the managed AP.
Profile	The AP profile configuration currently applied to the managed AP. The profile is assigned to the AP in the valid AP database. **NOTE:** Once an AP is discovered and managed by the UWS, if the profile is changed in the valid AP database (either locally or on the RADIUS server) the AP must be reset to configure with the new profile.
Software Version	The software version the AP is currently running.

Table 153: Managed Access Point Status (Cont.)

Field	*Description*
Configuration Status	This status indicates if the AP is configured successfully with the assigned profile. The status is one of the following: • Not Configured: The profile has not been sent to the AP yet, the AP may be discovered but not yet authenticated. • In Progress: The switch is currently sending the AP profile configuration packet to the AP. • Success: The entire profile has been sent to the AP and there were no configuration errors. • Partial Success: The entire profile has been sent to the AP and there were configuration errors (for example, some configuration parameters were not accepted), but the AP is operational. • Failure: The profile has been sent to the AP and there were configuration errors, the AP is not operational.
Age	Time since last communication between the UWS and the AP.
Sysuptime	The time since this AP was last rebooted.

Note: You can sort the lis t of APs by clicking any of the column headings. For example, to sort the APs by the profile they use, click **Profile**.

Command Buttons

The page includes the following buttons:

- **Delete**—Clears the selected entry from the current list. Only APs with a Configuration Status of Failed can be removed from the list.
- **Delete All**—Clears all APs with a Configuration Status of Failed from the current list.
- **Refresh**—Updates the page with the latest information.

Viewing Detailed Managed Access Point Status

To view detailed information about an AP that the switch manages, click the MAC address of the AP from the **Summary** page or select the MAC address of the AP from the drop-down menu on the **Detail** page.

To open this page, click the **WLAN** > **Status/Statistics** > **Managed AP > Status** > **Detail** tab.

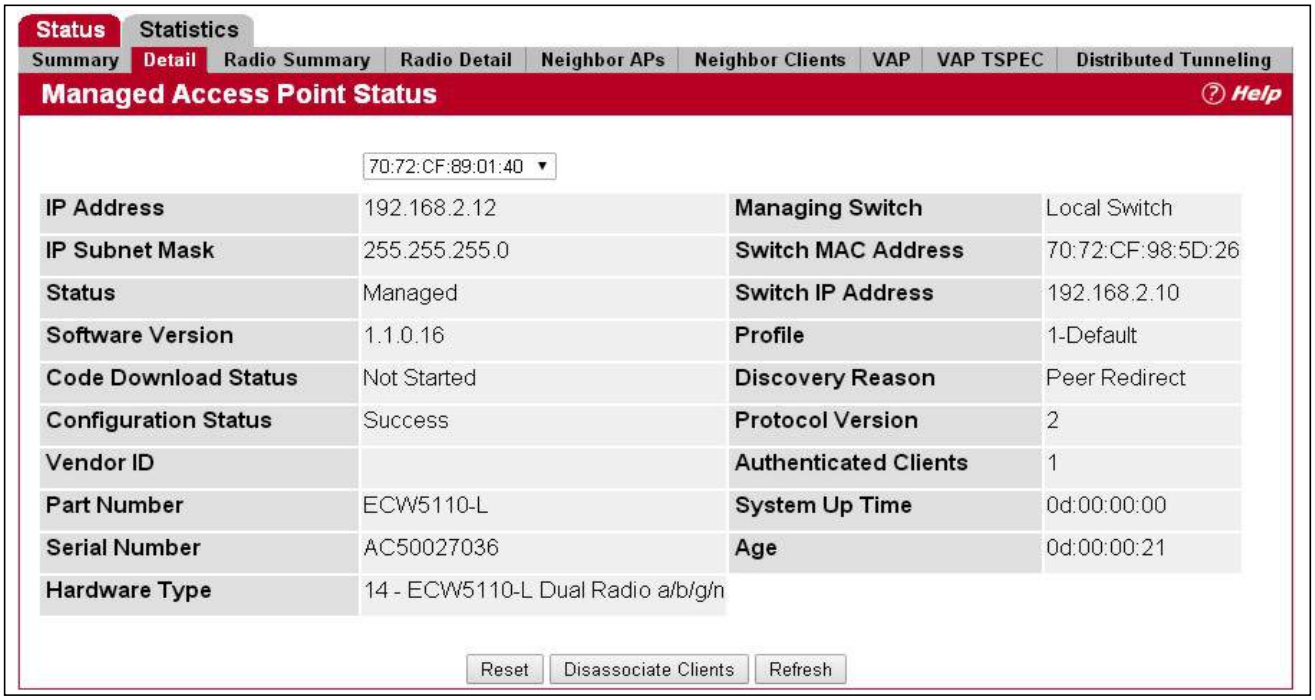


Figure 167: Managed Access Point Status Detail

Table 154 describes the fields you see on the **Detail** page for the managed access point status. The label at the top of the table shows the MAC address and location of the AP to which the values on the page apply. To view details about a different AP, select its MAC address from the drop-down menu.

Table 154: Detailed Managed Access Point Status

Field	*Description*
IP Address	The IP address of the managed AP.
IP Subnet Mask	The subnet mask of the managed AP

Table 154: Detailed Managed Access Point Status (Cont.)

Field	*Description*
Status	The current managed state of the AP. The possible values are: • Discovered: The AP is discovered and by the switch, but is not yet authenticated. • Authenticated: The AP has been validated and authenticated (if authentication is enabled), but it is not configured. • Upgrading: The AP is in the process of receiving or activating a new image. This status is applicable only when the wireless switch supports the Integrated AP Image Download mode. • Managed: The AP profile configuration has been applied to the AP and it's operating in managed mode. • Connection Failed: The UWS lost contact with the AP, a failed entry will remain in the managed AP database unless you remove it. Note that a managed AP will temporarily show a failed status during a reset.
Software Version	Indicates the version of software on the AP, this is learned from the AP during discovery.
Code Download Status	Indicates the current status of a code download request for this AP. The possible values include the following: • Not Started: No download has begun. • Requested: A download is planned for this AP, but the AP is not in the current download group, so it hasn't been told to start the download yet. • Code-Transfer-In-Progress: The AP has been told to download the code. • Failure: The AP reported a failing code download. • Aborted: The download was aborted before the AP loaded code from the TFTP server. • Waiting-For-APs-To-Download: A download finished on this AP, and it is waiting for other APs to finish download. Reset command is not sent to the AP in this state. • NVRAM-Update-In-Progress: Download completed successfully. The reset command sent to the AP. • Timed-Out: The AP did not reconnect to the UWS in the fixed time interval.
Configuration Status	Indicates whether the AP is configured successfully with the assigned profile. The status is one of the following: • Not Configured: The profile has not been sent to the AP yet, the AP may be discovered but not yet authenticated. • In Progress: The switch is currently sending the AP profile configuration packet to the AP. • Success: The entire profile has been sent to the AP and there were no configuration errors. • Partial Success: The entire profile has been sent to the AP and there were configuration errors, but the AP is operational. • Failure: The profile has been sent to the AP and there were configuration errors, the AP is not operational.
Vendor ID	Vendor of the AP software, this is learned from the AP during discovery.
Part Number	Hardware part number for the AP, which is learned from the AP during discovery.
Serial Number	Unique Serial number assigned to the AP, which is learned from the AP during discovery.
Hardware Type	Hardware platform for the AP, which is learned from the AP during discovery.
Managing Switch	Indicates whether the AP is managed by the local switch or a peer switch.

Table 154: Detailed Managed Access Point Status (Cont.)

Field	*Description*
Switch MAC Address	Identifies the MAC address of the switch that is managing the AP.
Switch IP Address	Identifies the IP address of the switch that is managing the AP.
Profile	The AP profile configuration currently applied to the managed AP, the profile is assigned to the AP in the valid AP database. ***Note:*** Once an AP is discovered and managed by the UWS, if the profile is changed in the valid AP database (either locally or on the RADIUS server) the AP must be reset to configure with the new profile.
Discovery Reason	This status value indicates how the managed AP was discovered, the status is one of the following values: • IP Poll Received: The AP was discovered via an IP poll from the UWS, its IP address is configured in the IP polling list. • Peer Redirect: The AP was discovered through a peer switch redirect, the AP tried to associate with another peer switch and learned the current UWS IP address from the peer (peer learned UWS IP address in RADIUS server response when validating the AP). • Switch IP Configured: The managed AP is configured with the UWS IP address. • Switch IP DHCP: The managed AP learned the current UWS IP address through DHCP option 43. • L2 Poll Received: The AP was discovered through the Edge-Core Wireless Device Discovery protocol.
Protocol Version	Indicates the protocol version supported by the software on the AP, which is learned from the AP during discovery.
Authenticated Clients	Total number of clients currently associated to the AP that have been authenticated. This is the sum of all authenticated clients for all the VAPs enabled on the AP.
System Up Time	Time in seconds since last power-on reset of the managed AP.
Age	Time since last communication between the UWS and the AP.

Command Buttons

The page includes the following buttons:

- **Reset**—Resets the managed AP. A pop-up message asks you to confirm that you want to reset the AP.
- **Disassociate Clients**—Disconnects all associated clients from the AP.
- **Refresh**—Updates the page with the latest information.

Viewing Managed Access Point Radio Summary Information

You can view general information about each operational radio on all APs managed by the switch. The **Managed Access Point Radio Summary** page shows the channel, transmit power, and number of associated wireless clients for all managed APs. For more information about a specific radio on an AP, click the radio.

To open this page, click the **WLAN** > **Status/Statistics** > **Managed AP** > **Status** > **Radio Summary** tab.

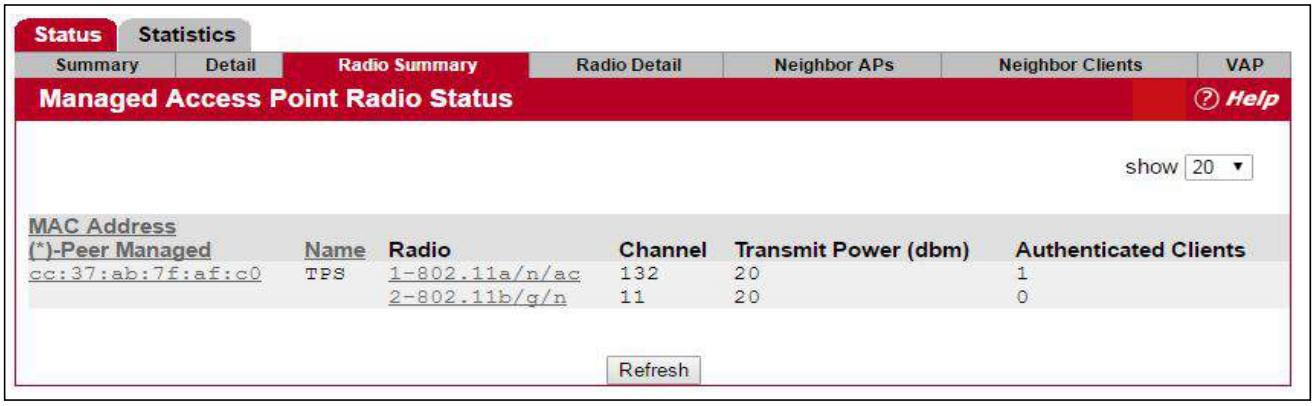


Figure 168: Managed Access Point Status Radio Summary

Table 155 describes the fields you see on the **Radio Summary** page for the managed access point status.

Table 155: Managed AP Radio Summary

Field	*Description*
MAC Address	The Ethernet address of the UWS managed AP. If the MAC address of the AP is followed by an asterisk (*), it is managed by a peer switch.
Name	A name for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates the radio interface and configured mode of the radio, if the radio is disabled the radio mode will be displayed as Off instead of showing the configured mode.
Channel	If radio is operational, the current operating channel for the radio.
Transmit Power	If radio is operational, the current transmit power for the radio.
Authenticated Clients	Total count of clients authenticated by the AP on the physical radio. This is a sum of all the clients authenticated by each VAP enabled on the radio.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Detailed Managed Access Point Radio Information

You can view detailed information about each radio on the APs that the UWS manages on the **Radio Detail** page for the managed access point radio status. Use the options above the table to select the AP and radio with the settings to view. The AP is identified by its MAC address and location. The radio is identified by its number and configured mode. If the radio is disabled, the radio mode will be displayed as Off.Table 156 describes the fields you see on the **Radio Detail** page for the managed access point status.

To open this page, click the **WLAN** > **Status/Statistics** > **Managed AP** > **Status** > **Radio Detail** tab.

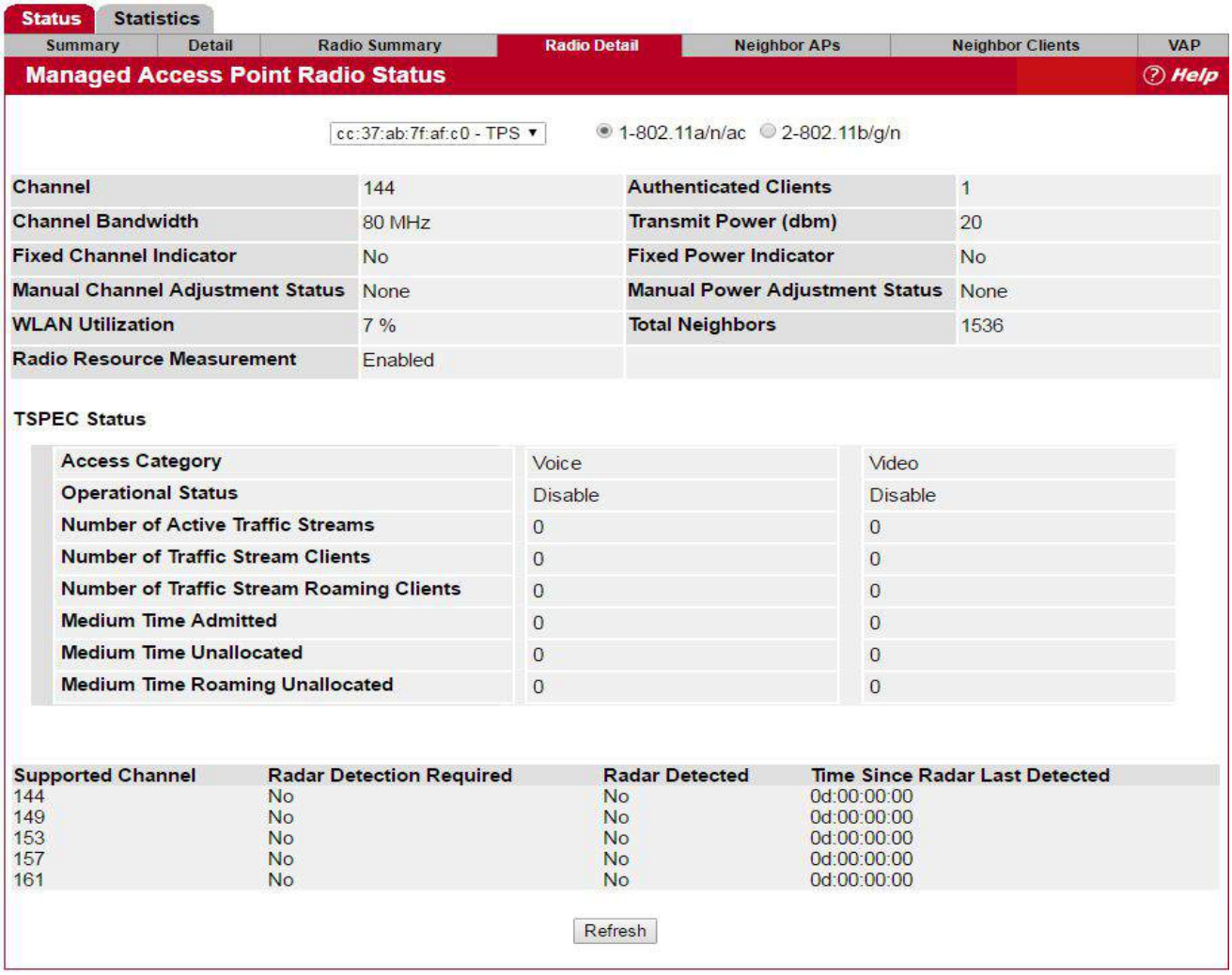


Figure 169: Managed Access Point Status Radio Detail

Table 156: Managed AP Radio Detail

Field	*Description*
Channel	If radio is operational, the current operating channel for the radio.
Channel Bandwidth	Indicates whether the channel bandwidth is 20 MHz or 40 MHz.

Table 156: Managed AP Radio Detail (Cont.)

Field	*Description*
Fixed Channel Indicator	This flag indicates if a fixed channel is configured and assigned to the radio, a fixed channel can be configured in the valid AP database (locally or on a RADIUS server).
Manual Channel Adjustment Status	Indicates the current state of a manual request to change the channel on this radio. The valid values are: • Not Started: No request has been made to change the channel. • Requested: A channel change has been requested by the user but has not been processed by the switch. • In Progress: The switch is processing a channel change request for this radio. • Success: A channel change request is complete. • Failure: A channel change request failed.
WLAN Utilization	Total network utilization for the physical radio. This value is based on radio statistics.
Radio Resource Measurement	Radio Resource Measurement (RRM) mode requires the Wireless System to send additional information in beacons, probe responses, and association responses. Enable or disable support for radio resource measurement in the AP profile. This feature is set independently for each radio and is enabled by default.
Authenticated Clients	Total count of clients authenticated with the AP on the physical radio. This is a sum of all the clients authenticated with the AP for each VAP enabled on the radio.
Transmit Power	If radio is operational, the current transmit power for the radio.
Fixed Power Indicator	This flag indicates if a fixed power setting is configured and assigned to the radio, a fixed transmit power can be configured in the valid AP database (locally or on a RADIUS server).
Manual Power Adjustment Status	Indicates the current state of a manual request to change the power setting on this radio. The valid values are: • None: No request has been made to change the power. • Requested: A power adjustment has been requested by the user but has not been processed by the switch. • In Progress: The switch is processing a power adjustment request for this radio. • Success: A power adjustment request is complete. • Failure: A power adjustment request failed.
Total Neighbors	Total number of neighbors (both APs and clients) that can be seen by this radio in its RF area.
TSPEC Status	
Access Category	Indicates whether the TSPEC data is for voice traffic or video traffic. The wireless system maintains separate counters for the voice and video categories.
Operational Status	Indicates the current operational mode for the category. The operational mode is influenced by both the individual ACM mode and overall TSPEC mode.
Number of Active Traffic Streams	Shows the number of active traffic streams on the AP. A traffic stream is a collection of data packets identified by the wireless client as belonging to a particular user priority. An example of a voice traffic stream is a Wi-Fi Certified telephone handset that marks its codec-generated data packets as voice priority traffic. An example of a video traffic stream is a video player application on a wireless laptop that prioritizes a video conference feed from a corporate server.
Number of Traffic Stream Clients	Shows the number of clients with an active traffic stream.

Table 156: Managed AP Radio Detail (Cont.)

Field	*Description*
Number of Traffic Stream Roaming Clients	Shows the number of clients in roaming mode with an active traffic stream. This value is also included in the Number of Traffic Stream Clients field.
Medium Time Admitted	Current sum of medium time (bandwidth) allocated to clients using a traffic stream. Medium time is measured in 32 µsec/sec units.
Medium Time Unallocated	Amount of medium time (bandwidth) not currently allocated. Medium time is measured in 32 µsec/sec units.
Medium Time Roaming Unallocated	Amount of medium time (bandwidth) not currently allocated for roaming clients. Medium time is measured in 32 µsec/sec units.

For radios that include IEEE 802.11a, IEEE 802.11a/n, or 5-GHz 802.11n support, the page displays an additional table with radar detection information.

Supported Channel	Radar Detection Required	Radar Detected	Time Since Radar Last Detected
36	No	No	0d:00:00:00
44	No	No	0d:00:00:00
52	No	No	0d:00:00:00
60	No	No	0d:00:00:00
100	No	No	0d:00:00:00
108	No	No	0d:00:00:00
116	No	No	0d:00:00:00
124	No	No	0d:00:00:00
132	No	No	0d:00:00:00
149	No	No	0d:00:00:00
157	No	No	0d:00:00:00

Table 157: Radio Detail Regulatory Domain

Field	*Description*
Supported Channel	Lists the radio channel used for transmitting and receiving wireless traffic.
Radar Detection Required	In some regulatory domains, radar detection is required on some channels in the 5-GHz band. If radar detection is required on the channel, the AP uses the 802.11h specification to avoid interference with other wireless devices.
Radar Detected	Indicates whether another 802.11 device was detected on the channel.
Time Since Radar Last Detected	Shows the amount of time that has passed since the device was last detected on the channel.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Managed Access Point Neighbor APs

During the RF scan, an access point collects and stores beacon information visible from neighboring access points. Access points can store the neighbor information for up to 64 neighbor APs. If the neighbor scan information exceeds the capacity, the oldest data in the neighbor list is overwritten.

Use the menu above the table to select the AP with the Neighbor AP information to view. The AP is identified by its MAC address and location. If the AP has two radios, select a radio to view the neighbor APs detected by using an RF scan on that radio. The radio is identified by its number and configured mode. If the radio is disabled, the radio mode will be displayed as Off.

To open this page, click the **WLAN** > **Status/Statistics** > **Managed AP > Status** > **Neighbor APs** tab.

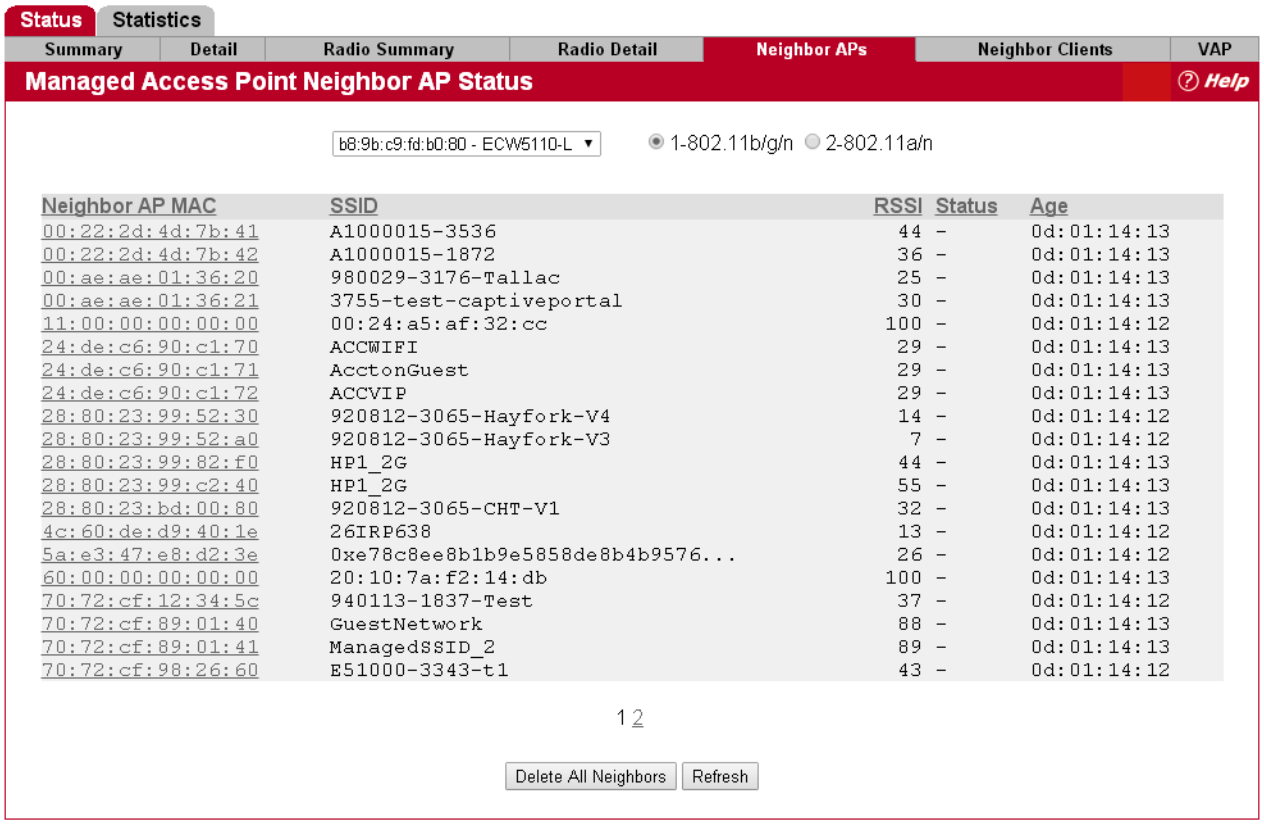


Figure 170: Managed Access Point Status Neighbor APs

Table 158 describes the fields you see on the **Neighbor APs** page for the managed access point status.

Table 158: Managed AP Neighbor Status

Field	*Description*
Neighbor AP MAC	The Ethernet MAC address of the neighbor AP network, this could be a physical radio interface or VAP MAC address. For Edge-Core APs this is always a VAP MAC address. The neighbor AP MAC address may be cross-referenced in the RF Scan status.
SSID	Service Set ID of the neighbor AP network.

Table 158: Managed AP Neighbor Status (Cont.)

Field	*Description*
RSSI	Received signal strength indication, this is an indicator of the signal strength relative to the neighbor and may give an idea of the neighbor's distance from the managed AP. The range is 1–100, where 1 is the weakest signal strength.
Status	Indicates the managed status of the AP, whether this is a valid AP known to the switch or a Rogue on the network. The valid values are: • Managed: The neighbor AP is managed by the wireless system. • Standalone: The AP is managed in standalone mode and configured as a valid AP entry (local or RADIUS). • Rogue: The AP is classified as a threat by one of the threat detection algorithms. • Unknown ("-"): The AP is detected in the network but is not classified as a threat by the threat detection algorithms.
Age	Indicates the time since this AP was last reported from an RF scan on the radio.

Command Buttons

The page includes the following buttons:

- **Delete All Neighbors**—Clears all entries from the Neighbor APs and Neighbor Clients list. This deletes all neighbors for all radios on all APs — not only for the currently selected AP and radio. The list is repopulated as neighbors are discovered.
- **Refresh**—Updates the page with the latest information.

Viewing Clients Associated with Neighbor Access Points

The **Neighbor Clients** page shows information about wireless clients that have been discovered by the selected AP. APs can store information for up to 512 wireless clients. If the information exceeds the capacity, the oldest data in the neighbor client list is overwritten.

Use the menu above the table to select the AP with the neighbor client information to view. The AP is identified by its MAC address and location. If the AP has two radios, select a radio to view the neighbor clients detected via an RF scan on that radio. The radio is identified by its number and configured mode. If the radio is disabled, the radio mode will be displayed as Off.

The **Delete All Neighbors** button clears the Neighbor AP and Neighbor Clients lists. The list is repopulated as neighbors and associated clients are discovered.

To open this page, click the **WLAN** > **Status/Statistics** > **Managed AP** > **Status** > **Neighbor Clients** tab.

Figure 171: Managed Access Point Neighbor Clients

Table 159 describes the fields you see on the **Neighbor Clients** page for the managed access point status.

Table 159: Neighbor AP Clients

Field	*Description*
Neighbor Client MAC	The Ethernet address of client station.
RSSI	Received signal strength indication, this is an indicator of the signal strength relative to the neighbor and may give an idea of the neighbor's distance from the managed AP. The range is 1–100, where 1 is the weakest signal strength.
Channel	The managed AP channel the client frame was received on, which may be different than the operating channel for this radio.

Table 159: Neighbor AP Clients (Cont.)

Field	*Description*
Discovery Reason	Indicates one or more discovery methods for the neighbor client. One or more of the following values may be displayed: • RF Scan Discovered: The client was reported from an RF scan on the radio. Note that client stations are difficult to detect via RF scan, the other methods are more common for client neighbor detection. • Probe Request: The managed AP received a probe request from the client. • Associated to Managed AP: This neighbor client is associated to another managed AP. • Associated to this AP: The client is associated to this managed AP on the displayed radio. • Associated to Peer AP: The client is associated to an AP managed by a peer switch. • Ad Hoc Rogue: The client was detected as part of an Ad Hoc network.
Age	Indicates the time since this client was last reported from an RF scan on the radio.

Command Buttons

The page includes the following buttons:

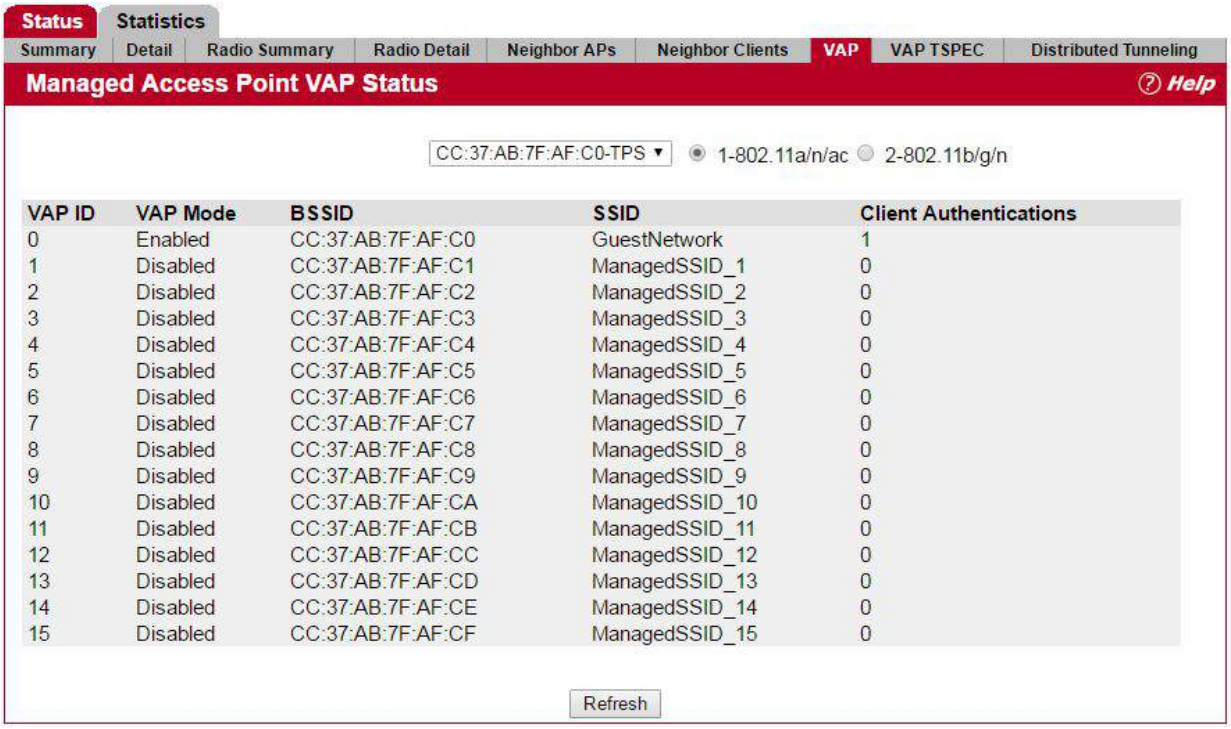
- **Delete All Neighbors**—Clears all entries from the Neighbor APs and Neighbor Clients list. The list is repopulated as neighbors are discovered.
- **Refresh**—Updates the page with the latest information.

Viewing Managed Access Point VAPs

There are 16 virtual access points (VAPs) available on each radio of an AP. For each radio of an access point managed by the switch, you can view a summary of the VAP configuration and the number of wireless clients associated with a particular VAP.

Use the menu above the table to select the AP with the VAP information to view. The AP is identified by its MAC address and location. If the AP has two radios, select a radio to view details about VAPs on that radio. The radio is identified by its number and configured mode. If the radio is disabled, the radio mode will be displayed as Off.

To open this page, click the **WLAN** > **Status/Statistics** > **Managed AP** > **Status** > **VAP** tab.



VAP ID	VAP Mode	BSSID	SSID	Client Authentications
0	Enabled	CC:37:AB:7F:AF:C0	GuestNetwork	1
1	Disabled	CC:37:AB:7F:AF:C1	ManagedSSID_1	0
2	Disabled	CC:37:AB:7F:AF:C2	ManagedSSID_2	0
3	Disabled	CC:37:AB:7F:AF:C3	ManagedSSID_3	0
4	Disabled	CC:37:AB:7F:AF:C4	ManagedSSID_4	0
5	Disabled	CC:37:AB:7F:AF:C5	ManagedSSID_5	0
6	Disabled	CC:37:AB:7F:AF:C6	ManagedSSID_6	0
7	Disabled	CC:37:AB:7F:AF:C7	ManagedSSID_7	0
8	Disabled	CC:37:AB:7F:AF:C8	ManagedSSID_8	0
9	Disabled	CC:37:AB:7F:AF:C9	ManagedSSID_9	0
10	Disabled	CC:37:AB:7F:AF:CA	ManagedSSID_10	0
11	Disabled	CC:37:AB:7F:AF:CB	ManagedSSID_11	0
12	Disabled	CC:37:AB:7F:AF:CC	ManagedSSID_12	0
13	Disabled	CC:37:AB:7F:AF:CD	ManagedSSID_13	0
14	Disabled	CC:37:AB:7F:AF:CE	ManagedSSID_14	0
15	Disabled	CC:37:AB:7F:AF:CF	ManagedSSID_15	0

Figure 172: Managed Access Point VAP

Table 160 describes the fields you see on the **VAPs** page for the managed access point status.

Table 160: Managed Access Point VAP Status

Field	*Description*
VAP ID	The integer ID used to identify the VAP (0-15), this is used to uniquely identify the VAP for configuration via CLI/SNMP.
VAP Mode	Indicates whether or not the VAP is enabled or disabled. VAPs are always configured, but are only sending beacons and accepting clients when they are Enabled.
BSSID	The Ethernet address of the VAP.
SSID	Indicates the network assigned to the VAP. The network for each VAP is configured within the AP profile and the SSID is based on the network configuration.
Client Authentications	Indicates the total number of clients currently authenticated with the VAP.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Managed Access Point VAP TSPEC Status

There are 16 virtual access points (VAPs) available on each radio of an AP. For each VAP on each radio of an AP managed by the switch, you can view information about the traffic that uses a traffic specification (TSPEC). A TSPEC is a set of parameters that define Quality of Service (QoS) characteristics of a traffic flow. A QoS-capable wireless client sends a TSPEC request to the AP to enable the AP to prioritize traffic streams and deliver appropriate resources to time- and delay-sensitive network traffic. TSPECs are commonly used with video and voice traffic.

To view TSPEC data for a AP, select the VAP TPSEC tab (after clicking the VAP tab), then select the AP, and the radio interface. The radio is identified by its number and configured mode. If the radio is disabled, the radio mode will be displayed as Off. The VAP is identified by the VAP ID.

To open this page, click the **WLAN** > **Status/Statistics** > **Managed AP** > **Status** > **VAP** tab. After the VAP TSPEC and Distributed Tunneling tabs are displayed, click the **VAP TSPEC** tab.

Figure 173: Managed Access Point Status VAP TSPEC

The following table describes the fields you see on the **VAP TSPEC** page.

Table 161: Managed Access Point VAP Status

Field	*Description*
MAC Address	MAC address of VAP.
Radio Interface	Select 802.11b/g/n or 802.11a/n.
VAP ID	The integer ID used to identify the VAP (0-15), this is used to uniquely identify the VAP for configuration via CLI/SNMP.
Access Category	Indicates whether the TSPEC data is for voice traffic or video traffic. The VAP maintains separate counters for the voice and video categories.

Table 161: Managed Access Point VAP Status (Cont.)

Field	*Description*
Operational Status	Indicates the current operational mode for the category. The operational mode is influenced by both the individual Admission Control Mandatory (ACM) mode and overall TSPEC mode.
Number of Active Traffic Streams	Shows the number of active traffic streams on the selected VAP. A traffic stream is a collection of data packets identified by the wireless client as belonging to a particular user priority. An example of a voice traffic stream is a Wi-Fi Certified telephone handset that marks its codec-generated data packets as voice priority traffic. An example of a video traffic stream is a video player application on a wireless laptop that prioritizes a video conference feed from a corporate server.
Number of Traffic Stream Clients	Shows the number of clients with an active traffic stream on the selected VAP.
Number of Traffic Stream Roaming Clients	Shows the number of clients in roaming mode with an active traffic stream on the selected VAP. This value is also included in the Number of Traffic Stream Clients field.
Medium Time Admitted	Current sum of medium time (bandwidth) allocated to clients using a traffic stream on the selected VAP. Medium time is measured in 32 µsec/sec units.
Medium Time Unallocated	Amount of medium time (bandwidth) not currently allocated for clients connected through this VAP. Medium time is measured in 32 µsec/sec units.
Medium Time Roaming Unallocated	Amount of medium time (bandwidth) not currently allocated for roaming clients. Medium time is measured in 32 µsec/sec units.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Distributed Tunneling Information

The distributed L2 tunneling mode is used to support L3 roaming for wireless clients without forwarding any data traffic to the wireless switch.

In the distributed L2 tunneling mode, when a client first associates with an AP in the wireless system, the AP forwards the wireless client's data using VLAN forwarding mode. The AP the client initially associates with is called the *Home AP*. The AP the client roams to is called the *Association AP*.

To open this page, click the **WLAN** > **Status/Statistics** > **Managed AP** > **Status** > **VAP** tab. After the VAP TSPEC and Distributed Tunneling tabs are displayed, click the **Distributed Tunneling** tab.

Use the menu below to select the AP with the distributed tunneling information to view. The AP is identified by its MAC address and VAP ID.

Figure 174: Managed Access Point Status Distributed Tunneling

Table 162 describes the fields you see on the **Distributed Tunneling Status** page for the managed access point status.

Table 162: Distributed Tunneling Status

Field	*Description*
MAC Address	MAC address of AP with distributed tunneling information.
Clients using AP as Home	Number of clients that roamed away from this AP using distributed tunneling mode and are tunneling data back to this AP.
Clients using AP as Associate	Number of clients that roamed to this AP using distributed tunneling mode and are tunneling data to the Home AP.
Distributed Tunnels	Number of APs to which this AP has a distributed L2 tunnel. The AP may be acting as Home AP or Association AP for clients using the tunnel.
Multicast Replications	Maximum number of tunnels on the Home AP that are members of the same VLAN.
VLAN with Max Multicast Replications	The VLAN ID that is currently replicated the most number of times by the AP for sending multicasts into distributed tunnels.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Managed Access Point Statistics

The managed AP statistics page shows information about traffic on the wired and wireless interfaces of the access point. This information can help diagnose network issues, such as throughput problems.

To open this page, click the **WLAN** > **Status/Statistics** > **Managed AP** > **Statistics** > **WLAN Summary** tab. The following figure shows the **Managed Access Point Statistics** page with two managed APs.

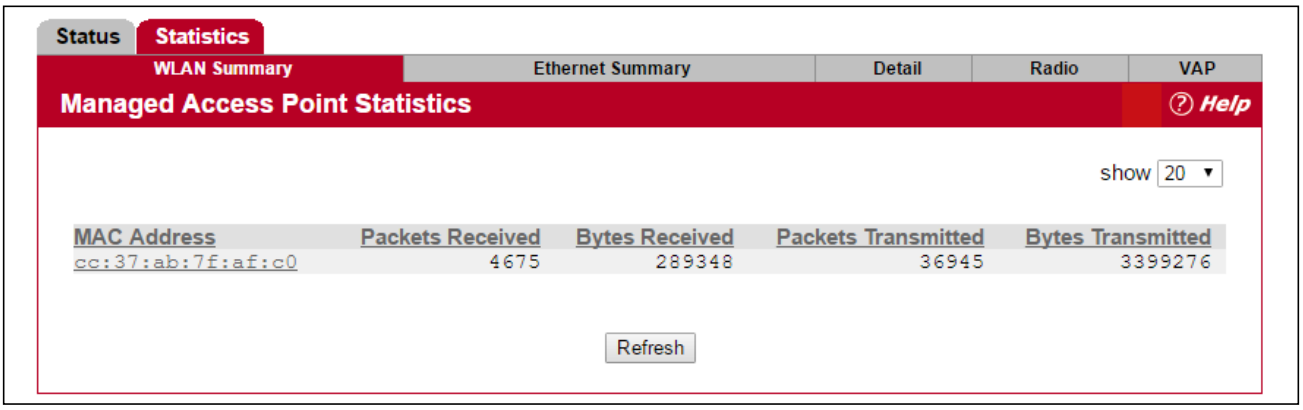


Figure 175: Managed AP Statistics

The following tabs are available from the **Managed AP Statistics** page:

- **WLAN Summary**: Shows summary information about the wireless interfaces on each AP the switch manages.
- **Ethernet Summary**: Shows summary information about the Ethernet (wired) interfaces on each AP the switch manages.
- **Detail**: Shows the number and type of packets transmitted and received on a specific AP.
- **Radio**: Shows per-radio information about the number and type of packets transmitted and received for a specific AP.
- **VAP**: Shows per-VAP information about the number of packets transmitted and received and the number of wireless client failures for a specific AP.

On the WLAN Summary and Ethernet Summary pages, click the MAC address of the AP to view detailed statistics about the AP.

Table 163: Managed Access Point WLAN Summary Statistics

Field	*Description*
MAC Address	The Ethernet address of the UWS-managed AP.
Packets Received	Total packets received by the AP on the wireless network.
Bytes Received	Total bytes received by the AP on the wireless network.
Packets Transmitted	Total packets transmitted by the AP on the wireless network.
Bytes Transmitted	Total bytes transmitted by the AP on the wireless network.

Note: You can sort the list of APs by clicking any of the column headings. For example, to sort the APs by the number of packets transmitted, click **Packets Transmitted**.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Managed Access Point Ethernet Statistics

The Ethernet summary statistics show information about the number of packets and bytes transmitted and received on the wired interface of each access point managed by the switch. The wired interface is physically connected to the LAN.

To open this page, click the **WLAN** > **Status/Statistics** > **Managed AP** > **Statistics** > **Ethernet Summary** tab.

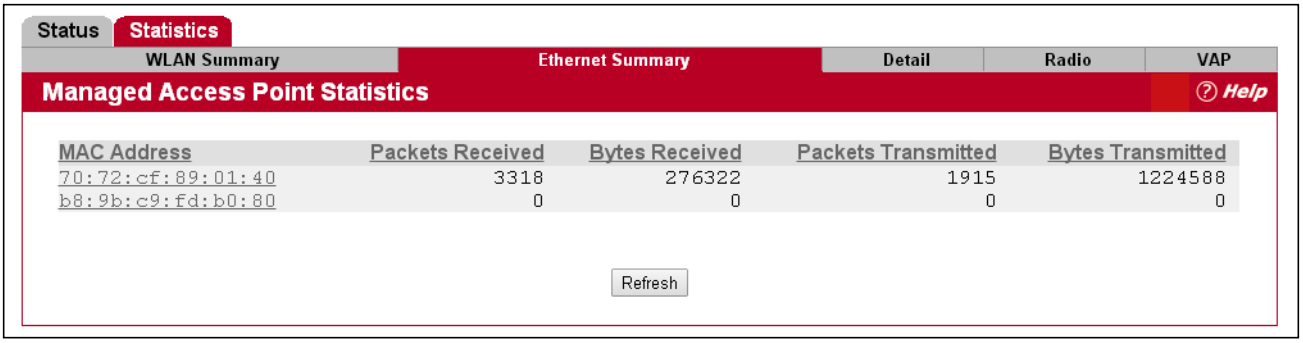


Figure 176: Managed AP Statistics Ethernet Summary

Table 164 describes the fields you see on the **Ethernet Summary** page for the managed access point statistics.

Table 164: Managed Access Point Ethernet Summary Statistics

Field	*Description*
MAC Address	The Ethernet address of the UWS-managed AP.
Packets Received	Total packets received by the AP on the wired network.
Bytes Received	Total bytes received by the AP on the wired network.
Packets Transmitted	Total packets transmitted by the AP on the wired network.
Bytes Transmitted	Total bytes transmitted by the AP on the wired network.

Command Buttons

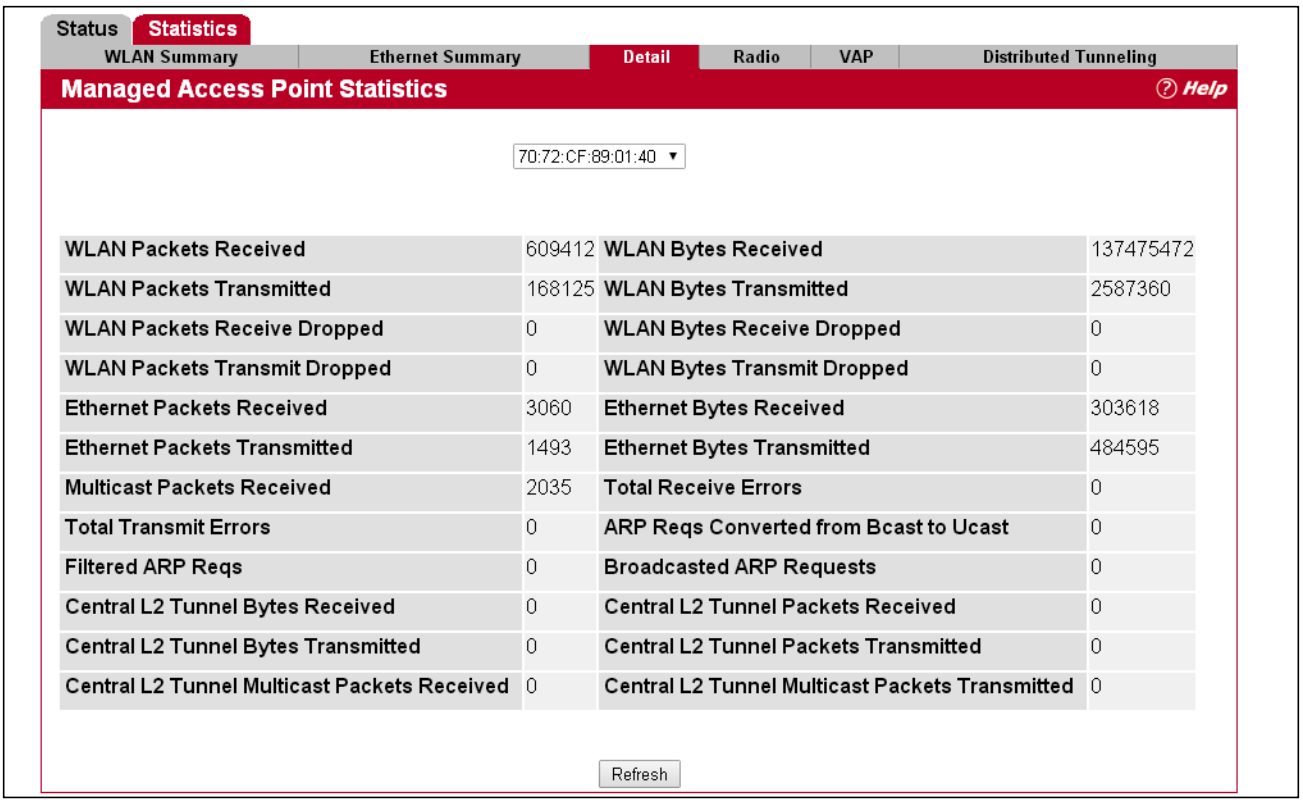
The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Detailed Managed Access Point Statistics

The detailed AP statistics show information about the packets and bytes transmitted and received on the wired and wireless interface of a particular access point managed by the switch. To view statistics for a specific AP that the switch manages, select its MAC address from the drop-down menu above the table. The location, if available, is also displayed with the MAC address.

To open this page, click the **WLAN** > **Status/Statistics** > **Managed AP** > **Statistics** > **Detail** tab.



WLAN Packets Received	609412	WLAN Bytes Received	137475472
WLAN Packets Transmitted	168125	WLAN Bytes Transmitted	2587360
WLAN Packets Receive Dropped	0	WLAN Bytes Receive Dropped	0
WLAN Packets Transmit Dropped	0	WLAN Bytes Transmit Dropped	0
Ethernet Packets Received	3060	Ethernet Bytes Received	303618
Ethernet Packets Transmitted	1493	Ethernet Bytes Transmitted	484595
Multicast Packets Received	2035	Total Receive Errors	0
Total Transmit Errors	0	ARP Reqs Converted from Bcast to Ucast	0
Filtered ARP Reqs	0	Broadcasted ARP Requests	0
Central L2 Tunnel Bytes Received	0	Central L2 Tunnel Packets Received	0
Central L2 Tunnel Bytes Transmitted	0	Central L2 Tunnel Packets Transmitted	0
Central L2 Tunnel Multicast Packets Received	0	Central L2 Tunnel Multicast Packets Transmitted	0

Figure 177: Managed AP Statistics Detail

Table 165 describes the fields you see on the **Detail** page for the managed access point statistics.

Table 165: Detailed Managed Access Point Statistics

Field	*Description*
WLAN Packets Received	Total packets received by the AP on the wireless network.
WLAN Bytes Received	Total bytes received by the AP on the wireless network.
WLAN Packets Transmitted	Total packets transmitted by the AP on the wireless network.
WLAN Bytes Transmitted	Total bytes transmitted by the AP on the wireless network.
WLAN Packets Receive Dropped	Number of packets received by the AP on the wireless network that were dropped.
WLAN Bytes Receive Dropped	Number of bytes received by the AP on the wireless network that were dropped.
WLAN Packets Transmit Dropped	Number of packets transmitted by the AP on the wireless network that were dropped.

Table 165: Detailed Managed Access Point Statistics (Cont.)

Field	*Description*
WLAN Bytes Transmit Dropped	Number of bytes transmitted by the AP on the wireless network that were dropped.
Ethernet Packets Received	Total packets received by the AP on the wired network.
Ethernet Bytes Received	Total bytes received by the AP on the wired network.
Ethernet Packets Transmitted	Total packets transmitted by the AP on the wired network.
Ethernet Bytes Transmitted	Total bytes transmitted by the AP on the wired network.
Multicast Packets Received	Total multicast packets received by the AP on the wired network.
Total Receive Errors	Total receive errors detected by the AP on the wired network.
Total Transmit Errors	Total transmit errors detected by the AP on the wired network.
ARP Reqs Converted from Bcast to Ucast	Number of ARP requests that the AP converted from a broadcast packet to a unicast packet before sending to the wireless link.
Filtered ARP Requests	Number of ARP requests that AP was able to drop instead of sending on the wireless link.
Broadcasted ARP Requests	The number of ARP requests sent as broadcasts on the VAPs. This counter does not include WDS links. The same ARP frame may be counted multiple times when it is broadcast on multiple VAPs. The counter is available even when ARP suppression is disabled.
Central L2 Tunnel Bytes Received	Total bytes received by the AP L2 tunnels on the wired network.
Central L2 Tunnel Packets Received	Total packets received by the AP L2 tunnels on the wired network.
Central L2 Tunnel Bytes Transmitted	Total bytes transmitted by the AP L2 tunnels on the wired network.
Central L2 Tunnel Packets Transmitted	Total packets transmitted by the AP L2 tunnels on the wired network.
Central L2 Tunnel Multicast Packets Received	Total multicast packets received by the AP L2 tunnels on the wired network.
Central L2 Tunnel Multicast Packets Transmitted	Total multicast packets transmitted by the AP L2 tunnels on the wired network.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Managed Access Point Radio Statistics

The radio statistics show detailed information about the packets and bytes transmitted and received on the radio (wireless) interface of a particular access point managed by the switch.

Use the options above the table to select the AP and radio with the settings to view. The AP is identified by its MAC address and location. The radio is identified by its number and configured mode. If the radio is disabled, the radio mode will be displayed as Off.

To open this page, click the **WLAN** > **Status/Statistics** > **Managed AP** > **Statistics** > **Radio** tab.

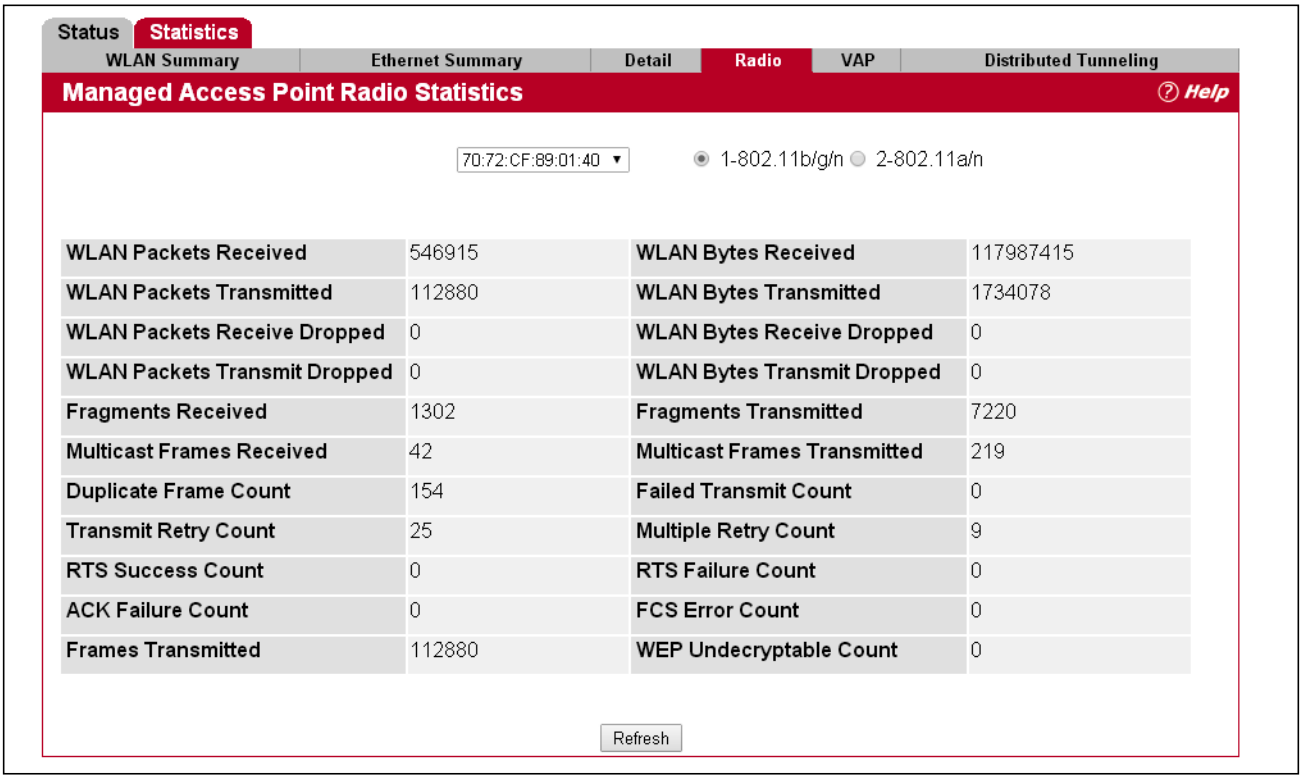


Figure 178: Managed AP Statistics Radio

Table 166 describes the fields you see on the **Radio** page for the managed access point statistics.

Table 166: Managed Access Point Radio Statistics

Field	*Description*
WLAN Packets Received	Total packets received by the AP on this radio interface.
WLAN Bytes Received	Total bytes received by the AP on this radio interface.
WLAN Packets Transmitted	Total packets transmitted by the AP on this radio interface.
WLAN Bytes Transmitted	Total bytes transmitted by the AP on this radio interface.
WLAN Packets Receive Dropped	Number of packets received by the AP on this radio interface that were dropped.
WLAN Bytes Receive Dropped	Number of bytes received by the AP on this radio interface that were dropped.

Table 166: Managed Access Point Radio Statistics (Cont.)

Field	*Description*
WLAN Packets Transmit Dropped	Number of packets transmitted by the AP on this radio interface that were dropped.
WLAN Bytes Transmit Dropped	Number of bytes transmitted by the AP on this radio interface that were dropped.
Fragments Received	Count of successfully received MPDU frames of type data or management.
Fragments Transmitted	Number of transmitted MPDU with an individual address or an MPDU with a multicast address of type Data or Management.
Multicast Frames Received	Count of MSDU frames received with the multicast bit set in the destination MAC address.
Multicast Frames Transmitted	Count of successfully transmitted MSDU frames where the multicast bit is set in the destination MAC address.
Duplicate Frame Count	Number of times a frame is received and the Sequence Control field indicates is a duplicate.
Failed Transmit Count	Number of times a MSDU is not transmitted successfully due to transmit attempts exceeding either the short retry limit or the long retry limit.
Transmit Retry Count	Number of times a MSDU is successfully transmitted after one or more retries.
Multiple Retry Count	Number of times a MSDU is successfully transmitted after more than one retry.
RTS Success Count	Count of CTS frames received in response to an RTS frame.
RTS Failure Count	Count of CTS frames not received in response to an RTS frame.
ACK Failure Count	Count of ACK frames not received when expected.
FCS Error Count	Count of FCS errors detected in a received MPDU frame.
Frames Transmitted	Count of each successfully transmitted MSDU.
WEP Undecryptable Count	Count of encrypted frames received and the key configuration of the transmitter indicates that the frame should not have been encrypted or that frame was discarded due to the receiving station not implementing the privacy option.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Managed Access Point VAP Statistics

The VAP statistics show information about the client failures and number of packets and bytes transmitted and received on each VAP on radio one or two for a particular access point managed by the switch.

Use the options above the table to select the AP, radio, and VAP with the settings to view. The AP is identified by its MAC address and location. The radio is identified by its number and configured mode. If the radio is disabled, the radio mode will be displayed as Off. The VAP is identified by the VAP ID and its SSID. All VAPs are available regardless of whether they are enabled.

To open this page, click the **WLAN** > **Status/Statistics** > **Managed AP** > **Statistics** > **VAP** tab.

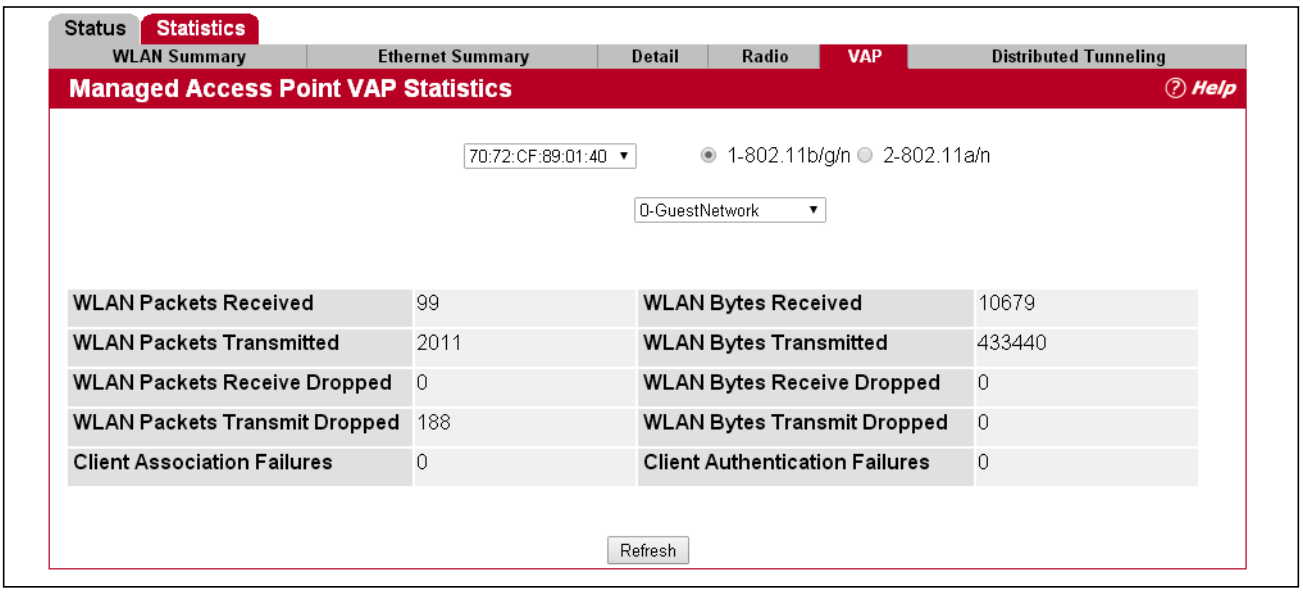


Figure 179: Managed AP Statistics VAP

Table 167 describes the fields you see on the **VAP** page for the managed access point statistics.

Table 167: Managed Access Point VAP Statistics

Field	*Description*
MAC Address	Select the MAC address of the VAP.
Radio Interface	Select 802.11b/g/n or 802.11a/n.
SSID	Select the SSID of the VAP.
WLAN Packets Received	Total packets received by the AP on this VAP.
WLAN Bytes Received	Total bytes received by the AP on this VAP.
WLAN Packets Transmitted	Total packets transmitted by the AP on this VAP.
WLAN Bytes Transmitted	Total bytes transmitted by the AP on this VAP.
WLAN Packets Receive Dropped	Number of packets received by the AP on this VAP that were dropped.
WLAN Bytes Receive Dropped	Number of bytes received by the AP on this VAP that were dropped.
WLAN Packets Transmit Dropped	Number of packets transmitted by the AP on this VAP that were dropped.
WLAN Bytes Transmit Dropped	Number of bytes transmitted by the AP on this VAP that were dropped.
Client Association Failures	Number of clients that have been denied association to the VAP.

Table 167: Managed Access Point VAP Statistics (Cont.)

Field	*Description*
Client Authentication Failures	Number of clients that have failed authentication to the VAP.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Distributed Tunneling Statistics

The distributed tunneling statistics show information about the number of packets and bytes transmitted and received by clients that use L2 distributed tunnels on an access point managed by the switch.

To open this page, click the **WLAN** > **Status/Statistics** > **Managed AP** > **Statistics** > **Distributed Tunneling** tab. Use the drop-down lists to select the AP with the settings to view. The AP is identified by its MAC address and SSID.

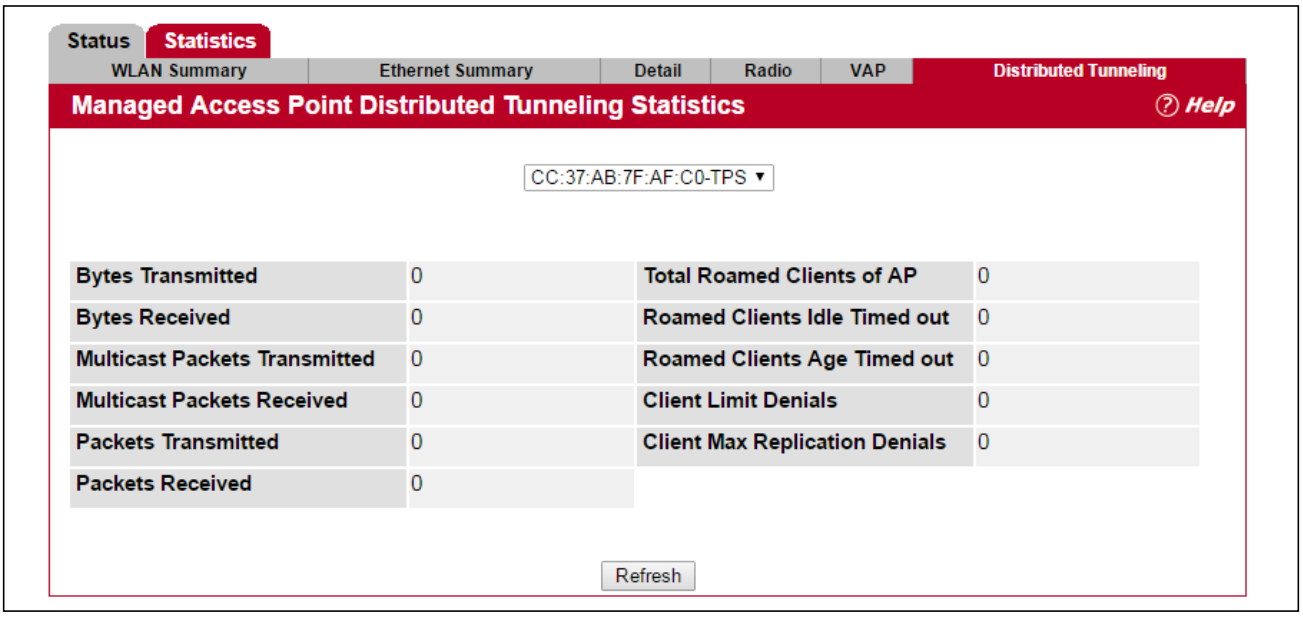


Figure 180: Managed AP Statistics Distributed Tunneling

Table 168 describes the fields you see on the Distributed Tunneling Statistics page for the managed access point.

Table 168: Managed Access Point Distributed Tunneling Statistics

Field	*Description*
MAC Address	MAC address of managed AP.
Bytes Transmitted	Total bytes transmitted via all distributed tunnels by the AP.
Bytes Received	Total bytes received via all distributed tunnels by the AP.
Multicast Packets Transmitted	Total multicast packets transmitted via all distributed tunnels by the AP.
Multicast Packets Received	Total multicast packets received via all distributed tunnels by the AP.

Table 168: Managed Access Point Distributed Tunneling Statistics (Cont.)

Field	*Description*
Packets Transmitted	Total packets transmitted via all distributed tunnels by the AP.
Packets Received	Total packets received via all distributed tunnels by the AP.
Total Roamed Clients of AP	Number of Clients that used this AP for distributed tunneling. The count include clients that roamed away and roamed to this AP.
Roamed Clients Idle Timed Out	Number of Clients that roamed away from this AP and were timed out due to not sending traffic on the tunnel.
Roamed Clients Age Timed Out	Number of Clients that roamed away from this AP and were timed out due to age of the tunnel.
Client Limit Denials	Number of times the AP denied the clients attempt to set up a distributed tunnel due to the AP reaching the configured tunneled client limit.
Client Max Replication Denials	Number of times the AP denied the clients attempt to set up a distributed tunnel due to the AP reaching the configured maximum number of VLAN replications.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Associated Client Status/Statistics

You can view a variety of information about the wireless clients that are associated with the APs the switch manages. To access the associated client information, click the **WLAN** > **Status/Statistics** > **Associated Client** > **Status** tab.

Use the lists to select the AP with the settings to view. The AP is identified by its MAC address and SSID.

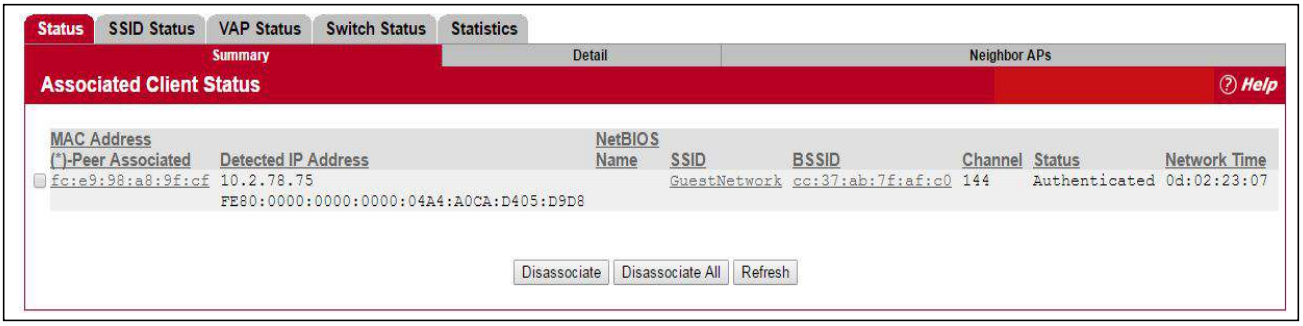


Figure 181: Associated Client Status Tabs

The following tabs are available on the **Associated Client** page:

Table 169: Associated Client Status Fields

Field	*Description*
Status	Shows status information about wireless clients that are associated with APs managed by the switch and contains the following information: • Summary: Shows basic information about associated clients. • Detail: Shows more detailed information about associated clients, such as which VLAN the client is assigned to and how long the client has been inactive. • Neighbor APs: Shows the managed APs that are within range of the wireless clients, which can help you determine the managed AP an associated client might use for roaming. • Distributed Tunneling: Shows information about the Distributed Tunnel status of the client. • TSPEC: Shows information about a client's active traffic streams. • RRM: Contains information about whether a client supports specific resource radio measurement features defined in the 802.11k specification.
SSID Status	Shows the SSID and client MAC address of all clients connected to specific networks.
VAP Status	Shows the clients associated with a specific VAP on a AP
Switch Status	Shows the switch IP address and client MAC address for each associated client.
Statistics	Shows statistics about wireless clients that are associated with APs managed by the switch and contains the following information: • Association Summary: Shows the statistics for a wireless client while it is associated with a single AP. • Session Summary: If a wireless client roams among different managed APs, the switch can track the statistics for the entire session. • Association Detail: Shows additional information about packets the associated client transmits and receives during association with a single managed AP. • Session Detail: Shows additional information about packets the associated client transmits and receives during a session, which can include statistics for one or more managed AP associations if the client has roamed.

Since the associated client database supports roaming across APs, an entry is not removed when a client disassociates from a specific AP. After a client has disassociated, the entry is deleted after the client times out. You configure the timeout value in the Client Roam Timeout field on the **WLAN > Advanced Configuration > Global** page. The timeout value corresponds to the time allowed for a client to roam to another managed AP.

Viewing Associated Client Summary Status

To open this page, click the **WLAN** > **Status/Statistics** > **Associated Client** > **Status** > **Summary** tab.

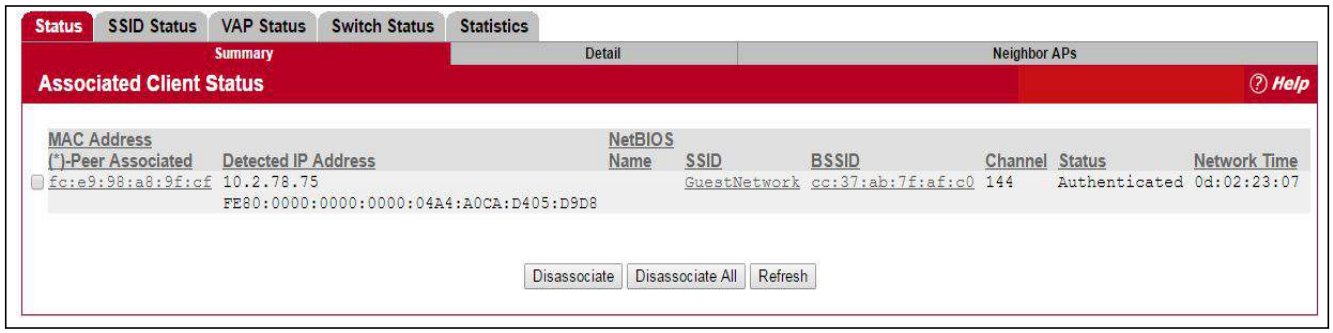


Figure 182: Associated Client Status Summary

Table 170 describes the information available on the **Summary** page for the associated client status.

Table 170: Associated Client Status Summary

Field	*Description*
MAC Address	The Ethernet address of the client station. If the MAC address is followed by an asterisk (*), the client is associated with an AP managed by a peer switch.
Detected IP Address	Identifies the IP address of the associated client, if available.
NetBIOS Name	Identifies the NetBIOS name of the wireless client. For Microsoft Windows hosts, the NetBIOS name is typically the same as, or based on the host name of the client.
SSID	Indicates the network on which the client is connected.
BSSID	Indicates the Ethernet MAC address for the managed AP VAP where this client is associated.
Channel	Indicates the operating channel for the client association.
Status	Indicates whether or not the client has associated and/or authenticated. The valid values are: • Associated: The client is currently associated to the managed AP. • Authenticated: The client is currently associated and authenticated to the managed AP. • Disassociated: The client has disassociated from the managed AP. If the client does not roam to another managed AP within the client roam timeout, it will be deleted.
Network Time	Indicates the amount of time that has passed since this client first authenticated with the network.

Command Buttons

The page includes the following buttons:

- **Disassociate**—Disassociates the selected client from the managed AP.
- **Disassociate All**—Disassociates all clients from the managed AP.
- **Refresh**—Updates the page with the latest information.

Viewing Detailed Associated Client Status

For each client associated with an AP that the switch manages, you can view detailed status information about the client and its association with the access point. Use the menu above the table to select the MAC address of the client with the information to view.

To open this page, click the **WLAN** > **Status/Statistics** > **Associated Client** > **Status** > **Detail** tab.

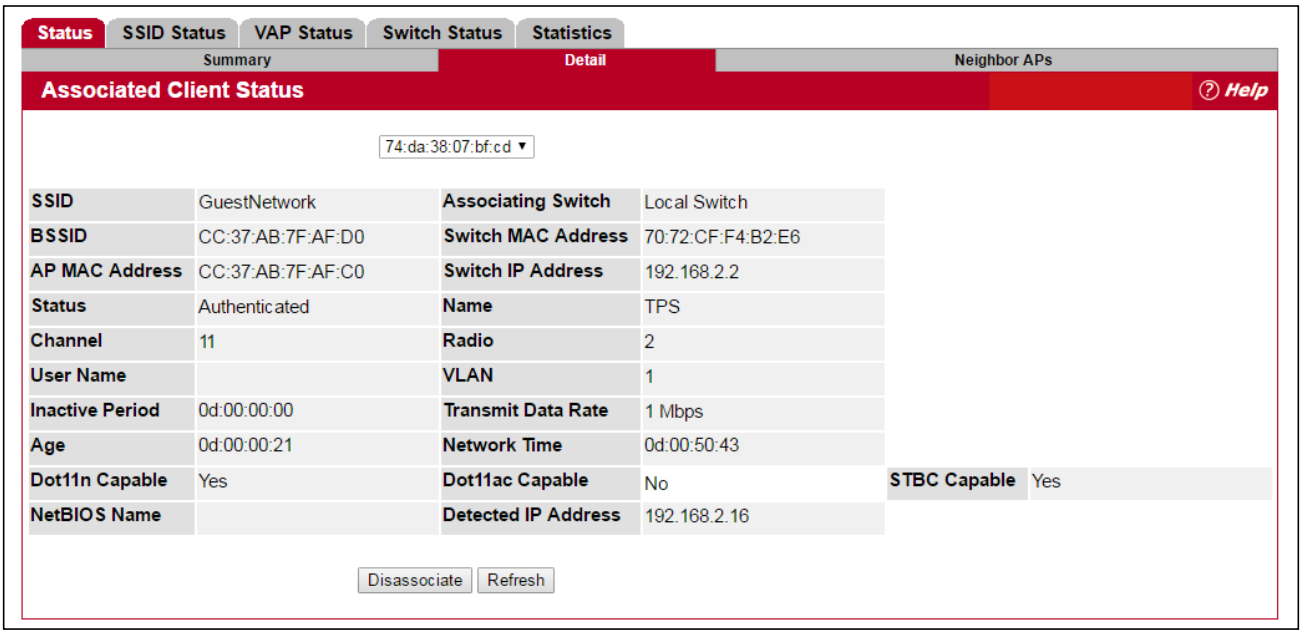


Figure 183: Associated Client Status Details

Table 171 describes the information available on the **Detail** page for the associated client status.

Table 171: Detailed Associated Client Status

Field	*Description*
SSID	Indicates the network on which the client is connected.
BSSID	Indicates the Ethernet MAC address for the managed AP VAP where this client is associated.
AP MAC Address	This field indicates the base AP Ethernet MAC address for the managed AP.
Status	Indicates whether or not the client has associated and/or authenticated. The valid values are: • Associated: The client is current associated to the managed AP. • Authenticated: The client is currently associated and authenticated to the managed AP. • Disassociated: The client has disassociated from the managed AP, if the client does not roam to another managed AP within the client roam timeout, it will be deleted.
Channel	Indicates the operating channel for the client association.
User Name	Indicates the user name of client that have authenticated via 802.1x. Clients on networks with other security modes will not have a user name.

Table 171: Detailed Associated Client Status (Cont.)

Field	*Description*
Inactive Period	This field shows the amount of time since data packets were last received from the client
Age	Indicates the amount of time that has passed since the switch received new status or statistics updates for this client.
Dot11n Capable	Indicates whether the associated client supports the IEEE 802.11n standard.
NetBIOS Name	Identifies the NetBIOS name of the wireless client. For Microsoft Windows hosts, the NetBIOS name is typically the same as, or based on the host name.
Associating Switch	Shows whether the AP that the wireless client is associated to is managed by the local switch or a peer switch.
Switch MAC Address	Shows the MAC address of the switch that manages the AP to which the wireless client is associated.
Switch IP Address	Shows the IP address of the switch that manages the AP to which the wireless client is associated.
Name	The name configured for the managed AP.
Radio	Displays the managed AP radio interface the client is associated to and its configured mode.
VLAN	If client is on a VAP using VLAN data forwarding mode, indicates the current assigned VLAN.
Transmit Data Rate	Indicates the rate at which the client station is currently transmitting data.
Network Time	Indicates the amount of time that has passed since this client first authenticated with the network.
Dot11ac Capable	Indicates whether the associated client supports the IEEE 802.11ac standard.
STBC Capable	Indicates whether the client supports Space Time Block Code, which enables the AP to send the same data stream on multiple antennas at the same time. This is different from MIMO where the data stream is divided between two antennas.
Detected IP Address	Identifies the IPv4 address of the client, if available.

Command Buttons

The page includes the following buttons:

- **Disassociate**—Disassociates the client from the managed AP.
- **Refresh**—Updates the page with the latest information.

Viewing Associated Client Neighbor AP Status

The **Neighbor AP** page for the associated client status shows information about access points that the client detects. The information on this page can help you determine the managed AP an associated client might use for roaming. Use the menu above the table to select the MAC address of the client with the information to view.

To open this page, click the **WLAN** > **Status/Statistics** > **Associated Client** > **Status** > **Neighbor APs** tab.

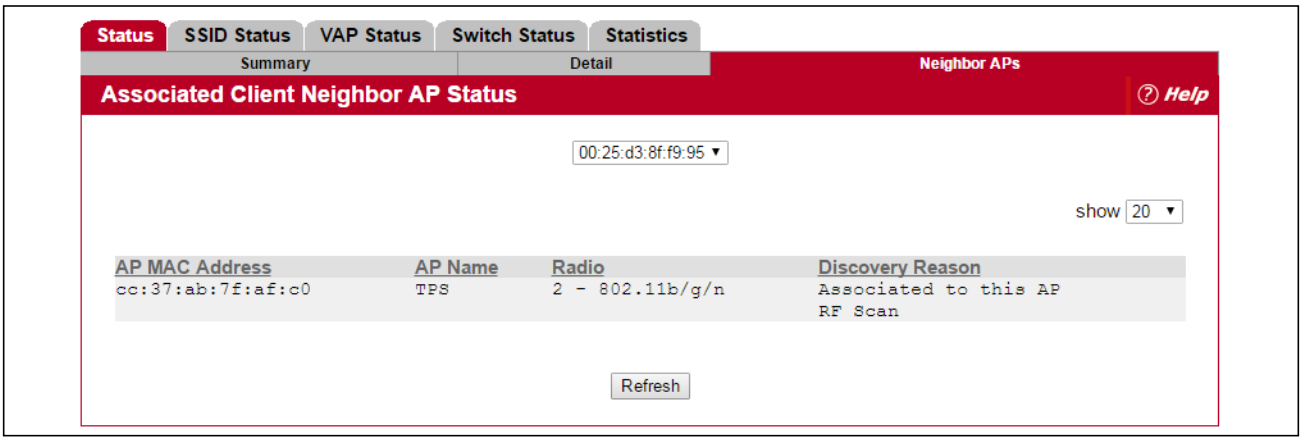


Figure 184: Associated Client Neighbor APs

Table 172 describes the information available on the **Neighbor AP** page for the associated client status.

Table 172: Associated Client Neighbor AP Status

Field	*Description*
AP MAC Address	The base Ethernet address of the UWS managed AP.
AP Name	The configured descriptive location for the managed AP
Radio	The radio interface and its configured mode that detected this client as a neighbor.
Discovery Reason	Indicates one or more discovery methods for the neighbor client. One or more of the following values may be displayed: • RF Scan: The client was reported from an RF scan on the radio. Note that client stations are difficult to detect via RF scan, the other methods are more common for client neighbor detection. • Probe Request: The managed AP received a probe request from the client. • Associated to Managed AP: This neighbor client is associated to another managed AP. • Associated to this AP: The client is associated to this managed AP on the displayed radio. • Associated to Peer AP: The client is associated to an AP managed by a peer switch. • Ad Hoc Rogue: The client was detected as part of an ad hoc network with this AP.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Associated Client SSID Status

Each managed AP can have up to 16 different networks that each have a unique SSID. Although several wireless clients might be connected to the same physical AP, they might not connect by using the same SSID. The **SSID Status** page lists the SSIDs of the networks that each wireless client associated with a managed AP has used for WLAN access.

To open this page, click the **WLAN** > **Status/Statistics** > **Associated Client** > **SSID Status** tab. To disconnect a client from an AP, select the box next to the SSID, and then click **Disassociate**.

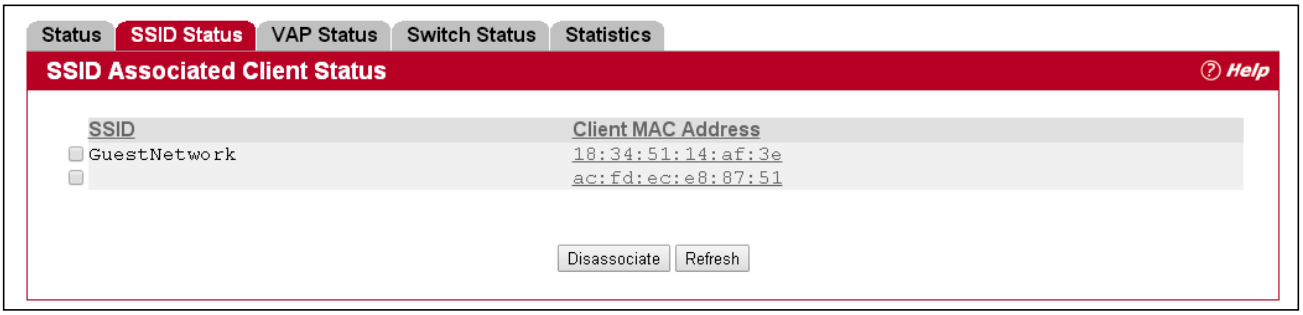


Figure 185: Associated Client SSID Status

Table 173 describes the information available on the **SSID Status** page for the associated client status.

Table 173: Associated Client SSID Status

Field	*Description*
SSID	Indicates the network on which the client is connected.
Client MAC Address	The Ethernet address of the client station.

Command Buttons

The page includes the following buttons:

- **Disassociate**—Disassociates the client from the managed AP.
- **Refresh**—Updates the page with the latest information.

Viewing Associated Client VAP Status

Each AP has 16 Virtual Access Points (VAPs) per radio, and every VAP has a unique MAC address (BSSID). The VAP Associated Client Status page shows information about the VAPs on the managed AP that have associated wireless clients.

To open this page, click the **WLAN** > **Status/Statistics** > **Associated Client** > **VAP Status** tab. To disconnect a client from an AP, select the box next to the BSSID, and then click **Disassociate**.

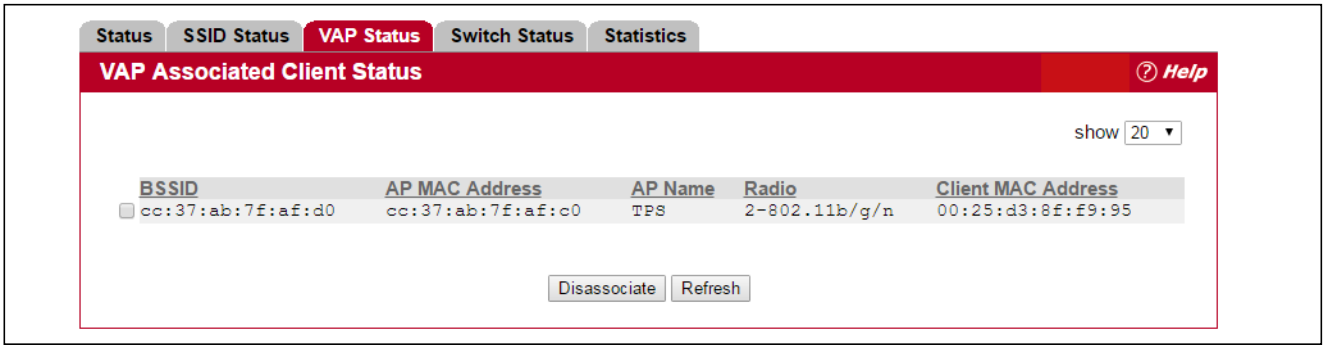


Figure 186: Associated Client VAP Status

Table 174 describes the information available on the **VAP Status** page for the associated client status.

Table 174: Associated Client VAP Status

Field	*Description*
BSSID	Indicates the Ethernet MAC address for the managed AP VAP where this client is associated.
AP MAC Address	This field indicates the base AP Ethernet MAC address for the managed AP.
AP Name	The descriptive location configured for the managed AP.
Radio	Displays the managed AP radio interface the client is associated to and its configured mode.
Client MAC Address	The Ethernet address of the client station.

Command Buttons

The page includes the following buttons:

- **Disassociate**—Disassociates the client from the managed AP.
- **Refresh**—Updates the page with the latest information.

Switch Associated Client Status

The **Switch Associated Client Status** page shows information about the switch that manages the AP to which the client is associated.

To open this page, click the **WLAN** > **Status/Statistics** > **Associated Client** > **Switch Status** tab. To disconnect a client from an AP, select the box next to the switch IP address, and then click **Disassociate**.

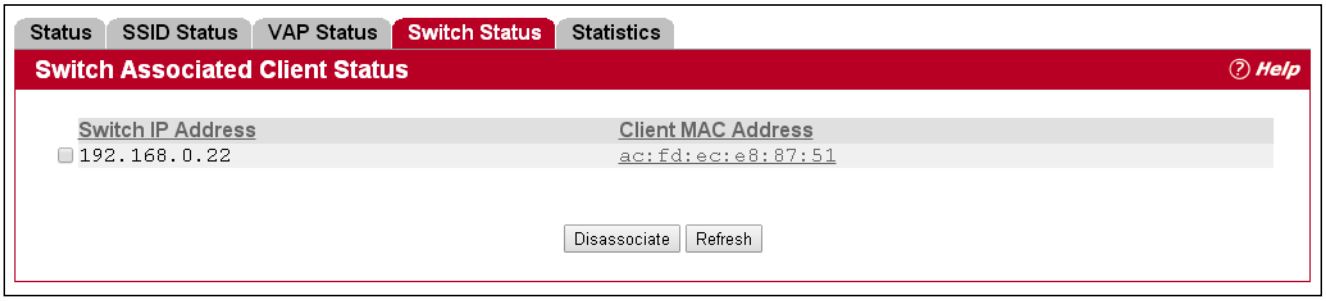


Figure 187: Associated Client Switch Status

Table 175 describes the information available on the **Switch Status** page for the associated client status.

Table 175: Associated Client Switch Status

Field	*Description*
Switch IP Address	Shows the IP address of the switch that manages the AP to which the client is associated.
Client MAC Address	Shows the MAC address of the switch that manages the AP to which the client is associated.

Command Buttons

The page includes the following buttons:

- **Disassociate**—Disassociates the client from the managed AP.
- **Refresh**—Updates the page with the latest information.

Viewing Associated Client Statistics

A wireless client can roam among APs without interruption in WLAN service. The UWS tracks the traffic the client sends and receives during the entire wireless session while the client roams among APs that the switch manages. The switch stores statistics about client traffic while it is associated with a single AP as well as throughout the roaming session.

To open this page, click the **WLAN** > **Status/Statistics** > **Associated Client** > **Statistics** > **Association Summary** tab. The statistics on the **Association Summary** page show information about the traffic a wireless client receives and transmits while it is associated with a single AP.

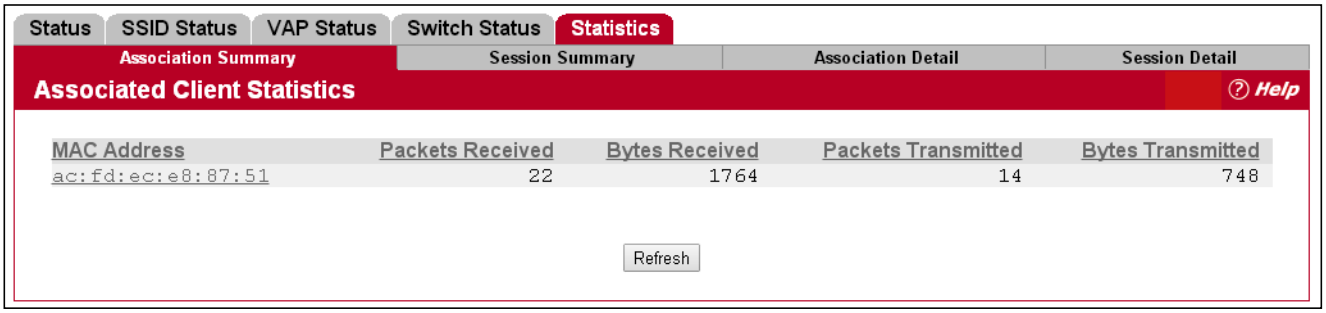


Figure 188: Associated Client Statistics Association Summary

Table 176 describes the information available on the **Association Summary** page for associated client statistics.

Table 176: Associated Client Association Summary Statistics

Field	*Description*
MAC Address	The Ethernet address of the client station.
Packets Received	Packets received from the client station.
Bytes Received	Bytes received from the client station.
Packets Transmitted	Packets transmitted to the client station.
Bytes Transmitted	Bytes transmitted to the client station.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Associated Client Session Summary Statistics

The statistics on the **Session Summary** page show information about the traffic a wireless client receives and transmits while it is connected to the same WLAN network shared by APs that the switch manages.

If the client roams from one AP to another AP but remains connected to the same network, the session continues and the session statistics continue to accumulate. If the client closes the wireless connection or roams out of the range of an AP managed by the switch, the session ends.

To open this page, click the **WLAN** > **Status/Statistics** > **Associated Client** > **Statistics** > **Session Summary** tab.

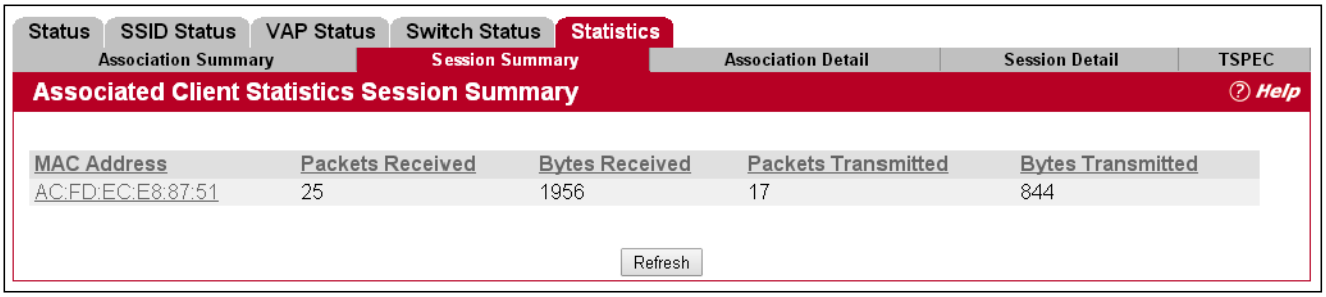


Figure 189: Associated Client Statistics Session Summary

Table 177 describes the information available on the **Session Summary** page for associated client statistics.

Table 177: Associated Client Session Summary Statistics

Field	*Description*
MAC Address	The Ethernet address of the client station.
Packets Received	Packets received from the client station.
Bytes Received	Total bytes received from the client station.
Packets Transmitted	Total packets transmitted to the client station.
Bytes Transmitted	Total bytes transmitted to the client station.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Detailed Associated Client Association Statistics

The statistics on the **Association Detail** page show information about the traffic a wireless client receives and transmits while it is associated with a single AP. Use the menu above the table to view details about an associated client. Each client is identified by its MAC address.

To open this page, click the **WLAN** > **Status/Statistics** > **Associated Client** > **Statistics** > **Association Detail** tab.

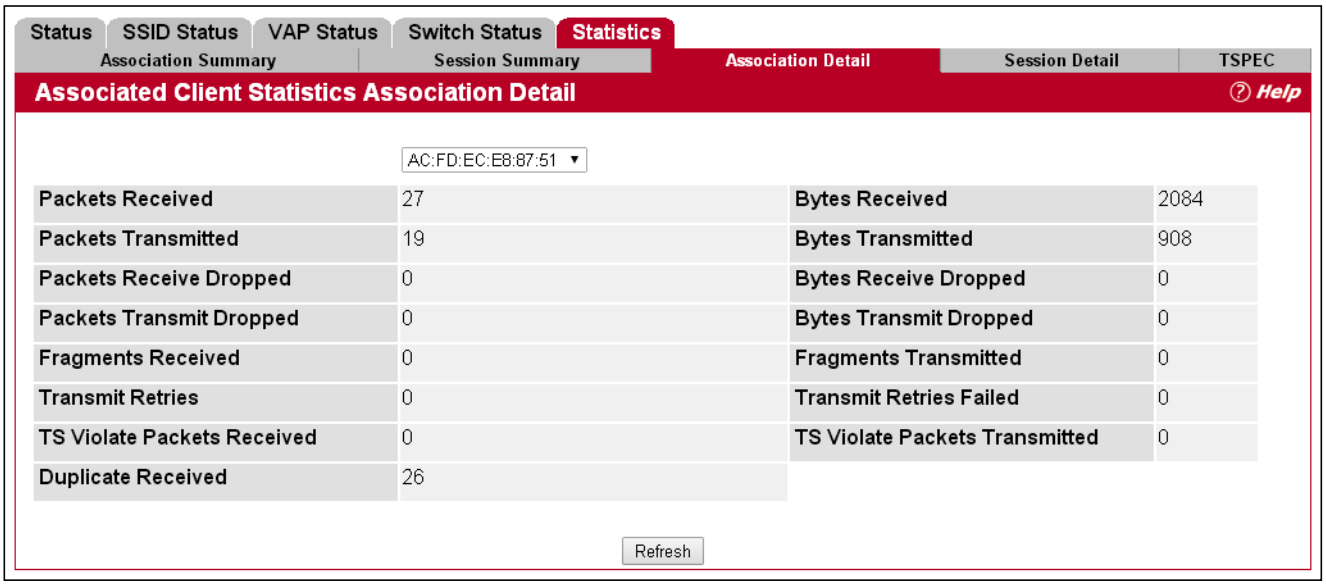


Figure 190: Associated Client Statistics Association Detail

Table 178 describes the information available on the **Association Detail** page for associated client statistics.

Table 178: Associated Client Association Detail Statistics

Field	*Description*
Packets Received	Total packets received from the client station.
Bytes Received	Total bytes received from the client station.
Packets Transmitted	Total packets transmitted to the client station.
Bytes Transmitted	Total bytes transmitted to the client station.
Packets Receive Dropped	Number of packets received from the client station that were dropped.
Bytes Receive Dropped	Number of bytes received from the client station that were dropped.
Packets Transmit Dropped	Number of packets transmitted to the client station that were dropped.
Bytes Transmit Dropped	Number of bytes transmitted to the client station that were dropped.
Fragments Received	Total fragmented packets received from the client station.
Fragments Transmitted	Total fragmented packets transmitted to the client station.
Transmit Retries	Number of times transmits to client station succeeded after one or more retries.
Transmit Retries Failed	Number of times transmits to client station failed after one or more retries.
Duplicates Received	Total duplicate packets received from the client station.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Detailed Associated Client Session Statistics

The statistics on the **Session Detail** page show information about the traffic a wireless client receives and transmits while it is connected to the same WLAN network shared by APs that the switch manages. Use the menu above the table to view details about an associated client. Each client is identified by its MAC address.

To open this page, click the **WLAN** > **Status/Statistics** > **Associated Client** > **Statistics** > **Session Detail** tab.

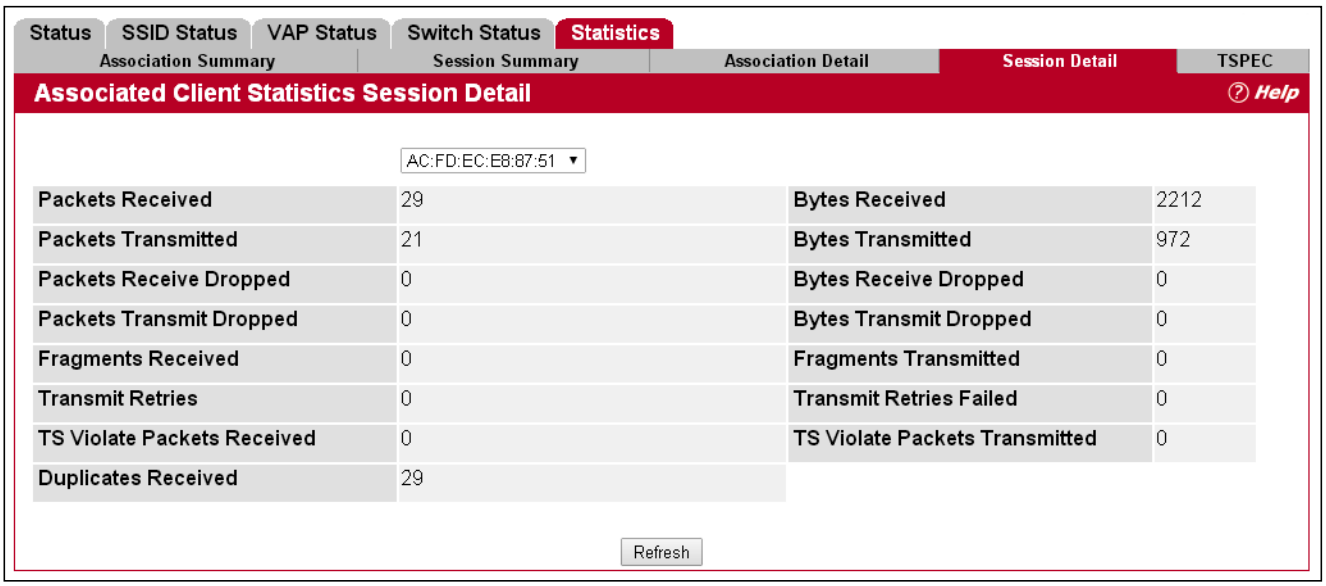


Figure 191: Associated Client Statistics Session Detail

Table 179 describes the information available on the **Session Detail** page for associated client statistics.

Table 179: Associated Client Session Detail Statistics

Field	*Description*
Packets Received	Total packets received from the client station.
Bytes Received	Total bytes received from the client station.
Packets Transmitted	Total packets transmitted to the client station.
Bytes Transmitted	Total bytes transmitted to the client station.
Packets Receive Dropped	Number of packets received from the client station that were dropped.
Bytes Receive Dropped	Number of bytes received from the client station that were dropped.
Packets Transmit Dropped	Number of packets transmitted to the client station that were dropped.
Bytes Transmit Dropped	Number of bytes transmitted to the client station that were dropped.
Fragments Received	Total fragmented packets received from the client station.
Fragments Transmitted	Total fragmented packets transmitted to the client station.

Table 179: Associated Client Session Detail Statistics (Cont.)

Field	*Description*
Transmit Retries	Number of times transmits to client station succeeded after one or more retries.
Transmit Retries Failed	Number of times transmits to client station failed after one or more retries.
Duplicates Received	Total duplicate packets received from the client station.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Detailed Associated Client TSPEC Statistics

The statistics on the **TSPEC** page show information about each client's active traffic streams. If there are no associated clients with active traffic streams, the page displays a message indicating that there are no traffic streams for any associated clients.

Note: The client TSPEC statistics do not persist across any client disassociation event, including a client roam. The TSPEC statistics reset any time a client disassociates from an AP.

Use the menu above the table to select the MAC address of the client with the information to view. Only clients with an active traffic stream appear in the selection list.

To open this page, click the **WLAN** > **Status/Statistics** > **Associated Client** > **Statistics** > **TSPEC** tab.

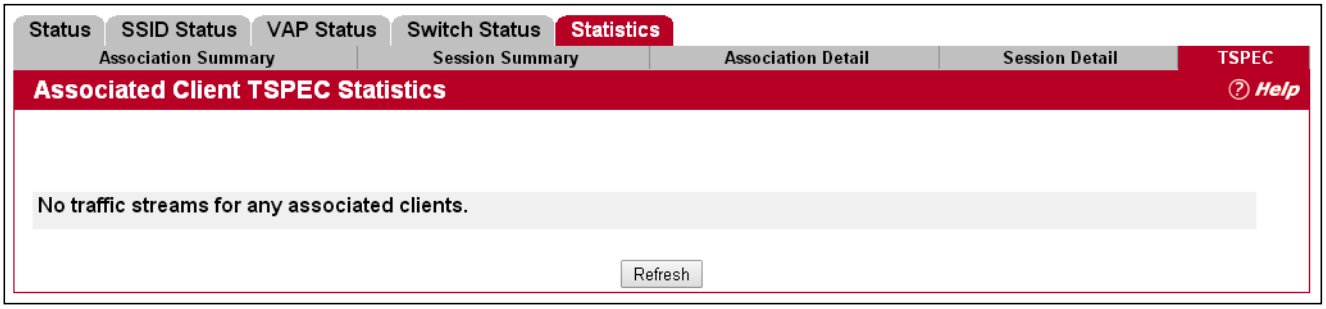


Figure 192: Associated Client Statistics TSPEC

Table 179 describes the information available on the **TSPEC** page for associated client statistics.

Table 180: Associated Client TSPEC Statistics

Field	*Description*
TS Packets Received	Count of packets received by an AP from a wireless client for the specified access category.
TS Bytes Received	Count of bytes received by an AP from a wireless client for the specified access category.

Table 180: Associated Client TSPEC Statistics

Field	*Description*
TS Packets Transmitted	Count of packets transmitted by an AP to a wireless client for the specified access category.
TS Bytes Transmitted	Count of bytes transmitted by an AP to a wireless client for the specified access category.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Peer Switch Status

The **Peer Switch Status** page provides information about other Unified Wireless Switches in the network. To access the peer switch information, click the **WLAN > Status/Statistics > Peer Switch** > **Status** tab.

Peer wireless switches within the same cluster exchange data about themselves, their managed APs, and clients. The switch maintains a database with this data so you can view information about a peer, such as its IP address and software version. If the switch loses contact with a peer, all of the data for that peer is deleted.

One switch in a cluster is elected as a Cluster Controller. The Cluster Controller collects status and statistics from all the other switches in the cluster, including information about the APs peer switches manage and the clients associated to those APs.

Figure 193: Peer Switch Status

Table 179 describes the information available on the **Peer Switch Status** page.

Table 181: Peer Switch Status

Field	*Description*
Cluster Controller IP Address	The IP address of the cluster controller for a group of peer switches.
Peer Switches	The number of peer switches in this cluster
IP Address	IP address of a peer wireless switch in the cluster.

Table 181: Peer Switch Status (Cont.)

Field	*Description*
Vendor ID	Vendor ID of the peer switch software.
Software Version	The software version for the given peer switch.
Protocol Version	Indicates the protocol version supported by the software on the peer switch.
Discovery Reason	The discovery method of the given peer switch, which can be through an L2 Poll or IP Poll (i.e., L2 or L3 discovery)
Managed AP Count	Shows the number of APs that the switch currently manages.
Age	Time since last communication with the switch in Hours, Minutes, and Seconds.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Peer Switch Configuration Status

You can push portions of the switch configuration from one switch to another switch in the cluster. The **Peer Switch Configuration Status** page displays information about the configuration sent by a peer switch in the cluster. It also identifies the IP address of each peer switch that received the configuration information. To access the peer switch configuration information, click the **WLAN > Status/Statistics > Peer Switch** > **Configuration** tab.

Note: To view information about the configuration received by the local switch, go to the **Status/ Statistics > Global** page and click the **Configuration Received** tab.

Figure 194: Peer Switch Configuration Status

The following table describes the fields available on the **Peer Switch Configuration Status** page.

Table 182: Peer Switch Configuration Status

Field	*Description*
Peer IP Address	Shows the IP address of each peer wireless switch in the cluster that received configuration information.
Configuration Switch IP Address	Shows the IP Address of the switch that sent the configuration information.

Table 182: Peer Switch Configuration Status (Cont.)

Field	*Description*
Configuration	Identifies which parts of the configuration the switch received from the peer switch. The possible configuration elements can be one or more of the following: • Global • Discovery • Channel/Power • AP Database • Channel/Power • AP Profiles • Known Client • Captive Portal • RADIUS Client • QoS ACL • QoS DiffServ If the switch has not received any configuration for another switch, the value is None.
Timestamp	Shows when the configuration was applied to the switch. The time is displayed as UTC time and therefore only useful if the administrator has configured each peer switch to use NTP

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Peer Switch Managed AP Status

The **Peer Switch Managed AP Status** page displays information about the APs that each peer switch in the cluster manages. To open this page, click the **WLAN > Status/Statistics > Peer Switch** > **Managed AP** tab. Use the drop-down list to select the peer switch with the AP information to display. Each peer switch is identified by its IP address.

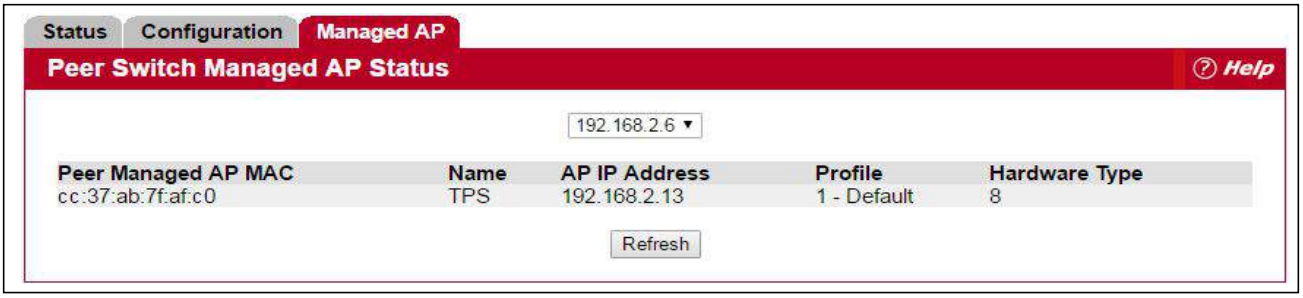


Figure 195: Peer Switch Managed AP Status

The following table describes the fields available on the **Peer Switch Managed AP Status** page.

Table 183: Peer Switch Managed AP Status

Field	*Description*
Peer Managed AP MAC	Shows the MAC address of each AP managed by the peer switch.
Peer Switch IP Address	Shows the IP address of the peer switch that manages the AP.
Name	The name configured for the managed AP.
AP IP Address	The IP address of the AP.
Profile	The AP profile applied to the AP by the switch.
Hardware Type	The Hardware ID associated with the AP hardware platform.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

WDS Managed APs

The Wireless Distribution System (WDS)-Managed AP feature allows you to add managed APs to the cluster using over-the-air WDS links through other managed APs. With WDS, APs may be located outdoors where wired connection to the data network is unavailable, or in remote buildings that are not connected to the main campus with a wired network.

The WDS AP group consists of the following managed APs:

- Root AP—Acts as a bridge or repeater on the wireless medium and communicates with the switch via the wired link
- Satellite AP—Communicates with the switch via a WDS link to the Root AP

The WDS links are secured using WPA2 Personal authentication and AES encryption.

For an detailed example on how to configure the root AP and satellite AP, refer to Appendix A: “Configuring Root/ Satellite APs,” on page 387.

WDS Group Status Summary

The **WDS Group Status Summary** page displays summary information about configured WDS links. At least one group must be configured for the fields to display. To configure a WDS AP group, use the pages available within the **WLAN** > **WDS** folder. To open the summary page, click **WLAN > Status/Statistics** > **WDS Managed APs**.

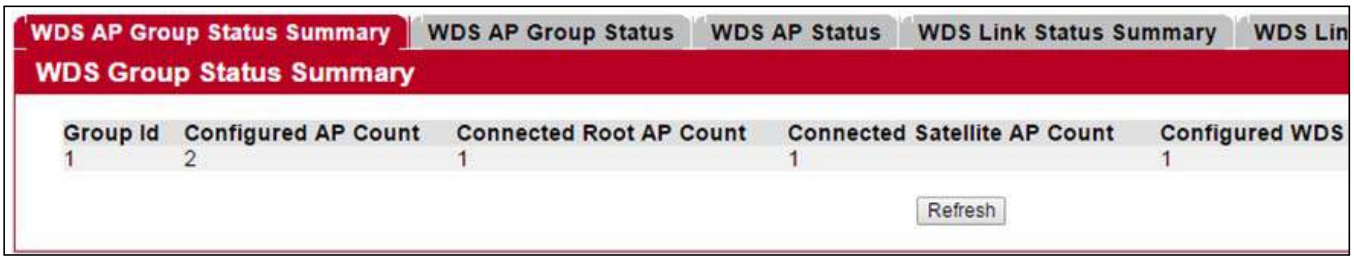


Figure 196: WDS Group Status Summary

The following table describes the fields available on the **WDS Group Status Summary** page.

Table 184: WDS Group Status Summary

Field	*Description*
Group ID	Unique number that identifies the WDS AP group
Configured AP Count	Number of APs configured in this WDS AP group
Connected Root AP Count	Number of Root APs currently being managed by the switch that are members of this WDS AP Group
Connected Satellite AP Count	Number of Satellite APs currently being managed by the switch that are members of this WDS AP Group
Configured WDS Link Count	Number of configured bidirectional links in the WDS AP Group.
Detected WDS Links Count	Number of WDS links detected in the system. APs on both sides of the link must detect each other in order for the link to be counted.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

WDS AP Group Status

The **WDS AP Group Status** page displays detailed information about the configured APs and links in the WDS Group. From this page, you can also send a new password to group members. To open this page, click the **WLAN > Status/Statistics > WDS Managed APs > WDS AP Group Status** tab.

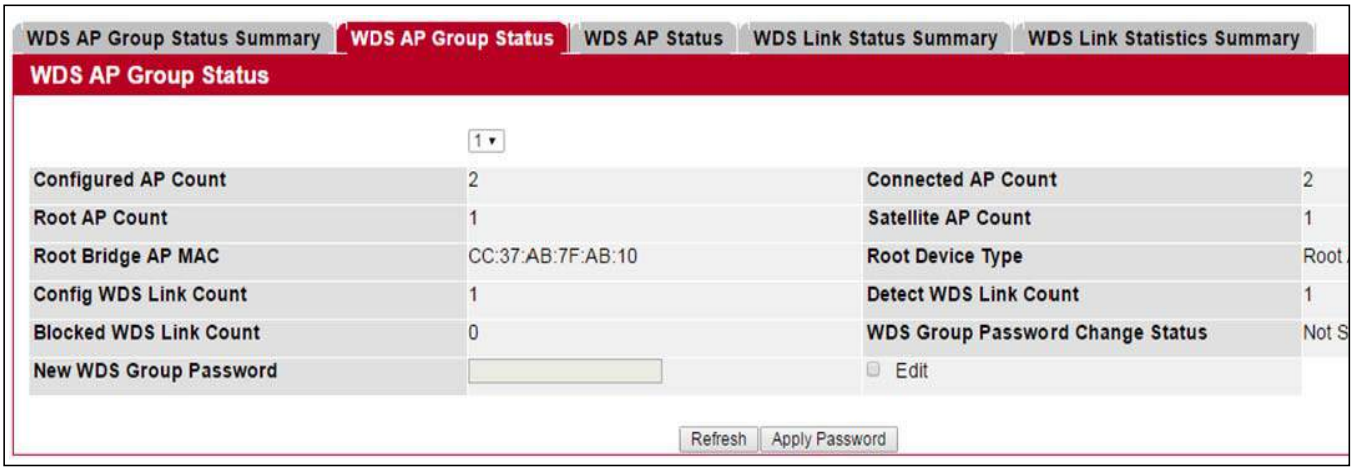


Figure 197: WDS AP Group Status

The following table describes the fields available on the **WDS AP Group Status** page.

Table 185: WDS AP Group Status

Field	*Description*
Group ID	Use the drop-down menu above the fields to select the group number that identifies the configured WDS AP group.
Configured AP Count	Number of APs configured in this WDS AP group
Root AP Count	Number of Root APs currently being managed by the switch that are members of this WDS AP Group.
Root Bridge AP MAC	MAC Address of the device elected as the Spanning Tree Root Bridge. If spanning tree is disabled this value is 00:00:00:00:00:00.
Config WDS Link Count	Number of configured bidirectional links in the WDS AP Group.
Blocked WDS Link Count	Number of WDS links blocked by the spanning tree protocol. If the AP on one side of the link reports the link as blocking, then the link is counted by this status parameter.
New WDS Group Password	To change the password for all switches and APs in this WDS Group, select the Edit checkbox, type the new password, and then click **Apply Password**.
Connected AP Count	Number of APs managed by the switch that are members of this WDS AP Group. This number is the sum of the Connected Root APs and Connected Satellite APs.
Satellite AP Count	Number of Satellite APs currently being managed by the switch that are members of this WDS AP Group.
Root Device Type	The type of device elected as the Spanning Tree Root bridge: • None (STP is disabled) • Root AP • Satellite AP • External Device (STP Root is not one of the APs)

Table 185: WDS AP Group Status

Field	*Description*
Detect WDS Link Count	Number of WDS links detected in the system. APs on both sides of the link must detect each other in order for the link to be counted.
WDS Group Password Change Status	Status of the last attempt to configure the password for the WDS Group: • Not Started • Success • Invalid Password • Requested • Timed Out

The page includes the following button:

- **Refresh**—Updates the page with the latest information.
- **Apply Password**—Applies the password entered in the New WDS Group Password field.

WDS Group AP Status Summary

The **WDS AP Group Status Summary** page displays summary information about the APs in a configured WDS Group. To open this page, click the **WLAN > Status/Statistics > WDS Managed APs > WDS AP Status** tab.

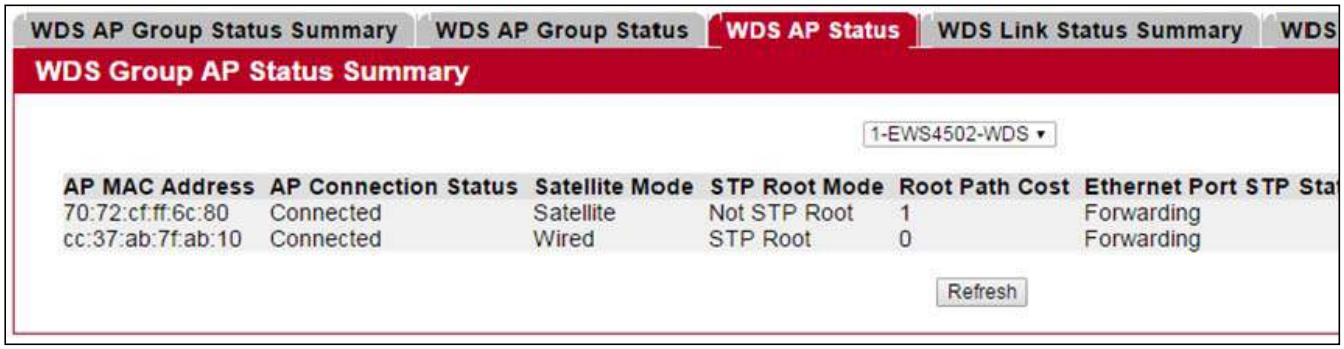


Figure 198: WDS Group AP Status Summary

The following table describes the fields available on the **WDS Group AP Status Summary** page.

Table 186: WDS Group AP Status Summary

Field	*Description*
Group ID	Use the drop-down menu above the fields to select the group number that identifies the configured WDS AP group.
AP MAC Address	Identifies the AP in the group by its MAC address
AP Connection Status	Indicates whether the AP is currently being managed by one of the switches in the cluster.
Satellite Mode	Indicates whether the AP is a Satellite AP connected to the network via a WDS link or a Root AP connected to the network via a wired link.
STP Root Mode	Indicates whether this AP is the root of the spanning tree. If spanning tree is disabled then the AP is always reported as Not STP Root.

Table 186: WDS Group AP Status Summary (Cont.)

Field	*Description*
Root Path Cost	Spanning Tree Path Cost to the root. The root AP always reports this value as 0. If spanning tree is disabled the value is also 0.
Ethernet Port STP State	When spanning tree is enabled on the APs in the WDS group this status parameter reports the spanning tree status of the Ethernet port, which is one of the following: • Disabled (STP is disabled or Link is down) • Forwarding • Learning • Listening • Blocking
Ethernet Port Mode	On Satellite APs the Ethernet port can be manually disabled. On root APs the port is always enabled.
Ethernet Port Link State	When the Ethernet port is enabled, this status reports the link state of the port.

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

WDS Group Link Status Summary

The **WDS AP Link Status Summary** page displays summary information about the link configuration and link state in a WDS Group. To open this page, click the **WLAN > Status/Statistics > WDS Managed APs > WDS Link Summary** tab.

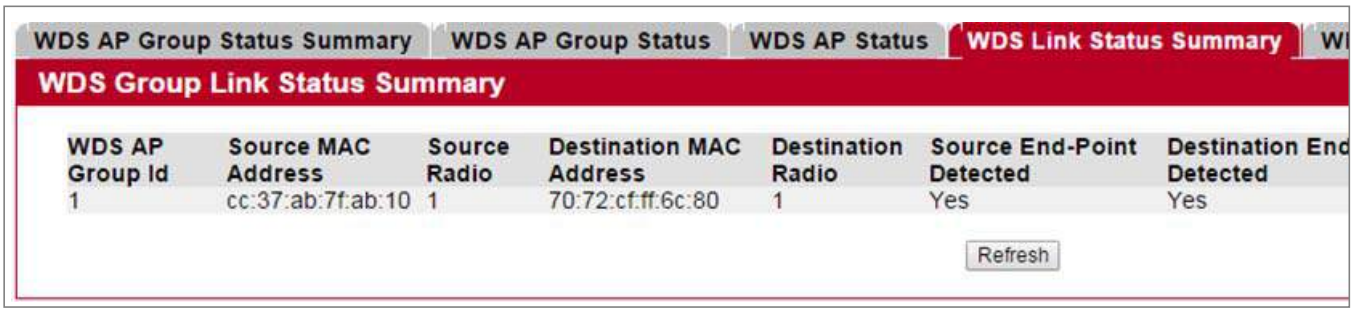


Figure 199: WDS AP Link Status Summary

The following table describes the fields available on the **WDS AP Link Status Summary** page.

Table 187: WDS AP Link Status Summary

Field	*Description*
WDS AP Group ID	The group number that identifies the configured WDS AP group.
Source MAC Address	The MAC address of one end-point of the WDS link
Radio Source	The radio number of the WDS link endpoint on the source AP.
Destination MAC Address	The MAC address of the Source AP in the group.
Destination Radio	The radio number of the WDS link endpoint on the destination AP.

Table 187: WDS AP Link Status Summary

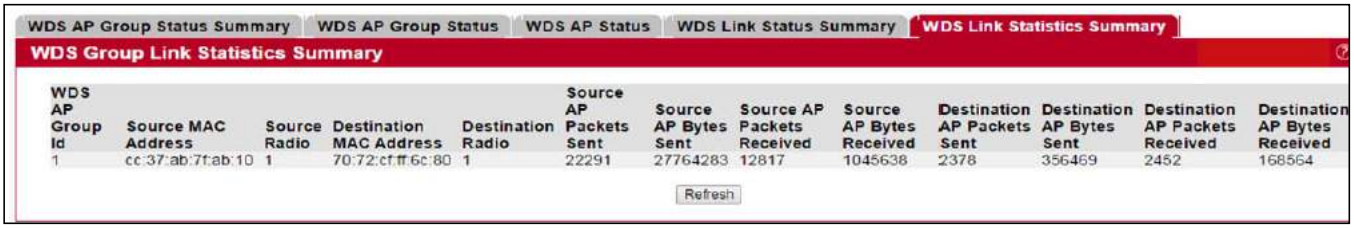
Field	*Description*
Source End-Point Detected	Indicates whether the AP specified by the destination MAC detected the AP specified by the source MAC.
Destination End-Point Detected	Indicates whether the AP specified by the source MAC detected the AP specified by the destination MAC.
Aggregation Mode	When parallel links are defined between two APs, this field indicates whether this link is part of the aggregation link pair.
Source STP State	Spanning Tree State of the link on the source AP, which is one of the following: • Disabled (STP is disabled or Link is down) • Forwarding • Learning • Listening • Blocking
Destination STP State	Spanning Tree State of the link on the destination AP, which is one of the following: • Disabled (STP is disabled or Link is down) • Forwarding • Learning • Listening • Blocking

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

WDS Group Link Statistics Summary

The **WDS Group Link Statistics Summary** page displays summary information about the packets sent and received on the WDS links. To open this page, click the **WLAN > Status/Statistics > WDS Managed APs > WDS Link Statistics** tab.



WDS AP Group Id	Source MAC Address	Source Radio	Destination MAC Address	Destination Radio	Source AP Packets Sent	Source AP Bytes Sent	Source AP Packets Received	Source AP Bytes Received	Destination AP Packets Sent	Destination AP Bytes Sent	Destination AP Packets Received	Destination AP Bytes Received
1	cc:37:ab:7f:ab:10	1	70:72:cf:ff:6c:80	1	22291	27764283	12817	1045638	2378	356469	2452	168564

Figure 200: WDS Group Link Statistics Summary

The following table describes the fields available on the **WDS AP Link Statistics Summary** page.

Note: The WDS links are bidirectional. The terms Source and Destination simply reflect the WDS link endpoints specified in the WDS Group configuration.

Table 188: WDS AP Link Statistics Summary

Field	*Description*
WDS AP Group ID	The group number that identifies the configured WDS AP group.
Source MAC Address	The MAC address of one end-point of the WDS link
Radio Source	The radio number of the WDS link endpoint on the source AP.
Destination MAC Address	The MAC address of the Source AP in the group.
Destination Radio	The radio number of the WDS link endpoint on the destination AP.
Source AP Packets Sent	Number of packets sent by the source AP.
Source AP Bytes Sent	Number of bytes sent by the source AP.
Source AP Packets Received	Number of packets received by the source AP.
Source AP Bytes Received	Number of bytes received by the source AP.
Destination AP Packets Sent	Number of packets sent by the destination AP.
Destination AP Bytes Sent	Number of bytes sent by the destination AP.
Destination AP Packets Received	Number of packets received by the destination AP.
Destination AP Bytes Received	Number of bytes received by the destination AP.

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Monitoring and Managing Intrusion Detection

This section contains the following subsections to help manage and monitor the APs and wireless clients in the Unified Wireless Switch network and to protect against rogue devices:

- Access Point Rogue/RF Scan Status
- Detected Client Status
- Ad Hoc Client Status
- Access Point Authentication Failure Status
- AP De-Authentication Attack Status

Status entries for the Intrusion Detection pages are collected at a point in time and eventually age out. The age value for each entry shows how long ago the switch recorded the entry. You can configure the age out time for status entries on the **WLAN > Advanced Configuration > Global** page. You can also manually delete status entries.

Access Point Rogue/RF Scan Status

The radios on each AP can periodically scan the radio frequency to collect information about other APs and wireless clients that are within range. In normal operating mode the AP always scans on the operational channel for the radio. Two other scan modes are available for each radio on the APs:

- **Scan Other Channels**: Configures the AP to periodically leave its operational channel and scan other channels within that frequency.
- **Scan Sentry**: Disables normal operation of the radio and performs a continuous radio scan. In this mode, no beacons are sent, and no clients are allowed to associate with the AP.

When Scan Other Channels or Scan Sentry modes are enabled, the AP scans all available channels on each radio. When the scan is complete, the AP sends information it collected during the RF scan to the switch that manages it. For information about how to configure the scan mode, see “Radio Configuration” on page 190.

The UWS considers an access point to be a rogue if it is detected during the RF scan process and is classified as a threat by one of the threat detection algorithms. To view the threat detection algorithms enabled on the system, go to the **WLAN > WLAN Configuration > WIDS Security** page.

From the **Access Point RF Scan Status** page, you can view information about all APs detected via RF scan, including those reported as Rogues. To open this page, click **WLAN** > **Intrusion Detection** > **Rouge/RF Scan**.

You can sort the APs in the list based any of the column headings. For example, to group all Rogue APs together, click **Status**.

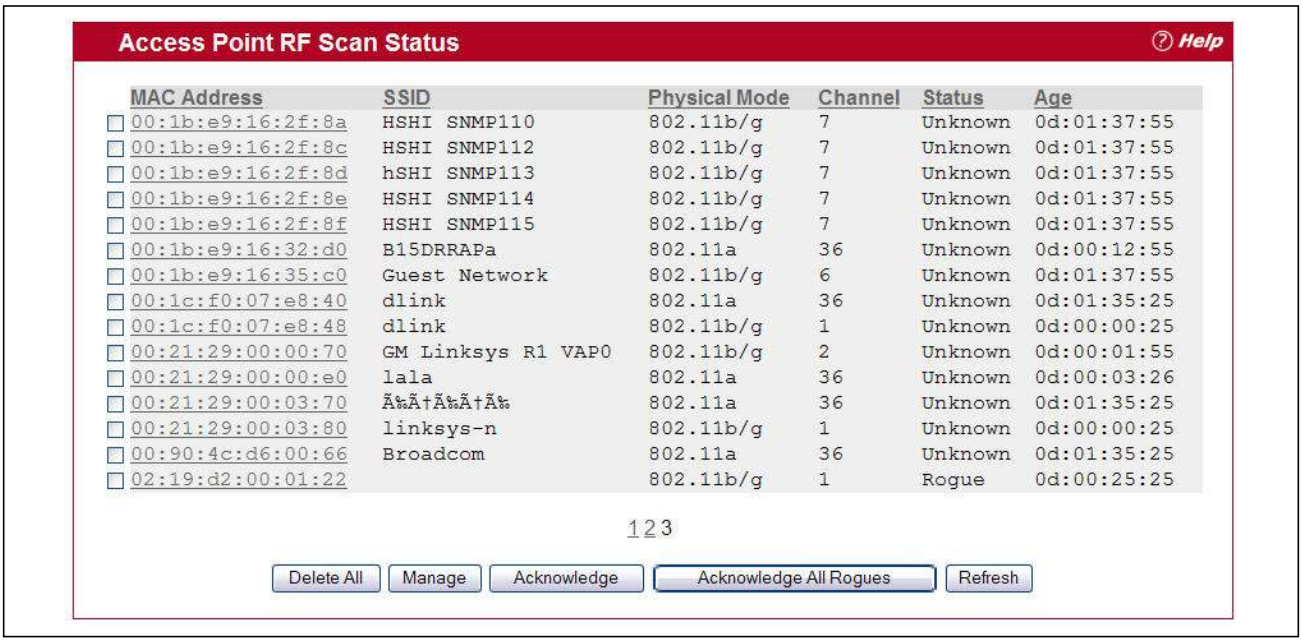


Figure 201: RF Scan

To view additional information about a detected AP, click the MAC address of the AP.

The following table describes the fields on the **Rogue/RF Scan** page.

Table 189: Access Point Rogue/RF Scan Status Fields

Field	*Description*
MAC Address	The Ethernet MAC address of the detected AP. This could be a physical radio interface or VAP MAC. For Edge-Core APs this is always a VAP MAC address.
SSID	Service Set ID of the network, which is broadcast in the detected beacon frame.
Physical Mode	Indicates the 802.11 mode being used on the AP.
Channel	Transmit channel of the AP.
Status	Indicates the managed status of the AP, whether this is a valid AP known to the switch or a Rogue on the network. The valid values are: • Managed: The neighbor AP is managed by the wireless system. • Standalone: The AP is managed in standalone mode and configured as a valid AP entry (local or RADIUS). • Rogue: The AP is classified as a threat by one of the threat detection algorithms. • Unknown: The AP is detected in the network but is not classified as a threat by the threat detection algorithms.
Age	Time since this AP was last detected in an RF scan.

Command Buttons

The page includes the following buttons:

- **Delete All**—Clears all APs from the RF scan list. The list repopulates as the APs are discovered.
- **Manage**—Configures a Rogue AP to be managed by the switch the next time it is discovered. The switch adds the selected AP to the Valid AP database as a Managed AP and assigns it the default AP profile. Then, you can use the switch to configure the AP settings. If you use a RADIUS server for AP validation, you must add the MAC address of the AP to the AP database on the RADIUS server.
- **Acknowledge**—Clear the rogue status of the selected AP in the RF Scan database.
- **Acknowledge All Rogues**—Acknowledges all APs with a Rogue status. The status of an acknowledged rogue is returned to the status it had when it was first detected. If the detected AP fails any of the tests that classify it as a threat, it will be listed as a Rogue again.
- **Refresh**—Updates the page with the latest information.

After you click the MAC address of an AP to view details, the detailed **Access Point RF Scan Status** page for the AP appears.

The detailed status for access points detected during the RF scan shows information about an individual AP detected through the RF scan. To view information about another AP detected through the RF Scan, return to the main **Rogue/RF Scan** page and click the MAC address of the AP with the information to view.

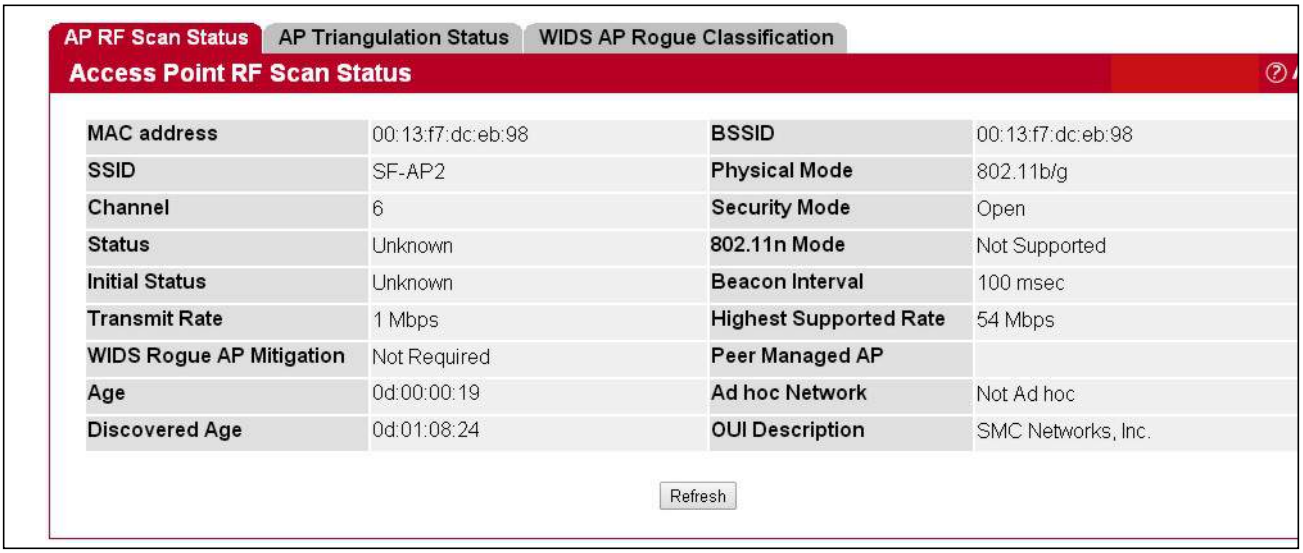


Figure 202: RF Scan AP Details

The following table shows the information the **Access Point RF Scan Status** page shows for an individual access point.

Table 190: Detailed Access Point RF Scan Status

Field	*Description*
AP MAC Address	***Note:*** This field displays only if the AP Status is Managed. Indicates the base MAC address of the AP. This field does not display if the AP status is Standalone, Rogue, or Unknown.

Table 190: Detailed Access Point RF Scan Status (Cont.)

Field	*Description*
SSID	Service Set ID of the network, which is broadcast in the detected beacon frame.
Channel	Transmit channel of the AP.
Status	Indicates the managed status of the AP, whether this is a valid AP known to the switch or a Rogue on the network. The valid values are: • Managed: The neighbor AP is managed by the wireless system. • Standalone: The AP is managed in standalone mode and configured as a valid AP entry (local or RADIUS). • Rogue: The AP is classified as a threat by one of the threat detection algorithms. • Unknown: The AP is detected in the network but is not classified as a threat by the threat detection algorithms.
Initial Status	If the AP is not rogue, the initial status is equal to Status (Managed, Standalone, or Unknown). For rogue APs, the initial status is the classification prior to this AP becoming rogue.
Transmit Rate	Indicates the rate at which the AP is currently transmitting data.
WIDS Rogue AP Mitigation	Status indicating whether rogue AP mitigation is in progress for this AP. If mitigation is not in progress then this field displays the reason, which can be one of the following: • Not Required (AP s not rogue) • Already mitigating too many APs. • AP Is operating on an illegal channel. • AP is spoofing valid managed AP MAC address. • AP is Ad hoc.
Age	Time since this AP was last detected in an RF scan.
Discovered Age	Time since this AP was first detected in an RF scan.
BSSID	Basic Service Set Identifier advertised by the AP in the beacon frames.
Radio	***Note:*** This field displays only if the AP Status is Managed. Indicates the radio interface of the AP. This field does not display if the AP status is Standalone, Rogue, or Unknown.
Physical Mode	Indicates the 802.11 mode being used on the AP.
Security Mode	Security mode used by the AP.
802.11n Mode	Indicates whether this AP supports IEEE 802.11n mode.
Beacon Interval	Beacon interval for the neighbor AP network.
Highest Supported Rate	Highest supported rate advertised by this AP in the beacon frames. The rate is in Mbps.
Peer Managed AP	Indicates whether this AP is managed by a switch in the cluster.
Ad hoc Network	Indicates whether the beacon frame was received from an ad hoc network.
OUI Description	Identifies the manufacturer of the AP or wireless client adapter based on the information in the OUI database on the switch.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Access Point Triangulation Status

Triangulation information is provided to help locate the rogue client by showing which managed APs detect the each device discovered through the RF Scan. Up to six triangulation entries are reported for each AP detected through the RF Scan: three entries by non-sentry APs and three entries by sentry APs. Since an AP may have one radio configured in sentry mode and another radio configured in non-sentry mode, the same AP can appear in both lists. If the AP has not been detected by three APs, then the list may contain zero, one or two entries.

To view information about another AP detected through the RF Scan, return to the main **Rogue/RF Scan** page and click on the MAC address of the AP with the information to view. To display detailed information about an entry in this list click on the MAC address to open the Access Point RF Scan Status page, then click on the **AP Triangulation Status** tab.

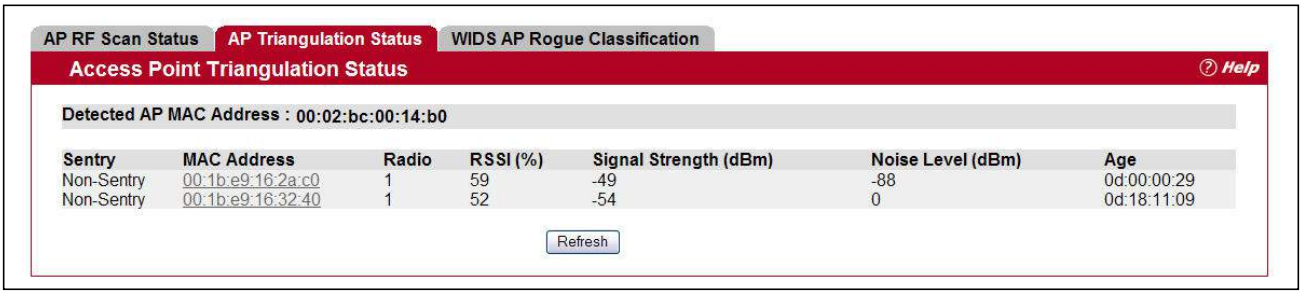


Figure 203: AP Triangulation Status

The following table shows the information the Access Point RF Scan Status page shows for an individual access point.

Table 191: Access Point Triangulation Status

Field	*Description*
Detected AP MAC Address	The Ethernet MAC address of the detected AP. This could be a physical radio interface or VAP MAC. For Edge-Core APs this is always a VAP MAC address.
Sentry	Identifies whether the AP that detected the entry is in sentry or non-sentry mode.
MAC Address	Shows the MAC address of the AP that detected the RF Scan entry. The address links to the Valid AP database.
Radio	Identifies the radio on the AP that detected the RF Scan entry.
RSSI	Shows the received signal strength indicator in terms of percentage for the non-sentry AP. The range is 0—100%. A value of 0 indicates the AP is not detected.
Signal Strength	Received signal strength for the non-sentry AP. The range is –127 dBm to 127 dBm, but most values are expected to range from –95 dBm to –10 dBm.
Noise Level	Noise reported on the channel by the non-sentry AP.
Age	Time since this AP was last detected in an RF scan.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing WIDS AP Rogue Classification Information

The Wireless Intrusion Detection System (WIDS) can help detect intrusion attempts into the wireless network and take automatic actions to protect the network. The UWS allows you to activate or deactivate various threat detection tests and set threat detection thresholds. The **WIDS AP Rogue Classification** page provides information about the results of these tests. If an AP has been classified as a rogue, this page provides information about which tests the AP might have failed to trigger the classification.

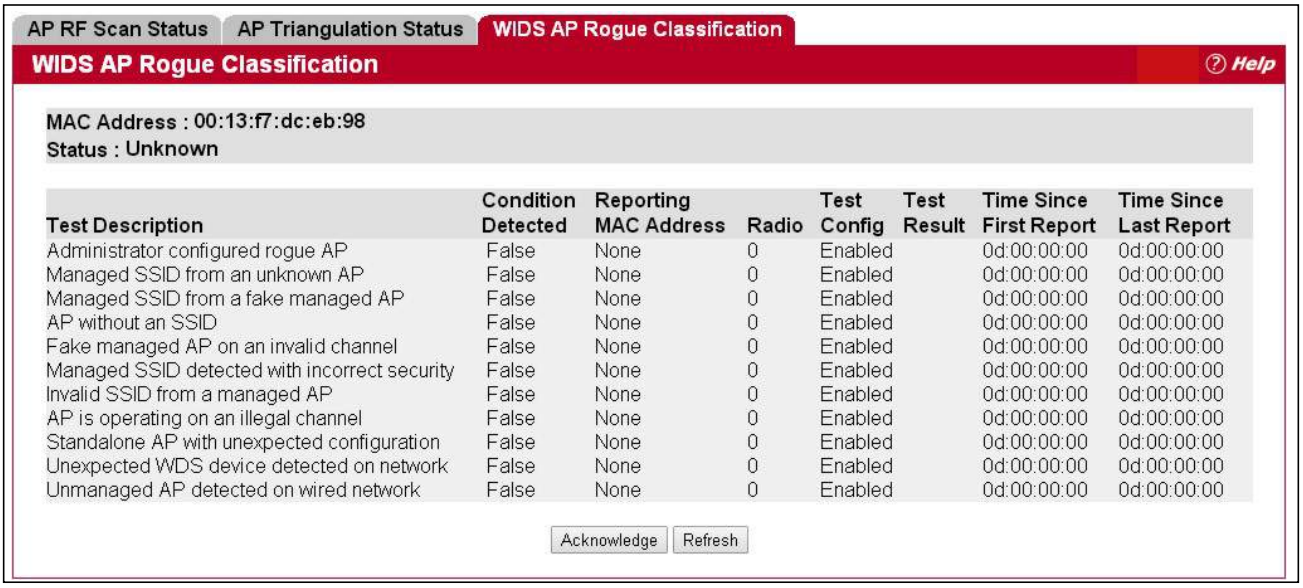
If an AP is classified as a rogue, the system provides additional information to identify the threat type that caused the switch to classify the AP as a rogue.

The WIDS RF Security encompasses three functions:

- Detect wireless devices by listening to control and data frames in the air.
- Classify whether the wireless device is a threat by comparing the received data to various databases as well as sending trace frames into the wired network and listening for the trace frames on the wireless network.
- Take action to protect the network from threats.

These changes can be done without disrupting network connectivity. Since some of the work is done by access points, the switch needs to send messages to the APs to modify its WIDS operational properties.

To view information about another AP detected through the RF Scan, return to the main **Rogue/RF** Scan page and click the MAC address of the AP with the information to view, then click on the **WIDS AP Rogue Classification** tab.



Test Description	Condition Detected	Reporting MAC Address	Radio	Test Config	Test Result	Time Since First Report	Time Since Last Report
Administrator configured rogue AP	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Managed SSID from an unknown AP	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Managed SSID from a fake managed AP	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
AP without an SSID	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Fake managed AP on an invalid channel	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Managed SSID detected with incorrect security	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Invalid SSID from a managed AP	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
AP is operating on an illegal channel	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Standalone AP with unexpected configuration	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Unexpected WDS device detected on network	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Unmanaged AP detected on wired network	False	None	0	Enabled		0d:00:00:00	0d:00:00:00

Figure 204: WIDS AP Rogue Classification

Table 192 shows the information on the WIDS AP Rogue page for an individual access point.

Table 192: WIDS AP Rogue Classification

Field	*Description*
MAC Address	The Ethernet MAC address of the detected AP. This could be a physical radio interface or VAP MAC. For Edge-Core APs this is always a VAP MAC address.
Status	Indicates the managed status of the AP, whether this is a valid AP known to the switch or a Rogue on the network. Valid values are: Managed: The neighbor AP is managed by the wireless system. Standalone: The AP is managed in standalone mode and configured as a valid AP entry (using local or RADIUS configuration). Rogue: The AP is classified as a threat by one of the threat detection algorithms. Unknown: The AP is detected in the network but is not classified as a threat by the threat detection algorithms.
Test Description	Identifies the tests that were performed, which includes the following: • Administrator-Configured rogue AP • Managed SSID received form an unknown AP • Managed SSID from a fake managed AP • AP without an SSID • Fake managed AP on an invalid channel • Managed SSID detected with incorrect security configuration • Invalid SSID received from managed AP. • AP is operating on an illegal channel • Standalone AP is operating with unexpected configuration. • Unexpected WDS device is detected on the network. • Unmanaged AP detected on wired network.
Condition Detected	Indicates whether the result of the test was true or false.
Reporting MAC Address	Identifies the MAC address of the AP that reported the test results.
Radio	Identifies which physical radio on the reporting AP was responsible for the test results.
Test Config	Shows whether this test is configured to report rogues. Each test can be globally enabled or disabled to report a positive result as a rogue.
Test Result	Shows whether this test reported the device as rogue. In some cases the test may report a positive result, be enabled, but not report the device as rogue because the device is allowed to operate in this mode.
Time Since First Report	Time stamp indicating how long ago this test first detected the condition.
Time Since Last Report	Time stamp indicating how long ago this test last detected the condition.

Command Buttons

The page includes the following buttons:

- **Acknowledge**—Clears the rogue status of the AP in the RF Scan database.
- **Refresh**—Updates the page with the latest information.

Detected Client Status

Wireless clients are detected by the wireless system when the clients either attempt to interact with the system or when the system detects traffic from the clients. The **Detected Client Status** page contains information about clients that have authenticated with an AP as well information about clients that disassociate and are no longer connected to the system.

The Cluster Controller receives information about associated clients from all switches in the cluster, and you can disassociate clients on any AP in the cluster from the Cluster Controller. To open this page, click **WLAN** > **Intrusion Detection** > **Detected Clients**.

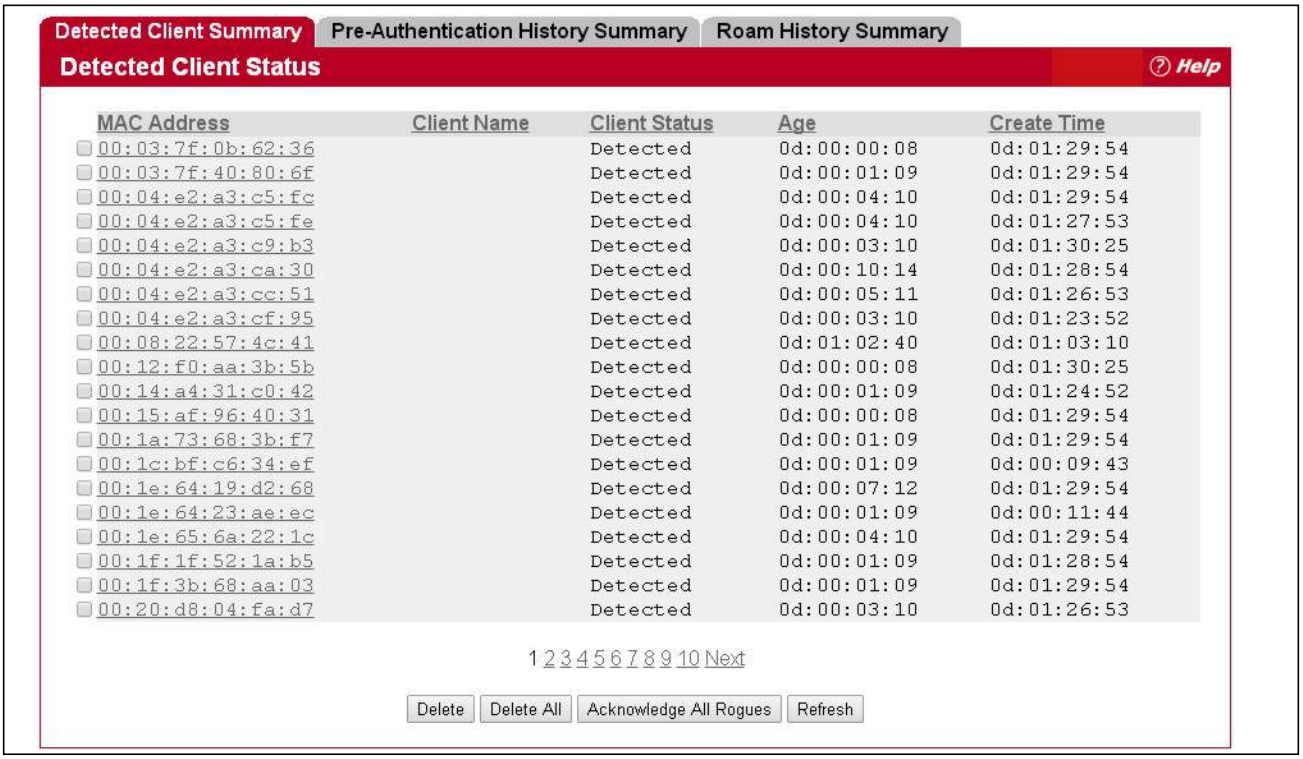


Figure 205: Detected Client Status

To learn more about a client listed on the page, click the MAC address of the client.

Table 193: Detected Client Status

Field	*Description*
MAC Address	The Ethernet address of the client.
Client Name	Shows the name of the client, if available, from the Known Client Database. If client is not in the database then the field is blank.

Table 193: Detected Client Status (Cont.)

Field	*Description*
Client Status	Shows the client status, which can be one of the following: • Authenticated—The wireless client is authenticated with the wireless system. • Detected—The wireless client is detected by the wireless system but is not a security threat. • Black-Listed—The client with this MAC address is specifically denied access via MAC Authentication. • Rogue—The client is classified as a threat by one of the threat detection algorithms.
Age	Time since any event has been received for this client that updated the detected client database entry.
Create Time	Time since this entry was first added to the detected clients database.

Command Buttons

The page includes the following buttons:

- **Delete**—Delete the selected client from the list. If the client is detected again, it will be added to the list.
- **Delete All**—Deletes all non-authenticated clients from the Detected Client database. As clients are detected, they are added to the database and appear in the list.
- **Acknowledge All Rogues**—Clear the rogue status of all clients listed as rogues in the Detected Client database, The status of an acknowledge client is returned to the status it had when it was first detected. If the detected client fails any of the tests that classify it as a threat, it will be listed as a Rogue again
- **Refresh**—Updates the page with the latest information.

Viewing Detailed Detected Client Status

Click one of the client MAC addresses in the **Intrusion Detection > Detected Client Status** page to show detailed information about specific clients detected on the wireless network. To view information about other clients detected on the network, return to the **Detected Clients** page and click a client MAC address.

Figure 206: Detailed Detected Client Status

Table 194: Detailed Detected Client Status

Field	*Description*
MAC Address	The Ethernet address of the client.
Client Status	Shows the client status, which can be one of the following: • Authenticated—Client is Authenticated with the system and is not Rogue. • Detected—Client is detected, not Authenticated, not rogue, and is not found in the Known Clients Database. • Known—Client is detected and found in the Known Clients Database, but is not authenticated. • Black-Listed—Client tried to associate with the system, but was rejected due to MAC authentication. • Rogue—Client failed the enabled threat tests.
Authentication Status	Indicates whether this client is authenticated. ***Note:*** The Client Status can be Rogue, but the authentication status can still be Authenticated.
Threat Detection	Indicates whether one of the threat detection tests has been triggered for this client. If the test is disabled, the client will not be marked as a rogue, but you can still investigate why the threat was triggered.

Table 194: Detailed Detected Client Status (Cont.)

Field	*Description*
Threat Mitigation Status	Indicates whether threat mitigation has been done for this client.
Time Since Entry Last Updated	Shows the amount of time that has passed since any event has been received for this client that updated the detected client database entry.
Time Since Entry Create	Shows the amount of time that has passed since this entry was first added to the detected clients database.
Client Name	Shows the name of the client, if available, from the Known Client Database. If the client is not in the database then the field is blank.
RSSI	If the client is authenticated with the managed AP, this field displays the last RSSI value reported by the AP with which the client is authenticated. The RSSI is a percentage from 1–100%. A value of 0 means the AP is not detected.
Signal	Last signal strength reported by the managed AP with which the client is authenticated. The possible range is –128 to 128 dBm.
Noise	Last channel noise reported by the managed AP with which the client is authenticated. The possible range is –128 to 128 dBm.
Probe Req Recorded	Number of probe requests recorded so far during the probe collection interval.
Probe Collection Interval	Shows the amount of time spent in each probe collection period. The probe collection helps the switch decide whether the client is a threat.
Highest Probes Detected	Shows the largest number of probes that the switch detected during a probe collection interval.
Channel	Identifies the channel that the client is using.
OUI Description	Organization Unit Identifier for the wireless chip using on this client.
Auth Msgs Recorded	Shows the number of IEEE 802.11 Authentication messages recorded so far during the authentication collection interval.
Auth Collection Interval	Shows the amount of time spent in each authentication collection period. The authentication collection helps the switch decide whether the client is a threat.
Highest Auth Msgs	Shows the largest number of authentication messages that the switch detected during an authentication collection interval.
De-Auth Msgs Recorded	Shows the number of IEEE 802.11 De-Authentication messages recorded so far during the de-authentication collection interval.
De-Auth Collection Interval	Shows the amount of time spent in each de-authentication collection period. The de-authentication collection helps the switch decide whether the client is a threat.
Highest De-Auth Msgs	Shows the largest number of de-authentication messages that the switch detected during a de-authentication collection interval.
Authentication Failures	Shows the number of 802.1X Authentication failures detected for this client.
Probes Detected	Shows the number of probes detected in the last RF Scan.
Broadcast BSSID Probes	Shows the number of probes to broadcast BSSID in the last RF Scan.
Broadcast SSID Probes	Shows the number of probes to broadcast SSID in the last RF Scan.
Specific BSSID Probes	Shows the number of probes to a specific BSSID in the last RF Scan.
Specific SSID Probes	Shows the number of probes to a specific SSID in the last RF Scan
Last Directed Probe BSSID	Shows the last directed probe BSSID detected in the RF Scan, which is a MAC address.
Last Directed Probe SSID	Shows the name of the last directed Probe SSID detected in the RF Scan.

Table 194: Detailed Detected Client Status (Cont.)

Field	*Description*
Threat Mitigation Sent	Shows whether threat mitigation has been done for this client.

Command Buttons

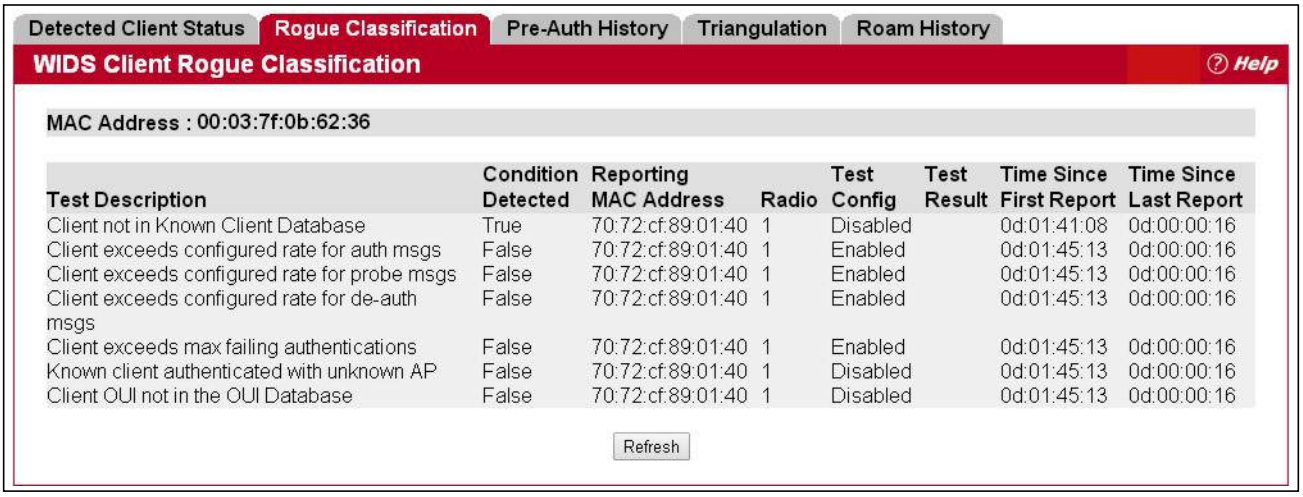
The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Acknowledge Rogue**—Clear the rogue status of the client in the Detected Client database, The status of an acknowledge client is returned to the status it had when it was first detected. If the detected client fails any of the tests that classify it as a threat, it will be listed as a Rogue again

Viewing WIDS Client Rogue Classification

The Wireless Intrusion Detection System (WIDS) can help detect intrusion attempts into the wireless network and take automatic actions to protect the network. The UWS allows you to activate or deactivate various threat detection tests and set threat detection thresholds. The **WIDS Client Rogue Classification** page provides information about the results of these tests. If a client has been classified as a rogue, this page provides information about which tests the client might have failed to trigger the classification.

To view WIDS information about another client detected through the RF Scan, return to the main **Detected Clients** page and click the MAC address of the client with the information to view. Then click the **Rouge Classification** tab.



Test Description	Condition Detected	Reporting MAC Address	Radio	Test Config	Test Result	Time Since First Report	Time Since Last Report
Client not in Known Client Database	True	70:72:cf:89:01:40	1	Disabled		0d:01:41:08	0d:00:00:16
Client exceeds configured rate for auth msgs	False	70:72:cf:89:01:40	1	Enabled		0d:01:45:13	0d:00:00:16
Client exceeds configured rate for probe msgs	False	70:72:cf:89:01:40	1	Enabled		0d:01:45:13	0d:00:00:16
Client exceeds configured rate for de-auth msgs	False	70:72:cf:89:01:40	1	Enabled		0d:01:45:13	0d:00:00:16
Client exceeds max failing authentications	False	70:72:cf:89:01:40	1	Enabled		0d:01:45:13	0d:00:00:16
Known client authenticated with unknown AP	False	70:72:cf:89:01:40	1	Disabled		0d:01:45:13	0d:00:00:16
Client OUI not in the OUI Database	False	70:72:cf:89:01:40	1	Disabled		0d:01:45:13	0d:00:00:16

Figure 207: WIDS Client Rogue Classification

The following table shows information about the security test performed on the detected client.

Table 195: WIDS Client Rogue Classification

Field	*Description*
MAC Address	The Ethernet MAC address of the detected wireless client.
Test Description	Identifies the tests that were performed, which includes the following: • Client not in the Known Client Database. • Client exceeds the configured rate for transmitting 802.11 authentication requests. • Client exceeds the configured rate for transmitting probe requests. • Client exceeds the configured rate for transmitting de-authentication requests. • Client exceeds the maximum number of failing authentications. • Known Client is authenticated with an Unknown AP. • Client OUI not in the OUI Database
Condition Detected	Indicates whether the result of the test was true or false.
Reporting MAC Address	Identifies the MAC address of the AP that reported the test results.
Radio	Identifies which physical radio on the reporting AP was responsible for the test results.
Test Config	Shows whether this test is configured to report rogues. Each test can be globally enabled or disabled to report a positive result as a rogue.
Test Result	Shows whether this test reported the device as rogue. In some cases the test may report a positive result, be enabled, but not report the device as rogue because the device is allowed to operate in this mode.
Time Since First Report	Time stamp indicating how long ago this test first detected the condition.
Time Since Last Report	Time stamp indicating how long ago this test last detected the condition.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Detected Client Pre-Authentication History

To help authenticated clients roam without losing sessions and needing to re-authenticate, wireless clients can attempt to authenticate to other APs within range that the client could possibly associate with. For successful pre-authentication, the target AP must have a VAP with an SSID and security configuration that matches that of the client, including MAC authentication, encryption method, and pre-shared key or RADIUS parameters. The the AP that the client is associated with captures all pre-authentication requests and sends them to the switch.

The **Detected Client Pre-Authentication History** page shows information about the pre-authentication requests that the detected client has made. Then click the **Pre-Auth History** tab.

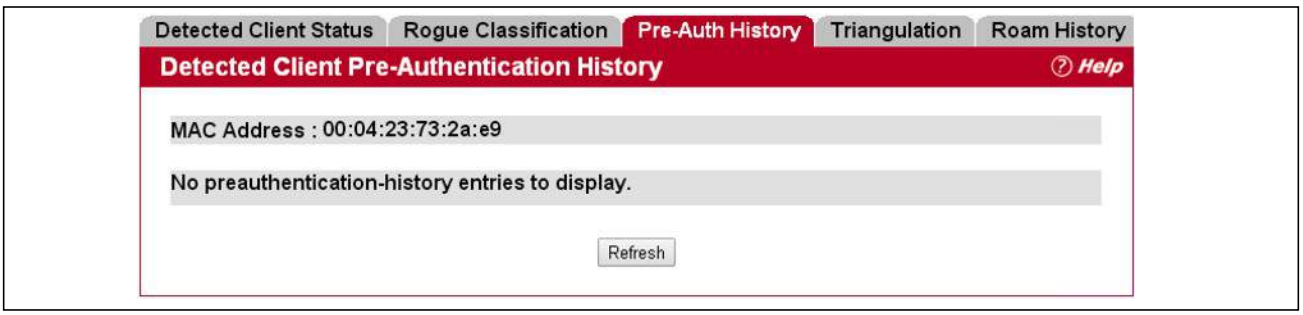


Figure 208: Detected Client Pre-Authentication History

The following table describes the fields on the **Detected Client Pre-Authentication History** page.

Table 196: Detected Client Pre-Authentication History

Field	*Description*
MAC Address	MAC address of the client.
AP MAC Address	MAC Address of the managed AP to which the client has pre-authenticated.
Radio Interface Number	Radio number to which the client is authenticated, which is either Radio 1 or Radio 2.
VAP MAC Address	VAP MAC address to which the client roamed.
SSID	SSID Name used by the VAP.
Age	Time since the history entry was added.
User Name	Indicates the user name of client that authenticated via 802.1X.
Pre-Authentication Status	Indicates whether the client successfully authenticated and shows a status of Success or Failure.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Detected Client Triangulation

The **Detected Client Triangulation** page lists up to three non-sentry and three sentry managed APs that have detected the client. The signal strength reported by the APs can help triangulate the location of the client. Since an AP can have one radio configured in sentry mode and another radio configured in non-sentry mode, the same AP might appear in both lists. If the AP or the Client has not been detected by three APs, the list can contain zero, one or two entries.

To open the Triangulation page, click **WLAN** > **Intrusion Detection** > **Detected Clients**. Click one of the MAC Addresses on **Detected Client Status** page, and then click the **Triangulation** tab.

Clicking an entry in the MAC Address field displays information described in the "Viewing Detailed Managed Access Point Status" on page 308

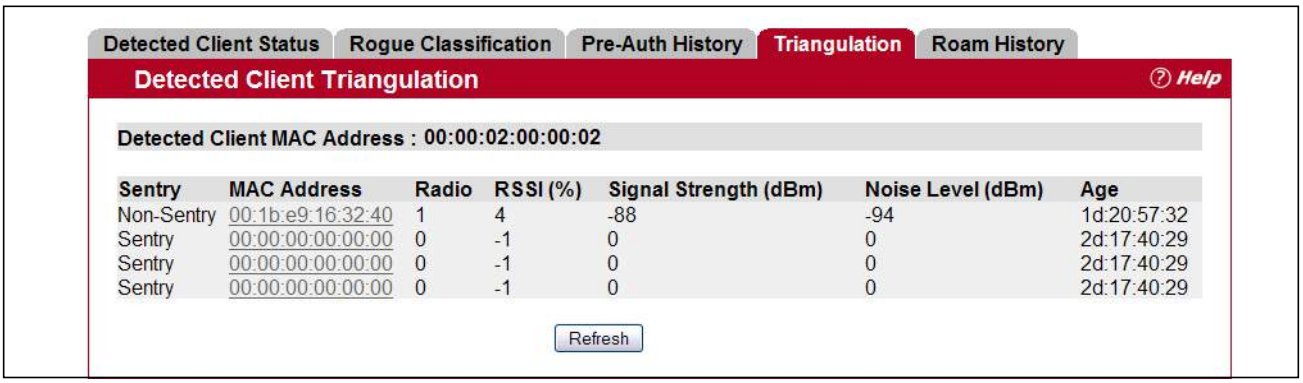


Figure 209: Detected Client Triangulation

The following table describes the fields on the **Detected Client Triangulation** page.

Table 197: Detected Client Triangulation

Field	*Description*
Detected Client MAC Address	MAC address of the client.
Sentry	Identifies whether the radio that detected the client is in sentry or non-sentry mode. • Non-Sentry: The radio that detected the client is not configured in sentry mode. This means the radio can accept connections from wireless clients and send and receive traffic • Sentry: The radio that detected the client is configured in sentry mode. Networks that deploy sentry APs or radios can detect devices on the network quicker and perform more thorough security analysis.
MAC Address	MAC Address of the managed AP that detected the client.
Radio	Radio number to which the client is authenticated, which is either Radio 1 or Radio 2.
RSSI	Received signal strength indicator in terms of percentage for the non-sentry AP. The range is 0–100, where the maximum value is 100. A value of 0 indicates that the client is not detected.
Signal Strength	Received signal strength in dBm. The possible range is –127 to 127. However, realistically, this value is expected to range from –95 to –10.
Noise Level	Noise reported on the channel by the non-sentry AP. The possible range is –127 to 127.

Table 197: Detected Client Triangulation (Cont.)

Field	*Description*
Age	Time since this AP detected the signal.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Detected Client Roam History

The wireless system keeps a record of clients as they roam from one managed AP to another managed AP. A history of up to 10 APs is kept for each client.

To open the Roam History page, click **WLAN** > **Intrusion Detection** > **Detected Clients**. Click one of the MAC Addresses on **Detected Client Status** page, and then click the **Roam History** tab. The **Detected Client Roam History** page shows the managed APs with which the client has associated. The first entry in the client list is the oldest. After the list fills up, the oldest entry is deleted and all other entries are moved one slot up.

Figure 210: Detected Client Roam History

The following table describes the fields on the **Detected Client Roam History** page.

Table 198: Detected Client Roam History

Field	*Description*
MAC Address	MAC address of the detected client.
AP MAC Address	MAC Address of the managed AP to which the client authenticated.
Radio Interface Number	Radio Number to which the client is authenticated.
VAP MAC Address	VAP MAC address to which the client roamed.
SSID	SSID Name used by the VAP.
New Authentication	A flag indicating whether the history entry represents a new authentication or a roam event.
Age	Time since the history entry was added.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Detected Client Pre-Authentication Summary

To help authenticated clients roam without losing sessions and needing to re-authenticate, wireless clients can attempt to authenticate to other APs within range that the client could possibly associate with. For successful pre-authentication, the target AP must have a VAP with an SSID and security configuration that matches that of the client, including MAC authentication, encryption method, and pre-shared key or RADIUS parameters. The the AP that the client is associated with captures all pre-authentication requests and sends them to the switch.

To open this page, click the **WLAN** > **Intrusion Detection** > **Detected Clients** > **Pre -Authentication History Summary** tab. The **Detected Client Pre-Authentication History Summary** page lists detected clients that have made pre-authentication requests and identifies the APs that have received the requests.

Figure 211: Detected Client Pre-Authentication History Summary

The following table describes the fields on the **Detected Client Pre-Authentication History Summary** page.

Table 199: Detected Client Pre-Authentication History Summary

Field	*Description*
MAC Address	MAC address of the client.
AP MAC Address	MAC Address of the managed AP to which the client has pre-authenticated. This field can show a history of up to ten pre-authentications for each client.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Detected Client Roam History Summary

The wireless system keeps a record of clients as they roam from one managed AP to another managed AP. A history of up to 10 APs is kept for each client.

To open this page, click the **WLAN** > **Intrusion Detection** > **Detected Clients** > **Roam History Summary** tab. The **Detected Client Roam History Summary** page lists each client that has roamed from at least one AP and provides information about the roaming history.

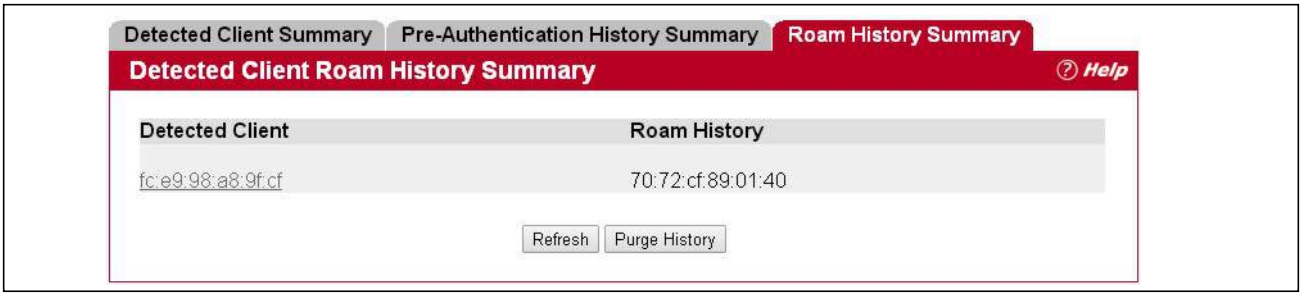


Figure 212: Detected Client Roam History Summary

The following table describes the fields on the **Detected Client Roam History Summary** page.

Table 200: Detected Client Roam History

Field	*Description*
Detected Client	MAC address of the detected client.
Roam History	MAC Address of the managed AP to which the client authenticated. This field lists the MAC address of the last 10 APs to which the client has roamed and authenticated.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Ad Hoc Client Status

An ad hoc client is a wireless client that gains access to the WLAN through a wireless client that is associated with an access point. The ad hoc client does not communicate directly with the AP. Ad hoc networks are a particular concern because they consume RF bandwidth and can present a security risk.

From the **WLAN** > **Intrusion Detection** > **Ad Hoc Clients** page, you can view and manage wireless clients that are connected to the WLAN through an ad hoc network.

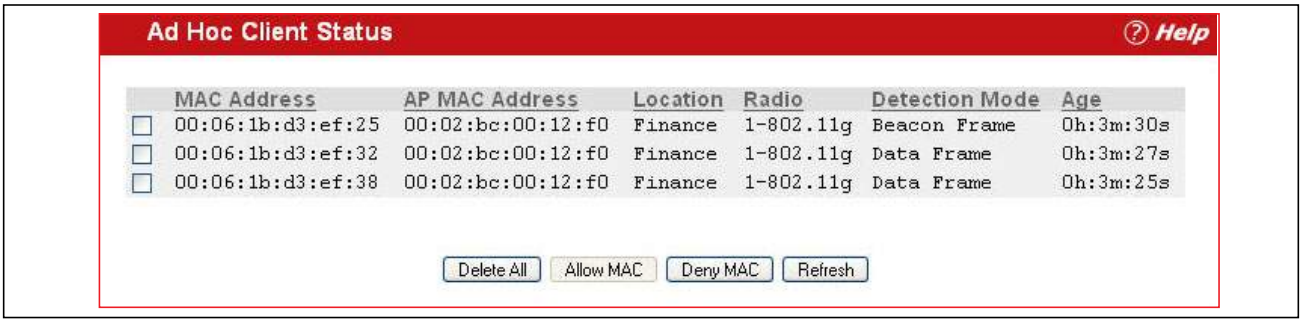


Figure 213: Ad Hoc Clients

To view or configure the default action specified for a wireless client (Allow, Deny, or Global Action), go to the **WLAN** > **WLAN Configuration > Known Client** page and click the MAC address of the client to view or configure.

The switch does not remove MAC entries from this list even when a client successfully authenticates with an AP. The historical ad hoc data gives you more time to take action against clients that establish ad hoc networks on the WLAN.

Table 201: Ad Hoc Client Status

Field	*Description*
MAC Address	The Ethernet address of the client. If the Detection Mode is Beacon then the client is represented as an AP in the RF Scan database and the Neighbor AP List. If the Detection Mode is Data Frame then the client information is in the Neighbor Client List.
AP MAC Address	The base Ethernet MAC Address of the managed AP which detected the client.
Name	The configured descriptive location for the managed AP.
Radio	The radio interface and its configured mode that detected the ad hoc device.
Detection Mode	The mechanism of detecting this Ad Hoc device. The possible values are Beacon Frame or Data Frame.
Age	Time since last detection of the ad hoc network.

Command Buttons

The page includes the following buttons:

- **Delete All**—Deletes all ad hoc client entries from the list.

Note: Clearing the list does not disassociate any of the ad hoc clients, and the clients might still be involved in the ad hoc network.

- **Deny**—Blocks an ad hoc client from WLAN access. The MAC address is added to the Known Client database where the default action is Deny.
- **Allow**—Allows an ad hoc client access to the WLAN. The MAC address is added to the Known Client database where the default action is Allow.
- **Refresh**—Updates the page with the latest information.

Note: If the **Deny** button is not available, it means all profiles use Allow as the default MAC Authentication action. Likewise, if the **Allow** button is not available, no profiles have an Allow default action.

Note: If you use RADIUS for MAC authentication in one or more AP profiles, you must add the MAC Address of the client to the RADIUS database.

Access Point Authentication Failure Status

An AP might fail to associate to the switch due to errors such as invalid packet format or vendor ID, or because the AP is not configured as a valid AP with the correct local or RADIUS authentication information.

To view a list of APs that failed to associate with the UWS, click **WLAN** > **Intrusion Detection** > **AP Authentication Failures**.

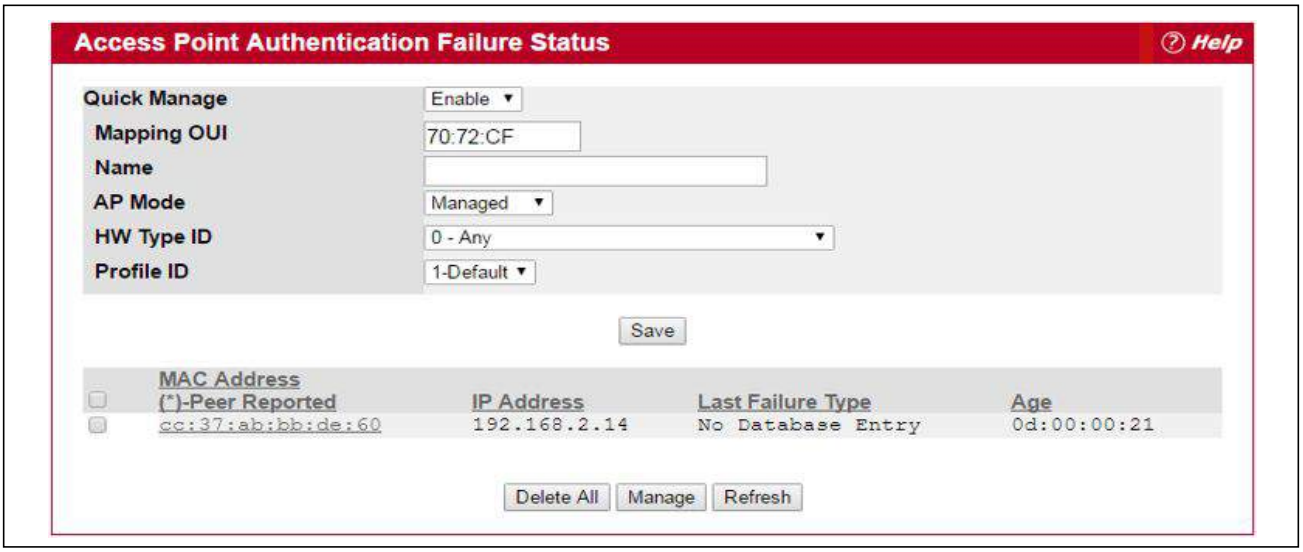


Figure 214: AP Authentication Failure Status

The AP authentication failure list shows information about APs that failed to establish communication with the UWS. The AP can fail due to one of the following reasons:

- No Database Entry—The MAC address of the AP is not in the local Valid AP database or the external RADIUS server database, so the AP has not been validated.
- Local Authentication—The authentication password configured in the AP did not match the password configured in the local database.

- Not Managed — The AP is in the Valid AP database, but the AP Mode in the local database is not set to Managed.
- RADIUS Authentication — The password configured in the RADIUS client for the RADIUS server was rejected by the server.
- RADIUS Challenged — The RADIUS server is configured to use the Challenge-Response authentication mode, which is incompatible with the AP.
- RADIUS Unreachable — The RADIUS server that the AP is configured to use is unreachable.
- Invalid RADIUS Response — The AP received a response packet from the RADIUS server that was not recognized or invalid.
- Invalid Profile ID — The profile ID specified in the RADIUS database may not exist on the switch. This can also happen with the local database when the configuration has been received from a peer switch.
- Profile Mismatch-Hardware Type — The AP hardware type specified in the AP Profile is not compatible with the actual AP hardware.
- AP Image Not Available — The switch does not have an appropriate image available to deploy to the AP. This error is valid only when the switch supports the Auto AP image upgrade and the Auto image upgrade mode is enabled.

If you use the local database for AP Validation, you can click the **WLAN > WLAN Configuration > Loc AP Database** tab to modify the AP configuration. If you use a RADIUS server for AP validation, you must add the MAC address of the AP to the RADIUS server database.

Click the MAC address of the AP to view more information about the AP. If the AP is not a Edge-Core AP, some values are unknown.

Table 202: Access Point Authentication Failure Status

Field	*Description*

Quick Manage	This feature configures settings for matching APs, allowing any AP with a matching OUI to be managed by the AC. APs with authenticated failure attempts will become managed and entered as valid entries into the local AP database. The parameters configured by this feature include:
	• **Quick Manage** — Enable this feature to use quick manage.
	• **Mapping OUI** — The OUI to automatically add to the local AP database.
	• **Name** — Enter a name to help identify the AP. This field is optional and accepts up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted.
	• **AP Mode** — You can configure the AP to be in one of three modes, although in Quick Manage AC/AP solution, the AP mode should be set to Managed Mode only:
	  • Standalone: The AP acts as an individual access point in the network. You do not manage the AP by using the wireless controller. Instead, you log into the AP itself and manage it by using the Administrator Web User Interface, CLI or SNMP.
	  • Managed: The AP is part of the Unified Wireless Switch, and you manage it by using the wireless controller. If an AP is in Managed Mode, the Administrator Web UI and SNMP services on the AP are disabled.
	  • Rogue: Select Rogue as the AP mode if you want to be notified (through an SNMP trap, if enabled) when this AP is detected in the network. Additionally, when this AP is detected through an RF scan, the status is listed as Rogue.
	• **HW Type ID** — This is the hardware type to use for APs entered in the binding profile. The hardware type is determined, in part, by the number of radios the AP supports (single or dual) and the IEEE 802.11 modes that the radio support (a/b/g or a/b/g/n or a/ac/b/g/n). The mismatch of an AP's hardware type would result in failure to add this particular AP to local AP database as a valid AP.
	• **Profile ID** — The profile bound to an AP when the OUI portion of the AP MAC matches the mapping OUI. Any unauthenticated AP with a matching OUI will automatically be registered as a valid entry in the local AP database. APs that use the same profile should have the same hardware capabilities so that the settings configured in this profile are valid for all APs within the profile.

MAC Address	The Ethernet address of the AP. If the MAC address of the AP is followed by an asterisk (*), it was reported by a peer switch.
IP Address	The IP address of the AP.

Table 202: Access Point Authentication Failure Status (Cont.)

Field	*Description*
Last Failure Type	Indicates the last type of failure that occurred, which can be one of the following: • Local Authentication • No Database Entry • Not Managed • RADIUS Authentication • RADIUS Challenged • RADIUS Unreachable • Invalid RADIUS Response • Invalid Profile ID • Profile Mismatch-Hardware Type • AP Image Not Available (This status is applicable only when the Integrated AP Code Image is supported by the platform).
Age	Time since failure occurred.

Enabling Quick Manage

To enable Quick Manage, click WLAN > Intrusion Detection > AP Authentication Failures, and take the following steps:

1. Select “Enable” to activate Quick Manage.
2. Enter the OUI of the AP manufacturer which can be automatically added to the local AP database at any attempt to discover then by wireless controller.
3. Enter the AP location. (Optional)
4. Set the AP Mode to “Managed” so that any AP with the correct OUI can be managed by wireless controller.
5. Select the appropriate HW Type ID from the drop-down list to which the AP is assigned.
6. Select the profile to which the managed AP is assigned when Quick Manage enters the AP as a valid entry in the local AP database.
7. Click “Save” to make the settings take effect immediately.

Command Buttons

The page includes the following buttons:

- **Delete All**—Removes the entries for all APs from the failure list.
- **Manage**—Adds the selected AP from the Access Point Failure list to the Valid AP database.
- **Refresh**—Updates the page with the latest information.

To view additional data (beacon information) for an AP in the authentication failure list, you can search for the MAC address of the failed AP on the Rogue/RF Scan page. However, some APs that attempt to contact the switch on the

wired network might not be detected during the RF scan. To view detailed information about the failure status of an AP, click on a MAC address. The following page is displayed.

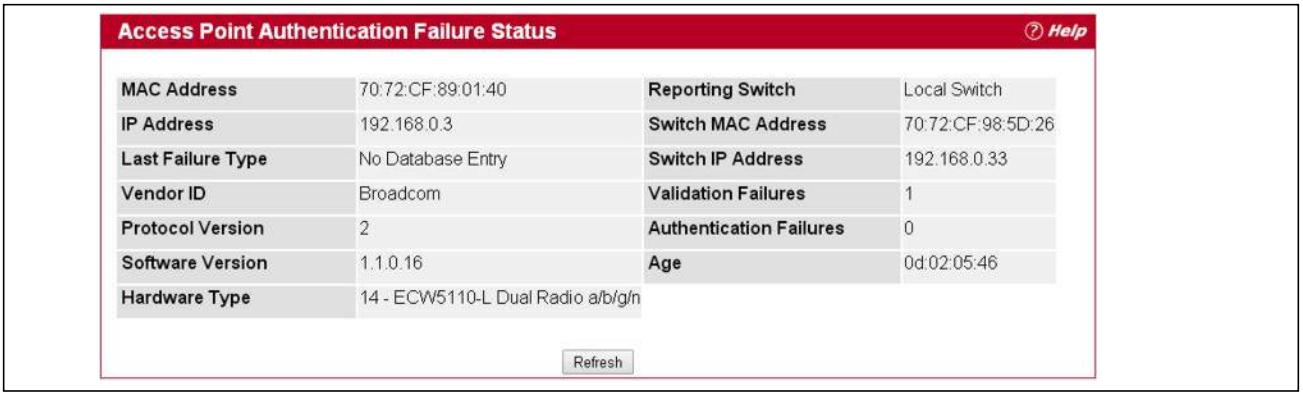


Figure 215: AP Authentication Failure Details

The following table describes the fields on the detailed **Access Point Authentication Failure Status** page.

Table 203: Access Point Authentication Failure Details

Field	*Description*
MAC Address	The Ethernet address of the AP.
IP Address	The network IP address of the AP.
Last Failure Type	Indicates the last type of failure that occurred, which can be one of the following: • Local Authentication • No Database Entry • Not Managed • RADIUS Authentication • RADIUS Challenged • RADIUS Unreachable • Invalid RADIUS Response • Invalid Profile ID • Profile Mismatch-Hardware Type • AP Image Not Available (This status is applicable only when the Integrated AP Code Image is supported by the platform).
Vendor ID	Vendor of the AP software.
Protocol Version	Indicates the protocol version supported by the software on the AP.
Software Version	Indicates the version of software on the AP.
Hardware Type	Hardware platform for the AP.
Reporting Switch	Shows whether the switch that reported the AP authentication failure is the local switch or a peer switch.
Switch MAC Address	Shows the IP address of the switch in the cluster that reported the AP authentication failure.
Switch IP Address	Shows the MAC address of the switch in the cluster that reported the AP authentication failure.

Table 203: Access Point Authentication Failure Details (Cont.)

Field	*Description*
Validation Failures	The count of association failures for this AP.
Authentication Failures	The count of authentication failures for this AP.
Age	Time since failure occurred.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

AP De-Authentication Attack Status

The **AP De-Authentication Attack Status** page contains information about rogue APs that the Cluster Controller has attacked by using the de-authentication attack feature.

The wireless switch can protect against rogue APs by sending de-authentication messages to the rouge AP. The de-authentication attack feature must be globally enabled in order for the wireless system to do this function. Make sure that no legitimate APs are classified as rogues before enabling the attack feature. This feature is disabled by default.

The wireless system can conduct the de-authentication attack against 16 APs at the same time. The intent of this attack is to serve as a temporary measure until the rogue AP is located and disabled.

The de-authentication attack is not effective for all rogue types, and therefore is not used on every detected rogue. The following rogues are not subjected to the attack:

- If the detected rogue is spoofing the BSSID of the valid managed AP then the wireless system does not attempt to use the attack because that attack may deny service to a legitimate AP and provide another avenue for a hacker to attack the system.
- The de-authentication attack is not effective against Ad hoc networks because these networks do not use authentication.
- The APs operating on channels outside of the country domain are not attacked because sending any traffic on illegal channels is against the law.

The wireless switch maintains a list of BSSIDs against which it is conducting a de-authentication attack. The switch sends the list of BSSIDs and channels on which the rogue APs are operating to every managed AP.

To open this page, click **WLAN** > **Intrusion Detection** > **AP De-Auth Attack Status**, and then click the MAC address of an AP in the list to access detailed RF Scan information for the AP.

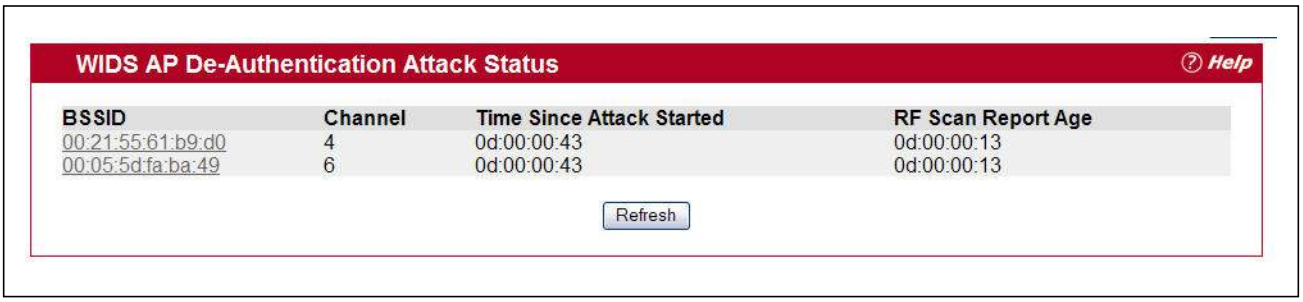


Figure 216: AP De-Authentication Attack Status

The following table describes the fields on the **AP De-Authentication Attack Status** page.

Table 204: AP De-Authentication Attack Status

Field	*Description*
BSSID	Shows the BSSID of the AP against which the attack is launched. The BSSID is a MAC address.
Channel	Identifies the channel on which the rogue AP is operating.
Time Since Attack Started	Shows the amount of time that has passed since the attack started on the AP.
RF Scan Report Age	Shows the amount of time that has passed since the RF Scan reported this AP.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

WDS Configuration

The Wireless Distribution System (WDS)-Managed AP feature allows you to add managed APs to the cluster using over-the-air WDS links through other managed APs. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required. With WDS, APs may be located outdoors where wired connection to the data network is unavailable, or in remote buildings that are not connected to the main campus with a wired network.

The WDS AP group consists of the following managed APs:

- Root AP—Acts as a bridge or repeater on the wireless medium and communicates with the switch via the wired link
- Satellite AP—Communicates with the switch via a WDS link to the Root AP

The WDS links are secured using WPA2 Personal authentication and AES encryption.

Each WDS-Managed AP group can contain up to 16 APs that are connected to each other. The WDS AP Group can have any number of Root APs and Satellite APs as long as the total number of APs is less than or equal to 16. You can configure up to eight WDS AP groups, but an AP can be a member of only one WDS AP Group.

Before an AP can be attached to the Wireless System as a Satellite AP, you might need to configure the following settings on the AP while it is in Standalone mode:

- Satellite AP mode. This setting enables the Satellite AP to discover and establish WDS link with the Root AP.
- Password for WPA2 Personal authentication used to establish the WDS links. Only the Satellite APs need this configuration. The Root APs get the password from the switch when they become managed.

Caution! Certain topologies for WDS managed APs can result in unpredictable behavior. For example, if a satellite AP has the Ethernet port enabled and has a wired connection to a switch that manages the same WDS group, the satellite AP cannot determine which path to establish a management connection on because spanning tree is not yet functional. A satellite AP, by definition, should have a connection to the managed switch only over the air. Otherwise, it is considered a root AP (if it is part of a WDS managed group). If there are multiple wireless paths from an AP to the managed switch, spanning tree for the WDS group must be enabled to prevent loops.

WDS Managed AP Group Configuration

Use the WDS Managed AP Group Configuration page to add or delete WDS-Managed AP groups and to configure group settings. Changes to the WDS AP Group do not take effect on the APs until the WDS AP Group database is pushed to the cluster. Use the Push Config button to ensure the changes you make are applied to the switches and APs in the cluster. APs that become managed after the WDS AP Group database is pushed to the cluster pick up the configuration.

Note: To ensure that the network is operating as intended, always push the configuration after making all desired changes to the WDS AP Group.

To open the WDS Managed AP Group Configuration page, click **WLAN** > **WDS Configuration** > **Group Configuration**.

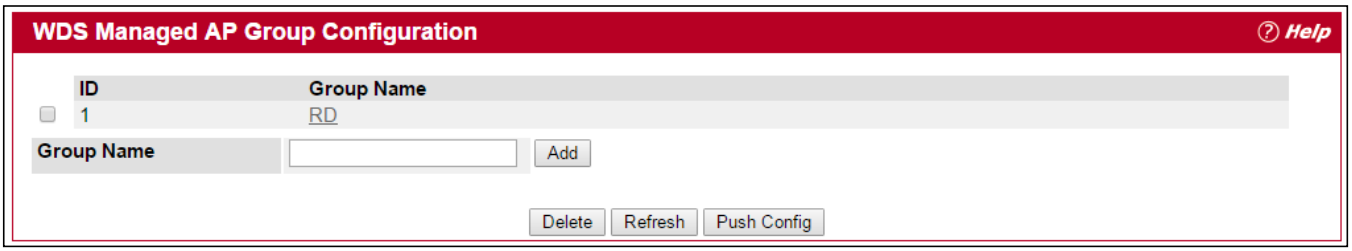


Figure 217: WDS Managed AP Group Configuration

The following table describes the fields on the **WDS Managed AP Group Configuration** page.

Table 205: WDS Managed AP Group Configuration

Field	*Description*
ID	A number from 1–8 that identifies the WDS AP group. This number is automatically assigned when you create the group.
Group Name	A descriptive name of the WDS AP group, which can contain up to 32 characters.

Command Buttons

The page includes the following button:

- **Add**—Adds the group with the name entered into the field.
- **Delete**—Deletes the selected group.
- **Refresh**—Updates the page with the latest information.
- **Push Config**—Pushes the WDS-Managed AP group information to all switches that are members of the cluster.

To show detailed information for a group entry in the WDS Managed AP Group Configuration page, click on an entry in the Group Name field.

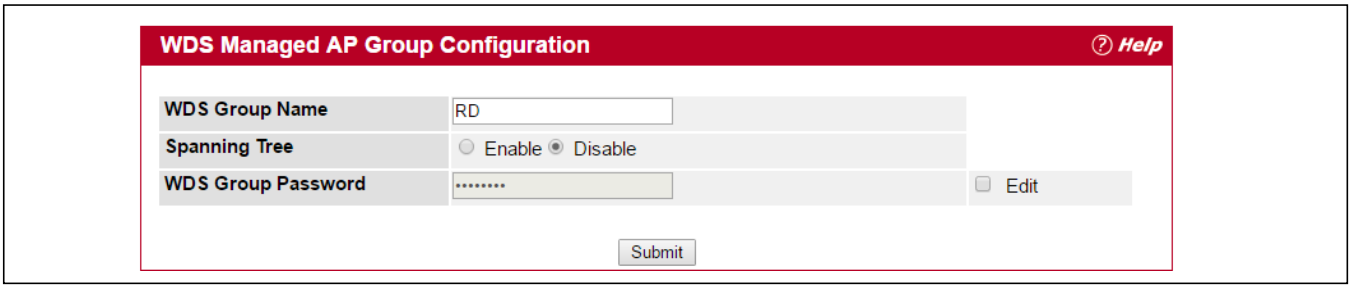


Figure 218: WDS Managed AP Group Configuration (Detailed Information)

The following table describes the detailed information fields for a group entry in the **WDS Managed AP Group Configuration** page.

Table 206: WDS Managed AP Group Configuration (Detailed Information)

Field	*Description*
WDS Group Name	A descriptive name of the WDS AP group, which can contain up to 32 characters. From this field, you can modify the name of an existing group, if desired.
Spanning Tree	Specifies whether to enable spanning tree on all APs in this WDS AP Group. Spanning tree must be enabled if there are any potential loops in the network. For example if a Satellite AP has links to two Root APs then spanning tree must be enabled. **Note**: The spanning tree protocol running on the APs interacts with the spanning tree protocol running on the edge switches to which the APs are connected.
WDS Group Password	Password used for securing the WPA2-Personal security on the WDS Link. Range: 8–63 ASCII characters. To create or change the password, select the Edit checkbox and type a password in the available field. This password must match the passwords set on the Satellite APs in this group. By default, the password is AP-Group-n, where n is the AP group ID.

Command Buttons

The page includes the following buttons:

- **Apply**—Updates the switch with the values you enter.

WDS Managed AP Configuration

After you create a WDS-Managed AP group, use the **WDS Managed AP Configuration** page to view the APs that are members of the group, add new members, and change STP Priority values for existing members.

Note: After you change WDS-Managed AP group settings, make sure you push the configuration to other switches in the cluster.

To open the WDS Managed AP Configuration page, click **WLAN** > **WDS Configuration** > **AP Configuration**.

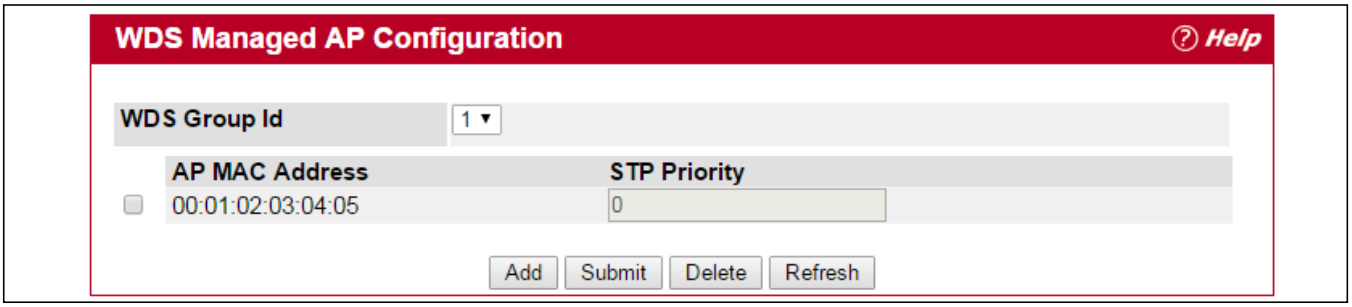


Figure 219: WDS Managed AP Configuration

The following table describes the fields on the **WDS Managed AP Configuration** page.

Table 207: WDS Managed AP Configuration

Field	*Description*
WDS Group ID	Select the ID associated with the group to configure.
AP MAC Address	MAC Address of the AP.
STP Priority	Spanning Tree Priority for this AP. The STP priority is used only when spanning tree mode is enabled. The STP priority determines which AP is selected as the root of the spanning tree and which AP has preference over another AP when multiple equal cost paths exist in the topology. A lower value for the spanning tree priority means that the AP is more likely to be used for bridging data into the campus network. You should assign a lower priority to the APs connected to the wired network than to the Satellite APs. The STP priority value is rounded down to a multiple of 4096. The range is 0–61440, and the default value is 36864.

The page includes the following buttons:

- **Add**—Allows you to configure a new AP for the selected group. When you click **Add**, the **WDS Managed AP Group Configuration** page displays.
- **Apply**—Select the checkbox associated with an AP to modify the STP Priority value for the AP. Click **Apply** to update the switch with the values you enter.
- **Delete**—Deletes the selected AP.
- **Refresh**—Updates the page with the latest information.

WDS AP Link Configuration

After you create a WDS-Managed AP group, use the **WDS AP Link Configuration** page to configure the WDS links between the APs that are members of the group.

Note: After you change WDS-Managed AP group settings, make sure you push the configuration to other switches in the cluster.

To open the WDS Managed AP Configuration page, click **WLAN** > **WDS Configuration** > **Link Configuration**.

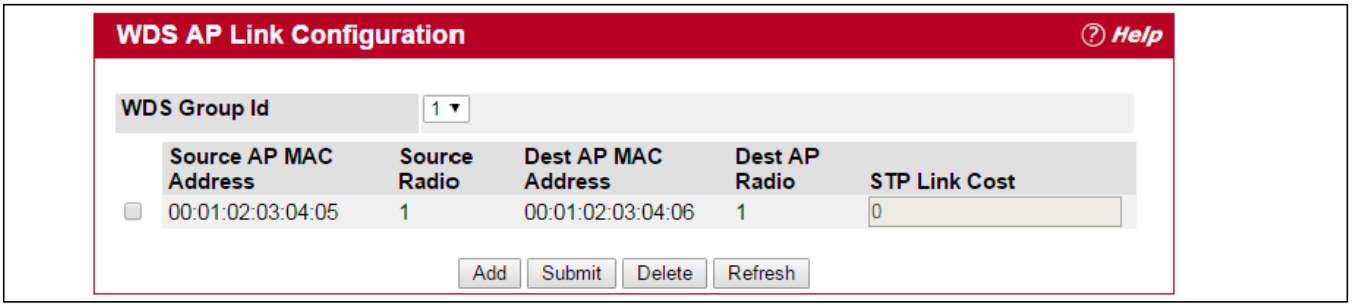


Figure 220: WDS AP Link Configuration

The following table describes the fields on the **WDS Managed AP Configuration** page.

Table 208: WDS Managed AP Configuration

Field	*Description*
WDS Group ID	Select the ID associated with the group to configure.
Source AP MAC Address	MAC Address of the source AP. **Note**: The WDS links are bidirectional. The terms Source and Destination simply reflect the WDS link endpoints specified when the WDS link is created.
Source Radio	The radio number of the WDS link endpoint on the source AP.
Dest AP MAC Address	The MAC address of the destination AP in the group.
Dest AP Radio	The radio number of the WDS link endpoint on the destination AP.
STP Link Cost	Spanning Tree Path cost for the WDS link. The range is 0–255. When multiple alternate paths are defined in the WDS group, the link cost is used to indicate which links are the primary links and which links are the secondary links. The spanning tree selects the path with the lowest link cost.

Appendix A: Configuring Root/Satellite APs

To set up WDS Root/Satellite APs, both of which can be managed/provisioned by the controller, follow the information shown below:

1. Connect the AC to an AP (this is the root WDS AP).
2. Connect the WDS Root AP to the Satellite AP using the group password (this is the WPA password).

   Set the group password for the Root AP from the AC “WDS Managed AP Group Configuration” web page.

   Manually set the group password for the Satellite AP in advance from the Satellite AP's web interface. This means that you must set the Satellite AP to Satellite mode in advance.
3. Power on the WDS Root AP and Satellite WDS AP. From the AP web interface:

   WDS Root AP: Set the “WDS Managed Mode” to “Root AP.”

   WDS Satellite AP: Set the “WDS Managed Mode” to “Satellite AP.”

   WDS Satellite AP: Set the “WDS Group Password” using a string of 8-63 characters.
4. Power on the AC: After AC starts to manage the Root WDS AP, the Root WDS AP's group password will be provisioned from AC.

   When the Root WDS AP's Group Password has been provisioned from AC, the WDS Root AP will have a WDS link with Satellite WDS AP.

   The AC can now manage the Satellite AP. The AC can also provision the WDS Satellite AP.

   - 2.4GHz WDS is easy to establish even when the channel mode is set to “auto.” 5GHz WDS may be more difficult to connect when the channel is set to “auto.” You may need to use a fixed channel for band 1 (i.e., set ch36 to make WDS work on the 5GHz band).
   - Here are some examples for your reference with 1 Root AP, linking 1 satellite AP, all of which are managed by the controller.

1. WDS Configuration on Root-AP (ECW7220-L)

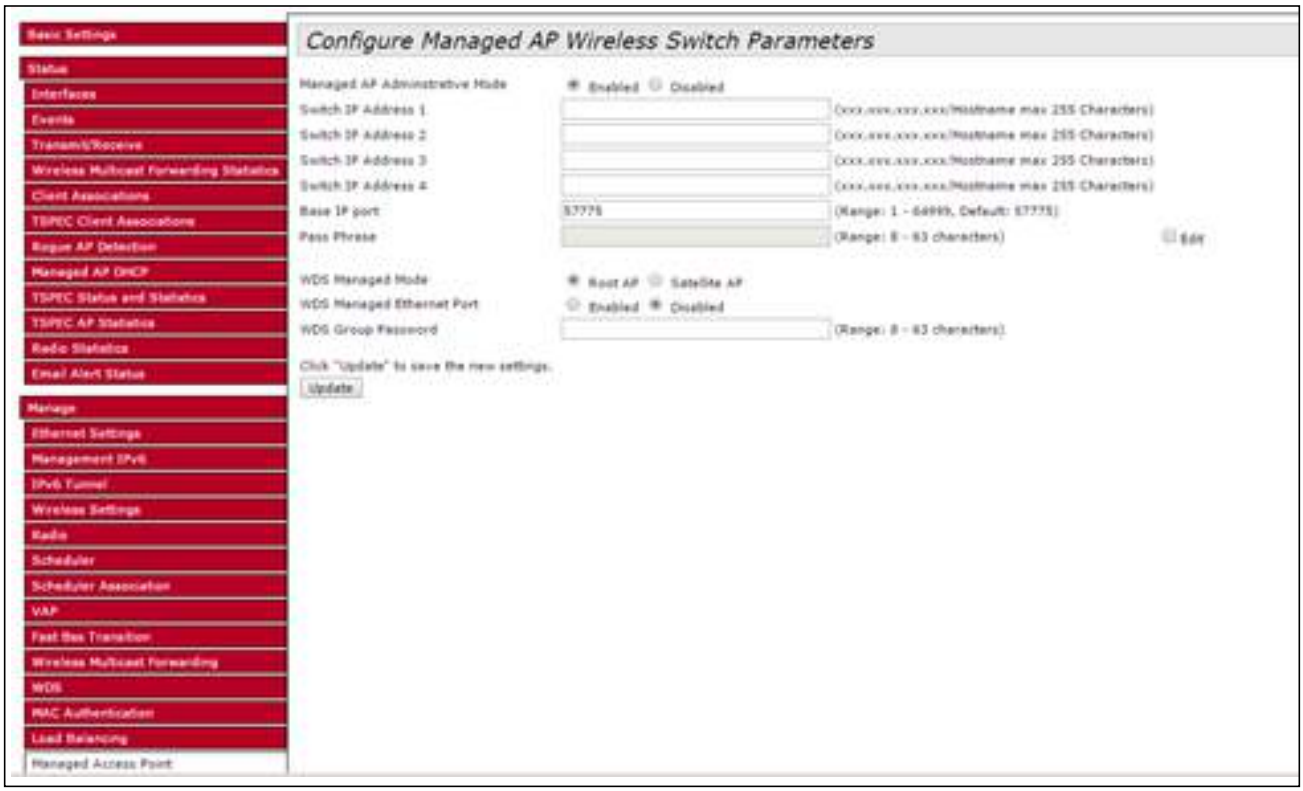


Figure 221: WDS Configuration on Root-AP

2. WDS Configuration on Satellite-AP (ECW7220-L)

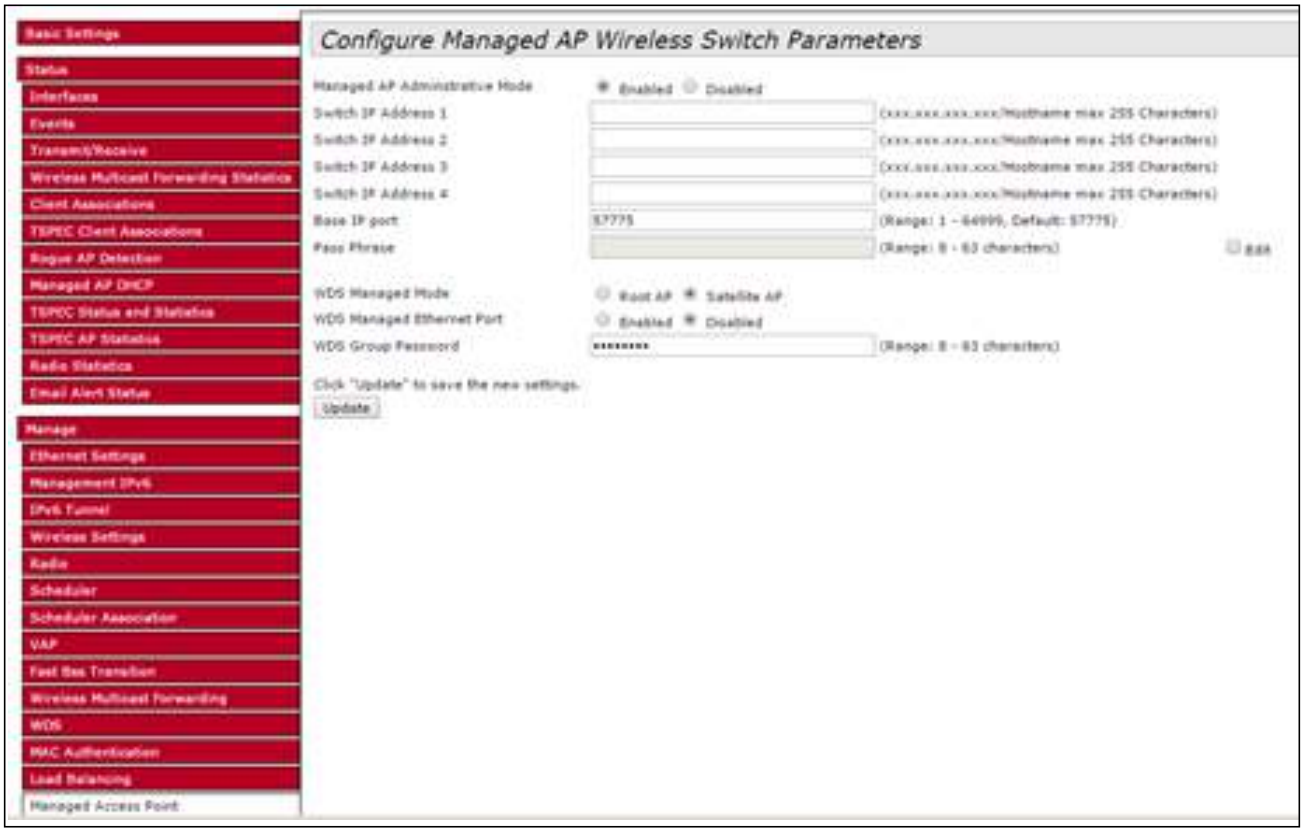


Figure 222: WDS Configuration on Satellite-AP

3. WDS AP Group Configuration on AC

3.1 WDS AP Group Configuration

Figure 223: WDS AP Group Configuration

3.1 WDS AP Group Configuration (after clicking on Group Name field)

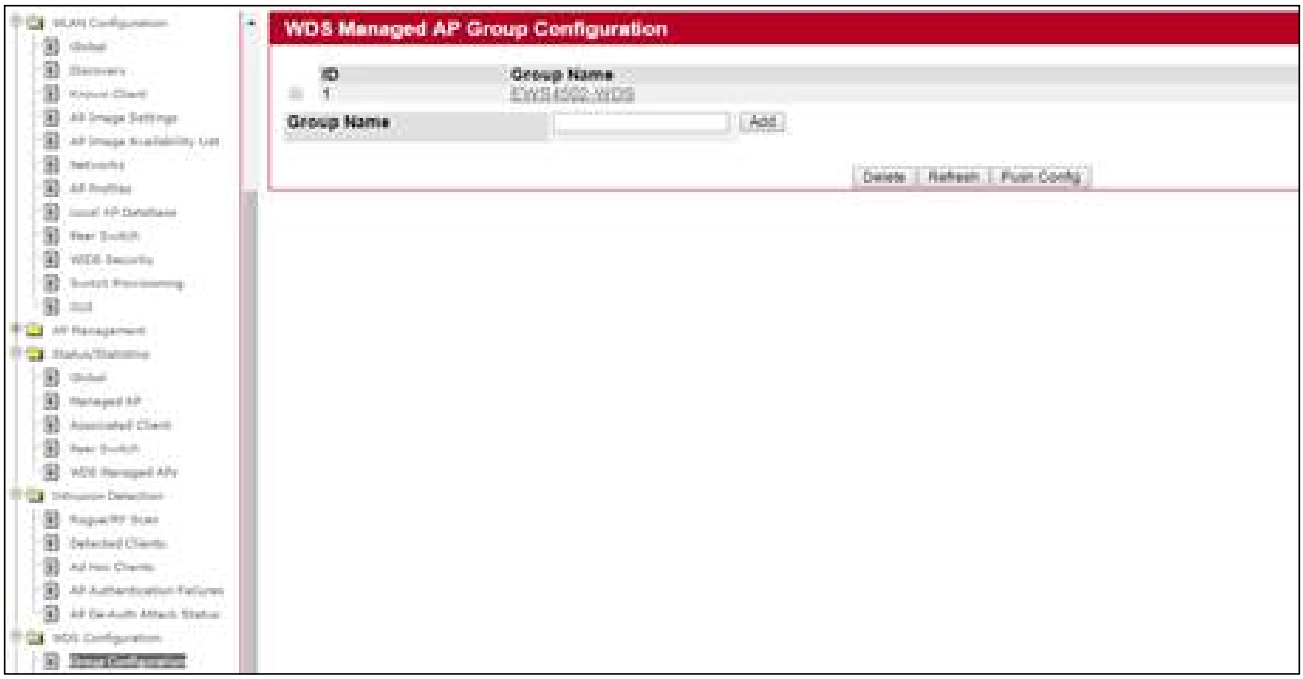


Figure 224: WDS AP Group Configuration(continued)

3.2 WDS Managed AP Configuration

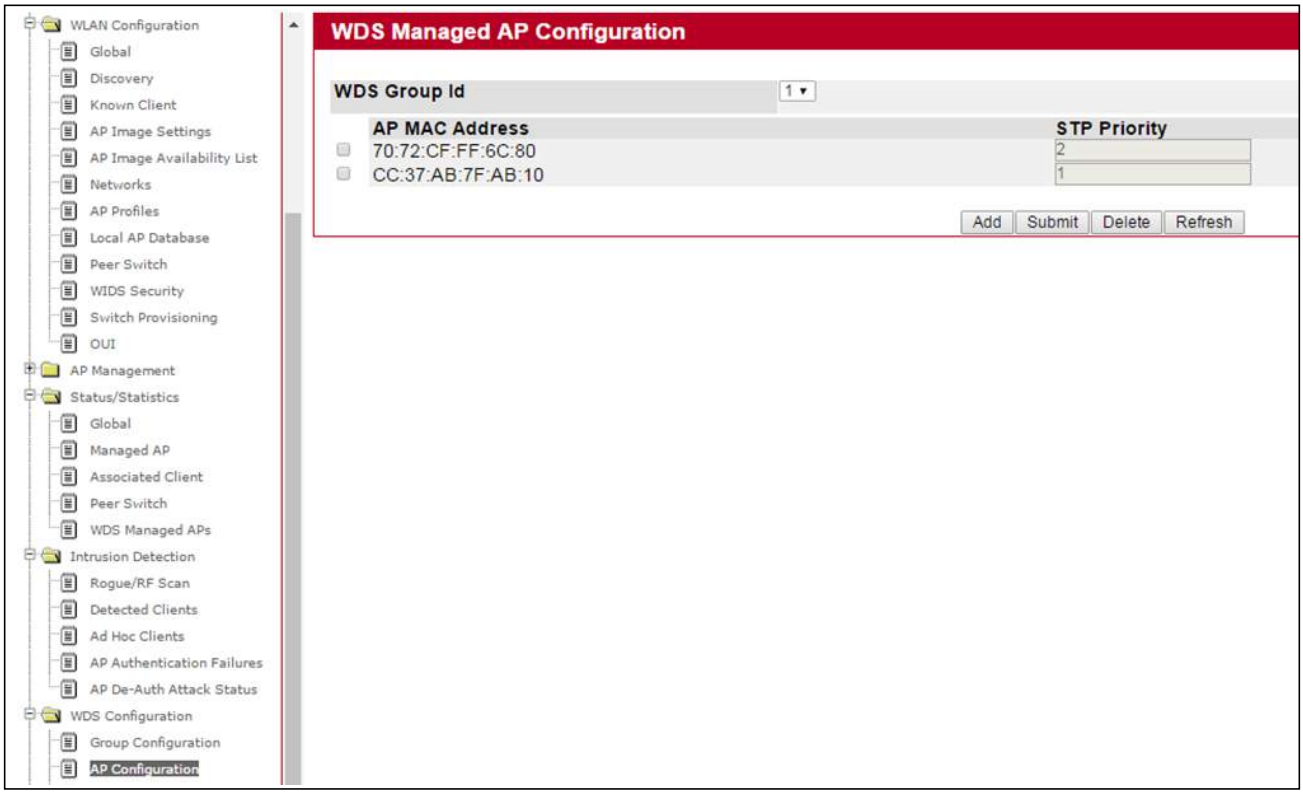


Figure 225: WDS Managed AP Configuration

3.3 WDS AP Link Configuration

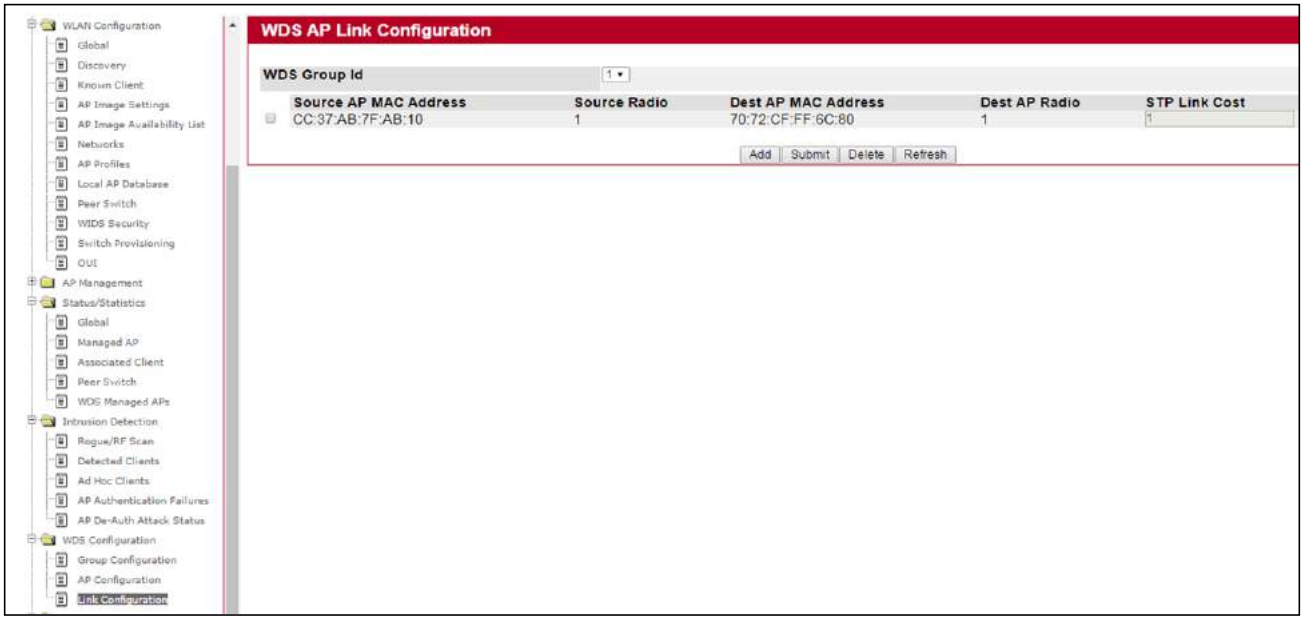


Figure 226: WDS AP Link Configuration

4. WDS Managed APs on AC

4.1 WDS AP Group Status Summary

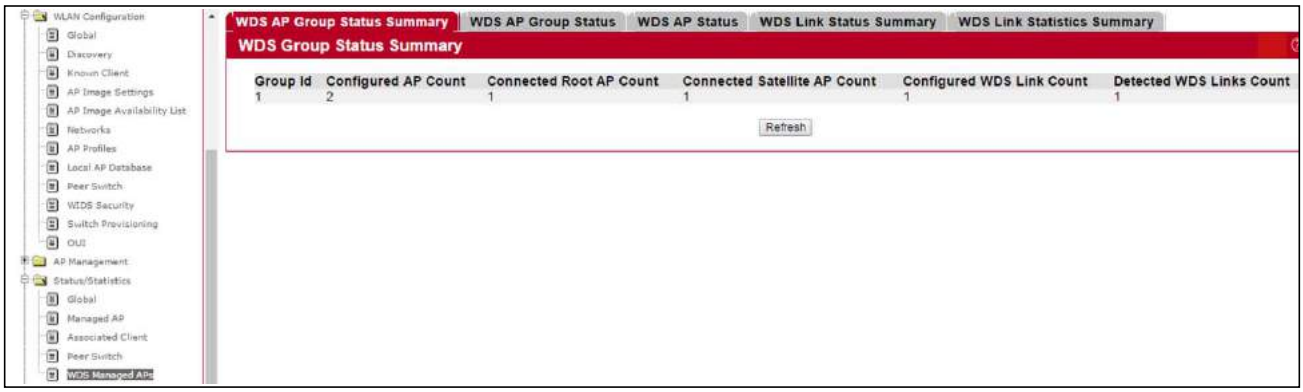


Figure 227: WDS Group Status Summary on AC

4.2 WDS AP Group Status

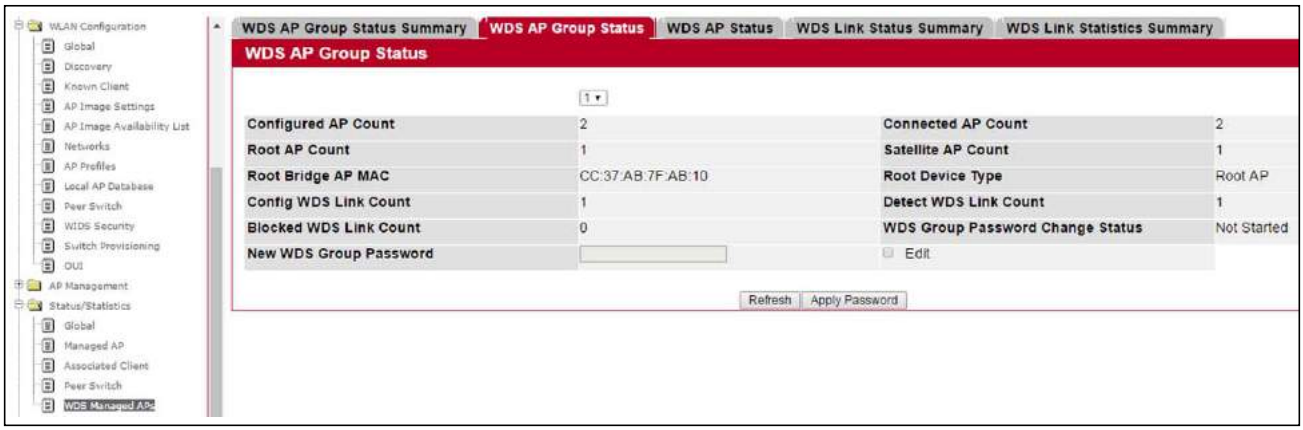


Figure 228: WDS AP Group Status

4.3 WDS AP Status

Figure 229: WDS AP Status

4.4 WDS AP Link Status Summary

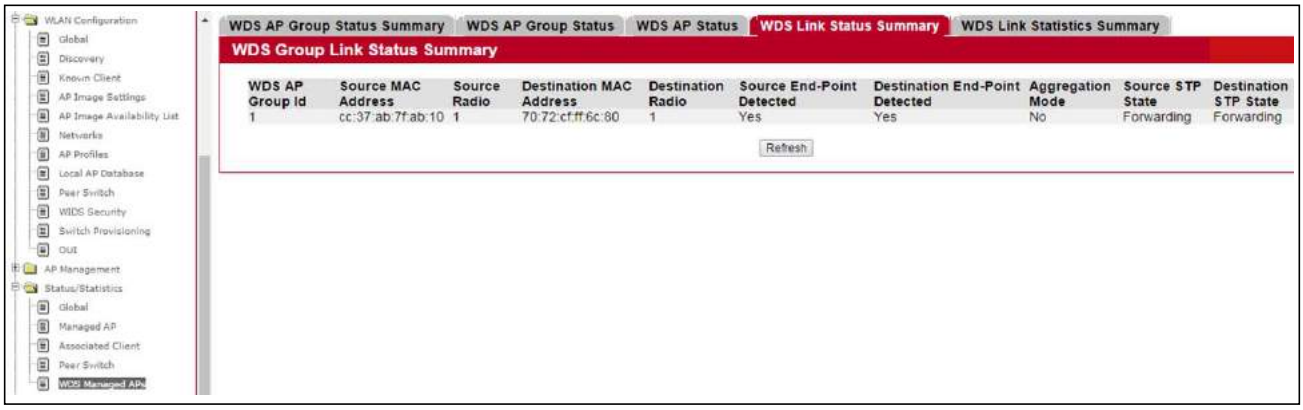


Figure 230: WDS AP Link Status Summary

4.5 WDS AP Link Statistics Summary

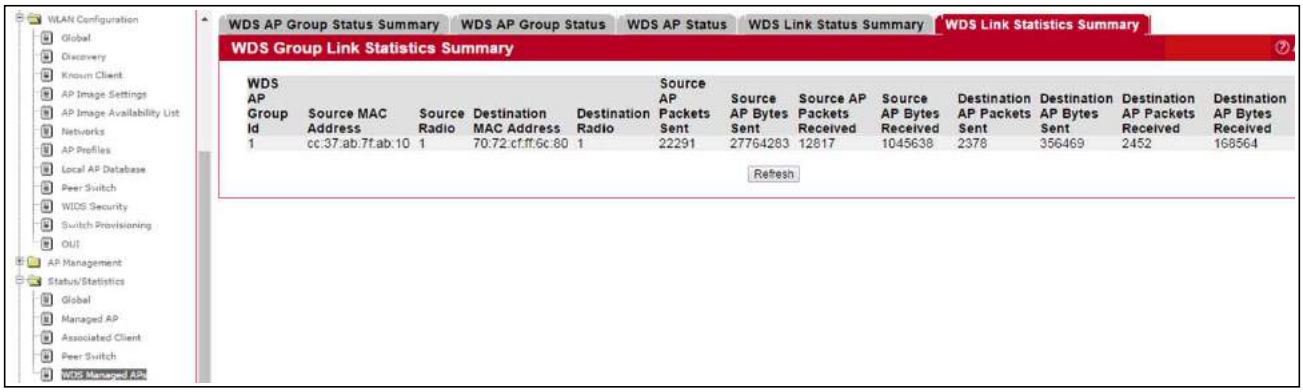


Figure 231: WDS AP Link Statistics Summary