



Cisco WAP125 Wireless-AC/N Dual Band Desktop Access Point with PoE Administration Guide

First Published: 2016-10-12

Last Modified: 2019-07-09

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.



The Java logo is a trademark or registered trademark of Sun Microsystems, Inc. in the U.S. or other countries.

© 2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Getting Started 1

- Getting Started with the Configuration 1
- Using the Access Point Setup Wizard 3
 - Using the Access Point Setup Wizard with mobile 4
- Changing Password 5
- TCP/UDP Service 6
- System Status 7
- Quick Start Configuration 7
- Window Navigation 8
 - Navigation Pane 9
 - Management Buttons 9

CHAPTER 2

Administration 11

- Firmware 11
 - Swapping the Firmware Image 11
 - HTTP/HTTPS Upgrade 12
 - TFTP Upgrade 12
- Reboot 13
 - Schedule Reboot 13
- Configuration Management 13
 - Backup Configuration Files 14
 - Download Configuration Files 14
 - Copying Configuration Files 15
 - Clearing Configuration Files 15

CHAPTER 3

System Configuration 17

LAN	17
IPv4 Configuration	17
DHCP Auto Configuration Settings	18
IPv6 Configuration	19
Port Settings	20
Spanning Tree Protocol	20
VLANs Setting	20
Neighbor Discover	21
LLDP	22
IPv6 Tunnel	22
Time	23
Automatically Acquiring the Time Settings through NTP	23
Manually Configuring the Time Settings	24
Notification	24
LED Display	24
Log Settings	25
Remote Log Server Table	26
View System Log	26
Email Alert/ Mail Server/ Message Configuration	27
Email Alert Examples	28
User Accounts	29
Adding a User	29
Changing a User Password	30
Management	30
System Settings	30
Connect Session Settings/HTTP/HTTPS Service	31
SSL Certificate File Status	32
SNMP / SNMPv2c Settings	33
SNMPv3 Views	34
SNMPv3 Groups	35
SNMPv3 Users	36
SNMPv3 Targets	37
Plug and Play (PnP)	38
Security	38

RADIUS Server	38
802.1x Supplicant	39
Rogue AP Detection	40
Viewing the Rogue AP List	41
Saving the Trusted AP List	42
Importing a Trusted AP List	42
Configure Password Complexity	43
Configure WAP-PSK Complexity	44

CHAPTER 4**Wireless 45**

Radio	45
Networks	50
Configuring VAPs	50
Configuring Security Settings	52
Client Filter	56
Configuring a Client Filter List Locally on the WAP device	56
Configuring MAC Authentication on the Radius Server	57
Scheduler	57
Scheduler Profile Configuration	57
Profile Rule Configuration	58
QoS	58

CHAPTER 5**Wireless Bridge 61**

Wireless Bridge	61
Configuring WDS Bridge	62
WPA/PSK on WDS Links	62
WorkGroup Bridge	63

CHAPTER 6**Fast Roaming 67**

Fast Roaming	67
Configuring Fast Roaming	67
Configuring Remote Key Holder List Profiles	68

CHAPTER 7**Access Control 71**

- ACL 71
 - IPv4 and IPv6 ACLs 71
 - Workflow to Configure ACLs 72
 - Configure IPv4 ACLs 72
 - Configure IPv6 ACLs 74
 - Configure MAC ACLs 77
- Client QoS 78
 - Configuring IPv4 Traffic Classes 79
 - Configuring IPv6 Traffic Classes 81
 - Configuring MAC Traffic Classes 83
 - QoS Policy 84
 - QoS Association 85
- Guest Access 86
 - Guest Access Instance Table 86
 - Guest Group Table 90
 - Guest User Account 90
 - Web Portal Customization 91

CHAPTER 8

Cisco Umbrella 93

- Cisco Umbrella 93

CHAPTER 9

Monitor 95

- Dashboard 95
 - LAN Status 96
 - Wireless Status 97
 - Traffic Statistics 98
- Clients 98
- Guests 100

CHAPTER 10

Troubleshoot 101

- Packet Capture 101
 - Local Packet Capture 102
 - Remote Packet Capture 103
 - Stream to a Remote Host 103

Stream to CloudShark	104
Wireshark	104
Packet Capture File Download	106
Using HTTP	106
Support Information	107
Download CPU/RAM Data	107

APPENDIX A	DeAuthentication Message Reason Codes	109
	Deauthentication Message Reason Codes	109
	Deauthentication Reason Code Table	109

APPENDIX B	Where to Go from Here	111
	Where to Go from Here	111



CHAPTER 1

Getting Started

This chapter contains the following sections:

- [Getting Started with the Configuration, on page 1](#)
- [Using the Access Point Setup Wizard, on page 3](#)
- [Changing Password, on page 5](#)
- [TCP/UDP Service, on page 6](#)
- [System Status, on page 7](#)
- [Quick Start Configuration, on page 7](#)
- [Window Navigation, on page 8](#)

Getting Started with the Configuration

This section specifies the system requirements for configuring the WAP device. It also provides the steps to access the web-based Configuration Utility.

Supported Browsers

Before you begin to use the configuration utility, make sure that you have a computer with one of the following browsers:

- Internet Explorer 11, Microsoft Edge or later
- Firefox 64 or later
- Chrome 72 or later
- Safari 5.1 or later

Browser Restrictions

- If using Internet Explorer 11, configure the following security settings:
 - Select **Tools > Internet Options > Security** tab.
 - Select **Local Intranet > Sites**.
 - Select **Advanced > Add**. Add the intranet address of the WAP device `http://<ip-address>` to the local intranet zone. The IP address can be specified as the subnet IP address so that all subnet addresses, are added to the local intranet zone.

- If you have multiple IPv6 interfaces on your management station, use the IPv6 global address instead of the IPv6 local address to access the WAP device from your browser.

Launching the Web-Based Configuration Utility

To access the configuration utility and configure the WAP device, do the following:

1. Connect the WAP device to the same network (IP subnet) as your computer. The factory default IP address configuration of the WAP device is DHCP. Make sure that your DHCP server is running and that can be accessed. Besides, the WAP device has a default static IP, 192.168.1.245. You may choose to connect to it by configuring your computer's IP address in the 192.168.1.xxx range.
2. Locate the IP address of the WAP device.
 1. The WAP device can be accessed and managed by using the Cisco FindIT Network Discovery Utility. This utility enables you to automatically discover all supported Cisco devices in the same local network segment as your computer. You can get a snapshot view of each device or launch the product configuration utility to view and configure the settings. For more information, see <http://www.cisco.com/go/findit>.
 2. The WAP device is Bonjour-enabled and automatically broadcasts its services and listens for services offered from other Bonjour-enabled devices. If you have a Bonjour-enabled browser, such as Microsoft Internet Explorer with a Bonjour plug-in, or the Apple Mac Safari browser, you can find the WAP device on your local network without knowing its IP address.

You can download the complete Bonjour for Microsoft Internet Explorer browser from the Apple's website at: <http://www.apple.com/bonjour/>.
3. Locate the IP address assigned by your DHCP server by accessing your router or DHCP server. For more information, see your DHCP server instructions.
3. Launch any of the supported web browsers.
4. In the address bar, enter the IP address obtained using the initial step and press **Enter**.
5. Enter the default username and password: `cisco` in the **Username** and **Password** fields.
6. Click **Log In**. The **Access Point Setup Wizard** appears.

Follow the Setup Wizard instructions to finish the installation. We strongly recommend that you use the Setup Wizard for the first installation. See [Using the Access Point Setup Wizard, on page 3](#) for more information.

For portable devices, such as your smart phone or tablet, follow the same steps as described earlier in this section to launch the Web-based Configuration Utility. After logging into the portable device, the **Access Point Setup Wizard with mobile** page appears. See [Using the Access Point Setup Wizard with mobile, on page 4](#) for more information.

Logging Out

By default, the configuration utility logs out after 10 minutes of inactivity. See [System Settings, on page 30](#) for instructions on changing the default timeout period.

To log out, click **Logout** in the top right corner of the configuration utility.

Using the Access Point Setup Wizard

The first time that you log into the Access Point or after it has been reset to the factory default settings, the Access Point Setup Wizard appears. This helps you perform the initial configurations. Use the following steps to complete the wizard:



Note If you click **Cancel** to bypass the wizard, the **Change Password** page appears. You can then change the default password and username for logging in. See [Changing Password](#) for more information.

You must log in again after changing your password:

- Step 1** Click **Next** on the **Welcome** page of the wizard.
- Step 2** In the **Firmware Upgrade** window, click **Upgrade** to upgrade the firmware.
- Note** Once the firmware has been upgraded, the device will reboot automatically and direct to the login page.
- Step 3** Click **Skip**.
- Step 4** In the **Restore Configuration** window, choose the configuration file you want to apply to the device and click **Apply**.
- Note** When you click **Apply**, the device will save the relevant configuration, reboot and direct to the login page.
- Step 5** Click **Skip**.
- Step 6** In the **Configure Device - IP Address** window, click **Dynamic IP Address (DHCP) (Recommended)** to receive an IP address from a DHCP server, or click **Static IP Address** to configure the IP address manually. For a description of these fields, see [IPv4 Configuration, on page 17](#).
- Step 7** Click **Next**. The **Configure Device—Set System Date And Time** window appears.
- Step 8** Choose your time zone, and then set the system time automatically from an NTP server or manually. For a description of these options, see [Time, on page 23](#).
- Step 9** Click **Next**. The **Configure Device—Set Password** window appears.
- Step 10** Enter a **New Password** and enter it again in the **Confirm Password** field.
- Note** Uncheck **Password Complexity** to disable the password security rules. However, we strongly recommend keeping the password security rules enabled. For more information about passwords, see [Security, on page 38](#).
- Step 11** Click **Next**. The **Configure Radio 1 (2.4GHz)—Name Your Wireless Network** window appears.
- Step 12** Enter a **Network Name**. This name serves as the SSID for the default wireless network.
- Step 13** Click **Next**. The **Configure Radio 1 (2.4 GHz)—Secure Your Wireless Network** window appears.
- Step 14** Choose a security encryption type and enter a security key. For a description of these options, see [Configuring Security Settings, on page 52](#).
- Step 15** Click **Next**. The **Configure Radio 1 (2.4GHz)—Assign The VLAN ID For Your Wireless Network** window appears.
- Step 16** Choose the **VLAN ID** for traffic received on the wireless network.
- We recommend that you assign a different VLAN ID from the default (1) to the wireless traffic, in order to segregate it from the management traffic on VLAN 1.

- Step 17** Click **Next**. Repeat the step 12 to step 16 to configure the settings for Radio 2 (5GHz) interface.
- Step 18** Click **Next**. The Enable Captive Portal—Create Your Guest Network window appears.
- Step 19** Select whether or not to set up an authentication method for guests on your network, and click **Next**.
If you click **No**, skip to Step 27.
If you click **Yes**, the Enable Captive Portal—Name Your Guest Network window appears.
- Step 20** Specify a **Guest Network Name**.
- Step 21** Click **Next**. The Enable Captive Portal—Secure Your Guest Network window appears.
- Step 22** Choose a security encryption type for the guest network and enter a security key. For a description of these options, see Configuring Security Settings.
- Step 23** Click **Next**. The **Enable Captive Portal—Assign the VLAN ID** window appears.
- Step 24** Specify a VLAN ID for the guest network. The guest network VLAN ID should be different from the management VLAN ID.
- Step 25** Click **Next**. The **Enable Captive Portal—Enable Redirect URL** window appears.
- Step 26** Check **Enable Redirect URL** and enter a fully qualified domain name (FQDN) or IP address in the **Redirect URL** field (including https://). If specified, the guest network users are redirected to the specified URL after authenticating.
- Step 27** Click **Next**. The **Summary—Confirm Your Settings** window appears.
- Step 28** Review the settings that you configured. Click **Back** to reconfigure one or more settings. If you click **Cancel**, all settings are returned to the previous or default values.
- Step 29** If they are correct, click **Submit**. Your setup settings are saved and a confirmation window appears.
- Step 30** Click **Finish**.
The WAP device is now configured successfully. You are required to log in again with the new password.

Using the Access Point Setup Wizard with mobile

The first time that you log into the Access Point with your portable device or after it has been reset to the factory default setting, the Access Point Setup Wizard with mobile style appears. This helps you perform the initial configurations. To configure the Access Point using the wizard, complete the following steps:



Note The default SSID under factory default mode is **CiscoSB-Setup**. Associate your portable device to the Access Point with this SSID and the pre-shared key, **cisco123**. Launch a browser and enter an arbitrary IP address or a domain name. A web page with login fields is displayed. Enter the default user name and password: **cisco**. Click **Log In**. The **Access Point Setup Wizard** is displayed.

- Step 1** Click **Next** on the **Welcome** page of the wizard.
- Step 2** In the **Configure IP address** window, the **Dynamic IP Address (DHCP) (Recommended)** is configured by default to receive an IP address from a DHCP server, or you may click **Static** to configure the IP address manually. For a description of these fields, see [IPv4 Configuration](#).
- Step 3** Click **Next**.

- Step 4** In the **Configure Device - Set Password** window, enter a new password and re-enter the password in the **Confirm Password** field.
- Step 5** Click **Next**. The **Configure your Wireless Network** window appears.
- Enter a Network Name which serves as the SSID for the default wireless network.
 - Enter a Security key (security type, WPA2 Personal - AES is by default)
 - Enter the VLAN ID for traffic received on the wireless network.
- Note** Check the check box to apply the same configuration to Radio 2 (5GHz) or switch to another radio tab and repeat Step 5 to configure again.
- Step 6** Click **Next**. The **Setup Captive Portal** window appears.
- Step 7** Click **Skip**. Go to Step 11.
- Step 8** Click **Yes**. The **Captive Portal configuration** window appears.
- Step 9** Select **Radio 1 (2.4 GHz)** or **Radio 2 (5GHz)**.
- Specify a Guest Network Name.
 - Enter a Security key (security type, WPA2 personal - AES is by default)
 - Specify a VLAN ID for the guest network.
 - Optionally, you may specify a redirect URL with a fully qualified domain name (FQDN) to redirect users to the specified URL after authentication.
- Step 10** Click **Next**. The **Summary** window appears.
- Step 11** Review the configured settings. Click **Back** to reconfigure one or more settings.
- Step 12** Ensure the data is correct and click **Submit** to save.
- Step 13** The WAP device is configured successfully. You are required to log in again with a new password.
-

Changing Password

For security reasons, you are required to change the administrative password at a set interval. You will need to access this page when the Password Aging Time is up.

Password complexity is enabled by default. The minimum password complexity requirements are shown on the **Change Password** page. The new password must comply with the default complexity rules, or it can be disabled temporarily by disabling the **Password Complexity**. See [Security, on page 38](#) for more information.

To change the default password, configure the following:

- **Username**—Enter a new username. The default name is cisco.
- **Old Password**—Enter the current password. The default password is cisco.
- **New Password**—Enter a new password.
- **Confirm Password**—Enter the new password again for confirmation.
- **Password Strength Meter**—Displays the strength of the new password.
- **Password Complexity**—The password complexity is enabled by default and requires that the new password conforms to the following complexity settings:
 - Is different from the username.

- Is different from the current password.
- Has a minimum length of eight characters.
- Contains characters from at least three character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard).



Note Check **Disable** to disable the password complexity rules. However, we strongly recommend that you keep the password complexity rules enabled.

TCP/UDP Service

The TCP/UDP Service table displays the protocols and services operating on the WAP.

- **Service** — The service name.
- **Protocol** — The underlying transport protocol that the service uses (TCP or UDP).
- **Local IP Address** — The local IP address of the connected device. All indicates that any IP address on the device can use this service.
- **Local Port** — The local port number.
- **Remote IP Address** — The IP address of a remote host using this service. All indicates that the service is available to all remote hosts that access the system.
- **Remote Port** — The port number of any remote device communicating with this service.
- **Connection State** — The state of the service. For UDP, only connections in the Active or Established states appear in the table. The TCP states are:
 - **Listening** — The service is listening for connection requests.
 - **Active** — A connection session is established and the packets are being transmitted and received.
 - **Established** — A connection session is established between the WAP device and a server or client.
 - **Time Wait** — The closing sequence has been initiated and the WAP device is waiting for a system-defined timeout period (typically 60 seconds) before closing the connection.



Note You can modify or rearrange the order on the TCP/UDP Service Table. Click **Refresh** to refresh the screen and show the most current information.

You can also enter parameters related to Service, Protocol and other details to filter the TCP/UDP Services displayed.

Click **Back** to return to the **Getting Started** page.

System Status

The **System Status** page displays the hardware model description, software version, and the various configuration parameters such as:

- **PID VID** — The hardware model and version of the WAP device.
- **Serial Number** — The serial number of the WAP device.
- **Host Name** — The hostname assigned to the WAP device.
- **MAC Address** — The MAC address of the WAP device.
- **IPv4 Address** — The IP address of the WAP device.
- **IPv6 Address** — The IPv6 address of the WAP device.
- **LAN Port** — Displays the status of Ethernet interface.
- **Radio 1 (2.4GHz)** — The 2.4GHz mode is enabled or disabled for the Radio 1 interface.
- **Radio 2 (5GHz)** — The 5GHz mode is enabled or disabled for the Radio 2 interface.
- **Power Source** — The system may be powered by a power adapter or may be receiving power over Ethernet (PoE) from a Power Sourcing Equipment (PSE).
- **System Uptime** — The time elapsed since the last reboot.
- **System Time** — The current system time.
- **Firmware Version (Active Image)** — The firmware version of the active image.
- **Firmware MD5 Checksum (Active Image)** — The checksum for the active image.
- **Firmware Version (Non-active)** — The firmware version of the backup image.
- **Firmware MD5 Checksum (Non-active)** — The checksum for the backup image.

Quick Start Configuration

To simplify the device configuration through quick navigation, the **Getting Started** page provides links for performing common tasks. The **Getting Started** page is the default window at start-up.

Category	Link Name (on the Page)	Linked Page
Quick Access	Setup Wizard	Using the Access Point Setup Wizard, on page 3
	Change Account Password	Adding a User, on page 29
	Backup/Restore Configuration	Configuration Management, on page 13
	Upgrade Device Firmware	Firmware, on page 11

Advanced Configuration	Wireless Settings	Radio, on page 45
	Management Setting	System Settings, on page 30
	LAN Setting	IPv4 Configuration, on page 17
	Guest Access	Guest Access, on page 86
More Information	Dashboard	Dashboard, on page 95
	TCP/UDP Service	TCP/UDP Service, on page 6
	View System Log	LED Display, on page 24
	Traffic Statistics	Traffic Statistics, on page 98

For additional information on the device, you can access the product support page or the Cisco Support Community by:




- Click **Support** to access the product support page.
- Click **Forums** to access the Cisco Support Community page.
- Click **More info on FindIT** to see information on FindIT utility.
- Click **Download FindIT** to download the FindIT utility.

Window Navigation

Use the navigation buttons to move around the graphical user interface of the WAP.

Configuration Utility Header

The configuration utility header contains standard information and appears at the top of every page. The header provides these buttons:

Button Name	Description
(User)	The account name (Administrator or Guest) of the user logged into the WAP device. The factory default username is cisco .
(Language)	Hover the mouse pointer over the button, and select a language. The factory default language is English.
	Click to log out of the configuration utility.
	Click to show the WAP device type and version number.
	Click to show the context-sensitive online help. The online help is designed to be viewed with browsers using UTF-8 encoding. If the online help shows errant characters, verify that the encoding settings on your browser are set to UTF-8.

Navigation Pane

A navigation pane, or main menu, is located on the left of each page. The navigation pane lists the top-level features of the WAP device. If an arrow occurs after a main menu item, you can select to expand and display the submenu of each group. You can then select the desired submenu item to open the associated page.

Management Buttons

The following table describes the commonly used buttons that appear on various pages in the system:

Button Name	Description
Add	Adds a new entry to a table or database.
Cancel	Cancels a change made to the page.
Clear All	Clears all entries in a log table.
Delete	Deletes an entry in a table.
Edit	Edits an existing entry.
Refresh	Refreshes the current page with the latest data.
Apply	Applies/Saves the settings or configuration.
Update	Updates the new information to the startup configuration.



CHAPTER 2

Administration

This chapter describes how to configure the Administration settings and perform the diagnostics. It contains the following topics:

- [Firmware, on page 11](#)
- [Reboot, on page 13](#)
- [Configuration Management, on page 13](#)

Firmware

The WAP device maintains two firmware images. One image is active and the other is inactive. If the active image fails to load during boot up, the inactive image is loaded and becomes the active image. You can also swap the active and inactive images.

When new versions of the firmware become available, you can upgrade the firmware on your WAP device to take advantage of new features and enhancements. The WAP device uses a TFTP or HTTP/HTTPS client for firmware upgrades.

After you upload the new firmware and the system reboots, the newly added firmware becomes the primary image. If the upgrade fails, the original firmware remains as the primary image.



Note When you upgrade the firmware, the WAP device retains the existing configuration settings.

Swapping the Firmware Image

To swap the firmware image running on the WAP device:

-
- Step 1** Select **Administration > Firmware**. The product ID (PID VID), active and inactive firmware version are displayed.
 - Step 2** Click **Swap Images**. A dialog box appears confirming the firmware image switch and subsequent reboot.
 - Step 3** Click **Yes** to proceed.

The process may take several minutes, during which time the WAP device is unavailable. Do not power down the WAP device while the image switch is in process. When the image switch is complete, the WAP device restarts. The WAP device resumes normal operation with the same configuration settings it had before the upgrade.

HTTP/HTTPS Upgrade

To upgrade using HTTP/HTTPS:

Step 1 Select **HTTP/HTTPS** as the transfer method.

Step 2 Click **Browse** and locate the firmware image file on your network.

The firmware upgrade file supplied must be a tar file. Do not attempt to use bin files or files of other formats for the upgrade; these types of files do not work.

Step 3 Click **Upgrade** to apply the new firmware image.

Uploading the new firmware may take several minutes. Do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload is aborted. When the process is complete, the WAP device restarts and resumes normal operation.

Step 4 To verify that the firmware was upgraded successfully, log into the web-based Configuration Utility, open the Upgrade Firmware page, and view the active firmware version.

TFTP Upgrade

To upgrade the firmware on the WAP device using TFTP:

Step 1 Select **TFTP** as the transfer method.

Step 2 Enter a name (1 to 256 characters) for the image file in the **Source File Name** field, including the path to the directory that contains the image to upload.

For example, to upload the ap_upgrade.tar image located in the /share/builds/ap directory, enter:
/share/builds/ap/ap_upgrade.tar

The firmware upgrade file supplied must be a tar file. Do not attempt to use bin files or files of other formats for the upgrade; these types of files do not work.

The filename cannot contain the following items: spaces, <, >, |, \, :, (,), &, ;, #, ?, *, and two or more successive periods.

Step 3 Enter the **TFTP Server IPv4 Address** and click **Upgrade**.

Uploading the new firmware may take several minutes. Do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload is aborted. When the process is complete, the WAP device restarts and resumes normal operation.

Step 4 To verify that the firmware upgrade completed successfully, log into the configuration utility, open the Upgrade Firmware page, and view the active firmware version.

Reboot

Use the Reboot page to reboot the WAP device or reset the WAP device to its factory defaults. To reboot or reset the WAP device do the following:

-
- Step 1** Select **Administration > Reboot**.
 - Step 2** To reboot the WAP device using the factory default configuration file, check **Restore to Factory Default Settings**. Any customized settings are lost.
 - Step 3** Click **Reboot**. A window is displayed prompting you to confirm or cancel the reboot.
 - Step 4** Click **Yes** to reboot.
-

Schedule Reboot

To schedule a reboot on the WAP device, follow these steps:

-
- Step 1** Check the **Schedule Reboot** check box to enable the schedule reboot function.
 - Step 2** There are two options to schedule a reboot.
 - **Date** — Set the exact date and time when to reboot the device.
 - **In** — Set the reboot time for the reboot to occur after the function is enabled.
- Note** For the **In** option, this feature will not retain after scheduled reboot. If WAP is power-cycled before scheduled reboot, the scheduler will still work as configured.
- Step 3** Click **Apply**.
-

Configuration Management

The WAP device configuration files are in XML format and contain all the information about the WAP device settings. You can back up (upload) the configuration files to a network host or TFTP server to manually edit the content or create backups. After you edit a backed-up configuration file, you can upload it to the WAP device to modify the configuration. The WAP device maintains these configuration files:

- **Startup Configuration** — The configuration file saved to the flash memory.
- **Backup Configuration** — An additional configuration file saved on the WAP device to use as a backup.
- **Mirror Configuration** — If the Startup Configuration is not modified for at least 24 hours, it is automatically saved to a Mirror Configuration file. The Mirror Configuration file is a snapshot of the past Startup Configuration. The Mirror Configuration is preserved across factory resets, so it can be used to recover a system configuration after a factory reset by copying the Mirror Configuration to the Startup Configuration.



Note In addition to downloading and uploading these files to another system, you can copy them to the different file types on the WAP device.

Backup Configuration Files

To back up (upload) the configuration file to a network host or TFTP server:

-
- Step 1** Select **Administration > Configuration Management > Download/Backup**.
- Step 2** Select **Via TFTP** or **Via HTTP/HTTPS** as the transfer method.
- Step 3** Select **Transfer From (Access Point to PC)** to backup the configuration data to the PC.
- Step 4** For a TFTP backup, enter the **Configuration Filename** with an.xml extension. Also include the path where the file is to be stored on the server and then enter the **TFTP Server IPv4 Address**.
- The filename cannot contain the following characters: spaces, <, >, |, \, :, (,), &, ;, #, ?, *, and two or more successive periods.
- Step 5** Select the configuration file to back up:
- **Startup Configuration** — Configuration file type used when the WAP device last booted. This does not include any configuration changes applied but not yet saved to the WAP device.
 - **Backup Configuration** — Backup configuration file type saved on the WAP device.
 - **Mirror Configuration** — If the Startup Configuration is not modified for at least 24 hours, it is automatically saved to a mirror configuration file. The Mirror Configuration is a snapshot of a past Startup Configuration. The Mirror Configuration is preserved across factory resets, so it can be used to recover a system configuration after a factory reset by copying the Mirror Configuration to the Startup Configuration.
- Step 6** Click **Apply** to begin the backup. For HTTP/HTTPS backups, a window appears to enable you to browse to the desired location for saving the file.
-

Download Configuration Files

You can download a file to the WAP device to update the configuration or to restore the WAP device to a previously backed-up configuration.

To download a configuration file to the WAP device:

-
- Step 1** Select **Administration > Configuration Management > Download/Backup**.
- Step 2** Select **Via TFTP** or **Via HTTP/HTTPS** as the transfer method.
- Step 3** Select **Transfer From (PC to Access Point)** to backup the configuration data to the PC.
- Step 4** For a TFTP backup, enter the **Configuration Filename** with an.xml extension. Also include the path where the file is to be stored on the server and then enter the **TFTP Server IPv4 Address**.

The filename cannot contain the following characters: spaces, <, >, |, \, :, (,), &, ;, #, ?, *, and two or more successive periods.

- Step 5** Select **Startup Configuration** or **Backup Configuration** to replace the file with the downloaded file.
- If the downloaded file overwrites the Startup Configuration file, and the file passes a validity check, then the downloaded configuration takes effect the next time the WAP device reboots.
- Step 6** Click **Apply** to begin the upgrade or backup. For HTTP/HTTPS downloads, a window appears to enable you to browse to select the file to download.
- Caution** Ensure that the power to the WAP device remains uninterrupted while the configuration file is downloading. If a power failure occurs while downloading the configuration file, the file is lost and the process must be restarted.

Copying Configuration Files

You can copy files within the WAP device file system. For example, you can copy the Backup Configuration file to the Startup Configuration file type, so that it is used the next time you boot up the WAP device.

To copy a file to another file type:

-
- Step 1** Select **Administration > Configuration Management > Copy**.
- Step 2** In the **Copy From** field, select one of the following source file types that you want to copy:
- **Startup Configuration** — Configuration file used for the startup.
 - **Backup Configuration** — Backup configuration file saved on the WAP device.
 - **Mirror Configuration** — If the Startup Configuration is not modified for at least 24 hours, it is automatically saved to a Mirror Configuration file. The Mirror Configuration is a snapshot of a past Startup Configuration. The Mirror Configuration is preserved across factory resets, so it can be used to recover a system configuration after a factory reset by copying the Mirror Configuration to the Startup Configuration.
- Step 3** In the **To** field, select the file type to be replaced with the file that you are copying.
- Step 4** Click **Apply** to begin the copy process.

Clearing Configuration Files

You can clear the Startup Configuration or Backup Configuration file. If you clear the Startup Configuration file, the Backup Configuration file becomes active the next time that you reboot the WAP device.

To delete the Startup Configuration or Backup Configuration file:

-
- Step 1** Select **Administration > Configuration Management > Clear**.
- Step 2** Select **Startup Configuration** or **Backup Configuration**.
- Step 3** Click **Clear Files**.

Step 4 Click Yes.



CHAPTER 3

System Configuration

This chapter describes how to configure the global system settings and perform diagnostics. It contains the following topics:

- [LAN, on page 17](#)
- [Time, on page 23](#)
- [Notification, on page 24](#)
- [User Accounts, on page 29](#)
- [Management, on page 30](#)
- [Security, on page 38](#)

LAN

This section describes the process to configure the port, VLAN, LLDP, IPv4, and IPv6 settings on the WAP device.

IPv4 Configuration

Use the **IPv4 Configuration** section to configure the IPv4 address.

Step 1 Select **LAN > IPv4 Configuration**.

Step 2 Configure the following IPv4 settings:

- **Connection Type**—By default, the DHCP client on the WAP device automatically broadcasts the requests for network information. If you want to use a static IP address, you must disable the DHCP client and manually configure the IP address and other network information.

Choose one of the following options:

- **DHCP**—The WAP device acquires its IP address from a DHCP server on the LAN.
- **Static IP**—Manually configure the IPv4 address. The IPv4 address should be in a form similar to xxx.xxx.xxx.xxx (192.168.1.100).
- **Static IP Address, Subnet Mask, and Default Gateway**—Enter the static IP address, subnet mask and default gateway.

- **Domain Name Servers** — Select one of the following options:
 - **Dynamic** — The WAP device acquires the DNS server addresses from a DHCP server on the LAN.
 - **Manual** — Enter up to two IP addresses in the fields provided.

Step 3 Click **Apply** to save the changes.

DHCP Auto Configuration Settings

- **DHCP Auto Configuration Options**— This option is enabled by default. When AP comes up with factory defaults, it first tries to auto configure using DHCP options.

During Auto Configuration:

- AP boots up with only Ethernet interface enabled and WLAN interfaces down.
- No services are available to User (except User Interfaces).
- DHCP Auto Configuration Options is disabled automatically after Wait Interval or TFTP upload of Configuration file whichever is earlier.
- Disabling the DHCP client (i.e., configure use a static IP address) or disabling DHCP Auto Configuration Options immediately aborts Auto configuration.

DHCP client automatically broadcasts requests for DHCP options 66 and 67. If DHCP and DHCP Auto Configuration Options are enabled, Access Point is Auto configured during next reboot considering the information received from DHCP Server for DHCP requests.



Note Configuration upload operation by User/Cisco overrides the Auto Configuration so that the chosen configuration file is given preference. In any other cases of rebooting the AP such as firmware upgrade or reboot operations, existing Auto Configuration settings will be effective.

- **TFTP Server IPv4 Address/Host Name**—If you configure TFTP server address, it is used in case of failure to retrieve file from other TFTP Servers specified by DHCP server during Auto Configuration. Enter IPv4 address or hostname information. If it happens to be in hostname format DNS server must be available to translate hostname into IP address.

The value is used during the Auto Configuration procedure during next boot-up.

- **Configuration File Name**—If you specify the configuration file name, it is retrieved from TFTP Server during Auto Configuration of AP, in case the boot file name is not received from DHCP server. Absence of this value indicates config.xml to be used. The file must have an xml extension if specified.

The value is used during the Auto Configuration procedure during next boot-up.

- **Wait Interval**—If configured, Access Point comes up with the local configuration and makes enabled services available to the user, after the wait interval. Access point aborts Auto configuration if TFTP transaction is not initiated within this interval specified. The default value is 3 minutes.

The value is used during the Auto Configuration procedure during next boot-up.

- **Status Log**—This field displays reason of Auto Configuration completion or abort.

IPv6 Configuration

Use the **IPv6 Configuration** section to configure the IPv6 address by performing the following steps:

Step 1 Select **LAN > IPv6 Configuration**.

Step 2 Configure the following parameters:

- **IPv6 Connection Type** — Select one of the following options:
 - **DHCPv6** — The IPv6 address is assigned by a DHCPv6 server.
 - **Static IPv6** — Manually configure the IPv6 address. The IPv6 address should be in a form similar to `xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx` (2001:DB8:CAD5:7D91).
- **IPv6 Administrative Mode** — Check **Enable** to enable IPv6 administrative mode.
- **IPv6 Auto Configuration Administrative Mode** — Check **Enable** to enable the IPv6 automatic address configuration.

When the IPv6 automatic address configuration is enabled, the WAP device recognizes its IPv6 addresses and gateway by processing the router advertisements received on the LAN port. The WAP device can have multiple auto-configured IPv6 addresses.
- **Static IPv6 Address** — Enter the static IPv6 address. The WAP device can have a static IPv6 address even if addresses have already been configured automatically.
- **Static IPv6 Address Prefix Length** — Enter the prefix length of the static address, which is an integer in the range of 0 to 128. The default is 0.
- **Static IPv6 Address Status** — It can be one of the following status:
 - **Operational** — The IP address has been verified as unique and is usable on the LAN interface.
 - **Tentative** — The WAP device automatically initiates a duplicate address detection (DAD) process when a static IP address is assigned. This IPv6 address is tentative as it is being verified on the network and cannot be used to transmit or receive traffic.
 - **Blank (no value)** — No IP address is assigned.
- **IPv6 Autoconfigured Global Addresses** — Lists the IPv6 addresses which have been automatically assigned to the device.
- **IPv6 Link Local Address** — The IPv6 address used by the local physical link. The link local address is not configurable and is assigned by using the IPv6 Neighbor Discovery process.
- **Default IPv6 Gateway** —The statically configured default IPv6 gateway.
- **IPv6 Domain Name Servers** — Select one of the following options:
 - **Dynamic** — The DNS servers are recognized dynamically through the DHCPv6.

- **Manual** — To manually specify up to two IPv6 DNS servers.
-

Port Settings

Use the **Port Settings Table** to view and configure the settings for the port that connects the WAP device to a LAN.

Step 1 Select **LAN > More > Port Settings Table**.

The Port Settings Table displays the following status and configurations for the LAN interface:

- **Link Status** — Displays the current port link status.
- **Port Speed** — When in review mode, it lists the current port speed. When in edit mode, and the Auto Negotiation is disabled, select a port speed such as 100 Mbps or 10 Mbps. The 1000 Mbps speed is the only supported when Auto-Negotiation is enabled.
- **Duplex Mode** — When in review mode, it lists the current port duplex mode. When in edit mode, and the Auto Negotiation is disabled, select either **Half** or **Full** duplex mode.
- **Auto Negotiation** — When enabled, the port negotiates with its link partner to set the fastest link speed and duplex mode available. When disabled, you can manually configure the Port Speed and Duplex Mode.
- **Green Ethernet** — Green Ethernet Mode supports both the auto-power-down mode and the EEE (Energy Efficient Ethernet, IEEE 802.3az) mode. The Green Ethernet Mode works only when the auto-negotiation on the port is enabled. The auto-power-down mode reduces the chip power when the signal from a link partner is not present. The WAP device automatically enters into a low-power mode when energy on the line is lost, and it resumes normal operation when energy is detected. The EEE mode supports QUIET times during low link utilization, allowing both sides of a link to disable portions of each PHY's operating circuit and save power.

Step 2 Click **Apply**.

Spanning Tree Protocol

In the **Spanning Tree Protocol** mode, the **Enable** checkbox is checked by default to enable the STP mode on the Cisco WAP device. When enabled, STP helps prevent switching loops. STP is recommended if you configure the WDS links.

VLANs Setting

Use the VLAN Configuration page to view and configure the VLANs settings.

Step 1 Select **LAN > More > VLANs Setting Table**.

Step 2 Configure these parameters:

- **Untagged VLAN ID** — Specifies a number between 1 and 4094 for the untagged VLAN ID. The default is 1. The traffic on the VLAN that you specify in this field is not be tagged with a VLAN ID when forwarded to the network.
- **Description** — Description of the related VLAN.
- **Management VLAN** — The Management VLAN is the VLAN used to access the WAP device through Telnet or the web GUI. There must be only one VLAN as the management VLAN. If no interface (wired or wireless) is assigned to the Management VLAN, there will be no interface that a user can use to access the configuration utility.
- **VLAN** — Select from the drop-down list (**Untagged or Tagged**) VLAN.

By default, all traffic on the WAP device uses the VLAN 1, the default untagged VLAN. This means that all traffic is untagged until you disable the untagged VLAN, change the untagged traffic VLAN ID, or change the VLAN ID for a VAP or client using RADIUS.

Step 3 Click **Apply**. The changes are saved to the Startup Configuration.

Neighbor Discover

Bonjour enables the WAP device and its services to be discovered by using multicast DNS (mDNS). Bonjour advertises services to the network and answers queries for the service types that it supports, simplifying network configuration in your environments.

The WAP device advertises these service types:

- **Cisco-specific device description (cisco-sb)** — This service enables clients to discover the Cisco WAP devices and other products deployed in your networks.
- **Management user interfaces** — This service identifies the management interfaces available on the WAP device (HTTP and SNMP).

When a Bonjour-enabled WAP device is attached to a network, any Bonjour client can discover and get access to the configuration utility without prior configuration.

A system administrator can use an installed Internet browser plug-in to discover the WAP device. The web-based Configuration Utility shows up as a tab in the browser.



Note The system administrator can view the Bonjour enabled WAP's using the latest Internet Explorer plug-in (Cisco FindIT tool). All WAP devices present in a cluster, are shown under the cluster name after the Bonjour discovery process. The administrator should ensure that the name of the cluster is unique within a network.

Bonjour works in both IPv4 and IPv6.

To enable the WAP device to be discovered through Bonjour, follow these steps:

- Step 1** Select **LAN > More > Neighbor Discover**.
- Step 2** Check **Enable** to enable Bonjour. By default, this option is enabled.
- Step 3** Click **Apply**. The changes are saved to the Startup Configuration.
-

LLDP

The Link Layer Discovery Protocol (LLDP) is defined by the IEEE 802.1AB standard and allows the WAP to advertise its system name, system capabilities, and power requirements. This information can help to identify system topology and detect bad configurations on the LAN. The WAP also supports the Link Layer Discovery Protocol for the Media Endpoint Devices (LLDP-MED), which standardizes additional information elements that devices can pass to each other to improve network management.

Step 1 To configure the LLDP settings, select **LAN > More > LLDP**.

Step 2 Configure the following parameters:

- **LLDP Mode** — Check **Enable** to enable the LLDP. Once enabled, the WAP transmits LLDP Protocol Data Units to the neighbor devices. By default, this mode is enabled.
- **TX Interval** — The number of seconds between each LLDP message transmissions. The valid range is 5 to 32768 seconds. The default value is 30 seconds.
- **POE Priority** — Select the priority level from the drop-down list (**Critical, High, Low or Unknown**). The PoE priority helps the Power Sourcing Equipment (PSE), determine which powered devices should be given priority in power allocation when the PSE doesn't have enough capacity to supply power to all connected devices.

Step 3 Click **Apply**.

IPv6 Tunnel

The WAP device supports the Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). The ISATAP enables the WAP device to transmit IPv6 packets encapsulated within the IPv4 packets over the LAN. The protocol enables the WAP device to communicate with remote IPv6-capable hosts even when the LAN that connects them does not support the IPv6.

The WAP device acts as an ISATAP client. An ISATAP-enabled host or router must reside on the LAN. The IP address or host name of the router is configured on the WAP device (by default, it is ISATAP). If configured as a host name, the WAP device communicates with a DNS server to resolve the name into one or more ISATAP router addresses. The WAP device then sends solicit messages to the routers. When an ISATAP-enabled router replies with an advertisement message, the WAP device and the router establish the tunnel. The tunnel interface is assigned a link-local and a global IPv6 address, which serve as virtual IPv6 interfaces on the IPv4 network.

When IPv6 hosts initiate the communication with the WAP device connected through the ISATAP router, the IPv6 packets are encapsulated into IPv4 packets by the ISATAP router.

1. **ISATAP Status** — Check **Enable** to enable ISATAP on the device. By default, this option is enabled.
2. **ISATAP Capable Host** — Enter the IP address or DNS name of the ISATAP router. The default value is isatap.
3. **ISATAP Query Interval** — Enter how often the WAP device should send queries to the DNS server to attempt to resolve the ISATAP host name into an IP address. The valid range is 120 to 3600 seconds. The default value is 120 seconds.

4. **ISATAP Solicitation Interval** — Enter how often the WAP device should send the router solicitation messages to the ISATAP routers. The WAP device sends the router solicitation messages only when there is no active ISATAP router. The valid range is 120 to 3600 seconds. The default value is 120 seconds.
5. **ISATAP IPv6 Link Local Address**— The IPv6 address used by the local physical link. The link local address is not configurable and is assigned by using the IPv6 Neighbor Discovery process.
6. **ISATAP IPv6 Global Address**— If the WAP device has been assigned one or more IPv6 addresses automatically, the addresses are listed.



Note When the tunnel is established, the ISATAP IPv6 Link Local Address and ISATAP IPv6 Global Address fields appear on the page. These are the virtual IPv6 interface addresses.

7. Click **Apply**.

Time

A system clock provides a network-synchronized time-stamping service for the message logs. The system clock can be configured manually or as a Network Time Protocol (NTP) client that obtains the clock data from a server.

Use the Time Settings page to configure the system time manually or from a preconfigured NTP server. By default, the WAP device is configured to obtain its time from a predefined list of NTP servers.

The current system time appears at the top of the page, along with the **System Clock Source** option.

Automatically Acquiring the Time Settings through NTP

To automatically acquire the time settings from a NTP server, follow these steps:

Step 1 Select **System Configuration > Time**.

Step 2 In the **System Clock Source** area, click **Network Time Protocol (NTP)**. By default, the NTP is enabled.

Step 3 Configure the following parameters:

- **NTP Server (1 through 4)** — Specify the IPv4 address, IPv6 address, or host name of a NTP server. A default NTP server is listed from **0.ciscosb.pool.ntp.org** to **3.ciscosb.pool.ntp.org**.

A host name can consist of one or more labels, which are sets of up to 63 alphanumeric characters. If a host name includes multiple labels, each is separated by a period (.). The entire series of labels and periods can be up to 253 characters long.

- **Time Zone** — Select the time zone for your location.
- **Adjust for Daylight Saving Time** — Ensure that you have chosen the appropriate time zone before you select this option. Check the checkbox to enable and configure the following fields:
 - **Starts** — Select the week, day, month, and time when the Daylight Savings time starts.
 - **Ends** — Select the week, day, month, and time when the Daylight Savings time ends.

- **Daylight Saving Offset** — Specify the number of minutes to move the clock forward when Daylight Savings Time begins and backward when it ends.

Step 4 Click **Apply**. The changes are saved to the Startup Configuration.

Manually Configuring the Time Settings

To manually configure the time settings:

Step 1 Select **System Configuration > Time**.

Step 2 In the System Clock Source area, choose **Manual**.

Step 3 Click **Sync Time with PC** to clone the system time settings from your local PC.

Step 4 You can also configure the following fields:

- **System Date** — Select the current month, day, and year date from the drop-down lists.
- **System Time** — Select the current hour and minutes in 24-hour clock format.
- **Time Zone** — Select the time zone for your location.
- **Adjust for Daylight Saving Time** — Ensure that you have chosen the appropriate time zone before you select this option. Check the checkbox to enable and configure the following fields:
 - **Starts** — Select the week, day, month, and time when daylight savings time starts.
 - **Ends** — Select the week, day, month, and time when daylight savings time ends.
 - **Daylight Saving Offset** — Specify the number of minutes to move the clock forward when daylight savings time begins and backward when it ends.

Step 5 Click **Apply**. The changes are saved to the Startup Configuration.

Note Click **Sync Time with PC**, the system time of the device will be same as the PC.

Notification

This section details the process to enable and configure notifications for the access point.

LED Display

The WAP device has two type of LEDs: System LED and Ethernet LED. Use the LED Display page to configure all LEDs.

To configure the LED Display do the following:

-
- Step 1** Select **Notification > LED Display**.
- Step 2** Select **Enable** to enable the LEDs. Select **Disable** to disable the LEDs. Select **Associate Scheduler** and go to Step 3.
- Step 3** Select a profile name from the drop-down list for the Associate Scheduler LED Display. By default there is no profile associated to the LEDs. The drop-down selection will show the configured Scheduler Profile Names configured in the **Wireless > Scheduler** page.
- When the LED is associated to a Scheduler Profile, this column shows the status depending on the presence or absence of an active profile rule at that time of the day.
- Step 4** Click **Apply**.
-

Log Settings

Use the Log Settings page to enable log messages to be saved in permanent memory. You can also send logs to a remote host.

If the system unexpectedly reboots, the log messages can be useful to diagnose the cause. However, log messages are erased when the system reboots unless you enable persistent logging.



Caution Enabling persistent logging can wear out the flash (nonvolatile) memory and degrade network performance. Only enable persistent logging to debug a problem. Make sure that you disable persistent logging after you finish debugging the problem.

Configuring the Persistent Log

- Step 1** Select **Notification > Log Settings**.
- Step 2** Configure these parameters:
- **Persistence** — Check **Enable** to save the system logs to the nonvolatile memory so that the logs are kept when the WAP device reboots. You can save up to 1000 log messages. When the limit of 1000 is reached, the oldest log message is overwritten by the newest message. Clear this field to save system logs to volatile memory. Logs in volatile memory are deleted when the system reboots.
 - **Severity** — Select the severity from the drop-down list (**Emergency, Alert, Critical, Error, Warning, Notice, Info or Debug**) used to filter the event messages that will be saved in the nonvolatile memory. All other messages will be saved in the volatile memory.
 - **Depth** — Enter the maximum number of messages, up to 1000, that can be stored in volatile memory. When the number that you configure in this field is reached, the oldest log event is overwritten by the newest log event.
- Step 3** Click **Apply**.
-

Remote Log Server Table

The kernel log is a comprehensive list of system events (shown in the System Log) and kernel messages.

You cannot view the kernel log messages directly from the configuration utility. You must first set up a remote log server to receive and capture the logs. Then, you can configure the WAP device to log to the remote log server. The WAP device supports up to two remote log servers.

The remote log server collection for the syslog messages provides these features:

- Allows aggregation of syslog messages from multiple APs.
- Stores a longer history of messages than is kept on a single WAP device.
- Triggers scripted management operations and alerts.

To specify a host on your network to serve as a remote log server:

Step 1 Select **Notification > Log Settings**.

Step 2 In the **Remote Log Server Table**, configure the following parameters:

- **Server IPv4/IPv6 Address/Name** — Enter the IPv4 or IPv6 address, or the host name of the remote log server.
A host name can consist of one or more labels, which are sets of up to 63 alphanumeric characters. If a host name includes multiple labels, each is separated by a period (.). The entire series of labels and periods can be up to 253 characters long.
- **Enable** — Check **Enable** to enable the remote log server. Next, define the log severity and UDP port.
- **Log Severity** — Check the severities that an event must have for it to be sent to remote log server.
- **UDP Port** — Enter the logical port number for the syslog process on the remote host. The range is from 1 to 65535. The default port is 514.

Using the default port is recommended. If you reconfigure the log port, make sure that the port number that you assign to syslog is available for use.

Step 3 Click **Apply**. The changes are saved to the Startup Configuration.

Note If you enable a remote log server, clicking **Apply** activates the remote logging. The WAP device sends its kernel messages in real-time for display to the remote log server monitor, a specified kernel log file, or other storage, depending on your configuration.

If you disabled a remote log server, click **Apply** to disable remote logging.

View System Log

The View System Log page displays the list of system events occurring on the device. The log is cleared upon a reboot and can be cleared by an administrator. Up to 1000 events can be shown. Older entries are removed from the list as needed to make room for new events.

To view the system logs, select **Notification > View System Log**.

The following information is displayed:

- **Time Stamp** — The system time when the event occurred.
- **Severity** — The severity level of the event.
- **Service** — The service associated with the event.
- **Description** — A description of the event.

You can filter or rearrange the settings on View System Log.

Click **Refresh** to refresh the screen and show the most current information.

Click **Clear All** to clear all entries from the log.

Click **Download** to download all entries from the log.

Email Alert/ Mail Server/ Message Configuration

The email alert feature supports mail server configuration, message severity configuration, and up to three email addresses to send urgent and non-urgent email alerts. Use the **Email Alert** to send messages to the configured email addresses when particular system events occur.



Tip Do not use your personal email address. This would unnecessarily expose your personal email login credentials. Use a separate email account instead. Also, be aware that many email accounts keep a copy of all sent messages by default. Anyone with access to this email account has access to the sent messages. Review the email settings to ensure that they conform to your privacy policy.

To configure the WAP device to send email alerts, perform the following steps:

Step 1 Select **Notification > Email Alert**.

Step 2 In the **Email Alert** area, configure the following parameters:

- **Administrative Mode** — Check **Enable** to enable the email alert feature.
- **From Email Address** — Enter the email address to be displayed as the sender of the email. The address is a 255-character string with only printable characters. No address is configured by default.
- **Log Duration** — Enter the frequency in minutes at which scheduled messages are sent. The range is from 30 to 1440 minutes. The default is 30 minutes.
- **Scheduled Message Severity** — Select the severity from the drop-down list (**Emergency, Alert, Critical, Error, Warning, Notice, Info** or **debug**) that an event must have for it to be sent to the configuration email address at the frequency specified by the Log Duration. The default severity is **Warning**.
- **Urgent Message Severity** — Select the severity from the drop-down list (**Emergency, Alert, Critical, Error, Warning, Notice, Info** or **debug**) that an event must have for it to be sent to the configured email address immediately. The default severity is **Alert**.

Step 3 In the **Mail Server Configuration** area, configure these parameters:

- **Server IPv4 Address/Name** — Enter the IP address or host name of the outgoing SMTP server. The server address must be a valid IPv4 address or host name. The IPv4 address should be in a form similar to xxx.xxx.xxx.xxx (192.0.2.10).

A host name can consist of one or more labels, which are sets of up to 63 alphanumeric characters. If a host name includes multiple labels, each is separated by a period (.). The entire series of labels and periods can be up to 253 characters long.

- **Data Encryption** — Choose the mode of security from the drop-down list (**Open or TLSv1**) for the outbound email alert. Using the secure TLSv1 protocol can prevent eavesdropping and tampering during the communication across the public network.
- **Port** — Enter the SMTP port number to use for outbound emails. The range is a valid port number from 0 to 65535. The default port is 465.
- **Username** — Enter the user name for the email account that will be used to send these emails. Typically (but not always) the user name is the full email address including the domain (such as Name@example.com). The specified account will be used as the email address of the sender. The user name can contain in the range of 1 to 64 alphanumeric characters that includes "@", "-", and ".".
- **Password** — Enter the password for the email account that will be used to send these emails. The password can be from 1 to 64 characters.

Step 4 In the **Message Configuration** area, configure the email addresses and subject line:

- **To Email Address 1/2/3** — Enter up to three addresses to receive the email alerts. Each email address must be a valid address.
- **Email Subject** — Enter the text to appear in the email subject line. This can be up to a 255-character alphanumeric string.

Step 5 Click **Apply**.

Email Alert Examples

The following example shows how to fill in the **Mail Server Configuration** parameters:

```
Gmail
Server IPv4 Address/Name = smtp.gmail.com
Data Encryption = TLSv1
Port = 465
Username = Your full email address you can use to login to your email account
associated with the above server
Password = xxxxxxxx is a valid password of your valid email account
To Email Address 1 = myemail@gmail.com
```

```
Windows Live Hotmail
Windows Live Hotmail recommends the following settings: Data Encryption: TLSv1
SMTP Server: smtp.live.com
SMTP Port: 587
Username: Your full email address, such as myName@hotmail.com or
myName@myDomain.com
Password: Your Windows Live account password
```

```
Yahoo! Mail
Yahoo requires using a paid account for this type of service. Yahoo
```

```

recommends the following settings:
Data Encryption: TLSv1
SMTP Server: plus.smtp.mail.yahoo.com
SMTP Port: 465 or 587
Username: Your email address, without the domain name such as myName (without
@yahoo.com)
Password: Your Yahoo account password

```

The following example shows a sample format of a general log email.

```

From: AP-192.168.2.10@mailserver.com
Sent: Wednesday, September 09, 2009 11:16 AM
To: administrator@mailserver.com
Subject: log message from AP

TIME          Priority > Process Id > > > Message
Sep 8 03:48:25 info >> login[1457]> > > root login on tty0
Sep 8 03:48:26 info >> mini_http-ssl[1175]>Max concurrent connections of 20
reached

```

User Accounts

One management user is configured on the WAP device by default:

- User Name: **cisco**
- Password: **cisco**

Use the **User Accounts** page to configure up to four additional users and change the user password.

Adding a User

Configure the following settings to add a new user:

Step 1 Select **System Configuration > User Accounts**.

The **User Account Table** shows the currently configured users. The user cisco is preconfigured in the system and has Read/Write privileges.

All other users can have Read Only access, but not Read/Write access.

Step 2 Click **+** to add a new row.

Step 3 Check the checkbox for a new user and enter a name for the new user.

Step 4 Enter a new password between 0 and 127 characters and confirm the same password in the appropriate fields.

The **Password Strength Meter** field indicates the password strength as follows:

- **Red** — The password fails to meet the minimum complexity requirements.
- **Orange** — The password meets the minimum complexity requirements but the password strength is weak.
- **Green** — The password is strong.

Step 5 Click **Apply**.

Note To delete a user, select the user name and click **Delete**. To edit an existing user, select the user name and click **Edit**, then click **Apply** to save all changes made to the configurations.

Changing a User Password

To change a user password:

Step 1 Select **System Configuration > User Accounts**.

The **User Account Table** shows the currently configured users. The user **cisco** is preconfigured in the system to have Read/Write privileges. The password for the user **cisco** can be changed.

Step 2 Select the user to configure and click **Edit**.

Step 3 Enter a new password between 0 and 127 characters and confirm the same password in the appropriate fields.

The **Password Strength Meter** indicates the password strength as follows:

- **Red** — The password fails to meet the minimum complexity requirements.
- **Orange** — The password meets the minimum complexity requirements but the password strength is weak.
- **Green** — The password is strong.

Step 4 Click **Apply**. The changes are saved to the Startup Configuration.

Note If you change your password, you must log in again to the system.

Management

This section describes how to configure the management settings on the WAP device.

System Settings

Use the **System Settings** section to configure the information that identifies the WAP device within the network.

To configure the system settings:

Step 1 Select **Management > Management** and configure the following parameters:

- **Host Name** — Enter the host name for the WAP device. By default, the name is the fully qualified domain name (FQDN) of the node. The default host name is **wap** concatenated with the last 6 hexadecimal digits of the MAC address of the WAP device. The host name label can contain only letters, digits, and hyphens. It cannot begin or end with a hyphen. No other symbols, punctuation characters, or blank spaces are permitted. The host name can be 1 to 63 characters long.

- **System Contact** — Enter the contact person for the WAP device. The system contact can be 0 to 255 characters long and can include spaces and special characters.
- **System Location** — Enter the physical location of the WAP device. The system location can be 0 to 255 characters long and can include spaces and special characters.

Step 2 Click **Apply**. The changes are saved to the Startup Configuration.

Connect Session Settings/HTTP/HTTPS Service

Use the **HTTP/HTTPS Service** to enable and configure the web-based management connections. If the HTTPS is used for secure management sessions, you can also use this page to manage the required SSL certificates.

To configure the HTTP and HTTPS services:

Step 1 Select **Management > Management**.

Step 2 In the **Connect Session Settings** area, configure the following parameters:

- **Maximum Sessions** — Enter the number of web sessions, including both the HTTP and HTTPS, that can be in use at the same time.

When a user logs on to the WAP's configuration utility, a session is created. This session is maintained until the user logs off or the session timeout expires. The range is from 1 to 10 sessions. The default is 5. If the maximum number of sessions are reached, the next user who attempts to log on to the configuration utility receives an error message about the session limit.

- **Session Timeout** — Enter the maximum amount of time, in minutes, that an inactive user remains logged on. When the configured timeout is reached, the user is automatically logged off. The range is from 2 to 60 minutes. The default is 10 minutes.

Step 3 In the **HTTP/HTTPS Service** area, configure the following parameters:

- **HTTP Service** — Enable or disable access through HTTP. By default, HTTP access is disabled. If you disable it, any current connections using that protocol are disconnected.
 - **HTTP Port** — Enter the logical port number to use for the HTTP connections, from 1025 to 65535. The default port number for the HTTP connections is the well-known IANA port number 80.
 - **Redirect HTTP to HTTPS** — Redirects management HTTP access attempts on the HTTP port to the HTTPS port. This field is available only when HTTP access is disabled.
- **HTTPS Service** — Enable or disable access through secure HTTP (HTTPS). By default, HTTPS access is enabled. If you disable it, any current connections using that protocol are disconnected.
 - **HTTPS Port** — Enter the logical port number to use for the HTTPS connections, from 1025 to 65535. The default port number for the HTTPS connections is the IANA port number 443.
 - **TLSv1.0, TLSv1.1, SSLv3** — Check or uncheck the checkbox to enable or disable the protocol of the HTTPS Service.

- **Management ACL Mode** — If the Mode is enabled, access through the web and SNMP is restricted to the specified IP hosts. You can configure up to 5 IPv4 and 5 IPv6 addresses under the **Management Access Control**. If this feature is disabled, anyone can access the configuration utility from any network client by supplying the correct user name and password of the WAP device.

Note Verify any IP address that you enter. If you enter an IP address that does not match your administrative computer, you will lose access to the configuration interface. We recommend that you give the administrative computer a static IP address, so the address does not change over time.

Step 4 Click **Apply**.

SSL Certificate File Status

To use the HTTPS services, the WAP device must have a valid SSL certificate. The WAP device can generate a certificate, or you can download it from your network or from a TFTP server.

In the **Generate SSL Certificate** area, click **SSL Settings**, then click **Generate** to generate the certificate for the WAP device. This procedure should be done after the WAP device has acquired an IP address to ensure that the common name for the certificate matches the IP address of the WAP device. Generating a new SSL certificate restarts the secure web server. The secure connection does not work until the new certificate is accepted on the browser.

In the **SSL Certificate File Status** area, you can view the current certificate on the WAP device. The following will be displayed:

- **Certificate File Present**
- **Certificate Expiration Date**
- **Certificate Issuer Common Name**

If a SSL certificate (with a .pem extension) exists on the WAP device, you can download it to your computer as a backup. In the **Transfer SSL Certificate from** (Device to PC) area, select **HTTP/HTTPS** or **TFTP** as the download option and click **Transfer**.

- If you select **HTTP/HTTPS**, confirm the download and then browse to the location to save the file on your network.
- If you select **TFTP**, enter a file name to assign to the download file, and enter the TFTP server IPv4 address where the file will be downloaded.

You can also upload a certificate file (with a .pem extension) from your computer to the WAP device. In the **Transfer SSL Certificate from** (PC to Device) area, select **HTTP/HTTPS** or **TFTP** as the upload option and click **Transfer**.

- For **HTTP/HTTPS**, browse to the network location, select the file, and click **Transfer**.
- For **TFTP**, enter the file name and the TFTP Server IPv4 Address, then click **Transfer**. The filename cannot contain the following characters: spaces, <, >, |, \, :, (,), &, ;, #, ? aszxaa, *, and two or more successive periods.

A confirmation appears when the upload was successful.

SNMP / SNMPv2c Settings

SNMP defines a standard for recording, storing, and sharing information about network devices. SNMP facilitates network management, troubleshooting, and maintenance. The WAP supports SNMP and can function as an SNMP managed device for seamless integration into network management systems.

Use the SNMP/SNMPv2c Settings section to enable SNMP and configure the basic protocol settings.

To configure general SNMP settings:

Step 1 Select **Management**> **SNMP Settings**.

Step 2 Check **Enable** to enable SNMP.

Step 3 Enter the **UDP Port** for the SNMP traffic. The default is 161. However, you can configure it so that the agent listens to the requests on a different port. The valid range is from 1025 to 65535.

Step 4 In the **SNMPv2c Settings** area, configure the SNMPv2c settings:

- **Read-only Community** — Enter a read-only community name for the SNMPv2 access. The valid range is 1 to 256 alphanumeric and special characters.

The community name acts as a simple authentication feature to restrict the devices on the network that can request data from the SNMP agent. The name functions as a password, and the request is assumed to be authentic if the sender knows the password.

- **Read-write Community** — Enter a read-write community name to be used for SNMP set requests. The valid range is from 1 to 256 alphanumeric and special characters. Setting a community name is similar to setting a password. Only the requests from the machines that identify themselves with this community name are accepted.
- **Management Station** — Determines which stations can access the WAP device through SNMP. Choose one of these options:
 - **All** — All stations can access the WAP device through SNMP.
 - **User Defined** — The set of user defined SNMP requests that are permitted.
- **NMS IPv4 Address/Name** — Enter the IPv4 IP address, DNS host name, or subnet of the network management system (NMS).

A DNS host name can consist of one or more labels, which are sets of up to 63 alphanumeric characters. If a host name includes multiple labels, each is separated by a period (.). The entire series of labels and periods can be up to 253 characters long.

As with community names, this setting provides a level of security on the SNMP settings. The SNMP agent only accepts the requests from the IP address, host name, or subnet specified here.

To specify a subnet, enter one or more subnetwork address ranges in the form address/mask length where the address is an IP address and mask length is the number of mask bits. Both formats address/mask and address/mask length are supported. For example, if you enter a range of 192.168.1.0/24, this specifies a subnetwork with address 192.168.1.0 and a subnet mask of 255.255.255.0.

- **NMS IPv6 Address/Name** — The IPv6 address, DNS host name, or subnet of the devices that can execute, get, and set requests to the managed devices. The IPv6 address should be in a form similar to xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8:CAD5:7D91).

Note A host name can consist of one or more labels, which are sets of up to 63 alphanumeric characters. If a host name includes multiple labels, each is separated by a period (.). The entire series of labels and periods can be up to 253 characters long.

Step 5 In the **SNMPv2c Trap Settings** area, configure the SNMPv2c trap settings:

- **Trap Community** — Enter a global community string associated with SNMP traps. Traps sent from the device provide this string as a community name. The valid range is from 1 to 60 alphanumeric and special characters.
- **Trap Destination Table** — Enter a list of up to three IP addresses or host names to receive the SNMP traps. Check the box and choose a **Host IP Address Type** (IPv4 or IPv6) before adding the **Host Name/IP Address**.

An example of a DNS host name is snmptraps.foo.com. Because the SNMP traps are sent randomly from the SNMP agent, it makes sense to specify where exactly the traps should be sent. You can have a maximum of three DNS host names. Ensure that you check **Enabled** and select the appropriate Host IP Address Type.

Step 6 Click **Apply**.

SNMPv3 Views

A SNMP MIB view is a family of view subtrees in the MIB hierarchy. A view subtree is identified by the pairing of an Object Identifier (OID) subtree value with a bit string mask value. Each MIB view is defined by two sets of view subtrees, included in or excluded from the MIB view. You can create MIB views to control the OID range that SNMPv3 users can access.

The WAP device supports a maximum of 16 views.

This section summarizes the critical guidelines for the SNMPv3 view configuration. Please read all the notes before proceeding.



Note A MIB view called all is created by default in the system. This view contains all management objects supported by the system.



Note By default, view-all and view-none SNMPv3 views are created on the WAP device. These views cannot be deleted or modified.

To add and configure an SNMP view, do the following:

Step 1 Select **Management > SNMP Settings > SNMPv3**.

Step 2 Click **+** to create a new row in the **SNMPv3 Views** table or check the check box for existing views, then click **Edit**.

- **View Name** — Enter a name that identifies the MIB view. View names can contain up to 32 alphanumeric characters.
- **Type** — Choose whether to include or exclude the view subtree or family of subtrees from the MIB view.
- **OID** — Enter an OID string for the subtree to include or exclude from the view. For example, the system subtree is specified by the OID string.1.3.6.1.2.1.1.

- **Mask** — Enter an OID mask. The mask is 47 characters in length. The format of the OID mask is xx.xx.xx (.)... or xx:xx:xx... (:) and is 16 octets in length. Each octet is two hexadecimal characters separated by either a period (.) or a colon (:). Only hex characters are accepted in this field. For example, OID mask FA.80 is 11111010.10000000.

A family mask is used to define a family of view subtrees. The family mask indicates which sub identifiers of the associated family OID string are significant to the family's definition. A family of view subtrees enables efficient control access to one row in a table.

Step 3 Click **Apply**.

Note To remove a view, check the view in the list and click **Delete**.

SNMPv3 Groups

The SNMPv3 groups allow you to combine users into groups of different authorization and access privileges. Each group is associated with one of three security levels:

- noAuthNoPriv
- authNoPriv
- authPriv

Access to MIBs for each group is controlled by associating a MIB view to a group for read or write access, separately.

By default, the WAP device has two groups:

- **RO** — A read-only group using authentication and data encryption. Users in this group use the MD5 key or password for authentication and a DES or AES128 for encryption. The SHA, DES and AES128 keys or passwords must be defined. By default, users of this group have read access to the default all MIB view.
- **RW** — A read/write group using authentication and data encryption. Users in this group use the MD5 key or password for authentication and a DES key or AES128 for encryption. The SHA, DES and AES128 keys or passwords must be defined. By default, users of this group have read and write access to the default all MIB view.



Note The default groups RO and RW cannot be deleted. The WAP device supports a maximum of eight groups.

To add and configure the SNMP group, perform the following steps:

Step 1 Select **Management > SNMP Settings > SNMPv3**.

Step 2 Click **+** to add a new row to the **SNMPv3 Groups** table.

Step 3 Check the box for the new group and configure the following parameters:

- **Group Name** — Enter the name of the group. The default group names are RO and RW. Group names can contain up to 32 alphanumeric characters.

- **Security Level** — Choose the security level for the group, from the following options:
 - **noAuthNoPriv** — No authentication and no data encryption (no security).
 - **authNoPriv** — Authentication, but no data encryption. With this security level, users send SNMP messages that use the SHA key or password for authentication, but not a DES key or AES128 for encryption.
 - **authPriv** — Authentication and data encryption. With this security level, users send the MD5 key or password for authentication and a DES for encryption. For groups that require authentication, encryption, or both, you must define the SHA, DES and AES128 keys or passwords on the SNMP Users page.
- **Write Views** — Choose the write access for the group's MIBs from one of the following options:
 - **view-all** — The group can create, alter, and delete MIBs.
 - **view-none** — The group cannot create, alter, or delete MIBs.
- **Read Views** — Choose the read access to MIBs for the group, from one of the following options:
 - **view-all** — The group is allowed to view and read all MIBs.
 - **view-none** — The group cannot view or read MIBs.

Step 4 Click **Apply** to add the group to the SNMPv3 Groups list.

Note To delete a group, check the group in the list and click **Delete**. To edit a group, check the group in the list and click **Edit**.

SNMPv3 Users

Use the **SNMP Users** table to define users, associate a security level to each user, and configure the security keys per user.

Each user is mapped to a SNMPv3 group, either from the predefined or user-defined groups, and, optionally, is configured for authentication and encryption. For authentication, only the SHA type is supported. For encryption, only the DES and AES128 types are supported. There are no default SNMPv3 users on the WAP device, and you can add up to eight users.

To add SNMP users follow these steps:

Step 1 Select **Management > SNMP Settings > SNMPv3**.

Step 2 Click **+** to add a new row to the **SNMPv3 Users** table.

Step 3 Check the box in the new row and configure these parameters:

- **User Name** — Enter the name that identifies the SNMPv3 user. User names can contain up to 32 alphanumeric characters.
- **Group** — Enter the name of group that the user is mapped to. The default groups are RW and RO. You can define additional groups on the SNMP Groups page.

- **Authentication Type** — Choose the type of authentication to use on the SNMPv3 requests from the user, from the following options:
 - **SHA** — Requires SHA authentication on SNMP requests from the user.
 - **None** — SNMPv3 requests from this user require no authentication.
- **Authentication Pass Phrase** — If you specify SHA as the authentication type, enter the pass phrase to enable the SNMP agent to authenticate the requests sent by the user. The pass phrase must be between 8 and 32 characters in length.
- **Encryption Type** — Choose the encryption/privacy type applied to the user's SNMP requests from the following options:
 - **DES** — Uses DES encryption on the SNMPv3 requests from the user.
 - **AES128** — Uses AES128 encryption on the SNMPv3 requests from the user.
 - **None**—SNMPv3 requests from this user require no privacy.
- **Encryption Pass Phrase** — If you specify DES as the encryption type, enter the pass phrase used to encrypt the SNMP requests. The pass phrase must be between 8 and 32 characters in length.

Step 4 Click **Apply**. The user is added to the SNMPv3 Users list and your changes are saved to the Startup Configuration.

Note To remove a user, select the user in the list and click **Delete**. To edit a user, select the user in the list and click **Edit**.

SNMPv3 Targets

The SNMPv3 targets send SNMP notifications using Inform messages to the SNMP manager. For SNMPv3 targets, only the Informs are sent, not traps. For SNMP versions 1 and 2, the traps are sent. Each target is defined with a target IP address, UDP port, and SNMPv3 user name.



Note The SNMPv3 user configuration should be completed before configuring the SNMPv3 targets. For more details, refer to [SNMPv3 Users](#).

The WAP device supports a maximum of eight targets.

To add SNMP targets follow these steps:

Step 1 Select **Management > SNMP Settings > SNMPv3 Targets**.

Step 2 Click **+** to add a new row to the **SNMPv3 Targets** table.

Step 3 Check the check box in the new row and configure the following parameters:

- **IP Address** — Enter the IPv4 or IPv6 address of the remote SNMP manager to receive the target.
- **UDP Port** — Enter the UDP port to use for sending SNMPv3 targets. The classical port number is 161.

- **Users** — Enter the name of the SNMP user to associate with the target. To configure SNMP users, see the [SNMPv3 Users, on page 36](#) page.

Step 4 Click **Apply**. The user is added to the **SNMPv3 Targets** list and your changes are saved to the Startup Configuration.

Note To remove a SMMP target, select the user in the list and click **Delete**. To edit a SMMP target, select the user in the list and click **Edit**.

Plug and Play (PnP)

Cisco Open Plug-n-Play (PnP) agent is a software application running on a Cisco SMB device. When a device is powered on, the Open Plug-n-Play agent discovery process, which is embedded in the device, attempts to discover the address of the Open Plug-n-Play server which helps automate the process of deploying and provisioning new devices into the network. This helps to apply configuration and install the required image without manual intervention. The Open Plug-n-Play agent uses methods like DHCP, Domain Name System (DNS), and Cisco cloud service discovery to acquire the desired IP address of the Open Plug-n-Play server.

Simplified deployment process of SMB device automates the following deployment related operational tasks

Step 1 Select **Management > PnP Settings**.

Step 2 Click **Enable**, and choose **PnP Transport** mode. Enter the following information.

Option	Description
PnP Transport	<ul style="list-style-type: none"> • Auto: Select this mode to download the image automatically from the PnP server through the AP. • Static: Select and specify values in the IP/FQDN and Port fields. Select the required certificate from the CA Certificate drop-down list. The default port number is 443.

Step 3 Click **Apply**.

Note To use a self-signed SSL certificate or in the absence of your certificate in the pre-installed CA list, select **User Specified** and click **Upload a certificate** to upload the certificate you want.

Security

This section describes how to configure the security settings on the WAP device.

RADIUS Server

Several features require communication with a RADIUS authentication server. For example, when you configure the Virtual Access Points (VAPs) on the WAP device, you can configure security methods that control the wireless client access (see [Radio, on page 45](#)). The WPA Enterprise security method uses an

external RADIUS server to authenticate the clients. The MAC address filtering feature, where the client access is restricted to a list, may also be configured to use a RADIUS server to control the access. The Captive Portal feature also uses RADIUS to authenticate the clients.

Use the Radius Server page to configure the RADIUS servers that are used by these features. You can configure up to four globally available IPv4 or IPv6 RADIUS servers. However, you must select whether the RADIUS client operates in IPv4 or IPv6 mode with respect to the global servers. One of the servers always acts as the primary server while the other act as the backup servers.



Note In addition to using the global RADIUS servers, you can also configure each VAP to use a specific set of RADIUS servers. See [Networks, on page 50](#) for more information.

To configure the global RADIUS servers follow these steps:

Step 1 Select **Security > Radius Server**.

Step 2 Configure these parameters:

- **Server IP Address Type** — Select the IP version that the RADIUS server uses. You can toggle between the address types to configure IPv4 and IPv6 global RADIUS address settings, but the WAP device contacts only the RADIUS server or servers with the address type that you select in this field.
- **Server IP Address-1 or Server IPv6 Address-1** — Enter the address for the primary global RADIUS server. When the first wireless client tries to authenticate with the WAP device, the WAP device sends an authentication request to the primary server. If the primary server responds to the authentication request, the WAP device continues to use this RADIUS server as the primary server, and authentication requests are sent to the address specified.
- **Server IP Address-2 or Server IPv6 Address-2** — Enter the addresses for backup IPv4 or IPv6 RADIUS servers. If authentication fails with the primary server, the configured backup server kicks in.
- **Key-1** — Enter the shared secret key that the WAP device uses to authenticate to the primary RADIUS server. You can use from 1 to 64 standard alphanumeric and special characters. The key is case sensitive and must match the key configured on the RADIUS server. The text that you enter appears as asterisks.
- **Key-2** — Enter the RADIUS key associated with the configured backup RADIUS servers. The server at Server IP (IPv6) Address 2 uses Key 2.
- **Enable RADIUS Accounting** — Check **Enable** to enable tracking and measuring of the resources that a particular user consumes, such as system time, amount of data transmitted and received, and so on. If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers.

Step 3 Click **Apply**. The changes are saved to the Startup Configuration.

802.1x Supplicant

The IEEE 802.1X authentication enables the WAP device to gain access to a secured wired network. You can enable the WAP device as an 802.1X supplicant (client) on the wired network. A user name and password with the MD5 algorithm encryption can be configured to allow the WAP device to authenticate using 802.1X.

On the networks that use IEEE 802.1X port-based network access control, a supplicant cannot gain access to the network until the 802.1X authenticator grants access. If your network uses 802.1X, you must configure 802.1X authentication information on the WAP device, so that it can supply it to the authenticator.

To configure the 802.1X supplicant settings follow these steps:

-
- Step 1** Click **Security > 802.1X Supplicant**.
- Step 2** In the 802.1x Supplicant area, check **Enable** to enable the **Administrative Mode**.
- Step 3** Configure the 802.1X operational status and basic settings:
- **EAP Method** — Choose the algorithm to be used for encrypting authentication user names and passwords. The options are:
 - **MD5** — A hash function defined in RFC 3748 that provides basic security.
 - **PEAP** — Protected Extensible Authentication Protocol, which provides a higher level of security than MD5 by encapsulating it within a TLS tunnel.
 - **TLS** — Transport Layer Security, as defined in RFC 5216, an open standard that provides a high level of security.
 - **Username** — Enter the username.
 - **Password** — Enter the password. The password character length can be a range from 1-64.
- Step 4** In the **Certificate File Upload** area, you can upload a certificate file to the WAP device:
- a) Choose either **HTTP** or **TFTP** as the transfer method.
 - b) If you selected HTTP, click **Browse** to select the file. See [Connect Session Settings/HTTP/HTTPS Service](#) for more information on configuring the HTTP server settings.
 - c) If you selected TFTP, enter the **Filename** and the **TFTP Server IPv4 Address**.
 - d) Click **Upload**. A confirmation window appears, followed by a progress bar to indicate the status of the upload.
- Step 5** Click **Apply**.
-

Rogue AP Detection

A Rogue AP is an access point that has been installed on a secure network without explicit authorization from a system administrator. The rogue AP poses a security threat because anyone with access to the premises can unconsciously or maliciously install an inexpensive wireless WAP device that can potentially allow unauthorized parties to access the network.

The WAP device performs a RF scan on all channels to detect all APs in the vicinity of the network. If rogue APs are detected, they are shown on the Rogue AP Detection page. If an AP listed as a rogue is legitimate, it can be added to the Known AP List.



Note The Detected Rogue AP List and Trusted AP List provide information. The AP does not have any control over the APs on the list and cannot apply any security policies to APs detected through the RF scan.

When the Rogue AP detection is enabled, the radio periodically switches from its operating channel to scan other channels within the same band.

Viewing the Rogue AP List

In order for the Rogue AP Detection to function, the wireless radio must be enabled. You should first enable the radio interface before enabling the Rogue AP detection for the radio interface.

To enable the radio to collect information about rogue APs:

Step 1 Select **Security > Rogue AP Detection**.

Step 2 Check **Enable** to enable the AP Detection for Radio 1 and Radio 2.

Step 3 Click **Apply**.

The Detected Rogue AP List table displays all detected rogue APs. The Trusted AP List displays all trusted APs. The following settings are displayed for each of the Rogue AP lists:

- **MAC Address** — The MAC address of the rogue AP.
- **Beacon Interval** — The beacon interval used by the rogue AP. Beacon frames are transmitted by an AP 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 is set on the [Radio](#) page.
- **Type** — The type of the device. The options are:
 - **AP** — An AP rogue device that supports the IEEE 802.11 Wireless Networking Framework in infrastructure mode.
 - **Ad hoc** — A rogue station running in Ad hoc mode. The Ad hoc mode is an IEEE 802.11 Wireless Networking Framework also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS).
- **SSID** — The Service Set Identifier (SSID) for the WAP device.
- **Privacy** — Indicates whether there is any security on the rogue device. The options are:
 - **Off** — Security mode is off (no security).
 - **On** — Security mode is on.
- **WPA** — Shows whether the WPA security is on or off for the rogue AP.
- **Band** — The IEEE 802.11 mode being used on the rogue AP, such as IEEE 802.11a, IEEE 802.11b, IEEE 802.11g. The number shown indicates the mode:
 - 2.4 indicates IEEE 802.11b, 802.11g, or 802.11n mode (or a combination of the modes).
 - 5 indicates IEEE 802.11a or 802.11n mode (or both modes).
- **Channel** — The channel on which the rogue AP is currently broadcasting.

- **Rate** — The rate in megabits per second at which the rogue AP is currently transmitting. The current rate is always one of the rates shown in the Supported Rates field.
- **Signal** — The strength of the radio signal emitting from the rogue AP. If you hover the mouse pointer over the bars, a number representing the strength in decibels (dB) appears.
- **Beacons** — The total number of beacons received from the rogue AP since it was first discovered.
- **Last Beacon** — The date and time of the last beacon received from the rogue AP.
- **Rates** — Supported and basic (advertised) rates set for the rogue AP. Rates are shown in megabits per second (Mbps). All Supported Rates are listed, with Basic Rates shown in bold. Rate sets are configured on the [Radio](#) page.

- Step 4** Check the AP List, then click the **Move to Trusted AP List** in order to move the AP to the **Trusted AP List**. If the AP is in the **Trusted AP List**, click the **Detected Rogue AP List** in order to move the AP to the **Detected Rogue AP List**.
- Step 5** Click **Refresh** to refresh the screen and display the most current information.
-

Saving the Trusted AP List

To create a Trusted AP List and save it to a file:

- Step 1** Select **Security** and click **View Rogue AP List...** in the **Rogue AP Detection** section. The **Rogue AP Detection** page is displayed.
- Step 2** In the **Detected Rogue AP List**, click **Move to Trusted AP List** for the APs that are known to you. The trusted APs move to the **Trusted AP List**.
- Step 3** In the **Download/Backup Trusted AP List** area, click **Backup (AP to PC)**.
- Step 4** Click **Apply**.

The list contains the MAC addresses of all APs that have been added to the **Trusted AP List**. By default, the filename is Rogue1.cfg. You can use a text editor or web browser to open the file and view its contents.

Importing a Trusted AP List

You can import a list of known APs from a saved list. The list may be acquired from another AP or created from a text file. If the MAC address of an AP appears in the Trusted AP List, it is not detected as a rogue.

To import an AP list from a file:

- Step 1** Select **Security > Rogue AP Detection > View Rogue AP List...**
- Step 2** In the **Download/Backup Trusted AP List** area, click **Download (PC to AP)**.
- Step 3** In the **Source File Name** field, click **Browse** to choose the file to import.

The imported file must be a plain-text file with a .txt or .cfg extension. Entries in the file are MAC addresses in hexadecimal format with each octet separated by colons, for example, 00:11:22:33:44:55. You must separate entries with a single space. For the AP to accept the file, it must contain only MAC addresses.

- Step 4** In the **File Management Destination** field, choose whether to replace the existing **Trusted AP List** or add the entries in the imported file to the **Trusted AP List**. The options are:
- **Replace** — Imports the list and replaces the contents of the **Trusted AP List**.
 - **Merge** — Imports the list and adds the APs in the imported file to the APs currently shown in the **Trusted AP List**.

- Step 5** Click **Apply**.

When the import is complete, the screen refreshes and the MAC addresses of the APs in the imported file appear in the **Trusted AP List**.

Configure Password Complexity

Use the Password Complexity page to modify the complexity requirements for passwords used to access the configuration utility. Complex passwords increase security.

To configure the password complexity requirements follow the subsequent steps:

- Step 1** Select **Security > Configure Password Complexity**.

- Step 2** Check **Enable** to enable **Password Complexity**.

- Step 3** Configure the following parameters:

- **Password Minimum Character Class** — Enter the minimum number of character classes that must be represented in the password string. The four possible character classes are uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard. The default value for this field is 3. The range can be between 0-4 characters.
- **Password Different from Current** — Check to enable that users enter a different password when their current password expires. If left unchecked, users can reenter the same password when it expires.
- **Maximum Password Length** — The maximum password character length is a range from 64 to 127. The default is 64.
- **Minimum Password Length** — The minimum password character length is a range from 0 to 32. The default is 8.
- **Password Aging Support** — Check to enable password expiration after a configured time period.
- **Password Aging Time** — Enter the number of days before a newly created password expires, from 1 to 365. The default is 180 days.

- Step 4** Click **Apply**. The changes are saved to the Startup Configuration.

Note When the **Password Aging Time** is up, you will be required to access the [Changing Password](#) page.

Configure WAP-PSK Complexity

When you configure the VAPs on the WAP device, you can select a method of securely authenticating clients. If you select the WPA Personal protocol (also known as WPA pre-shared key or WPA-PSK) as the security method, you can configure the complexity requirements on the WPA-PSK Complexity page to be used in the authentication process. More complex keys provide increased security.

To configure the WPA-PSK complexity:

-
- Step 1** Select **Security > Configure WPA-PSK Complexity**.
- Step 2** Check **Enable** to enable the WAP device to check the WPA-PSK keys against the configured criteria. If disabled, none of the configured settings are used. The **WPA-PSK Complexity** is disabled by default.
- Step 3** Configure these parameters:
- **WPA-PSK Minimum Character Class** — Choose the minimum number of character classes that must be represented in the key string. The four possible character classes are uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard. The default value for this field is 3. The range can be between 0-4 characters.
 - **WPA-PSK Different from Current** — Check **Enable** to enable users to configure a different key after their current key expires. If disabled, users can use the old or previous key after their current key expires.
 - **Maximum WPA-PSK Length** — Enter a key length value. The maximum key length in number of characters is from 32 to 63. The default is 63.
 - **Minimum WPA-PSK Length** — Enter a key length value. The minimum key length in number of characters is from 8 to 16. The default is 8.
- Step 4** Click **Apply**.
-



CHAPTER 4

Wireless

This chapter describes how to configure the wireless radio properties. It includes the following topics:

- [Radio, on page 45](#)
- [Networks, on page 50](#)
- [Client Filter, on page 56](#)
- [Scheduler, on page 57](#)
- [QoS, on page 58](#)

Radio

The radio is the physical part of the WAP that creates a wireless network. The radio settings on the WAP control the behavior of the radio and determine what kind of wireless signals the WAP emits.

To configure the wireless radio settings, perform the following steps:

Step 1 Select **Wireless > Radio**.

Step 2 Select one of the following radio mode options:

- **2.4G Only** — Support 2.4G Radio with a 2x2 MIMO mode.
- **5G Only** — Support 5G Radio with a 2x2 MIMO mode.
- **Dual Band** — Support 2.4G and 5G Radio with two 1x1 SISO chains.

This is a single-silicon solution for operating the radio in either a 2x2 MIMO mode or as two 1x1 chains. This enables the user to perform different tasks in two different bands or in the same bands (with some restrictions) simultaneously.

Step 3 In the Basic Settings area, configure these parameters for the selected radio interface:

Note Local regulations may prohibit the use of certain radio modes. Not all modes are available in all countries.

- **Radio** — Check **Enable** to enable the radio interface.
- **Wireless Network Mode** — The IEEE 802.11 standard and frequency the radio uses. The default value of Mode is 802.11b/g/n for Radio 1 and 802.11a/n/ac for Radio 2. For each radio, select one of the available modes.

2.4G supports the following radio modes:

- **802.11b/g** — 802.11b and 802.11g clients can connect to the WAP device.

- **802.11b/g/n (default)** — 802.11b, 802.11g, and 802.11n clients operating in the 2.4-GHz frequency can connect to the WAP device.
- **2.4 GHz 802.11n** — 802.11n clients operating in the 2.4-GHz frequency can connect to the WAP device.

5G supports the following radio modes:

- **802.11a** — 802.11a clients can connect to the WAP device.
- **802.11a/n/ac** — 802.11a clients, 802.11n, and 802.11ac clients operating in the 5-GHz frequency can connect to the WAP device.
- **802.11n/ac** — 802.11n clients and 802.11ac clients operating in the 5-GHz frequency can connect to the WAP device
- **Wireless Band Selection (802.11n and 802.11ac modes only)** — The 802.11n specification allows a coexisting 20/40 MHz band in addition to the legacy 20 MHz band available with other modes. The 20/40 MHz band enables higher data rates but leaves fewer bands available for use by other 2.4 GHz and 5 GHz devices.

The 802.11ac specification allows an 80 MHz-wide band in addition to the 20 MHz and 40 MHz band.

Set the field to 20 MHz to restrict the use of the wireless band selection to a 20 MHz band. For the 802.11ac mode, set the field to 40 MHz to prevent the radio from using the 80 MHz wireless band selection.

- **Primary Channel (802.11n modes with 20/40 MHz bandwidth only)** — 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.

Choose one of these options:

- **Upper** — Sets the primary channel as the upper 20-MHz channel in the 40-MHz band.
- **Lower** — Sets the primary channel as the lower 20-MHz channel in the 40-MHz band. Lower is the default selection.
- **Channel** — The portion of the radio spectrum that the radio uses for transmitting and receiving.

The range of available channels is determined by the mode of the radio interface and the country code setting. If you select Auto for the channel setting, the WAP device scans available channels and selects a channel where the least amount of traffic is detected.

Each mode offers a number of channels, depending on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC), the International Telecommunication Union (ITU-R) or the European Telecommunications Standards Institute (ETSI).

- **Scheduler** — For the radio interface, select the profile from the list. The default value is **None**.

Note To create a profile, navigate to **Wireless > Scheduler**.

Step 4 In the Advanced Settings area, configure these parameters:

- **Short Guard Interval Supported** — This field is available only if the selected radio mode includes 802.11n. The guard interval is the dead time, in nanoseconds, between the 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 percent

improvement in data throughput. The client with which the WAP device is communicating must also support the short guard interval.

Choose one of these options:

- **Yes** — The WAP device transmits data using a 400-nanosecond guard interval when communicating with clients that also support the short guard interval. This is the default selection.
- **No** — The WAP device transmits data using an 800-nanosecond guard interval.
- **Protection** — The protection feature contains rules to guarantee that 802.11 transmissions do not cause interference with legacy stations or applications. By default, protection is enabled (Auto). With protection enabled, protection is invoked if the legacy devices are within the range of the WAP device.

You can disable the protection (Off); however, the legacy clients or the WAP devices within the range can be affected by the 802.11n transmissions. Protection is also available when the mode is 802.11b/g. When protection is enabled in this mode, it protects the 802.11b clients and the WAP devices from the 802.11g transmissions.

Note This setting does not affect the ability of the client to associate with the WAP device.

- **Beacon Interval** — The interval between the transmission of beacon frames. The WAP device transmits these frames 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). Enter an integer from 20 to 2000 milliseconds. The default is 100 milliseconds.
- **DTIM Period** — The Delivery Traffic Information Map (DTIM) period. Enter an integer from 1 to 255 beacons. The default is 2 beacons.

The 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 WAP device awaiting pickup.

The DTIM period indicates how often the clients served by this WAP device should check for buffered data awaiting pickup.

The measurement is in beacons. For example, if you set it to 1, the clients check for buffered data on the WAP device at every beacon. If you set it to 10, the clients check on every 10th beacon.

- **Fragmentation Threshold** — The frame size threshold is in bytes. The valid integer must be even and in the range of 256 to 2346. The default is 2346.

The fragmentation threshold is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold set, the fragmentation is activated and the packet is sent as multiple 802.11 frames.

If the packet being transmitted is equal to or less than the threshold, the fragmentation is not used. Setting the threshold to the largest value (2,346 bytes, which is the default) effectively disables the fragmentation.

By default, the fragmentation is off. We recommend not using fragmentation unless you suspect the radio interference. The additional headers applied to each fragment increase the overhead on the network and can greatly reduce the throughput.

- **RTS Threshold** — The Request to Send (RTS) Threshold value. The valid integer range must be from 0 to 65535. The default is 65535 octets.

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 the traffic flow through the WAP device. If you specify a low threshold value, the RTS packets are sent more frequently, which consumes more bandwidth and reduces the throughput of

the packet. However, sending more RTS packets can help the network recover from interference or collisions that might occur on a busy network, or on a network experiencing electromagnetic interference.

- **Max Associated Clients** — The maximum number of stations allowed to access the WAP device at any one time. You can enter an integer between 0 and 100. The default is 100 stations.

- **Transmit Power** — A percentage value for the transmit power level of the WAP device.

The default value of Full - 100 % can be more cost-efficient than a lower percentage because it gives the WAP device a maximum broadcast range and reduces the number of access points needed.

To increase the capacity of the network, place the WAP devices closer together and reduce the value of the transmit power. This setting helps reduce overlap and interference among the access points. A lower transmit power setting can also keep your network more secure because the weaker wireless signals are less likely to propagate outside of the physical location of your network.

Some channel ranges and country code combinations have relatively low maximum transmit power. When attempting to set the transmit power to the lower ranges (for example, Medium - 25 percent or Low - 12 percent), the expected drop in power may not occur, because certain power amplifiers have minimum transmit power requirements.

- **Frame-burst Support** — Generally enabling the Frame-burst support improves the radio performance in the downstream direction.
- **Airtime Fairness Mode** — The airtime fairness (ATF) feature was implemented to address the issue of slower-data transfers throttling the higher-speed ones.
- **Maximum Utilization Threshold** — Enter the percentage of network bandwidth utilization allowed on the radio before the WAP device stops accepting new client associations. The valid integer range is from 0 to 100 percent. The default is 0 percent. When set to 0, all new associations are allowed regardless of the utilization rate.
- **Fixed Multicast Rate** — The transmission rate in Mbps for broadcast and multicast packets. This setting can be useful in an environment where the wireless multicast video streaming occurs, provided the wireless clients are capable of handling the configured rate.

When **Auto** is selected, the WAP device chooses the best rate for the associated clients. The range of valid values is determined by the configured radio mode.

- **Legacy Rate Sets** — Rates are expressed in megabits per second.

The Supported Rate Sets indicate the rates that the WAP device supports. You can check multiple rates. The WAP device automatically chooses the most efficient rate based on the factors such as error rates and the distance of the client stations from the WAP device.

The Basic Rate Sets indicate the rates that the WAP device advertises to the network for the purposes of setting up communication with other access points and client stations on the network. It is generally more efficient to have a WAP device broadcast a subset of its supported rate sets.

- **Broadcast/Multicast Rate Limiting** — Multicast and broadcast rate limiting can improve overall network performance by limiting the number of packets transmitted across the network.

By default, this feature is disabled. Until you enable this feature, these fields are disabled:

- **Rate Limit** — The rate limit for multicast and broadcast traffic which should be greater than 1, but less than 50 packets per second. Any traffic that falls below this rate limit will always conform and be transmitted to the appropriate destination. The default and maximum rate limit setting is 50 packets per second.
- **Rate Limit Burst** — An amount of traffic, measured in bytes, which is allowed to pass as a temporary burst even if it is above the defined maximum rate. The default and maximum rate limit burst setting is 75 packets per second.

- **VHT Features** — The purpose of this feature is to enable or disable the Broadcom specific extensions in VHT for Broadcom-to-Broadcom links. The VHT feature enables support for 256QAM VHT rates not specified by the 802.11 ac Draft. The rates are all VHT LDPC mode, MCS 9 Nss 1 20Mhz, MCS 9 Nss 2 20Mhz, MCS 6 Nss 3 80Mhz. The VHT feature is supported for 802.11 ac PHY.

Step 5 Click **Configure TSPEC** and configure these parameters:

- **TSPEC Violation Interval** — In the TSPEC Violation Interval field, enter the time interval in seconds for the WAP device to report associated clients that do not adhere to mandatory admission control procedures. The reporting occurs through the system log and SNMP traps. Enter a time from 0 to 900 seconds. The default time is 300 seconds.
- **TSPEC Mode** — Regulates the overall TSPEC mode on the WAP device. By default, the TSPEC mode is off. The options are:
 - **On** — The WAP device handles TSPEC requests according to the TSPEC settings that you configure on the Radio page.
 - **Off** — The WAP device ignores TSPEC requests from client stations.
- **TSPEC Voice ACM Mode** — Regulates mandatory admission control (ACM) for the voice access category. By default, TSPEC Voice ACM mode is off. The options are:
 - **On** — A station is required to send a TSPEC request for bandwidth to the WAP device before sending or receiving a voice traffic stream. The WAP device responds with the result of the request, which includes the allotted medium time if the TSPEC was admitted.
 - **Off** — A station can send and receive the voice priority traffic without requiring an admitted TSPEC. The WAP device ignores voice TSPEC requests from client stations.
- **TSPEC Voice ACM Limit** — The upper limit on the amount of traffic that the WAP device attempts to transmit on the wireless medium using a voice AC to gain access. The default limit is 20 percent of the total traffic.
- **TSPEC Video ACM Mode** — Regulates mandatory admission control for the video access category. By default, TSPEC Video ACM mode is off. The options are:
 - **On** — A station is required to send a TSPEC request for bandwidth to the WAP device before sending or receiving a video traffic stream. The WAP device responds with the result of the request, which includes the allotted medium time if the TSPEC was admitted.
 - **Off** — A station can send and receive video priority traffic without requiring an admitted TSPEC; the WAP device ignores video TSPEC requests from client stations.
- **TSPEC Video ACM Limit** — The upper limit on the amount of traffic that the WAP device attempts to transmit on the wireless medium using a video AC to gain access. The default limit is 15 percent of total traffic.
- **TSPEC AP Inactivity Timeout** — The amount of time for a WAP device to detect a downlink traffic specification as idle before deleting it. The valid integer range is from 0 to 120 seconds and the default is 30 seconds.
- **TSPEC Station Inactivity Timeout** — The amount of time for a WAP device to detect an uplink traffic specification as idle before deleting it. The valid integer range is from 0 to 120 seconds and the default is 30 seconds.
- **TSPEC Legacy WMM Queue Map Mode** — Check **Enable** to enable the intermixing of legacy traffic on queues operating as ACM. By default, this mode is off.

Step 6 Click **OK** and then click **Apply**.

Networks

Virtual Access Points (VAPs), segment the wireless LAN into multiple broadcast domains that are wireless equivalent of the Ethernet VLANs. VAPs simulate multiple access points on one physical WAP device. Up to four VAPs are supported on this Cisco WAP device.

Each VAP can be independently enabled or disabled, with the exception of VAP0. The VAP0 is the physical radio interface and remains enabled as long as the radio is enabled. To disable the VAP0, the radio itself must be disabled.

Each VAP is identified by a user-configured Service Set Identifier (SSID). Multiple VAPs cannot have the same SSID name. SSID broadcasts can be enabled or disabled independently on each VAP. SSID broadcast is enabled by default.

SSID Naming Conventions

The default SSID for VAP0 is **ciscosb**. Every additional VAP created has a blank SSID name. The SSIDs for all VAPs can be configured to other values. The SSID can be any alphanumeric, case-sensitive entry from 2 to 32 characters.

The following characters are allowed:

- ASCII 0x20 through 0x7E.
- Trailing and leading spaces (ASCII 0x20) are not permitted.



Note This means that spaces are allowed within the SSID, but not as the first or last character including the period “.” (ASCII 0x2E).

VLAN IDs

Each VAP is associated with a VLAN, and is identified by a VLAN ID (VID). A VID can be any value from 1 to 4094, inclusive. This Cisco WAP device supports nine active VLANs (eight for WLAN plus one management VLAN).

By default, the VID assigned to the configuration utility for the WAP device is 1, which is also the default untagged VID. If the management VID is the same as the VID assigned to a VAP, then the WLAN clients associated with this specific VAP can administer the WAP device. If needed, an access control list (ACL) can be created to disable administration from WLAN clients.

Configuring VAPs

To configure VAPs:

Step 1 Select **Wireless > Networks**.

Step 2 In the **Radio** field, click the radio interface (**Radio 1** or **Radio 2**) to which the VAP configuration parameters are applied.

Step 3 If VAP0 is the only VAP configured on the system, and you want to add a VAP, click **+**. Then, check the VAP.

Step 4 Configure the following:

- **VLAN ID** — Specify the VLAN ID of the VLAN to associate with the VAP.

Be sure to enter a VLAN ID that is properly configured on the network. Network problems can result if the VAP associates the wireless clients with an improperly configured VLAN.

When a wireless client connects to the WAP device by using this VAP, the WAP device tags all traffic from the wireless client with the configured VLAN ID, unless you enter the port VLAN ID or use a RADIUS server to assign a wireless client to a VLAN. The range for the VLAN ID is from 1 to 4094.

If you change the VLAN ID to a different ID than the current management VLAN ID, the WLAN clients associated with this specific VAP cannot administer the device. You can verify the configuration of the untagged and management VLAN IDs on the LAN page. See [IPv4 Configuration, on page 17](#) for more information.

- **SSID Name** — Enter the name for the wireless network. The SSID is an alphanumeric string of up to 32 characters. Choose a unique SSID for each VAP.

If you are connected as a wireless client to the same WAP device that you are administering, resetting the SSID will cause you to lose connectivity to the WAP device. You will need to reconnect to the new SSID after you save this new setting.

- **SSID Broadcast** — Enables and disables the broadcast of the SSID.

Specify whether to allow the WAP device to broadcast the SSID in its beacon frames. The Broadcast SSID parameter is enabled by default. When the VAP does not broadcast its SSID, the network name is not shown in the list of available networks on a client station. Instead, you must manually enter the exact network name into the wireless connection utility on the client so that it can connect.

Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it does not prevent even the simplest of attempts by a hacker to connect or monitor unencrypted traffic. Suppressing the SSID broadcast offers a very minimal level of protection on an otherwise exposed network (such as a guest network) where the priority is to make it easy for clients to get a connection and where no sensitive information is available.

WMF — The Wireless Multicast Forwarding provides an efficient way to transfer multicast traffic on the wireless device and overcome multicast transmission issues on the WLAN using the repeated unicast or multicast the frames.

- **Security** — Choose the type of authentication required for access to the VAP. The options are:
 - None
 - WPA Personal
 - WPA Enterprise

If you choose a security mode other than None, additional fields appear. For more information on configuring the wireless security settings, see [Configuring Security Settings](#).

We recommend using WPA Personal or WPA Enterprise as the authentication type as it provides stronger security protection.

Note Static WEP can be used for wireless computers or devices that do not support WPA Personal and WPA Enterprise. To set security with Static WEP, configure the radio as 802.11a or 802.11b/g mode. The 802.11n mode restricts the use of Static as the security.

- **Client Filter** — Specifies whether the stations that can access the VAP are restricted to a configured global list of MAC addresses. You can choose one of these types of Client filter:
 - **Disabled** — Does not use the Client filter.
 - **Local** — Uses the MAC authentication list that is configured on the Client Filter page.
 - **RADIUS** — Uses the MAC authentication list on an external RADIUS server.
- **Channel Isolation** — Check to enable the channel isolation.

When disabled, the wireless clients can communicate with one another normally by sending traffic through the WAP device.

When enabled, the WAP device blocks communication between the wireless clients on the same VAP. The WAP device still allows data traffic between its wireless clients and the wired devices on the network, across a WDS link, and with other wireless clients associated with a different VAP, but not among the wireless clients
- **Band Steer** — Check to enable the band steer when both the radios are up. It effectively utilizes the 5-GHz band by steering dual-band supported clients from the 2.4-GHz band to the 5-GHz band.
 - It is configured on a per-VAP basis and needs to be enabled on both the radios.
 - It is not encouraged on the VAPs with time-sensitive voice or video traffic.
 - It does not consider the n-bandwidth of the radio. Even if the 5-GHz radio happens to use 20 MHz bandwidth, it tries to steer clients to that radio.
- **Scheduler** — Select a scheduler profile from the list, VAP0 can't be associated to a scheduler profile.
- **Guest Access Instance** — Associate a CP instance to a VAP. The associated CP instance settings applies to users who attempt to authenticate on the VAP. Select the instance name for each VAP you want to associate an instance with.

Note A VAP can associate to one Guest Access Instance in **Access Control > Guest Access** page. You must configure a **Guest Access Instance** first.

Step 5 Click **Apply**.

Caution After new settings are saved, the corresponding processes may be stopped and restarted. When this condition happens, the WAP device may lose its connectivity. It is recommend that you change the WAP device settings at this time.

Note To delete a VAP, check the VAP and click **Delete**. To edit a VAP, check the VAP and click **Edit**. To save your changes, click **Apply** when complete.

Configuring Security Settings

This section describes the security settings that can be configured on the WAP device on the **Networks** page. There are three security setting options to choose from: None, WPA Personal and WPA Enterprise.

None

If you select **None** as your security mode, no additional security settings are required on the device. This mode means that any data transferred to and from the WAP device is not encrypted. This security mode can be used during initial network configuration or for troubleshooting, but the same is not recommended for a regular use on the internal network as this mode is not secure.

WPA Personal

The WPA Personal is a Wi-Fi Alliance IEEE 802.11i standard, which includes AES-CCMP and TKIP encryption. The WPA Personal uses a pre-shared key (PSK) instead of using IEEE 802.1X and EAP as is used in the Enterprise WPA security mode. The PSK is used for an initial check of credentials only. WPA Personal is also referred to as WPA-PSK.

This security mode is backwards-compatible for the wireless clients that support the original WPA.

To configure WPA Personal, configure the following:

- **WPA Versions** — Choose the types of client stations from the following:
 - **WPA-TKIP** — This network has client stations that only support the original WPA and TKIP security protocol. Note that selecting the WPA-TKIP only is not allowed as per the latest Wi-Fi Alliance requirements.
 - **WPA2-AES** — All client stations on the network support WPA2 and AES-CCMP cipher/security protocol. This provides the best security per IEEE 802.11i standard. As per the latest Wi-Fi Alliance requirement, the AP has to support this mode all the time.

If the network has a mix of clients, some of which support WPA2 and others which support only the original WPA, select both. 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 in place of some security.

WPA clients must have one of these keys to be able to associate with the WAP device:

- A valid TKIP key
 - A valid AES-CCMP key
- **PMF (Protection Management Frame)** — Provides security for the unencrypted 802.11 management frames. When Security Mode is disabled, the PMF is set to No PMF and is not editable (Hidden or Grey). When the security Mode is set to WPA2-xxx, the PMF is Capable by default and is editable. The following three check box values can be configured for it.
 - **Not Required**
 - **Capable**
 - **Required**



Note The WiFi Alliance requires the PMF to be enabled and set to Capable (Default). You may disable it when the non-compliant wireless clients experience instability or connectivity issues.

- **Key** — The shared secret key for WPA Personal security. Enter a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include uppercase and lowercase alphabetic letters, the numeric digits, and special symbols such as @ and #.
- **Show Key as Clear Text** — When enabled, the text you type is visible. When disabled, the text is not masked as you enter it.
- **Key Strength Meter** — The WAP device checks the key against complexity criteria such as how many different types of characters (uppercase and lowercase alphabetic letters, numbers, and special characters) are used and how long is the string. If the WPA-PSK complexity check feature is enabled, the key is not accepted unless it meets the minimum criteria. See [Configure WAP-PSK Complexity, on page 44](#) for information on configuring the complexity check.
- **Broadcast Key Refresh Rate** — The interval at which the broadcast (group) key is refreshed for clients associated with this VAP. The default is 86400 seconds and the valid range is from 0 to 86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

WPA Enterprise

The WPA Enterprise with RADIUS is an implementation of the Wi-Fi Alliance IEEE 802.11i standard, which includes CCMP (AES), and TKIP encryption. The Enterprise mode requires the use of a RADIUS server to authenticate the users.

This security mode is backwards-compatible with the wireless clients that support the original WPA.

The dynamic VLAN mode is enabled by default, which allows RADIUS authentication server to decide which VLAN is used for the stations.

These parameters configure WPA Enterprise:

- **WPA Versions** — Choose the types of client stations to be supported. The options are:
 - **WPA-TKIP** — The network has some client stations that only support original WPA and TKIP security protocol. Note that selecting only WPA-TKIP for the access point is not allowed as per the latest Wi-Fi Alliance requirement.
 - **WPA2-AES** — All client stations on the network support WPA2 version and AES-CCMP cipher/security protocol. This provides the best security per the IEEE 802.11i standard. As per the latest Wi-Fi Alliance requirement, the AP has to support this mode all the time.
- **Enable Pre-authentication** — If you choose only WPA2 or both WPA and WPA2 as the WPA version, you can enable pre-authentication for the WPA2 clients.

Check this option if you want the WPA2 wireless clients to send the pre-authentication packets. The pre-authentication information is relayed from the WAP device that the client is currently using to the target WAP device. Enabling this feature can help speed up the authentication for roaming clients who connect to multiple APs.

This option does not apply if you selected WPA for WPA versions because the original WPA does not support this feature.

Client stations configured to use WPA with RADIUS must have one of these addresses and keys:

- A valid TKIP RADIUS IP address and RADIUS key
- A valid CCMP (AES) IP address and RADIUS key

- **PMF (Protection Management Frame)**— Provides security for the unencrypted 802.11 management frames. When Security Mode is disabled or WEP, the PMF is set to **No PMF** and is not editable (Hidden or Grey). When the security Mode is set to **WPA2-xxx**, the PMF is **Capable** by default and is editable. The following three check box values can be configured for it.

- **Not Required**
- **Capable**
- **Required**



Note WiFi Alliance requires PMF to be enabled with default setting of **Capable**. You may disable it when non-compliant wireless clients experience instability or connectivity issues.

- **Use Global RADIUS Server Settings** — By default, each VAP uses the global RADIUS settings that you define for the WAP device. However, you can configure each VAP to use a different set of RADIUS servers.

Check this option to use the global RADIUS server settings, or uncheck this option to use a separate RADIUS server for the VAP and enter the RADIUS server IP address and key in the appropriate fields.
- **Server IP Address Type** — The IP version that the RADIUS server uses. You can toggle between the address types to configure the IPv4 and IPv6 global RADIUS address settings, but the WAP device contacts only the RADIUS server or servers for the address type that you select in this field.
- **Server IP Address-1 or Server IPv6 Address-1** — The address for the primary RADIUS server for this VAP.
- **Server IP Address-2 or Server IPv6 Address-2** — Up to three IPv4 and/or IPv6 addresses to use as the backup RADIUS servers for this VAP. If authentication fails with the primary server, each configured backup server is tried in sequence.
- **Key-1** — The shared secret key for the global RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive, and you must configure the same key on the WAP device and on your RADIUS server. The text that you enter is shown as asterisks to prevent others from seeing the RADIUS key as you type.
- **Key-2** — The RADIUS key associated with the configured backup RADIUS servers. The server at Server IP (IPv6) Address 2 uses Key 2.
- **Enable RADIUS Accounting** — Tracks and measures the resources a particular user has consumed such as system time, amount of data transmitted and received, and so on. If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers.
- **Active Server** — Enables the administrative selection of the active RADIUS server, rather than having the WAP device attempt to contact each configured server in sequence and choose the first server that is up.
- **Broadcast Key Refresh Rate** — The interval at which the broadcast (group) key is refreshed for clients associated with this VAP. The default is 86400 seconds. The valid range is from 0 to 86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

- **Session Key Refresh Rate** — The interval at which the WAP device refreshes session (unicast) keys for each client associated with the VAP. The valid range is from 30 to 86400 seconds. A value of 0 indicates that the session key is not refreshed. The default value is 0.

Client Filter

Client filter can be used to permit or deny listed client stations to authenticate with the WAP device. MAC authentication is configured on the [Networks, on page 50](#) page. Based on the VAP configuration, the WAP device may refer to a Client filter list stored on an external RADIUS server, or may refer a Client filter list stored locally on the WAP device.

Configuring a Client Filter List Locally on the WAP device

The WAP device supports one local Client filter list only. The filter can be configured to grant access only to the MAC addresses on the list, or to deny access only to addresses on the list.

Up to 512 Client addresses can be added to the filter list.

To configure the Client filter follow these steps:

-
- Step 1** Select **Wireless > Client Filter**.
- Step 2** Choose how the WAP device uses the filter list:
- **Permit (Permit Only Clients in the List)** —Any station that is not in the Stations List is denied access to the network through the WAP device.
 - **Deny (Deny All Clients in the List)**—Only the stations that appear in the list are denied access to the network through the WAP device. All other stations are permitted access.
- Note** The filter setting also applies to the Client filter list stored on the RADIUS server, if one exists.
- Step 3** Continue entering MAC addresses until the list is complete. Click the arrow next to **Associated Clients** to display the list. Choose one of the MAC address and then click **Add**. One rule will be added to the **MAC Address Table**. The **Associated Clients** list includes the following:
- **MAC Address**—The MAC address of the associated wireless client.
 - **Host Name**—The hostname of the associated wireless client.
 - **IP Address**—The IP address of the associated wireless client.
 - **Network (SSID)**— The Service Set Identifier (SSID) for the WAP device. The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the Network Name.
- Step 4** Click **Apply**.
-

Configuring MAC Authentication on the Radius Server

If one or more VAPs are configured to use a Client filter you must configure the station list on the RADIUS server. The format for the list is described in this table.

RADIUS Server Attribute	Description	Value
User-Name (1)	MAC address of the client station.	Valid Ethernet MAC address
User-Password (2)	A fixed global password used to look up a client MAC entry.	NOPASSWORD

Scheduler

The Radio and VAP scheduler allows you to configure a rule with a specific time interval for the VAPs or radios to be operational.

You can use this feature to schedule the radio to operate or allow access to the VAPs only during the office working hours in order to achieve security and reduce power consumption.

The WAP device supports up to 16 profiles. Only valid rules are added to the profile. Up to 16 rules are grouped together to form a scheduling profile. Periodic time entries belonging to the same profile cannot overlap.

Scheduler Profile Configuration

You can create up to 16 scheduler profile names. By default, no profiles are created.

To view the scheduler status and add a scheduler profile:

Step 1 Select **Wireless > Scheduler**.

Step 2 Check **Enable** to ensure that the **Administrative Mode** is enabled. By default it is disabled.

The **Scheduler Operational Status** area indicates the current operation status of the Scheduler:

- **Status** — The operational status (Enabled or Disabled) of the Scheduler. The default is Disabled.
- **Reason** — The reason for the scheduler operational status. Possible values are:
 - **Is Active** — The scheduler is administratively enabled.
 - **Administrative Mode is disabled** — The scheduler administrative mode is disabled.
 - **System Time is outdated** — The system time is outdated.
 - **Managed Mode** — The scheduler is in managed mode.

- Step 3** To add a profile, enter a profile name in the **Create a Profile Name** text box and click **Add**. The profile name can be up to 32 alphanumeric characters.

Profile Rule Configuration

You can configure up to 16 rules for a profile. Each rule specifies the start time, end time, and day (or days) of the week that 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, hour, and minute) for the start and end time. Rules cannot conflict; for example, you can configure one rule to start on each weekday and another to start on each weekend day, but you cannot configure one rule to begin daily and another rule to begin on weekends.

To configure a profile rule:

- Step 1** Choose the profile from the **Select a Profile Name** list.
- Step 2** Click **+**.
The new rule is displayed in the **Profile Rule Table**.
- Step 3** Check the check box before the **Profile Name** and click **Edit**.
- Step 4** From the **Day of the Week** menu, choose the recurring schedule for the rule. You can configure the rule to occur daily, each weekday, each weekend day (Saturday and Sunday), or any single day of the week.
- Step 5** Set the start and end times:
- **Start Time (24hh:mm)**— Set the time when the radio or VAP is enabled. The time is in hh:mm 24-hour format. The range is <00-23>:<00-59>. The default is 00:00.
 - **End Time (24hh:mm)** — Set the time when the radio or VAP is disabled. The time is in hh:mm 24-hour format. The range is <00-23>:<00-59>. The default is 00:00.
- Step 6** Click **Apply**.
- Note** A scheduler profile must be associated with a radio interface or a VAP interface to be in effect.
To delete a rule, select the profile from the **Profile Name** column and click **Delete**.

QoS

The Quality of Service (QoS) settings allow for configuration of the transmission queues for optimized throughput and enhanced performance when handling differentiated wireless traffic. This traffic can be VoIP, other types of audio, video, streaming media, and traditional IP data.

To configure QoS on the WAP device, set the parameters on the transmission queues for different types of wireless traffic and specify the minimum and maximum wait times for transmission.

The WAP Enhanced Distributed Channel Access (EDCA) parameters affect the traffic flowing from the WAP device to the client station. The station EDCA parameters affect the traffic flowing from the client station to the WAP device.

In normal use, the default values for the WAP device and the station EDCA should not be changed. Changing these values affects the QoS provided.

To configure the WAP device and EDCA parameters:

Step 1 Select **Wireless > QoS**.

Step 2 Choose the radio interface (**Radio 1 or Radio 2**).

Step 3 Choose one of these options from the EDCA drop-down list:

- **WFA Defaults** — Populates the WAP device and the Station EDCA parameters with Wi-Fi Alliance default values, which are best for general, mixed traffic.
- **Optimized For Voice** — Populates the WAP device and the Station EDCA parameters with values that are best for voice traffic.
- **Custom** — Enables you to choose custom EDCA parameters.

These four queues are defined for different types of data transmitted from WAP- to-station. If you choose a Custom template, the parameters that define the queues are configurable; otherwise, they are set to predefined values appropriate to your selection. The four queues are:

- **Data 0 (Voice)** — High priority queue, with minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
- **Data 1 (Video)** — High priority queue, with minimum delay. Time-sensitive video data is automatically sent to this queue.
- **Data 2 (Best Effort)** — Medium priority queue, with medium throughput and delay. Most traditional IP data is sent to this queue.
- **Data 3 (Background)** — Lowest priority queue, with high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

Step 4 Check **Enable** to enable Wi-Fi MultiMedia (WMM) extensions.

Wi-Fi MultiMedia (WMM)— This field is enabled by default. With WMM enabled, QoS prioritization and coordination of wireless medium access is on. With WMM enabled, QoS settings on the WAP device control downstream traffic flowing from the WAP device to client station (AP EDCA parameters) and the upstream traffic flowing from the station to the AP (station EDCA parameters).

Disabling WMM deactivates QoS control of station EDCA parameters on upstream traffic flowing from the station to the WAP device. With WMM disabled, you can still set some parameters on the downstream traffic flowing from the WAP device to the client station (AP EDCA parameters).

Step 5 Configure the following EDCA and Station EDCA parameters:

- **Arbitration Inter-Frame Space (AIFS)** — Wait time for the data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 255.
- **Minimum Contention Window** — An input to the algorithm that determines the initial random backoff wait time (window) for a retry of a transmission failure.

This value is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined. The first random number generated is 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 continues until the size of the random backoff value reaches the number defined in the Maximum Contention Window.

Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. This value must be lower than the value for the Maximum Contention Window.

- **Maximum Contention Window** — 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.

After the Maximum Contention Window size is reached, retries continue until a maximum number of retries allowed is reached.

Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023. This value must be higher than the value for the Minimum Contention Window.

- **Maximum Burst** — A WAP EDCA parameter that applies only to traffic flowing from the WAP 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 are 0.0 through 999.
- **TXOP Limit (Station only)** — The TXOP Limit is a station EDCA parameter that only applies to traffic flowing from the client station to the WAP device. The Transmission Opportunity (TXOP) is an interval of time, in milliseconds, when a WME client station has the right to initiate transmissions onto the wireless medium (WM) towards the WAP device. The TXOP Limit maximum value is 65535.

Step 6 Configure the following additional settings:

- **No Acknowledgment** — Check **Enable** to specify that the WAP device should not acknowledge frames with QoSNoAck as the service class value.
- **Unscheduled Automatic Power Save Delivery (APSD)** — Check **Enable** to enable APSD. The APSD is recommended if VoIP phones access the network through the WAP device.

Step 7 Click **Apply**.



CHAPTER 5

Wireless Bridge

This chapter describes how to configure the **Wireless Bridge** settings. It contains the following topics:

- [Wireless Bridge](#), on page 61
- [Configuring WDS Bridge](#), on page 62
- [WPA/PSK on WDS Links](#), on page 62
- [WorkGroup Bridge](#), on page 63

Wireless Bridge

The Wireless Distribution System (WDS) allows you to connect multiple WAP devices. With WDS, the WAP devices communicate with one another wirelessly. This provides a seamless experience for roaming the clients and managing multiple wireless networks. You can configure the WAP device in point-to-point or point-to-multipoint bridge mode based on the number of links to connect.

In the point-to-point mode, the WAP device accepts client associations and communicates with the wireless clients. The WAP device forwards all traffic meant for the other network over the tunnel that is established between the access points. The bridge does not add to the hop count. It functions as a simple OSI Layer 2 network device.

In the point-to-multipoint bridge mode, one WAP device acts as the common link between multiple access points. In this mode, the central WAP device accepts the client associations and communicates with the clients. All other access points associate only with the central WAP device that forwards the packets to the appropriate wireless bridge for routing purposes.

The WAP device can also act as a repeater. In this mode, the WAP device serves as a connection between two WAP devices that may be too far apart to be within cell range. When acting as a repeater, the WAP device does not have a wired connection to the LAN and repeats signals by using the wireless connection. No special configuration is required for the WAP device to function as a repeater, and there are no repeater mode settings. The wireless clients can still connect to an WAP device that is operating as a repeater.

Before you configure WDS on the WAP device, note these guidelines:

- All Cisco WAP devices participating in a WDS link must have the following identical settings:
 - Radio
 - IEEE 802.11 Mode
 - Channel Bandwidth

- Channel (Auto is not recommended)

When operating bridging in the 802.11n 2.4 GHz band, set the Channel Bandwidth to 20 MHz, rather than the default 20/40 MHz. In the 2.4 GHz, 20/40 MHz band, the operating bandwidth can change from 40 MHz to 20 MHz if any 20 MHz WAP devices are detected in the area. The mismatched channel bandwidth can cause the link to disconnect.

- When using WDS, be sure to configure WDS on both WAP devices participating in the WDS link.
- You can have only one WDS link between any pair of WAP devices. That is, a remote MAC address may appear only once on the WDS page for a particular WAP device.

Configuring WDS Bridge

To configure a WDS bridge:

-
- Step 1** Select **Wireless Bridge**.
- Step 2** Click **WDS** as the Wireless Bridge mode.
- Step 3** Check **Enable** to enable a WDS port in the WDS Settings.
- Step 4** Configure the remaining parameters:
- **Radio** — Specifies the Radio ID (Radio 1 (2.4 GHz) or Radio 2 (5GHz)).
 - **Local MAC Address** — Specifies the physical or MAC address of the current or local WAP device to which data is transmitted from.
 - **Remote MAC Address** — Specifies the MAC address of the destination WAP device. You can find the MAC address on the Monitor > Dashboard > Wireless page.
 - **Encryption** — Select the type of encryption to use on the WDS link (**None or WPA Personal**).
- If you are not concerned about the security issues on the WDS link, you may decide not to set any type of encryption. Alternatively, if you have security concerns, you can choose the WPA Personal. In WPA Personal mode, the WAP device uses WPA2-PSK with CCMP (AES) encryption over the WDS link. See [WPA/PSK on WDS Links, on page 62](#) for more information about encryption options.
- Step 5** Repeat these steps for up to four WDS interfaces.
- Step 6** Click **Apply**.
- Step 7** Replicate this procedure on devices connecting to the bridge.
- Note** You can verify if the bridge link is up by accessing the **Monitor > Dashboard > Wireless** page. In the Interface Status table, the WDS(x) status should state **Up**.
-

WPA/PSK on WDS Links

These additional fields appear when you select WPA/PSK as the encryption type:

- **WDS ID** — Enter an appropriate name for the new WDS link that you have created. It is important that the same WDS ID is also entered at the other end of the WDS link. If this WDS ID is not the same for both WAP devices on the WDS link, they will not be able to communicate and exchange data.

The WDS ID can be any alphanumeric combination within a range of 2-32 characters.

- **Key** — Enter a unique shared key for the WDS bridge. This unique shared key must also be entered for the WAP device at the other end of the WDS link. If this key is not the same for both WAPs, they will not be able to communicate and exchange data.

The WPA-PSK key is a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include uppercase and lowercase alphabetic letters, the numeric digits, and special symbols such as @ and #.

WorkGroup Bridge

The Work Group Bridge feature enables the WAP device to extend the accessibility of a remote network. In the Work Group Bridge mode, the WAP device acts as a wireless station (STA) on the wireless LAN. It can bridge traffic between a remote wired network or associated wireless clients and the wireless LAN that is connected using the Work Group Bridge mode.

The Work Group Bridge feature enables support for STA-mode and AP-mode operation simultaneously. The WAP device can operate in one Basic Service Set (BSS) as an STA device while operating on another BSS as a WAP device. When the Work Group Bridge mode is enabled, the WAP device supports only one BSS for wireless clients that associate with it, and another BSS with which the WAP device associates as a wireless client.

We recommend that you use the Work Group Bridge mode only when the WDS bridge feature cannot be operational with a peer WAP device. WDS is a better solution and is preferred over the Work Group Bridge solution. Use WDS if you are bridging the Cisco WAP150 and Cisco WAP361 devices. If you are not, then consider the Work Group Bridge. When the Work Group Bridge feature is enabled, the WAP configurations are not applied; only the Work Group Bridge configuration is applied.



Note The WDS feature does not work when the Work Group Bridge mode is enabled on the WAP device.

In Work Group Bridge mode, the BSS managed by the WAP device while operating in WAP device mode is referred to as the access point interface, and associated STAs as the downstream STAs. The BSS managed by the other WAP device (that is, the one to which the WAP device associates as an STA) is referred to as the infrastructure client interface, and the other WAP device is referred as the upstream AP.

The devices connected to the wired interface of the WAP device, as well as the downstream stations associated with the access point interface of the device, can access the network connected by the infrastructure client interface. To allow the bridging of packets, the VLAN configuration for the access point interface and the wired interface must match that of the infrastructure client interface.

The Work Group Bridge mode can be used as a range extender to enable BSS to provide access to remote or hard-to-reach networks. A single radio can be configured to forward packets from associated STAs to another WAP device in the same ESS, without using WDS.

Before you configure **Work Group Bridge** on the WAP device, note these guidelines:

- All WAP devices participating in Work Group Bridge must have the following identical settings:

- Radio
- IEEE 802.11 Mode
- Channel Bandwidth
- Channel (Auto is not recommended)

See [Radio, on page 45](#) (Basic Settings) for information on configuring these settings.

- Work Group Bridge mode currently supports only IPv4 traffic.
- Work Group Bridge mode is not supported across a Single Point Setup.

To configure Work Group Bridge mode:

- Step 1** Select **Wireless Bridge**.
- Step 2** Click **WorkGroup**.
- Step 3** Select the WGB Port to which the configuration parameters will be applied.
- Step 4** Click **edit** to configure the following parameters for the Infrastructure Client Interface (Uplink / Downlink):

Table 1: Infrastructure Client Interface (Uplink / Downlink)

WGB Port	Uplink	Downlink
Enabled	Check the check box to enable the Infrastructure Client Interface.	Check the check box to enable the Infrastructure Client Interface.
Radio	Specifies the Radio Id (Radio 1 (2.4 GHz) or Radio 2 (5GHz)).	Specifies the Radio Id (Radio 1 (2.4 GHz) or Radio 2 (5GHz)).
SSID	Specifies the current SSID of the BSS. Note There is an arrow next to SSID for SSID Scanning. This feature is disabled by default, and is enabled only if AP Detection is enabled in Rogue AP Detection (which is also disabled by default).	The SSID for the Access Point Interface cannot be the same as the Infrastructure Client SSID.
Encryption	The type of security to use for authenticating as a client station on the upstream WAP device. It can be one of the following: <ul style="list-style-type: none"> • None • WPA Personal • WPA Enterprise 	The type of security to use for authenticating. The options are: <ul style="list-style-type: none"> • None • WPA Personal
Connection Status	Indicates whether the WAP is connected to the upstream WAP device.	Not Applicable (N/A)

WGB Port	Uplink	Downlink
VLAN ID	Specifies the VLAN associated with the BSS.	Configure the Access Point Interface with the same VLAN ID as advertised on the Infrastructure Client Interface.
<p>Note The Infrastructure Client Interface will be associated with the upstream WAP device with the configured credentials. The WAP device may obtain its IP address from a DHCP server on the upstream link. Alternatively, you can assign a static IP address.</p>		
SSID Broadcast	Specifies if the broadcast of the SSID is available, enabled or disabled.	Check if you want the downstream SSID to be broadcast. SSID Broadcast is enabled by default.
Client Filter	Not Applicable (N/A)	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> • Disabled—The set of clients in the APs BSS that can access the upstream network is not restricted to the clients specified in a MAC address list. • Local—The set of clients in the APs BSS that can access the upstream network is restricted to the clients specified in a locally defined MAC address list. • RADIUS—The set of clients in the APs BSS that can access the upstream network is restricted to the clients specified in a MAC address list on a RADIUS server.
<p>Note If you choose Local or RADIUS, see Client Filter, on page 56 for instructions on creating the Client filter list.</p>		

Step 5 Click **Apply**. The associated downstream clients now have connectivity to the upstream network.



CHAPTER 6

Fast Roaming

This chapter describes how to configure the Fast Roaming settings. It contains the following topics:

- [Fast Roaming](#), on page 67
- [Configuring Fast Roaming](#), on page 67
- [Configuring Remote Key Holder List Profiles](#), on page 68

Fast Roaming

Fast roaming, also known as IEEE 802.11r or Fast BSS Transition (FT), allows a client device to *roam* quickly in environments implementing the WPA2 Enterprise security, by ensuring that the client device does not need to re-authenticate to the RADIUS server every time it roams from one access point to another.

Fast transition roaming is an amendment to the IEEE 802.11 standard that permits continuous connectivity aboard wireless devices in motion, with fast and secure handoffs from an AP to another managed AP in a seamless manner. In order to ensure voice quality and network security, a portable station must be able to maintain a secure, low-latency voice call while roaming between APs that are handling other traffic.

This device supports the FBT (Fast BSS Transition) as defined in 802.11r for fast handoff with WPA2 Enterprise security. For Voice over WI-FI Enterprise, only a subset of the features defined in 802.11r are supported. The fast BSS transition decreases latency during roaming.

FBT is enabled per VAP per radio.



Note Before you configure FBT on a VAP, be sure to verify that the VAP is configured with WPA2 security, pre-authentication disabled and MFP disabled.

Configuring Fast Roaming

These steps give a general description of how to configure fast roaming:

-
- Step 1** Select **Fast Roaming > Roaming Table**.
 - Step 2** Click **+** to add a new row to the roaming table.
 - Step 3** Configure the following parameters:

- **Enable** — This option is checked by default.
- **BSSID** — Select the VAP (**2.4GVAP 0** or **5G VAP 0**) to enable.
- **Mobility Domain** — Specifies the Mobility Domain identifier (MDID) of the FBT VAP. The MDID is used to indicate a group of APs within an ESS, between which a STA can use fast BSS transition services. Fast BSS transitions are allowed only between APs that have the same MDID and are within the same ESS. They are not allowed between APs with different MDIDs or in different ESSs.
- **FT Mode** — Fast Transition protocol allows Mobile Station (MS) to fully authenticate only with the first AP in the domain (the group of APs that support FT Protocol and are connected over Distribution System (DS)), and use shorter association procedure with the next APs in the same domain. Choose one of the following methods of FT:
 - **Over Air** — In the Over Air method the Mobile Station communicates over a direct 802.11 link to the new AP.
 - **Over DS** — In the Over DS method the MS communicates with the new AP via the old AP.
- **R0 Key Holder** — Specifies the NAS identifier to be sent in the radius Access Request Message. The NAS Identifier is used as R0 Key holder ID.
- **R1 Key Holder** — Specifies the R1 Key Holder ID that names the holder of PMK-R1 in the authenticator.
- **Remote Key Holder List** — Select a Remote Key Holder List from the drop down menu that you have created.

Step 4 Click **Apply**.

Note To delete or modify a roaming setting, select it and then click **Delete** or **Edit**.

After configuring the FBT settings, click **Apply** to save the settings. Changing some settings might cause the AP to stop and restart the system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when the WLAN traffic is low.

Configuring Remote Key Holder List Profiles

To configure Remote R0 Key Holder List profiles:

- Step 1** Select **Fast Roaming > Remote Key Holder List Profile**.
- Step 2** Click **+** to add a new profile or **edit** to modify an existing profile. The **Remote Key Holder List Profiles** page is displayed.
- Step 3** Specify a name for the Remote Key Holder List Profile.
- Step 4** Configure the following parameters. A maximum of 10 entries of R0 Key holders are allowed to be configured per VAP.
 - **MAC Address** — Enter the destination's VAP MAC address which is the R0 key holder. The RRB PULL message is sent to this AP MAC address to fetch the PMKR1 key. This MAC address must be unique across all the VAPs.
 - **NAS ID** — NAS ID configured on the destination FBT enabled VAP.
 - **RRB Key** — Key used to encrypt RRM protocol messages.

Step 5 Repeat steps 1 through 4 and then configure the R1 key holder in the Remote R1 Key Holder Data List. A maximum of 10 entries of R1 key holders are allowed to be configured per VAP. The key holder data is configured per VAP.

- **MAC Address** — Destination's VAP MAC address which is the R1 Key holder. The PMKR1 is sent in RRB PUSH message to this AP MAC address. This MAC Address must be unique across all the VAPs.
- **R1 Key Holder** — The R1 key Holder ID that names the holder of PMK-R1 in the authenticator.
- **RRB Key** — Key used to encrypt RRM protocol messages.

Note After you configure the Remote Key Holder Data List settings, you can click **Restore** to restore the old settings, or click **Apply** to save the settings. Click **Cancel** to go back before **Fast Roaming** page.

Click **Apply** after copying or deleting a profile.

Caution Clicking **Export** for selected profile/s will export only those profiles. Clicking **Export** with no profiles selected will **Export** all the profiles.



CHAPTER 7

Access Control

This chapter describes how to configure the ACL and the quality of service (QoS) feature on the WAP device. It contains the following topics:

- [ACL, on page 71](#)
- [Client QoS, on page 78](#)
- [Guest Access, on page 86](#)

ACL

Access Control Lists (ACLs) are a collection of permit and deny conditions, called rules, that provide security by blocking unauthorized users and allowing authorized users to access specific resources. ACLs can block any unwarranted attempts to reach network resources.

The WAP device supports up to 50 IPv4, IPv6, and MAC ACLs and up to 10 rules in each ACL. Each ACL supports multiple interfaces.

IPv4 and IPv6 ACLs

Each ACL is a set of rules applied to traffic received by the WAP device. 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 or more fields within a packet, such as the source or destination IP address, the source or destination port, or the protocol carried in the packet. The IP ACLs classify traffic for Layers 3 and 4.



Note There is an implicit deny at the end of every rule created. To avoid denying all, we strongly recommend that you add a permit rule to the ACL to allow traffic.

MAC ACLs

MAC ACLs are Layer 2 ACLs. You can configure the rules to inspect fields of a frame such as the source or destination MAC address, the VLAN ID, or the class of service. When a frame enters the WAP device port, the WAP device inspects the frame and checks the ACL rules against the content of the frame. If any of the rules match the content, a permit or deny action is taken on the frame.

Workflow to Configure ACLs

Use the ACL Rule(s) to configure the ACLs, and then apply the rules to a specified interface.

To configure the ACLs follow these steps:

-
- Step 1** Select **Access Control > ACL**.
 - Step 2** In the ACL Table, click **+** to add a new row and create an ACL.
 - Step 3** Enter a name for the ACL.
 - Step 4** Select the ACL type from the drop down list (**IPv4**, **IPv6** or **MAC**).
 - Step 5** Click **+**, select the associated interfaces to apply the ACL, and click **OK**. If you want to change the associated interfaces, you can click **-** to delete the selected interfaces, and click **+** to choose the new associated interfaces.
 - Step 6** Click **More** to view the ACL's parameters.
 - Step 7** Next, to configure the rules for the ACL. For IPv4 ACLs, see [Configure IPv4 ACLs, on page 72](#). For IPv6 ACLs, see [Configure IPv6 ACLs, on page 74](#). For MAC ACLs, see [Configure MAC ACLs, on page 77](#).
 - Step 8** Click **Apply** to save all changes.
-

Configure IPv4 ACLs

To configure an IPv4 ACL:

-
- Step 1** Select **Access Control > ACL**.
 - Step 2** Click **+** to add an ACL.
 - Step 3** In the **ACL Name** field, enter the name of the ACL. The name is limited to 31 alphanumeric and special characters without any space.
 - Step 4** Choose **IPv4** as the **ACL Type** from the ACL Type list. The IPv4 ACL's control access to the network resources are based on the Layer 3 and Layer 4 criteria.
 - Step 5** Click **+** and select the associated interfaces to apply the ACL. Click **OK**. If you want to change the associated interfaces, you can click **-** to delete the selected interface, and click **+** to choose new associated interfaces.
 - Step 6** Click **More...** to view the configuration parameters. Click **+** to add a rule and configure the following:

Note If no rules are added, the WAP denies all the traffic by default.

- **Rule Priority** — When an ACL has multiple rules, the rules are applied to the packet or frame in order of priority. A smaller number means a higher priority. The priority of the new rule will be the lowest of all explicit rules. Note that there is always an implicit rule denying all traffic with lowest priority.

- **Action** — Choose whether to **Deny** or **Permit** the action. The default action is **Deny**.

When you choose **Permit**, the rule allows all traffic that meets the rule criteria to enter the WAP device. Traffic that does not meet the criteria is dropped.

When you choose **Deny**, the rule blocks all traffic that meets the rule criteria from entering the WAP device. 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.

- **Service (Protocol)** — Uses a Layer 3 or Layer 4 protocol match condition based on the value of the IP Protocol field. You can choose one of these options:
 - **All Traffic** — Allows all traffic that meets the rule criteria
 - **Select From List** — Choose one of these protocols: **IP, ICMP, IGMP, TCP, or UDP.**
 - **Custom** — Enter a standard IANA-assigned protocol ID from 0 to 255. Choose this method to identify a protocol not listed in the Select From List.

- **Source IPv4 Address** — Requires the packet's source IP address to match the address defined in the appropriate fields.
 - **Any**— Allows for any IP address.
 - **Single Address** — Enter the IP address to apply this criteria.
 - **Address/Mask** — Enter the source IP address wild card mask. The wild card mask determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wild card of 0.0.0.0 indicates that all bits are important.

A wild card mask is basically the inverse of a subnet mask. For example, to match the criteria to a single host address, use a wild card mask of 0.0.0.0. To match the criteria to a 24-bit subnet (for example, 192.168.10.0/24), use a wild card mask of 0.0.0.255.

- **Source Port** — Includes a source port in the match condition for the rule. The source port is identified in the datagram header
 - **All Traffic**— Allows all traffic that meets the rule criteria.
 - **Select From List** — Choose the keyword associated with the source port to match: **ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.** Each of these keywords translates into its equivalent port number.
 - **Custom** — Enter the IANA port number to match to the source port identified in the datagram header. The port range is 0 to 65535 and includes three different types of ports:
 - 0 to 1023 — Well known ports
 - 1024 to 49151 — Registered ports
 - 49152 to 65535 — Dynamic and/or private port

- **Destination IPv4 Address** — Requires a packet's destination IP address to match the address defined in the appropriate fields.
 - **Any** — Enter any IP address.
 - **Single Address** — Enter an IP address to apply this criteria.
 - **Address/ Mask** — Enter the destination IP address wild card mask. The wild card mask determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wild card of 0.0.0.0 indicates that all bits are important.

A wild card mask is basically the inverse of a subnet mask. For example, to match the criteria to a single host address, use a wild card mask of 0.0.0.0. To match the criteria to a 24-bit subnet (for example, 192.168.10.0/24), use a wild card mask of 0.0.0.255.

- **Destination Port** — Includes a destination port in the match condition for the rule. The destination port is identified in the datagram header.
 - **Any** — Any port that meets the rule criteria.
 - **Select From List** — Choose the keyword associated with the destination port to match: **ftp, ftpdata, http, smtp, snmp, telnet, tftp, www**. Each of these keywords translates into its equivalent port number.
 - **Custom** — Enter the IANA port number to match to the destination port identified in the datagram header. The port range is from 0 to 65535 and includes three different types of ports:
 - 0 to 1023 — Well known ports
 - 1024 to 49151 — Registered ports
 - 49152 to 65535 — Dynamic and/or private port

- **Type Of Service** — Matches the packets based on specific service type.
 - **Any** — Any type of service.
 - **Select From List** — Matches the packets based on their DSCP Assured Forwarding (AS), Class of Service (CS), or Expedited Forwarding (EF) values.
 - **DSCP** — Matches the packets based on a custom DSCP value. If selected, enter an value from 0 to 63 in this field.
 - **Precedence** — Matches the packets based on their IP precedence value. If selected, enter an IP Precedence value from 0 to 7.
 - **ToS/Mask** — Enter an IP ToS Mask value to identify the bit positions in the IP ToS Bits value that are used for comparison against the IP ToS field in a packet.

The IP ToS Mask value is a two-digit hexadecimal number from 00 to FF, representing an inverted (that is, wild card) mask. The zero-valued bits in the IP ToS Mask denote the bit positions in the IP 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 an IP ToS Bits value of 0 and an IP ToS Mask of 00.

Step 7 Click **OK**. The changes are saved to the Startup Configuration.

Note To delete or modify an ACL, select the ACL and then click **Delete** or **Edit**

To delete or modify a rule, select the rule in the **Details Of Rule(s)** area and click **Delete** or **Edit**.

Step 8 Click **Apply**.

Configure IPv6 ACLs

To configure an IPv6 ACL:

Step 1 Select **Access Control > ACL**.

- Step 2** Click **+** to add an ACL.
- Step 3** In the **ACL Name** field, enter the name of the ACL.
- Step 4** Choose **IPv6** as the ACL type from the **ACL Type** list. The IPv4 ACL's control access to the network resources are based on the Layer 3 and Layer 4 criteria.
- Step 5** Click **+** and select the associated interfaces to apply the ACL. Next, click **OK**. If you want to change the associated interfaces, you can click **-** to delete the selected interface then click **+** to choose new associated interfaces.
- Step 6** Click **More...** to view the configuration parameters. Click **+** to add a rule and configure the following:

Note If no rules are added, the WAP denies all traffic by default.

- **Rule Priority** — When an ACL has multiple rules, the rules are applied to the packet or frame in order of priority. A smaller number means a higher priority. The priority of the new rule will be the lowest of all explicit rules. You can click the up or down button to change its priority. Note that there is always an implicit rule denying all traffic with lowest priority.
- **Action** — Choose whether to **Deny** or **Permit** the action. The default action is **Deny**.
When you choose **Permit**, the rule allows all traffic that meets the rule criteria to enter the WAP device. Traffic that does not meet the criteria is dropped.
When you choose **Deny**, the rule blocks all traffic that meets the rule criteria from entering the WAP device. 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.
- **Service (Protocol)** — Uses a Layer 3 or Layer 4 protocol match condition based on the value of the IP Protocol field. You can choose one of these options:
 - **All Traffic** — Allows all traffic that meets the rule criteria.
 - **Select From List** — Choose one of these protocols: **IPv6, ICMPv6, IGMP, TCP, or UDP**.
 - **Custom** — Enter a standard IANA-assigned protocol ID from 0 to 255. Choose this method to identify a protocol not listed in the Select From List.
- **Source IPv6 Address** — Requires the packet's source IP address to match the address defined in the appropriate fields.
 - **Any**— Allows for any IP address.
 - **Single Address** — Enter the IP address to apply this criteria.
 - **Address/Mask** — Enter the source IP address wild card mask. The wild card mask determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wild card of 0.0.0.0 indicates that all bits are important.
A wild card mask is basically the inverse of a subnet mask. For example, to match the criteria to a single host address, use a wild card mask of 0.0.0.0. To match the criteria to a 24-bit subnet (for example, 192.168.10.0/24), use a wild card mask of 0.0.0.255.
- **Source Port** — Includes a source port in the match condition for the rule. The source port is identified in the datagram header.
 - **Any**— Allows for any source port.
 - **Select From List** — Choose the keyword associated with the source port to match: **ftp, ftpdata, http, smtp, snmp, telnet, tftp, www**. Each of these keywords translates into its equivalent port number.

- **Custom** — Enter the IANA port number to match to the source port identified in the datagram header. The port range is 0 to 65535 and includes three different types of ports:
 - 0 to 1023 — Well known ports
 - 1024 to 49151 — Registered ports
 - 49152 to 65535 — Dynamic and/or private port

- **Destination IPv6 Address** — Requires a packet's destination IP address to match the address defined in the appropriate fields.
 - **Any** — Enter any IP address.
 - **Single Address** — Enter an IP address to apply this criteria.
 - **Address/ Mask** — Enter the destination IP address wild card mask. The wild card mask determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wild card of 0.0.0.0 indicates that all bits are important.

A wild card mask is basically the inverse of a subnet mask. For example, to match the criteria to a single host address, use a wild card mask of 0.0.0.0. To match the criteria to a 24-bit subnet (for example, 192.168.10.0/24), use a wild card mask of 0.0.0.255.

- **Destination Port** — Includes a destination port in the match condition for the rule. The destination port is identified in the datagram header.
 - **Any** — Any port that meets the rule criteria.
 - **Select From List** — Choose the keyword associated with the destination port to match: **ftp, ftpdata, http, smtp, snmp, telnet, tftp, www**. Each of these keywords translates into its equivalent port number.
 - **Custom** — Enter the IANA port number to match to the destination port identified in the datagram header. The port range is from 0 to 65535 and includes three different types of ports:
 - 0 to 1023 — Well known ports
 - 1024 to 49151 — Registered ports
 - 49152 to 65535 — Dynamic and/or private port

- **Flow Label** — Specifies a 20-bit number that is unique to an IPv6 packet.
 - **Any** — Any 20-bit number.
 - **DSCP** — Matches the number based on a custom DSCP value.

- **DSCP** — Matches the packets based on their IP DSCP value.
 - **Any** — Allows for any DSCP value.
 - **Select From List** — Select a DSCP value from the drop down list.
 - **Custom** — Enter a custom DSCP value, from 0 to 63.

Step 7 Click **OK**. The changes are saved to the Startup Configuration.

- Note** To delete or modify an ACL, select the ACL and then click **Delete** or **Edit**.
To delete or modify a rule, select the rule in the **Details Of Rule(s)** area and click **Delete** or **Edit**.

Step 8 Click **Apply**.

Configure MAC ACLs

To configure a MAC ACL:

- Step 1** Select **Access Control > ACL**.
- Step 2** Click **+** to add a MAC ACL.
- Step 3** In the ACL Name field, enter the name to identify the ACL.
- Step 4** Choose **MAC** as the type of ACL from the list. MAC ACLs control access based on Layer 2 criteria.
- Step 5** Click **+** and select the associated interfaces to apply the ACL and click **OK**. If you want to change the associated interfaces, you can click **-** to delete the selected interface and then click **+** to choose new associated interfaces.
- Step 6** Then, click **More** to view the configuration parameters. Click **+** to add a rule and configure the following parameters:
- **Rule Priority** — When an ACL has multiple rules, the rules are applied to the packet or frame in the order of their priorities. Smaller number means higher priority. The priority of the new rule will be the lowest of all explicit rules and you can click the up or down button to change its priority. Note that there is always an implicit rule denying all traffic with lowest priority.
 - **Action** — Choose whether to **Deny** or **Permit** the action. The default action is **Deny**.
When you choose **Permit**, the rule allows all traffic that meets the rule criteria to enter the WAP device. Traffic that does not meet the criteria is dropped.
When you choose **Deny**, the rule blocks all traffic that meets the rule criteria from entering the WAP device. 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.
 - **Service (ETH Type)** — Choose to compare the match criteria against the value in the header of an Ethernet frame. You can select an ETH Type from the drop down list.
 - **Any** — Allows for any protocol.
 - **Select From List** — Choose one of these protocol types: **ARP, IPv4, IPv6, IPX, NetBIOS, PPPoE**.
 - **Custom** — Enter a custom protocol identifier to which the packets are matched. The value is a four-digit hexadecimal number in the range of 0600 to FFFF.
 - **Source MAC Address** — Requires the packet's source MAC address to match the address defined in the appropriate fields.
 - **Any** — Allows for any source MAC address.
 - **Single Address** — Enter the source MAC address to compare against an Ethernet frame.
 - **Address/ Mask** — Enter the source MAC address mask specifying which bits in the source MAC to compare against an Ethernet frame.

For each bit position in the MAC mask, a 0 indicates that the corresponding address bit is significant and a 1 indicates that the address bit is ignored. For example, to check only the first four octets of a MAC address, a MAC mask of 00:00:00:00:ff:ff is used. A MAC mask of 00:00:00:00:00:00 checks all address bits and is used to match a single MAC address.

- **Destination MAC Address** — Requires the packet's destination MAC address to match the address defined in the appropriate fields.
 - **Any** — Allows for any destination MAC address.
 - **Single Address** — Enter the destination MAC address to compare against an Ethernet frame.
 - **Address/Mask** — Enter the destination MAC address mask to specify which bits in the destination MAC to compare against an Ethernet frame
- **VLAN ID** — The VLAN ID to compare against an Ethernet frame.
 - **Any** — Allows for any VLAN ID.
 - **Custom** — Enter the specific VLAN ID to compare against an Ethernet frame. This field is located in the first/only 802.1Q VLAN tag. The port range is 1 to 4094.
- **Class Of Service** — Specifies the class of service 802.1p user priority value.
 - **Any** — Allows for any class of service.
 - **Custom** — Enter an 802.1p user priority to compare against an Ethernet frame. The valid range is from 0 to 7.

Step 7 Click **OK**. The changes are saved to the Startup Configuration.

Note To delete or modify an ACL, select the ACL and then click **Delete** or **Edit**. To delete or modify a rule, select the rule in the **Rule Configuration** area and click **Delete** or **Edit**.

Step 8 Click **Apply**.

Client QoS

Client Quality Of Service (QoS) is used to control the wireless clients connected to the network, and manages the bandwidth that is used. Client QoS can control the traffic such as the HTTP traffic or traffic from a specific subnet by the use of Access Control Lists (ACLs). An ACL is a collection of permit and deny conditions, called rules, that provide security and block unauthorized users and allow authorized users to access specific resources. ACLs can block any unwarranted attempts to reach network resources.

Traffic Classes

The QoS feature contains Differentiated Services (DiffServ) support that allows traffic to be classified into streams. It is also given a certain QoS treatment in accordance with defined per-hop behaviors.

The standard IP-based networks are designed to provide best-effort data delivery service. Best effort service implies that the network delivers the data in a timely fashion, although there is no guarantee that it will. During times of congestion, packets may be delayed, sent sporadically, or dropped. For typical Internet applications,

such as email and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. However, on applications with strict timing requirements, such as voice or multimedia, any degradation of service has undesirable effects.

A DiffServ configuration begins with defining class maps, which classify traffic according to their IP protocol and other criteria. Each class map can then be associated with a policy map, which defines how to handle the traffic class. Classes that include time-sensitive traffic can be assigned to the policy maps.

Configuring IPv4 Traffic Classes

To add and configure an IPv4 class map:

Step 1 Select **Client QoS > Traffic Classes**.

Step 2 Click **+** to add a Traffic Class.

Note The maximum number of class maps is 50.

Step 3 In the **Traffic Class Name** text box, enter the name for the new class map. The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

Step 4 In the **Class Type**, choose **IPv4** from the list. The IPv4 traffic classes applies only to IPv4 traffic on the WAP device.

Step 5 Configure the following:

- **Source Address** — Requires a packet's source IPv4 address to match the IPv4 address defined in the appropriate fields.
 - **Any** — Any IPv4 address to be used as the source address.
 - **Single Address** — Enter a single IPv4 address to apply this criteria.
 - **Address/ Mask**— Enter the source IPv4 address mask. The mask for DiffServ is a network-style bit mask in IP dotted decimal format indicating which part(s) of the destination IP address to use for matching against packet content.

A DiffServ mask of 255.255.255.255 indicates that all bits are important, and mask of 0.0.0.0 indicates that no bits are important. The opposite is true with an ACL wild card mask. For example, to match the criteria to a single host address, use a mask of 255.255.255.255. To match the criteria to a 24-bit subnet (for example, 192.168.10.0/24), use a mask of 255.255.255.0.
- **Destination Address** — Requires a packet's destination IPv4 address to match the IPv4 address defined in the appropriate fields.
 - **Any** — Any IPv4 address to be used as the destination address.
 - **Single Address** — Enter the IPv4 address to apply this criteria.
 - **Address/Mask** — Enter the destination IP address mask.

Step 6 Click **More...**, and configure the following parameters:

- **Protocol** — Uses a Layer 3 or Layer 4 protocol match condition based on the value of the IP Protocol field in IPv4 packets or the Next Header field in IPv6 packets. Choose the protocol to match by keyword or enter a protocol ID:
 - **All Traffic** — Allows all traffic from any protocol.

- **Select From List** — Matches the selected protocol: **IP, ICMP, IGMP, TCP** or **UDP**.
- **Custom** — Matches a protocol that is not listed by name. Enter the protocol ID. The protocol ID is a standard value assigned by IANA. The range is a number from 0 to 255.

Note If **Protocol** is All Traffic, **Source Address** and **Destination Address** are not optional.

- **Source Port** — Includes a source port in the match condition for the rule. The source port is identified in the datagram header.
 - **Any** — Any port is allowed as the source port.
 - **Select From List** — Matches a keyword associated with the source port: **ftp, ftpdata, http, smtp, snmp, telnet, tftp** or **www**. Each of these keywords translates into its equivalent port number.
 - **Custom** — Matches the source port number in the datagram header to an IANA port number that you specify. The port range is from 0 to 65535 and includes three different types of ports:
 - 0 to 1023 — Well-Known ports
 - 1024 to 49151 — Registered ports
 - 49152 to 65535 — Dynamic and/or private ports
- **Destination Port** — Includes a destination port in the match condition for the rule. The destination port is identified in the datagram header.
 - **Any** — Any port is allowed as the destination port.
 - **Select From List** — Matches a keyword associated with the source port: **ftp, ftpdata, http, smtp, snmp, telnet, tftp** or **www**. Each of these keywords translates into its equivalent port number.
 - **Custom** — Matches the source port number in the datagram header to an IANA port number that you specify. The port range is from 0 to 65535 and includes three different types of ports:
 - 0 to 1023 — Well-known ports
 - 1024 to 49151 — Registered ports
 - 49152 to 65535 — Dynamic and/or private ports
- **Service Type** — Specifies the type of service to use in matching the packets to the class criteria.
 - **Any** — Allows for any type of service as a match criterion.
 - **IP DSCP Select from List** — Choose a DSCP value to use as a match criterion.
 - **IP DSCP Match to Value** — Enter a custom DSCP value from 0 to 63.
 - **IP Precedence** — Matches the packet's IP precedence value to the IP precedence value defined in this field. The IP precedence range is from 0 to 7.
 - **IP ToS Bits** — Uses the packet's type of service (ToS) bits in the IP header as the match criteria. The IP ToS bit value ranges between (00 to FF). The high-order three bits represent the IP precedence value. The high-order six bits represent the IP DSCP value.
 - **IP ToS Mask** — Enter an IP ToS Mask value to identify the bit positions in the IP ToS Bits value that are used for comparison against the IP ToS field in a packet.

The IP ToS Mask value is a two-digit hexadecimal number from 00 to FF. The nonzero-valued bits in the IP ToS Mask denote the bit positions in the IP ToS Bits value that are used for comparison against the IP ToS field of a packet.

Step 7 Click **OK**. The changes are saved to the Startup Configuration.

Note To delete or modify a class map, select the **Traffic Class Name** from the list and click **Delete** or **Edit**. The class map cannot be deleted if it is already attached to a policy.

Step 8 Click **Apply**.

Configuring IPv6 Traffic Classes

To add and configure an IPv6 class map:

Step 1 Select **Client QoS > Traffic Classes**.

Step 2 Click **+** to add a Traffic Class.

Note The maximum number of class maps is 50.

Step 3 In the **Traffic Class Name** field, enter the name for the new class map. The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

Step 4 Choose **IPv6** as the type of Traffic Classes from the list. The IPv6 traffic classes applies only to IPv6 traffic on the WAP device.

Step 5 Configure the following:

- **Source Address** — Requires a packet's source IPv6 address to match the IPv6 address defined in the appropriate fields.
 - **Any** — Any IPv6 address to be used as the source address.
 - **Single Address** — Enter the IPv6 address to apply this criteria.
 - **Address/ Mask**— Enter the prefix length of the source IPv6 address.
- **Destination Address** — Requires a packet's destination IPv4 address to match the IPv4 address defined in the appropriate fields.
 - **Any** — Any IPv6 address to be used as the destination address.
 - **Single Address** — Enter the IPv6 address to apply this criteria.
 - **Address/Mask** — Enter the destination IPv6 address and Enter the prefix length of the destination IPv6 address.

Step 6 Click **More...**, and configure the following parameters:

- **Protocol** — Uses a Layer 3 or Layer 4 protocol match condition based on the value of the IP Protocol field in IPv4 packets or the Next Header field in IPv6 packets. Choose the protocol to match by keyword or enter a protocol ID:
 - **All Traffic** — Allows all traffic from any protocol.

- **Select From List** — Matches the selected protocol: **IPv6, ICMPv6, TCP** or **UDP**.
- **Custom** — Matches a protocol that is not listed by name. Enter the protocol ID. The protocol ID is a standard value assigned by IANA. The range is a number from 0 to 255.
- **Source Port** — Includes a source port in the match condition for the rule. The source port is identified in the datagram header.

Note If **Protocol** is All Traffic, **Source Address** and **Destination Address** are not optional.

- **Any** — Any port is allowed as the source port.
- **Select From List** — Matches a keyword associated with the source port: **ftp, ftpdata, http, smtp, snmp, telnet, ftp** or **www**. Each of these keywords translates into its equivalent port number.
- **Custom** — Matches the source port number in the datagram header to an IANA port number that you specify. The port range is from 0 to 65535 and includes three different types of ports:
 - 0 to 1023 — Well-Known Ports
 - 1024 to 49151 — Registered Ports
 - 49152 to 65535 — Dynamic and/or Private Port
- **Destination Port** — Includes a destination port in the match condition for the rule. The destination port is identified in the datagram header.
 - Any — Any port is allowed as the destination port.
 - **Select From List** — Matches a keyword associated with the source port: **ftp, ftpdata, http, smtp, snmp, telnet, tftp** or **www**. Each of these keywords translates into its equivalent port number.
 - **Custom** — Matches the source port number in the datagram header to an IANA port number that you specify. The port range is from 0 to 65535 and includes three different types of ports:
 - 0 to 1023 — Well-Known Ports
 - 1024 to 49151 — Registered Ports
 - 49152 to 65535 — Dynamic and/or Private Port
- **IPv6 Flow Label** — The Flow Label is used by a node to label packets in a flow.
 - **Any** — Any 20-bit number that is unique to an IPv6 packet.
 - **User Defined** — Enter a 20-bit number that is unique to an IPv6 packet. It is used by end stations to signify QoS handling in routers (range 0 to FFFFF).
- **Service Type** — Specifies the type of service to use in matching the packets to the class criteria.
 - **Any** — Allows for any type of service as a match criterion.
 - **IP DSCP Select from List** — Choose a DSCP value to use as a match criterion.
 - **IP DSCP Match to Value** — Enter a custom DSCP value from 0 to 63

Step 7 Click **OK**. The changes are saved to the Startup Configuration.

Note To delete or modify a class map, select the **Traffic Class Name** from the list and click **Delete** or **Edit**. The class map cannot be deleted if it is already attached to a policy.

Step 8 Click **Apply**.

Configuring MAC Traffic Classes

To add and configure a MAC class map:

Step 1 Select **Client QoS > Traffic Classes**.

Step 2 Click **+** to add a Traffic Class.

Note The maximum number of class maps is 50.

Step 3 In the Traffic Class Name field, enter the name for the new class map. The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

Step 4 Choose **MAC** as the type of class map from the Class Map Type list. The MAC class map applies to Layer 2 criteria.

Step 5 **Source Address** — Includes a source MAC address in the match condition for the rule.

- **Any** — Any MAC address to be used as the source address.
- **Single Address** — Enter the source MAC address to compare against an Ethernet frame.
- **Address/Mask** — Enter the source MAC address mask specifying which bits in the destination MAC address to compare against an Ethernet frame.

For each bit position in the MAC mask, a 1 indicates that the corresponding address bit is significant and a 0 indicates that the address bit is ignored. For example, to check only the first four octets of a MAC address, a MAC mask of ff:ff:ff:ff:00:00 is used. A MAC mask of ff:ff:ff:ff:ff:ff checks all address bits and is used to match a single MAC address.

Step 6 **Destination Address** — Includes a destination MAC address in the match condition for the rule.

- **Any** — Any MAC address to be used as the destination address.
- **Single Address** — Enter the destination MAC address to compare against an Ethernet frame.
- **Address/Mask** — Enter the destination MAC address mask specifying which bits in the destination MAC address to compare against an Ethernet frame.

Step 7 Click **More**, and configure the following parameters:

- **Protocol** — Compares the match criteria against the value in the header of an Ethernet frame. Choose an EtherType keyword or enter an EtherType value to specify the match criteria:
 - **All Traffic** — Allows all traffic from any protocol.
 - **Select From List** — Matches the Ethertype in the datagram header with the selected protocol types: Apple Talk, ARP, IPv4, IPv6, IPX, NETBIOS, PPPoE.
 - **Custom** — Matches the Ethertype in the datagram header with a custom protocol identifier that is specified. The value can be a four-digit hexadecimal number in the range of 0600 to FFFF.

Note If **Protocol** is All Traffic, **Source Address** and **Destination Address** are not optional.

- **Class Of Service** — Specifies the class of service 802.1p user priority value.
 - **Any** — Allows for any class of service.
 - **User Defined** — Enter an 802.1p user priority to compare against an Ethernet frame. The valid range is from 0 to 7.
- **VLAN ID** — The VLAN ID to compare against an Ethernet frame.
 - **Any** — Allows for any VLAN ID.
 - **User Defined** — Enter the specific VLAN ID to compare against an Ethernet frame. This field is located in the first/only 802.1Q VLAN tag. The port range is 1 to 4094.

Step 8 Click **OK**. The changes are saved to the Startup Configuration.

Note To delete or modify a class map, choose the class map from the list and click **Delete**. The class map cannot be deleted if it is already attached to a policy.

Step 9 Click **Apply**.

QoS Policy

Packets are classified and processed based on the defined criteria. The classification criteria is defined by a class on the Class Map page. The processing is defined by the policy attributes on the **Policy Map** page. Policy attributes may be defined on a per-class instance basis and determine how traffic that matches the class criteria is handled.

The WAP device can hold up to 50 policies and up to 10 classes in each policy.

To add and configure a policy map:

Step 1 Select **Client QoS > QoS Policy**.

Step 2 Click **+** to add a QoS Policy. In the QoS Policy Name field, enter the name for the QoS policy. The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

Step 3 You can select an associated traffic class that was created previously.

Step 4 In the **QoS Policy Definition** area, configure these parameters for the policy map:

- **Committed Rate** — The committed rate, in Kbps, to which traffic must conform. The range is between 1 to 1000000 Kbps.
- **Committed Burst** — The committed burst size, in bytes, to which traffic must conform. The range is from 1 to 1600000Kbps.
- **Action** — Select from one of the following options:
 - **Send** — Specifies that all packets for the associated traffic stream are to be forwarded if the traffic class criteria is met.

- **Drop** — Specifies that all packets for the associated traffic stream are to be dropped if the traffic class criteria is met.
- **Remark Traffic** — Marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header. If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.
 - **Remark COS** — Network traffic can be partitioned into multiple priority levels or Classes of Service. CoS values range from 0 to 7 with 0 as the lowest priority and 7 as the highest priority.
 - **Remark DSCP** — Specifies a particular per-hop behavior (PHB) that is applied to a packet, based on the QoS provided. Select a value from the drop-down list.
 - **Remark IP Precedence** — Marks all packets for the associated traffic stream with the specified IP precedence value. The IP precedence value is an integer from 0 to 7

Step 5 Click **add a policy attr.** You can add another class map, but the class map count for this specific policy has the maximum limit of 10.

Step 6 Click **Apply.**

Note To delete or modify a QoS policy, select the QoS policy from the list and click **Delete** or **Edit.**

QoS Association

The QoS Association page provides additional control over certain QoS aspects of the wireless and Ethernet interface.

In addition to controlling the general traffic categories, the QoS allows you to configure the per-client conditioning of the various microflows through the QoS Policy Name. The QoS Policy Name is a useful tool for establishing general microflow definition and treatment characteristics that can be applied to each wireless client, both inbound and outbound, when it is authenticated on the network.

To configure the QoS Association parameters:

Step 1 Select **Client QoS > QoS Association.**

Step 2 In the **QoS Association Table**, click **+** to add a QoS association.

Step 3 From the **QoS Policy Name** drop down list, choose a QoS Policy name.

Step 4 Configure the following:

- **Association Interface** — Select the interface from the drop down list (**2.4G-ciscosb, 5G-ciscosb or LAN0**).
- **Rate Limit (From AP to Client)** — The maximum allowed transmission rate from the WAP device to the client in bits per second (bps). The valid range is from 0 to 866Mbps.
- **Rate Limit (From Client to AP)** — The maximum allowed transmission rate from the client to the WAP device in bits per second (bps). The valid range is from 0 to 866Mbps.

Step 5 Click **Apply.**

Note An interface can be bound with either a QoS policy or an ACL, but not both.

Guest Access

You can create up to two CP instances on the WAP device. The CP instance is a defined set of instance parameters. The instance can be associated with one or more VAPs.

When you use a wireless client connect to VAP, and access any URL, the web will redirect the URL to **Web Portal Locale** page, which you have configured in the **Access Control/Guest Access** page.

Web Portal Locale Table defines the show style of the authentication web page while the **Guest Group Table** decides the users' username and password.

To configure Guest Access Instance:

-
- Step 1** Edit **Web Portal Locale Table** to design the display of the authentication web page. Click the **Preview** tab to view the display.
 - Step 2** Edit the **Guest Group Table**, click the value link on **Total Guest Users** number to add a user and click **Apply**.
 - Step 3** Configure the **Guest Access Instance Table**, select **Guest Group** and **Web Portal Locale** which you configured by using the above steps.
 - Step 4** Go to **Wireless > Networks** to associate the VAP Guest Access and configure the **Guest Access Instance**.
-

Guest Access Instance Table

-
- Step 1** Select **Guest Access > Guest Access Instance Table**.
 - Step 2** Specify a name for the CP instance in the **Guest Access Instance Name** field. The name can contain up to 32 alphanumeric characters.
 - Step 3** The Captive Portal Instance Parameters area reappears with additional options. Configure these parameters:
 - **Protocol** — Choose either HTTP or HTTPS as the protocol for the CP instance 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.
 - **Authentication Method** — Choose the authentication method for CP to use to verify the clients. The options are:
 - **Local Database** — The WAP device uses a local database to authenticate the users. Configure the following if using the Local Database setting.
 - **Guest Group Name**—Enter a name for the guest group.
 - **Idle Timeout**—Enter the time in minutes for idle timeout.

- **Maximum Bandwidth Up**— Enter the maximum upload speed, in megabits per second, that a client can transmit traffic when using the Captive Portal. This setting limits the bandwidth used to send data into the network. The range is from 0 to 300 Mbps. The default is 0.
 - **Maximum Bandwidth Down**— Enter the maximum download speed, in megabits per second, that a client can receive traffic when using the Captive Portal. This setting limits the bandwidth used to receive data from the network. The range is from 0 to 300 Mbps. The default is 0.
 - **Total Guest User**— Total number of guest users.
- **Radius Authenticated** — The WAP device uses a database on a remote RADIUS server to authenticate the users. Configure the following if using the Radius Authenticated setting.
- **Radius IP Network** — Select the Radius IP network from the drop down list (**IPv4 or IPv6**).
 - **Global RADIUS**— Check **Enable** to enable global RADIUS. If you want the CP feature to use a different set of RADIUS servers, uncheck the box and configure the servers in the fields on this page.
 - **RADIUS Accounting** — Check **Enable** to track and measure the resources that a particular user has consumed, such as the system time and the amount of data transmitted and received.

If you enable RADIUS accounting, it is enabled for the primary RADIUS server, all backup servers, and all configured servers.
 - **Server IP Address-1 or Server IPv6 Address-1**— Enter the IPv4 or IPv6 address for the primary RADIUS server for this VAP. The IPv4 address should be in a form similar to xxx.xxx.xxx.xxx (192.0.2.10). The IPv6 address should be in a form similar to xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8:CAD5:7D91).

When the first wireless client tries to authenticate with a VAP, the WAP device sends an authentication request to the primary server. If the primary server responds to the authentication request, the WAP device continues to use this RADIUS server as the primary server, and the authentication requests are sent to the specified address.

Server IP Address-2 or Server IPv6 Address-2—Enter up to three IPv4 or IPv6 backup RADIUS server addresses. If the authentication fails with the primary server, each configured backup server is tried in sequence.
 - **Key-1**— Enter the shared secret key that the WAP device uses to authenticate to the primary RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive and must match the key configured on the RADIUS server. The text that you enter is shown as asterisks.

Key-2—Enter the RADIUS key associated with the configured backup RADIUS servers. The server at Server IP Address-1 uses Key-1, Server IP Address-2 uses Key-2, and so on.
- **No Authenticated** — The users do not need to be authenticated by a database.
- **3rd Party Credentials** — The WAP device uses the credentials on the social media to authenticate the users. Configure the following if using 3rd party credentials Authenticated setting.
- **Accepted credentials** — Select Facebook or Google or both of them to be the credentials authentication.
 - **Walled Garden** — The relevant default configuration will be set automatically while **Accepted credentials** are selected.

- Note** Cisco integrates data protection, privacy, and security requirements into product design and development methodologies from ideation through launch. For more information, see <https://www.cisco.com/c/en/us/about/trust-center/gdpr.html>.
- **Active Directory Service** — The WAP device uses a database on a remote ADS server to authenticate the users. Configure the following if using the ADS Authenticated setting.
 - **Active Directory Servers** — Add new ADS server by clicking the **+** icon. You can add up to 3 servers. Use **arrow** to move and prioritize the servers. Choose **trash can** to delete the configuration. Use the **Test** to check if the ADS server is valid.
 - **External Capture Portal (EXCAP)** — The WAP device uses an external site to customize and authenticate users on the captive portal page. For this purpose, it uses Purple WiFi: <https://purple.ai/> to access on an external site.

In the Purple WiFi page, create a purple account and register. Specify the venue and location when requested. Add the hardware details based on the MAC address of the WAP. This generates a User Guide with all the required information for configuring the EXCAP interface on the WAP.

- Note** Make sure that your Purple WiFi account is configured right before on-boarding the Cisco AP. This ensures an appropriate functioning of the Purple WiFi redirection service.

Configure the following if using an external captive portal setting.

- **Splash Page URL** — Enter the URL (including <https://>) for the portal page which is obtained after successful registration into the Purple WiFi. The range is 0 to 256 characters. The EXCAP hosts the initial login page called the splash page on the cloud or on an external web server which may be outside the AP network. For example: <https://region3.purpleportal.net/access/> if your region is ASIA-PACIFIC in Purple Wi-Fi.
- **Walled Garden** — Specify a list of domains that users can access before passing through the Web portal page. Items in the list should be separated by a comma, and domains can include wildcards in the form of an asterisk (*). The below should be set if you want to use them on Purple Wi-Fi's EXCAP solution:

Purple WiFi (MUST)	region3.purpleportal.net, (It must be based on your region in Purple Wi-Fi) cloudfront.net, venuewifi.com, openweathermap.org, stripe.com
Facebook (Optional)	facebook.com, fbcdn.net, akamaihd.net, facebook.net
Twitter (Optional)	twitter.com, twimg.com
LinkedIn (Optional)	linkedin.com, licdn.net, licdn.com
Instagram (Optional)	instagram.com
Vkontakte (Optional)	vk.com, oath.vk.com, vk.me

- **Server IP Address-1** — Enter the IPv4 address for the primary RADIUS server for this VAP. The IPv4 address should be in a form similar to xxx.xxx.xxx.xxx

When the first wireless client tries to authenticate with a VAP, the WAP device sends an authentication request to the primary server. If the primary server responds to the authentication request, the WAP device continues to use this RADIUS server as the primary server, and the authentication requests are sent to the specified address.

- **Server IP Address-2** — Enter the IPv4 backup RADIUS server addresses. If the authentication fails with the primary server, the configured backup server is tried.
- **Key-1** — Enter the shared secret key that the WAP device uses to authenticate to the primary RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive and must match the key configured on the RADIUS server. The text that you enter is shown as asterisks.
- **Key-2** — Enter the RADIUS key associated with the configured backup RADIUS servers. The server at Server IP Address-1 uses Key-1, Server IP Address-2 uses Key-2.

For the Purple WiFi, the Server IP Address-1 and Address-2 varies for different regions. The table below specifies the same:

Regions	Address-1	Address-2
AMERICAS	34.94.146.135	34.94.183.201
EUROPE	35.230.139.41	35.246.18.82
ASIA-PACIFIC	35.244.93.31	35.244.98.247
The value for Key-1 and Key-2 is 6n8!5ETGb^nd		

- **RADIUS Accounting** — Check Enable to track and measure the resources that a particular user has consumed, such as the system time and the amount of data transmitted and received.

If you enable RADIUS accounting, it is enabled for the primary RADIUS server and the backup server.

- **Guest Group** — If the Authentication Method is set to Local Database or Radius Authenticated, select a Guest Group that was created previously. All users who belong to the group are permitted to access the network through this portal.
- **Redirect URL** — To enable the URL Redirect, enter the URL (including http://). The range is from 0 to 256 characters.
- **Session Timeout** — Enter the time remaining, in seconds, for the CP session to be valid. After the time reaches zero, the client is de-authenticated. The range is from 0 to 1440 minutes. The default value is 0.
- **Web Portal Locale** — Select a web portal locale that was created previously from the drop-down list.

Step 4 Click **Apply**. Your changes are saved to the Startup Configuration.

Note Redirect URL and Web Portal Locale are not of use in EXCAP mode.

Please refer to Hardware manual in Purple Wi-Fi for more detailed settings of EXCAP

Guest Group Table

On the device, each local user is assigned to a user group and the group is assigned to a CP instance. The group facilitates managing the assignment of users to CP instances.

The user group named Default is built-in and cannot be deleted.

To configure a local user:

Step 1 Select **Guest Access > Guest Group Table**.

Step 2 In the Guest Groups Settings area, configure the following parameters:

- **Guest Group Name** — Specify the name for the new guest group. The default Guest Group Name is **Default**

Step 3 Configure these parameters:

- **Idle Timeout** — Enter the period of time that a user remains in the CP authenticated client list after the client disassociates from the WAP device. If the time specified in this field expires before the client attempts to re-authenticate, the client entry is removed from the authenticated client list. The range is from 0 to 1440 minutes. The default value is 60. The timeout value configured here has precedence over the value configured for the CP instance, unless the user value is set to 0. When it is set to 0, the timeout value configured for the CP instance is used.
- **Maximum Bandwidth Up** — Enter the maximum upload speed, in megabits per second, that a client can transmit traffic when using the Captive Portal. This setting limits the bandwidth used to send data into the network. The range is from 0 to 866 Mbps. The default is 0.
- **Maximum Bandwidth Down** — Enter the maximum download speed, in megabits per second, that a client can receive traffic when using the Captive Portal. This setting limits the bandwidth used to receive data from the network. The range is from 0 to 866 Mbps. The default is 0.
- **Total Guest Users** — Displays the number of total guest users. Click the value link on the **Total Guest Users** to display the **Guest User Account** page.

Step 4 Click **Apply**.

Guest User Account

To configure a guest user account:

Step 1 Select **Guest Access > Guest Group Table**.

Step 2 Click the number link on the **Total Guest Users** field to display the **Guest User Account Table** in the **Guest User Account** page.

Step 3 Click **+** to add a user.

Step 4 **Guest User Name** — Enter the name for the new guest user. The name can contain up to 32 alphanumeric characters.

Step 5 **Guest User Password** — Enter the password. The password can contain 8 to 64 alphanumeric and special characters.

Step 6 Click **Apply**.

- Note** You can click **Back** button link to view the **Guest Access** page.
- To delete or modify a guest user, you need to select it and then click **Delete** or **Edit**.

Web Portal Customization

After the CP instance is associated with a VAP, create a locale and map it to the CP instance. When the user accesses a VAP that is associated with a CP instance, the authentication page will appear.

Use the Web Portal Customization page to create unique pages for different locales on your network, and to customize the text and images on the pages.

Step 1 Select **Guest Access > Web Portal Locale Table**.

Step 2 In this table, click **+** to access the **Web Portal Customization** page. To modify the locale, check the row and click **Edit** or click **Delete** to delete.

You can create up to three different authentication pages with different locales on your network.

Step 3 In the **Web Portal Customization** page, configure the following parameters:

- **Web Portal Locale Name** — Enter a web locale name to assign to the page. The name can be from 1 to 32 alphanumeric characters.

Step 4 The **Guest Access Instance Name** cannot be edited. The editable fields are populated with default values. Configure the following parameters:

- **Guest Access Instance Name** — Displays the name of the guest access instance.
- **Background Image** — Click **Browse** to choose the image. You can click **Upload** to upload the images for CP instances. The filesize must be 64K or less.
- **Logo Image** — Click **Browse** to choose the logo image. You can click **Upload** to upload the logo images. The filesize must be 64K or less.
- **Foreground Color** — Enter the HTML code for the foreground color in 6-digit hexadecimal format. The range is from 1 to 32 characters. The default is #FFFFFF.
- **Background Color** — Enter the HTML code for the background color in 6-digit hexadecimal format. The range is from 1 to 32 characters. The default is #FFFFFF.
- **Separator Color** — Enter the HTML code for the color of the thick horizontal line that separates the page header from the page body, in 6-digit hexadecimal format. The range is from 1 to 32 characters. The default is #FFFFFF.
- **Account Image** — Click **Browse** to choose the image. You can click **Upload** to upload the account images. The filesize must be 64K or lesser per alert message.
- **Fonts**—Select a font from the drop down list. This font will be used when displaying all text.
- **Account Prompting** — Enter a user name. The range is from 1 to 32 characters.
- **Username Prompting** — The label for the user name text box. The range is from 1 to 32 characters.
- **Password Prompting** — The label for the user password text box. The range is from 1 to 64 characters.

- **Button Prompting** — The label on the button that users click to submit their user name and password for authentication. The range is from 2 to 32 characters. The default is Connect.
- **Browser Head Prompting** — The text that appears in the browser title bar. The range is from 1 to 128 characters. The default is Captive Portal.
- **Portal Title Prompting** — The text that appears in the page header, to the right of the logo. The range is from 1 to 128 characters. The default is Welcome to the Wireless Network.
- **Account Tips Prompting** — The text that appears in the page body below the user name and password text boxes. The range is from 1 to 256 characters. The default is To start using this service, enter your credentials and click the connect button.
- **Acceptance Policy** — The text that appears in the Acceptance Use Policy box. The range is from 1 to 4096 characters. The default is Acceptance Use Policy.
- **Acceptance Prompting** — The text that instructs users to select the check box to acknowledge reading and accepting the Acceptance Use Policy. The range is from 1 to 128 characters.
- **No Acceptance Warning** — The text that appears in a pop-up window when a user submits login credentials without selecting the Acceptance Use Policy check box. The range is from 1 to 128 characters.
- **Work In Progress Prompting**—The text that appears during the authentication process. The range is from 1 to 128 characters.
- **Invalid Credentials Prompting** — The text that appears when a user fails the authentication. The range is from 1 to 128 characters.
- **Connect Success Prompting** — The text that appears when the client has authenticated to the VAP. The range is from 1 to 128 characters.
- **Welcome Prompting** — The text that appears when the client has connected to the network. The range is from 1 to 256 characters.
- **Restore** — Deletes the current locale.

Step 5 Click **Apply**. Your changes are saved to the Startup Configuration.

Step 6 Click **Preview** to view the updated page.

Clicking **Preview** will show the text and the images that have already been saved to the Startup Configuration. If you make a change, click **Apply** before clicking **Preview** to see your changes.



CHAPTER 8

Cisco Umbrella

This chapter describes how to configure the **Cisco Umbrella** service. It contains the following topics:

- [Cisco Umbrella, on page 93](#)

Cisco Umbrella

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet. It acts as a gateway between the internet and your systems and data to block malware, botnets and phishing over any port, protocol or app.

Using an Umbrella account, the integration will transparently intercept DNS queries and redirect them to Umbrella. This device will appear in the Umbrella dashboard as a network device for applying policy and viewing reports.

Step 1 Check the check box to enable the Cisco Umbrella functionality.

Step 2 Enter the **Secret** and **API Key** which you obtain from the **Cisco Umbrella** website in the required fields.

Note Log in to your Cisco Umbrella using: the URL: <https://login.umbrella.com/> and go to the dashboard. Navigate to **Admin > Platform API Keys** to add a name and create the Secret and Key information.

Step 3 Enter the domain name you trust in the **Local Domains to Bypass (optional)** field and the packets will reach the destination without going through the Umbrella. Items in the list should be separated by a comma, while the domains can include wildcards in the form of an asterisk (*). For example: *.cisco.com.*

Note This is required for all intranet domains and split DNS domains.

Step 4 Enter a tag name in the **Device Tag (optional)** field to tag the device. The **Device Tag** describes the device or a particular origin assigned to the device. Ensure it is unique to your organization.

Note Any change in the Secret, API Key and the Device Tag will trigger re-registration to create a network device.

Step 5 Check the **DNSCrypt** check box to enable DNS encryption.

Note **DNSCrypt** is used to secure DNS communication between a DNS client and a DNS resolver. It prevents several types of DNS attacks, and snooping. Default is enabled.

Step 6 Click **Apply** to apply these configurations. The status of the registration is indicated in the **Registration Status** field. The status can be **Successful**, **Registering** or **Failed**.



CHAPTER 9

Monitor

This chapter describes how to display status and statistics of the WAP device. It contains the following topics:

- [Dashboard, on page 95](#)
- [Clients, on page 98](#)
- [Guests, on page 100](#)

Dashboard

The Dashboard will display the throughput status, and will provide you with easy steps to configure or monitor your network device. This page is updated every 30 seconds.

Connected Clients

The total number of clients currently associated with the WAP device. Click the box, to be redirected to the Clients page.

Internet/LAN/Wireless

Round icons on the top right of the page, show Internet, LAN and wireless connection status.

Internet

- **Red round** — No Internet connection.
- **Green round** — Internet connection is good.

LAN

- **Red round** — No wired connection.
- **Green round** — Wired connection.

Click the **LAN** link to view the **LAN Status** page.

Wireless

- **Red round** — All radios are disabled.
- **Green round** — At least one radio is working. One or two radios are enabled.

Click the **Wireless** link to view the **Wireless Status** page.

2.4G Radio Throughput

This line chart displays 2.4G Radio Throughput and updates every 30 seconds.

- **Upload**—Throughput of the last 30 seconds transmitted.
- **Download**—Throughput of the last 30 seconds received.

Click **Upload** or **Download** to not display data.

5G Radio Throughput

This line chart displays 5G Radio Throughput and updates every 30 seconds.

- **Upload**—Throughput of the last 30 seconds transmitted.
- **Download**—Throughput of the last 30 seconds received.

Click **Upload** or **Download** to not display data.

Top Clients

According to the traffic order, this bar chart displays the top 5 Traffic clients devices

- **Upload**—Throughput of the last 30 seconds transmitted.
- **Download**—Throughput of the last 30 seconds received.

Click **Upload** or **Download** to not display data.

SSID Utilization

According to the traffic order, this pie chart displays the top 5 Traffic SSID

- **Traffic** —total number of bytes transmitted and received.

Network Usage

This line chart displays the eth throughput

- **Upload**—Throughput of the last 30 seconds transmitted.
- **Download**—Throughput of the last 30 seconds received.

Click **Upload** or **Download** to not display data.

Quick Access

To simplify the device configuration through quick navigation, the **Getting Started** page provides links for performing common tasks. For more details, see [Quick Start Configuration, on page 7](#).

LAN Status

Click on the LAN circle to display the following configuration and status settings on the LAN interface.

- **MAC Address** — The MAC address of the WAP device.
- **IP Address** — The IP address of the WAP device.
- **Subnet Mask** — The subnet mask of the WAP device
- **Default Gateway** — The default gateway of the WAP device.

- **Domain Name Server-1** — The IP address of the domain name server 1 used by the WAP device.
- **Domain Name Server-2** — The IP address of the domain name server 2 used by the WAP device.
- **Green Ethernet Mode** — Green Ethernet mode of the Ethernet interface.
- **IPv6 Address** — The IPv6 address of the WAP device.
- **IPv6 Autoconfigured Global Addresses** — The IPv6 autoconfigured global addresses.
- **IPv6 Link Local Address** — The IPv6 link local address of the WAP device.
- **Default IPv6 Gateway** — The default IPv6 gateway of the WAP device.
- **IPv6-DNS-1** — The IPv6 address of the IPv6 DNS server 1 used by the WAP device.
- **IPv6-DNS-2** — The IPv6 address of the IPv6 DNS server 2 used by the WAP device.
- **VLAN ID** — Identifier of the VLAN.



Note These settings apply to the internal interface. Click **Edit** to change any of these settings. You will be redirected to the **LAN** page.

Click **Refresh** to refresh the screen and show the most current information.

Click **Back** to return to the **Dashboard** page.

Wireless Status

Click the **Wireless** circle to display the wireless radio interfaces, such as:

- **Wireless Radio** — The wireless radio mode is enabled or disabled for the radio interface.
- **MAC Address** — The MAC address associated with the radio interface.
- **Mode** — The 802.11 mode (a/b/g/n/ac) used by the radio interface.
- **Channel** — The channel used by the radio interface.
- **Operational Bandwidth** — The operational bandwidth used by the radio interface.
- Click **Edit** to change any of these settings. You will be redirected to the **Radio** page.

Click **Refresh** to refresh the screen and show the most current information.

Click **Back** to return to the **Dashboard** page.

Interface Status

The Interface Status table displays the following status information for each Virtual Access Point (VAP) and on each Wireless Distribution System (WDS) interface:

- **Network Interface** — The wireless interface of the WAP device.
- **Name (SSID)** — The wireless interface name.
- **Status** — The administrative status (up or down) of the VAP.

- **MAC Address** — The MAC address of the radio interface.
- **VLAN ID** — The VLAN ID of the radio interface.
- **Profile** — The name of any associated scheduler profile.
- **State** — The current state (active or inactive). The state indicates whether the VAP is exchanging data with a client.

Traffic Statistics

The **Traffic Statistics** page shows the real-time transmit and receive statistics for the Ethernet interface, the Virtual Access Points (VAPs), and all WDS interfaces. All transmit and receive statistics reflect the totals since the WAP device was last started. If you reboot the WAP device, these figures indicate the transmit and receive totals since the reboot.

To view traffic statistics, select **Monitor > Dashboard > Quick Access > Traffic Statistics**.

The following information is displayed:

- **Interface**—Name of the Ethernet interface, each VAP interface, and each WDS interface. The name for each VAP interface is followed by its SSID in parentheses
- **Total Packets**—The total number of packets sent and received by the WAP device is displayed in the **Transmit Traffic Statistics** table and the **Receive Traffic Statistics** table respectively.
- **Total Bytes**—The total number of bytes sent and received by the WAP device is displayed in the **Transmit Traffic Statistics** table and the **Receive Traffic Statistics** table respectively.
- **Total Dropped Packets**—The total number of dropped packets sent and received by the WAP device is displayed in the **Transmit Traffic Statistics** table and the **Receive Traffic Statistics** table respectively.
- **Total Dropped Bytes**—The total number of dropped bytes sent and received by the WAP device is displayed in the **Transmit Traffic Statistics** table and the **Receive Traffic Statistics** table respectively.
- **Errors**—The total number of errors related to sending and receiving data on the WAP device.



Note You can click **Refresh** to view the updated information.

Clients

Clients

The Clients page displays the client stations associated with the device.

Total Number Of Associated Clients—The total number of clients on the WAP device.

Client Summary

Displays the client summary by 802.11 client type currently on the device.

Average Bandwidth

Displays the average client bandwidth in Mbps.

- **Upload** — Throughput of the last 30 seconds transmitted.
- **Download** — Throughput of the last 30 seconds received.



Note Click **Upload** or **Download** to not display data.

Lowest Signal-to-Noise (SNR) Clients

List the lowest 5 devices according to SNR.

Lowest Speed Clients

List the lowest 5 devices according to speed order.

Associated Clients

- **Clients Details** — The hostname and MAC address of the associated wireless client.
- **IP Address** — The IP address of the associated wireless client.
- **Network (SSID)** — The Service Set Identifier (SSID) for the WAP device. The SSID is an alphanumeric string of up to 32 characters that uniquely identifies a wireless local area network. It is also referred to as the Network Name.
- **Mode** — The IEEE 802.11 mode being used on the client, such as IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.
- **Data Rate** — The current transmitting data rate.
- **Channel** — The channel on which the Client is current in connection with. The channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. You can use the Radio page to set the channel.
- **Traffic (Up /Down)** — The total number of bytes sent (Up) or received (Down) by the client device.
- **SNR (dB)** — Displays the SNR strength in decibels (dB).
- **Throughput Meter** — The last 30 seconds' throughput / Data Rate.



Note You can order the clients through Clients Details, Network (SSID), and so on.
You can filter clients the through Clients Details, Network (SSID), and so on.

Guests

The **Guests** page provides two tables. One is the Authenticated Clients table, which displays the clients that have authenticated on any Captive Portal instance. The other one is the Failed Authenticated Clients table, which displays information on the clients that attempted to authenticate on a Captive Portal and failed.

To view the list of authenticated clients or the list of clients who failed the authentication, select **Monitor > Guests**.

The following information is displayed:

- **MAC** — The MAC address of the client.
- **IP Address** — The IP address of the client.
- **User Name** — The Captive Portal user name of the client.
- **Protocol** — The protocol that the user used to establish the connection (HTTP or HTTPS).
- **Verification** — The method used to authenticate the user on the Captive Portal, which can be one of these values:
 - **Guest** — The user does not need to be authenticated by a database.
 - **Local** — The WAP device uses a local database to authenticate the users.
 - **RADIUS** — The WAP device uses a database on a remote RADIUS server to authenticate the users.
- **VAP/Radio ID** — The VAP and radio that the user is associated with.
- **Timeout** — The time remaining, in seconds, for the CP session to be valid. After the time reaches zero, the client is de-authenticated.
- **Away Time** — The time remaining, in seconds, for the client entry to be valid. The timer starts when the client dissociates from the CP. After the time reaches zero, the client is de-authenticated.
- **UP/Down (MB)** — The number of bytes transmitted and received by the WAP device from the user station.
- **Failure Time** — The time that the authentication failure occurred. A timestamp is included that shows the time of the failure.

You can click **Export** to upload the current Authenticated or Failed clients message.



Note

Ensure that you select the Authenticated client or Failed client to upload and then click **Export**.



CHAPTER 10

Troubleshoot

This chapter describes how to configure Packet Capture over multiple WAP devices for troubleshooting. It includes the following topics:

- [Packet Capture, on page 101](#)
- [Support Information, on page 107](#)

Packet Capture

The wireless packet capture feature enables capturing and storing the packets received and transmitted by the WAP device. The captured packets can then be analyzed by a network protocol analyzer for troubleshooting or performance optimization.

There are two methods of packet capture:

- **Local Capture Method** — Captured packets are stored in a file on the WAP device. The WAP device can transfer the file to a TFTP server. The file is formatted in pcap format and can be examined using Wireshark. You can choose **Save File on this Device** to select the local capture method.
- **Remote Capture Method** — Captured packets are redirected in real time to an external computer running Wireshark. You can choose **Stream to a Remote Host** to select the remote capture method.

Captured packets could be redirected in real time to CloudShark, a web-based packet decoder and analyzer site. It is similar to Wireshark UI for packet analysis. You can choose **Stream to CloudShark** to select the remote capture method.

The WAP device can capture these types of packets:

- 802.11 packets received and transmitted on the radio interfaces. Packets captured on the radio interfaces include the 802.11 header.
- 802.3 packets received and transmitted on the Ethernet interface.
- 802.3 packets received and transmitted on the internal logical interfaces, such as VAPs and WDS interfaces.

Use the Packet Capture page to configure the parameters of the packet capture, start a local or remote packet capture, view the current packet capture status, and download a packet capture file.

Local Packet Capture

To initiate a local packet capture:

- Step 1** Select **Troubleshoot > Packet Capture**.
- Step 2** Ensure that **Save File on this Device** is selected for the Packet Capture Method.
- Step 3** Configure these parameters:
- **Interface** — Enter a capture interface type for packet capture:
 - **Ethernet** — 802.3 traffic on the Ethernet port.
 - **Radio 1 (5 GHz) / Radio 2 (2.4 GHz)** — 802.11 traffic on the radio interface.
 - **Duration** — Enter the time duration in seconds for the capture. The range is from 10 to 3600. The default is 60.
 - **Max File Size** — Enter the maximum allowed size for the capture file in kilobytes (KB). The range is from 64 to 4096. The default is 1024.
- Step 4** There are two modes for packet capture.
- **All Wireless Traffic** — Captures all wireless packets.
 - **Traffic to/from this AP** — Captures the packets sent from the AP or received by the AP.
- Step 5** Click **Enable Filters**. There are three checkboxes available (**Ignore Beacons, Filter on Client, Filter on SSID**).
- **Ignore Beacons** — Enables or disables the capturing of 802.11 beacons detected or transmitted by the radio.
 - **Filter on Client** — Specifies the MAC address for WLAN client filter. Note that the Client filter is active only when a capture is performed on an 802.11 interface.
 - **Filter on SSID** — Select a SSID name for packet capture.
- Step 6** Click **Apply**. The changes are saved to the Startup Configuration.
- Step 7** Click **Start Capture** and then click **Refresh** to obtain the **Packet Capture Status** which contains of the following data:
- a) **Current Capture Status**
 - b) **Packet Capture Time**
 - c) **Packet Capture File Size**
- In Packet File Capture mode, the WAP device stores the captured packets in the RAM file system. Upon activation, the packet capture proceeds until one of these events occurs:
- The capture time reaches the configured duration.
 - The capture file reaches its maximum size.
 - The administrator stops the capture.
-

Remote Packet Capture

The Remote Packet Capture feature enables you to specify a remote port as the destination port for packet captures. This feature works in conjunction with the Wireshark network analyzer tool for Windows. A packet capture server runs on the WAP device and sends the captured packets through a TCP connection to the Wireshark tool. Wireshark is an open source tool and is available for free; it can be downloaded from <https://www.wireshark.org/>.

A Microsoft Windows computer running the Wireshark tool allows you to display, log, and analyze the captured traffic. The remote packet capture facility is a standard feature of the Wireshark tool for Windows.



Note While the remote packet capture is not supported by the Linux, the Wiresharktool works under Linux and already created capture files can be viewed.

When the remote capture mode is in use, the WAP device does not store any captured data locally in its file system.

If a firewall is installed between the Wireshark computer and the WAP device, the Wireshark must be allowed to pass through the firewall policy of the computer. The firewall must also be configured to allow the Wireshark computer to initiate a TCP connection to the WAP device.

Stream to a Remote Host

To initiate a remote capture on a WAP device using **Stream to a Remote Host** option:

-
- Step 1** Select **Troubleshoot > Packet Capture**.
- Step 2** For the **Packet Capture Method**, click **Stream to a Remote Host** radio button.
- Step 3** In the **Remote Capture Port** field, use the default port (2002), or if you are using a port other than the default, enter the desired port number used to connect Wireshark to the WAP device. The port range is from 1025 to 65530.
- Step 4** There are two modes for packet capture.
- **All Wireless Traffic** — capture all wireless packets in the air.
 - **Traffic to/from this AP** — capture the packet sent from the AP or the AP received.
- Step 5** Next, check **Enable Filters**. Then choose from the following options:
- **Ignore Beacons** — Enables or disables the capturing of 802.11 beacons detected or transmitted by the radio.
 - **Filter on Client** — Specifies the MAC address for WLAN Client filter. Note that the Client filter is active only when a capture is performed on an 802.11 interface.
 - **Filter on SSID** — Select a SSID name for packet capture.
- Step 6** If you want to save the settings for use at another time, click **Apply**. However, the selection of Remote as the Packet Capture Method is not saved.
- Step 7** Click **Start Capture** to start the capture. To stop the capture, click **Stop Capture**.
-

Stream to CloudShark

To initiate a remote capture on a WAP device using **Stream to CloudShark** option, do the following:

-
- Step 1** Select **Troubleshoot > Packet Capture**.
- Step 2** For the **Packet Capture Method**, click **Stream to CloudShark** radio button.
- Step 3** Configure the following parameters:
- Interface — Enter a capture interface type for packet capture
 - Ethernet — 802.3 traffic on the Ethernet port
 - Radio 1 (2.4GHz) / Radio 2 (5GHz) — 802.11 traffic on the radio interface
 - Duration — Enter the time duration in seconds for capture. No duration limitation from CloudShark. The default is 60.
 - CloudShark URL - Enter the host name of CloudShark. The default URL: <https://www.cloudshark.org>
 - CloudShark API Key - Enter the valid API token you registered from CloudShark
- Step 4** The communication with CloudShark is by HTTPS. If you want to use self-signed SSL certificate, select **Yes** option and click **Upload a certificate** to upload the certificate you signed.
- Step 5** Enter the protocols you want to capture in Filter expression field. Only those packets after being filtered will be transferred to CloudShark
- Step 6** There are two modes for packet capture:
- All Wireless Traffic** — Capture all wireless packets.
 - Traffic To/From this AP** — Capture the packet sent from the AP or AP received.
- Step 7** Click **Enable Filters**. The following three options are available:
- Ignore Beacons** — Enables or disables the capturing of 802.11 beacons detected or transmitted by the Radio
 - Filter on Client** — Specifies the MAC address for WLAN Client Filter.
Note The Client Filter is active only when a capture is performed on an 802.11 interface.
 - Filter on SSID** — Select a SSID name for packet capture.
- Step 8** Click **Apply**. The changes are saved to the Startup Configuration.
- Step 9** Click **Start Capture**. In the Packet Capture mode, the packets captured are transmitted to CloudShark site in real time. Upon activation, the packet capture proceeds until one of the following events occur:
- The capture time reaches the configured duration.
 - The capture file reaches its maximum size.
 - The administrator stops the capture.

Wireshark

First, download Wireshark and install it on your computer. You can download Wireshark from <https://www.wireshark.org/>.

To initiate the Wireshark network analyzer tool for Microsoft Windows, follow these steps:

-
- Step 1** On your computer, initiate the Wireshark tool.

- Step 2** In the menu, click **Capture > Options**. A popup window appears.
- Step 3** In the Interface field, select **Remote**. A popup window appears.
- Step 4** In the Host field, enter the IP address of the WAP device.
- Step 5** In the Port field, enter the port number of the WAP device. For example, enter 2002 if you used the default, or enter the port number if you used a port other than the default.
- Step 6** Click **OK**.
- Step 7** Select the interface from which you need to capture the packets. At the Wireshark popup window, next to the IP address, there is a drop-down menu to select the interfaces. The interface can be one of the following:

Linux bridge interface in the wap device

```
--rpcap://[192.168.1.220]:2002/brtrunk
```

Wired LAN interface

```
-- rpcap://[192.168.1.220]:2002/eth0
```

VAP0 traffic on radio 1

```
-- rpcap://[192.168.1.220]:2002/wlan0
```

802.11 traffic

```
-- rpcap://[192.168.1.220]:2002/radio1
```

At WAP361, VAP1 ~ VAP7 traffic

```
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7
```

At WAP150, VAP1 ~ VAP3 traffic

```
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap3
```

You can trace up to four interfaces on the WAP device simultaneously. However, you must start a separate Wireshark session for each interface. To initiate additional remote capture sessions, repeat the Wireshark configuration steps. No configuration required on the WAP device.

Note The system uses four consecutive port numbers, starting with the configured port for the remote packet capture sessions. Verify that you have four consecutive port numbers available. We recommend that if you do not use the default port; use a port number greater than 1024.

When you are capturing traffic on the radio interface, you can disable beacon capture, but other 802.11 control frames are still sent to Wireshark. You can set up a display filter to show only:

- Data frames in the trace.
- Traffic on specific Basic Service Set IDs (BSSIDs).
- Traffic between two clients.

Some examples of useful display filters are:

- Exclude beacons and ACK/RTS/CTS frames:
!(wlan.fc.type_subtype == 8 || wlan.fc.type == 1)
- Data frames only:
wlan.fc.type == 2
- Traffic on a specific BSSID:

```
wlan.bssid == 00:02:bc:00:17:d0
```

- All traffic to and from a specific client:

```
wlan.addr == 00:00:e8:4e:5f:8e
```

In remote capture mode, traffic is sent to the computer running Wireshark through one of the network interfaces. Depending on the location of the Wireshark tool, the traffic can be sent on an Ethernet interface or one of the radios. To avoid a traffic flood caused by tracing the packets, the WAP device automatically installs a capture filter to filter out all packets destined to the Wireshark application. For example, if the Wireshark IP port is configured to be 58000, then this capture filter is automatically installed on the WAP device:

```
not port range 58000-58004
```

Due to performance and security issues, the packet capture mode is not saved in NVRAM on the WAP device. If the WAP device resets, the capture mode is disabled and then you must enable it again to resume capturing traffic. Packet capture parameters (other than the mode) are saved in NVRAM.

Enabling the packet capture feature can create a security issue: Unauthorized clients may be able to connect to the WAP device and trace user data. The performance of the WAP device also is negatively impacted during packet capture, and this impact continues to a lesser extent even when there is no active Wireshark session. To minimize the performance impact on the WAP device during traffic capture, install capture filters to limit which traffic is sent to the Wireshark tool. When capturing 802.11 traffic, a large portion of the captured frames tend to be beacons (typically sent every 100 ms by all access points). Although Wireshark supports a display filter for beacon frames, it does not support a capture filter to prevent the WAP device from forwarding the captured beacon packets to the Wireshark tool. To reduce the performance impact of capturing the 802.11 beacons, disable the capture beacons mode.

Packet Capture File Download

You can download a capture file by TFTP to a configured TFTP server, or by HTTP/HTTPS to a computer. A capture is automatically stopped when the capture file download command is triggered.

Because the capture file is located in the RAM file system, it disappears if the WAP device is reset.

To download a packet capture file using TFTP:

-
- Step 1** Click **Download to TFTP Server**.
 - Step 2** Specify a **Server IPv4 Address** in the field provided.
 - Step 3** Enter the **Destination File Name** to download if different from the default. By default, the captured packets are stored in the folder file /tmp/apcapture.pcap on the WAP device.
 - Step 4** Click **Download**.
-

Using HTTP

To download a packet capture file using HTTP:

-
- Step 1** Click **Download to this Device**. A confirmation pop-up message will appear.

Step 2 Click **Yes**. A pop-up enables you to select a network location to save the file.

Support Information

This Support Information page displays the status of the CPU and RAM.

To record and display the CPU/RAM activity, follow these steps:

Step 1 Select **Troubleshoot > Support Information**.

Step 2 Click **CPU**— The device to record and display the CPU activity. To stop the recording, re-click **CPU**.

Step 3 Click **RAM**— The device to record and display the RAM activity. To stop the recording, re-click **RAM**.

The chart displays the **CPU/RAM** status as follows:

- A blue line shows the CPU activity.
 - A red line show RAM activity.
 - The first line chart update data every 1 seconds. It will show the CPU/RAM activity in 60 seconds.
 - The second line chart update data every 5 seconds. It will show the CPU/RAM activity in 5 minutes.
-

Download CPU/RAM Data

Use the Support Information page to download CPU/RAM activity in your selected time. You can provide the text file to the technical support personnel to assist them in troubleshooting problems. To download the CPU/RAM data, do the following:

Step 1 Select **Troubleshoot > Support Information**.

Step 2 In the **Download Data** section, check **Enable** and **Apply** to enable the download.

Step 3 Select the time you wish to perform the download: **Today, Last 7 Days, Last 30 Days, All, Custom**.

Step 4 Complete the **To** and **From** fields with the yyyy-mm-dd and then set the time with the hh:mm:ss.

Step 5 Click **Download** to generate the file based on the current system settings. After a short pause, a window appears to enable you to save the file to your computer.



APPENDIX **A**

DeAuthentication Message Reason Codes

This appendix contains the following sections:

- [Deauthentication Message Reason Codes, on page 109](#)
- [Deauthentication Reason Code Table, on page 109](#)

Deauthentication Message Reason Codes

When a client deauthenticates from the WAP device, a message is sent to the system log. The message includes a reason code that may be helpful in determining why a client was deauthenticated. You can view log messages when you click **System Configuration** > **Notification** > **View System Log**.

For more information, see [Deauthentication Reason Code Table, on page 109](#)

Deauthentication Reason Code Table

The following table describes the deauthentication reason codes.

Table 2: Deauthentication Reason Code Table

Reason code	Meaning
0	Reserved
1	Unspecified reason
2	Previous authentication no longer valid
3	Deauthenticated because sending station (STA) is leaving or has left Independent Basic Service Set (IBSS) or ESS
4	Disassociated due to inactivity
5	Disassociated because WAP device is unable to handle all currently associated STAs
6	Class 2 frame received from nonauthenticated STA
7	Class 3 frame received from nonassociated STA

Reason code	Meaning
8	Disassociated because sending STA is leaving or has left Basic Service Set (BSS)
9	STA requesting (re)association is not authenticated with responding STA
10	Disassociated because the information in the Power Capability element is unacceptable
11	Disassociated because the information in the Supported Channels element is unacceptable
12	Reserved
13	Invalid element, that is, an element defined in this standard for which the content does not meet the specifications in Clause 8
14	Message integrity code (MIC) failure
15	4-Way Handshake timeout
16	Group Key Handshake timeout
17	Element in 4-Way Handshake different from (Re)Association Request/Probe Response/Beacon frame
18	Invalid group cipher
19	Invalid pairwise cipher
20	Invalid AKMP
21	Unsupported RSNE version
22	Invalid RSNE capabilities
23	IEEE 802.1X authentication failed
24	Cipher suite rejected because of the security policy



APPENDIX **B**

Where to Go from Here

This appendix contains the following section:

- [Where to Go from Here, on page 111](#)

Where to Go from Here

Support	
Cisco Support Community	http://www.cisco.com/go/smallbizsupport
Cisco Support and Resources	http://www.cisco.com/go/smallbizhelp
Phone Support Contacts	http://www.cisco.com/go/sbcs
Cisco Firmware Downloads	http://www.cisco.com/go/smallbizfirmware Select a link to download the firmware for your Cisco product. No login is required.
Cisco Open Source Requests	If you wish to receive a copy of the source code to which you are entitled under the applicable free/open source license(s) (such as the GNU Lesser/General Public License), please send your request to: external-opensource-requests@cisco.com . In your requests please include the Cisco product name, version, and the 18 digit reference number (for example: 7XEEX17D99-3X49X08 1) found in the product open source documentation.
Cisco WAP125 Administration Guide	http://www.cisco.com/go/100_wap_resources
Cisco Power Adapters	http://www.cisco.com/go/wap_accessories

