283935

ADMINISTRATION GUIDE

Cisco Small Business

WAP121 Wireless-N Access Point with PoE and

WAP321 Wireless-N Selectable-Band Access Point with PoE

78-20373-01

Contents

1

Getting Started

This chapter provides an introduction to the web-based access point configuration utility, and includes these topics:

- **Starting the Web-based Configuration Utility**
- **Using the Access Point Setup Wizard**
- **Getting Started**
- **Window Navigation**

Starting the Web-based Configuration Utility

This section describes system requirements and how to navigate the web-based configuration utility.

Supported Browsers

- Internet Explorer 7.0 or later
- Chrome 5.0 or later
- Firefox 3.0 or later
- Safari 3.0 or later

Browser Restrictions

- If you are using Internet Explorer 6, you cannot directly use an IPv6 address to access the WAP device. You can, however, use the DNS (Domain Name System) server to create a domain name that contains the IPv6 address, and then use that domain name in the address bar in place of the IPv6 address.
- When using Internet Explorer 8, you can configure security settings from Internet Explorer. Click **Tools > Internet Options** and then select the **Security** tab. Select **Local Intranet** and click **Sites**. Click **Advanced** and

then click **Add**. Add the intranet address of the WAP device (*http://<ip-address>*) to the local intranet zone. The IP address can also be specified as the subnet IP address, so that all addresses in the subnet 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 open the web-based configuration utility:

STEP 1 Open a Web browser.

STEP 2 Enter the IP address of the WAP device that you are configuring in the address bar on the browser, and then press **Enter**. The *Login* page opens.

- To find your IP address, you can use the Cisco FindIT Network Discovery Utility. This tool enables you to automatically discover all supported Cisco Small Business devices in the same local network segment as your computer. For more information, see www.cisco.com/go/findit.
- For further instructions on how to locate the IP address of your WAP device, see the Quick Start Guide. See **Where to Go From Here** for document locations.

STEP 3 Enter the user name and password. The factory default user name is **cisco** and the default password is **cisco**.

STEP 4 Click **Login**. The Access Point Startup Wizard page opens.

If this is the first time that you logged on with the default user name (**cisco**) and the default password (**cisco**) or your password has expired, the *Change Admin Password* page opens. Enter the new password and confirm it, click **Apply**, and then click **Close**. The new password is saved. Then, enter the user name **cisco** and the new password on the *Login* page.

See **Using the Access Point Setup Wizard, page 10** for instructions on using the wizard.

Logging Out

By default, the web-based configuration utility logs out after 10 minutes of inactivity. See **HTTP/HTTPS Service** for instructions on changing the default timeout period.

To logout, click **Logout** in the top right corner of the web-based configuration utility.

Using the Access Point Setup Wizard

The first time that you log into the WAP device (or after it has been reset to the factory default settings), the *Access Point Startup Wizard* displays to help you perform initial configurations. Follow these steps to complete the wizard:

NOTE If you click **Cancel** to bypass the Wizard, the *Change Password* page displays. You can then change the default password for logging in. For all other settings, the factory default configuration will apply.

STEP 1 Click **Next** on the Welcome page of the Wizard. The *Configure Device - IP Address* window displays.

STEP 2 Click **Dynamic IP Address (DHCP)** if you want the WAP device to receive an IP address from a DHCP server. Or select **Static IP Address** to configure IP Address manually. For a description of these fields, see **LAN Settings, page 56**.

STEP 3 Click **Next**. The *Configure Device - Set System Date and Time* window displays.

STEP 4 Select your time zone, and then set the system time manually or set up the WAP device to get its time from an NTP server. For a description of these options, see **Time Settings, page 31**.

STEP 5 Click **Next**. The *Enable Security - Set Password* window displays.

STEP 6 Enter a **New Password** and enter it again in the **Confirm Password** text box. For more information about passwords, see **User Accounts, page 29**.

> **NOTE** You can click the Password Complexity check box if you wish to disable the password security rules. However, it is strongly recommend to keep the password security rules enabled.

STEP 7 Click **Next**. The *Enable Security - Name Your Wireless Network* window displays.

STEP 8 Enter a **Network Name**. This name serves as the SSID for the default wireless network.

STEP 9 Click **Next**. The *Enable Security - Secure Your Wireless Network* window displays.

STEP 10 Choose a security encryption type and enter a security key. For a description of these options, see **System Security, page 106**.

STEP 11 Click **Next**. The Wizard displays the *Enable Security- Confirm Security Settings* window.

STEP 12 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 13 If they are correct, click **Submit**. Your WAP setup settings will be saved and a confirmation window displays

STEP 14 Click **Finish**. The *Getting Started* window displays.

Getting Started

To simplify device configuration through quick navigation, the *Getting Started* page provides links for performing common tasks. The *Getting Started* page is the default window every time you log into the web-based configuration utility and it provides links for performing common tasks.

Links on the Getting Started Page

Category	Link Name (on the Page)	Linked Page
Initial Setup	Run Setup Wizard	*Using the Access Point Setup Wizard*
	Configure Radio Settings	*Radio*
	Configure Wireless Network Settings	*Networks*
	Configure LAN Settings	*LAN Settings*
	Run WPS	*WPS Setup*
Device Status	System Summary	*System Summary*
	Wireless Status	*Network Interfaces*

Links on the Getting Started Page (Continued)

Category	Link Name (on the Page)	Linked Page
Quick Access	Change Account Password	*User Accounts*
	Upgrade Device Firmware	*Firmware Upgrade*
	Backup/Restore Configuration	*Download/Backup Configuration File*
Other Resources	Support	Cisco WAP support site
	Forums	Cisco Support Community site

Window Navigation

This section describes the features of the web-based configuration utility.

Configuration Utility Header

Configuration Utility Header

The Configuration Utility header contains standard information and is displayed at the top on every page. It provides these buttons:

Buttons

Button Name	Description
(User)	The account name (Administrator or Guest) of the user logged into the WAP device. The factory default user name is **cisco**.
Log Out	Click to log out of the web-based configuration utility.
About	Click to display the WAP device type and version number.
Help	Click to display the online help.

Navigation Window

Navigation Window / Main Menu

A navigation window, or main menu, is located on the left side of each page. The navigation window is a list of the top-level features of the WAP devices. If a main menu item is preceded by an arrow, click to expand and display the sub-menu of each group. You can then click on the desired sub-menu item to open the associated page.

Management Buttons

Management Buttons

The table below describes the commonly used buttons that appear on various pages in the system.

Management Buttons

Button Name	Description
Add	Adds a new entry to the table or database.
Cancel	Cancels the changes made to the page.
Clear All	Clears all entries in the log table.
Delete	Deletes an entry in a table. Select an entry first.
Edit	Edits or modifies an existing entry. Select an entry first.
Refresh	Redisplays the current page with the latest data.
Save	Saves the settings or configuration.
Update	Updates the new information to the Running Configuration.

2

Viewing Statistics

This chapter describes how to display Cisco WAP121 and WAP321 statistics and contains these topics.

System Summary

The *System Summary* page displays basic information such as the hardware model description, software version, and system up time.

To view system information, click **Status and Statistics** > **System Summary** in the navigation window. Or, click **System Summary** under **Device Status** on the *Getting Started* page.

The *System Summary* page displays this information:

- **PID VID**—The WAP hardware model and version.

- **Serial Number**—The serial number of the Cisco WAP121 and WAP321.
- **Base MAC Address**—The WAP MAC address.
- **Firmware Version**—The firmware version number of the active image.
- **Firmware MD5 Checksum**—The checksum for the active image.
- **Host Name**—A name assigned to the device.
- **System Uptime**—The time that has elapsed since the last reboot.
- **System Time**—The current system time.

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

- **Service**—The name of the service, if available.
- **Protocol**—The underlying transport protocol that the service uses (TCP or UDP).
- **Local IP Address**—The IP address, if any, of a remote device that is connected to this service on the WAP device. **All** indicates that any IP address on the device can use this service.
- **Local Port**—The port number for the service.
- **Remote IP Address**—The IP address of a remote host, if any, that is 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 state display in the table. In the Active state, a connection is established between the WAP device and a client or server. The TCP states are:
  - **Listening**—The service is listening for connection requests.
  - **Active**—A connection session is established and packets are being transmitted and received.
  - **Established**—A connection session is established between the WAP device and a server or client, depending on each device's role with respect to this protocol.

- **Time Wait**—The closing sequence has been initiated and the WAP is waiting for a system-defined timeout period (typically 60 seconds) before closing the connection.

You can click **Refresh** to refresh the screen and display the most current information.

Network Interfaces

Use the *Network Interfaces* page to display configuration and status information about the wired and wireless interfaces. To display this page, click **Status and Statistics** > **Network Interface** in the navigation window.

The *Network Interfaces* page displays this information:

- **LAN Status**—These settings apply to the internal interface. For the WAP321, the display includes if Green Ethernet mode is enabled.

  To change any of these settings, click the **Edit** link. After you click Edit, you are redirected to the *LAN* page. See **LAN Settings, page 56** for descriptions of these fields.

- **Radio Status**—These settings include the Wireless Radio mode (Enabled or Disabled), the MAC address associated with each radio interface, the 802.11 mode (a/b/g/n), and the channel used by the interface.

  To change the wireless settings, click the **Edit** link. After you click Edit, you are redirected to the *Radio* page. See **Radio, page 60** for descriptions of these fields.

You can click **Refresh** to refresh the screen and display the most current information.

Traffic Statistics

Use the *Traffic Statistics* page to view basic information about the WAP. It also provides a real-time display of transmit and receive statistics for the Ethernet interface and the Virtual Access Points (VAPs) on both radio interfaces. All transmit and receive statistics reflect the totals since the WAP was last started. If you reboot the WAP, these figures indicate transmit and receive totals since the reboot.

To display this page, click **Status and Statistics** > **Traffic Statistics** in the navigation window.

The *Traffic Statistics* page displays summary data and statistics for traffic in each direction.

- **Network Interface**—Name of the Ethernet or VAP interface.
- **Name (SSID)**—Wireless network name. Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network. The SSID is set on the VAP tab. See **Configuring VAPs, page 71**.
- **Status**—Whether the interface is up or down.
- **MAC Address**—MAC address for the specified interface. The WAP device has a unique MAC address for each interface.
- **VLAN ID**—Virtual LAN (VLAN) ID. You can use VLANs to establish multiple internal and guest networks on the same WAP device. The VLAN ID is set on the VAP tab. See **Configuring VAPs, page 71**. The statistics display separately for the transmit and receive traffic.
- **Total Packets**—The total packets sent (in Transmit table) or received (in Received table) by this WAP device.
- **Total Bytes**—The total bytes sent (in Transmit table) or received (in Received table) by this WAP device.
- **Total Dropped Packets**—The total number of dropped packets sent (in Transmit table) or received (in Received table) by this WAP device.
- **Total Dropped Bytes**—The total number of dropped bytes sent (in Transmit table) or received (in Received table) by this WAP device.
- **Errors**—The total number of errors related to sending and receiving data on this WAP device.

You can click **Refresh** to refresh the screen and display the most current information.

WorkGroup Bridge Transmit/Receive

The *WorkGroup Bridge Transmit/Receive* page displays packet and byte counts for traffic between stations on a workgroup bridge. For information on configuring workgroup bridges, see **Work Group Bridge, page 90**.

To display this page, click **Status and Statistics** > **WorkGroup Bridge** in the navigation window.

This information displays for each network interface that is configured as a workgroup bridge interface:

- **Network Interface**—Name of the Ethernet or VAP interface.
- **Status and Statistics**—Whether the interface is disconnected or is administratively configured as up or down.
- **VLAN ID**—Virtual LAN (VLAN) ID. You can use VLANs to establish multiple internal and guest networks on the same WAP device. The VLAN ID is set on the VAP tab. See **Configuring VAPs, page 71**.
- **Name (SSID)**—Wireless network name. Also known as the SSID, this alphanumeric key uniquely identifies a wireless local area network. The SSID is set on the VAP tab. See **Configuring VAPs, page 71**.

This additional information displays for the transmit and receive direction for each workgroup bridge interface:

- **Total Packets**—The total number of packets bridged between the wired clients in the workgroup bridge and the wireless network.
- **Total Bytes**—The total number of bytes bridged between the wired clients in the workgroup bridge and the wireless network.

You can click **Refresh** to refresh the screen and display the most current information.

Associated Clients

You can use the *Associated Clients* page to view the client stations associated with a particular access point.

To display this page, click **Status and Statistics** > **Associated Clients** in the navigation window.

The associated stations are displayed along with information about packet traffic transmitted and received for each station.

- **Total Number of Associated Clients**—The total number of clients currently associated with the WAP device.
- **Network Interface**—The VAP the client is associated with. For example, an entry of wlan0vap2 means the client is associated with the radio interface (wlan0) and VAP 2.
- **Station**—The MAC address of the associated wireless client.
- **Status**—The Authenticated and Associated Status shows the underlying IEEE 802.11 authentication and association status, which is present no matter which type of security the client uses to connect to the WAP device. This status does not show IEEE 802.1X authentication or association status.

  These are some points to keep in mind with regard to this field:

  - If the WAP device security mode is None or Static WEP, the authentication and association status of clients showing on the Client Associations tab will be in line with what is expected; that is, if a client shows as authenticated to the WAP device, it will be able to transmit and receive data. (This is because Static WEP uses only IEEE 802.11 authentication.)
  - If the WAP device uses IEEE 802.1X or WPA security, it is possible for a client association to show on this tab as authenticated (through IEEE 802.11 security) but not actually authenticated through the second layer of security.
- **From Station/To Station**—For the From Station, the below counters indicate the packets or bytes received by the wireless client. For the To Station, these counters indicate the number of packets and bytes transmitted from the WAP device to the wireless client.
  - **Packets**—Number of packets received (transmitted) from the wireless client.

- **Bytes**—Number of bytes received (transmitted) from the wireless client.
- **Drop Packets**—Number of packets dropped after being received (transmitted).
- **Drop Bytes**—Number of bytes that dropped after being received (transmitted).
- **TS Violate Packets (From Station)**—Number of packets sent from a client STA to the WAP device in excess of its active Traffic Stream (TS) uplink bandwidth, or for an access category requiring admission control to which the client STA has not been admitted.
- **TS Violate Packets (To Station)**—Number of packets sent from the WAP device to a client STA in excess of its active TS downlink bandwidth, or for an access category requiring admission control to which the client STA has not been admitted.

- **Up Time**—The amount of time the client has been associated with the WAP device.

You can click **Refresh** to refresh the screen and display the most current information.

TSPEC Client Associations

The *TSPEC Client Associations* page provides information about the TSPEC client data transmitted and received by this access point. The tables on this page show voice and video packets transmitted and received by the association, along with status information.

This page shows a real-time display of the transmit and receive statistics for the TSPEC clients. All transmit and receive statistics shown are totals since the client association started.

A TSPEC is a traffic specification that is sent from a QoS-capable wireless client to a WAP device requesting a certain amount of network access for the Traffic Stream (TS) it represents. A traffic stream is a collection of data packets identified by the wireless client as belonging to a particular user priority. An example of a voice traffic stream is a Wi-Fi CERTIFIED telephone handset that marks its codec-generated data packets as voice priority traffic. An example of a video traffic stream is a video player application on a wireless laptop that prioritizes a video conference feed from a corporate server.

To view TSPEC client association statistics, click **Status and Statistics > TSPEC Client Associations** in the navigation window.

This information is provided on the *TSPEC Client Associations* page.

Status:

- **Network Interface**—Radio interface used by the client.
- **SSID**—Service set identifier associated with this TS client.
- **Station**—Client station MAC address.
- **TS Identifier**—TSPEC Traffic Session Identifier (range 0-7).
- **Access Category**—TS Access Category (voice or video).
- **Direction**—Traffic direction for this TS. Direction can be one of these options:
  - uplink—From client to device.
  - downlink—From device to client.
  - bidirectional
- **User Priority**—User Priority (UP) for this TS. The UP is sent with each packet in the UP portion of the IP header. Typical values are as follows:
  - 6 or 7 for voice
  - 4 or 5 for video

  The value may differ depending on other priority traffic sessions.
- **Medium Time**—Time that the TS traffic occupies the transmission medium.
- **Excess Usage Events**—Number of times that the client has exceeded the medium time established for its TSPEC. Minor, infrequent violations are ignored.
- **VAP MAC Address**—Virtual Access Point MAC address.

Statistics:

- **Network**—Radio interface used by the client.
- **Station**—Client station MAC address.
- **TS Identifier**—TSPEC Traffic Session Identifier (range 0-7).
- **Access Category**—TS Access Category (voice or video).

- **Direction**—The traffic direction for this TS. Direction can be one of these options:
  - uplink—From client to device.
  - downlink—From device to client.
  - bidirectional
- **From Station**—Shows the number of packets and bytes received from the wireless client and the number of packets and bytes that were dropped after being received. These statistics also display:
  - **Packets**—Number of packets in excess of an admitted TSPEC.
  - **Bytes**—Number of bytes when no TSPEC has been established and admission is required by the WAP device.
- **To Station**—The number of packets and bytes transmitted from the WAP device to the wireless client and the number of packets and bytes that were dropped upon transmission. These statistics also display:
  - **Packets**—Number of packets in excess of an admitted TSPEC.
  - **Bytes**—Number of bytes for which no TSPEC has been established when admission is required by the WAP device.

You can click **Refresh** to refresh the screen and display the most current information.

TSPEC Status and Statistics

The *TSPEC Status and Statistics* page provides this information:

- Summary information about TSPEC sessions by radio.
- Summary information about TSPEC sessions by VAP.
- Real-time transmit and receive statistics for the radio interface and the network interface(s).

All of the transmit and receive statistics shown are totals since the WAP device was last started. If you reboot the WAP device, these figures indicate transmit and receive totals since the reboot.

To view TSPEC status and statistics, click **Status and Statistics > TSPEC Status and Statistics** in the navigation window.

The *TSPEC Status and Statistics* page provides this status information for the WLAN (Radio) and VAP interfaces:

- **Network Interface**—Name of the Radio or VAP interface.
- **Access Category**—Current Access Category associated with this Traffic Stream (voice or video).
- **Status**—Whether the TSPEC session is enabled (up) or not (down) for the corresponding Access Category.

  NOTE This is a configuration status (it does not necessarily represent the current session activity).
- **Active Traffic Stream**—Number of currently active TSPEC Traffic Streams for this radio and Access Category.
- **Traffic Stream Clients**—Number of Traffic Stream clients associated with this radio and Access Category.
- **Medium Time Admitted**—Time allocated for this Access Category over the transmission medium to carry data. This value should be less than or equal to the maximum bandwidth allowed over the medium for this TS.
- **Medium Time Unallocated**—Time of unused bandwidth for this Access Category.

These statistics display separately for the transmit and receive paths on the wireless radio interface:

- **Access Category**—The Access Category associated with this Traffic Stream (voice or video).
- **Total Packets**—Total number of TS packets sent (in Transmit table) or received (in Received table) by this Radio for the specified Access Category.
- **Total Bytes**—Total number of bytes received in the specified access category.

These statistics display separately for the transmit and receive paths on the network interfaces (VAPs):

- **Total Voice Packets**—Total number of TS voice packets sent (in Transmit table) or received (in Received table) by this WAP device for this VAP.
- **Total Voice Bytes**—Total TS voice bytes sent (in Transmit table) or received (in Received table) by this WAP device for this VAP.

- **Total Video Packets**—Total number of TS video packets sent (in Transmit table) or received (in Received table) by this WAP device for this VAP.
- **Total Video Bytes**—Total TS video bytes sent (in Transmit table) or received (in Received table) by this WAP device for this VAP.

You can click **Refresh** to refresh the screen and display the most current information.

TSPEC AP Statistics

The *TSPEC AP Statistics* page provides information on the voice and video Traffic Streams accepted and rejected by the WAP device. To view this page, click **Status and Statistics > TSPEC AP Statistics** in the navigation window.

The *TSPEC AP Statistics* page displays this information:

- **TSPEC Statistics Summary for Voice ACM**—The total number of accepted and the total number of rejected voice traffic streams.
- **TSPEC Statistics Summary for Video ACM**—The total number of accepted and the total number of rejected video traffic streams.

You can click **Refresh** to refresh the screen and display the most current information.

RADIO Statistics

You can use the *Radio Statistics* page to display packet-level and byte-level statistics for each wireless radio interface. To view this page, click **Status and Statistics > Radio Statistics** in the navigation window.

This information displays:

- **Packets Received**—Total packets received by the WAP device.
- **Bytes Received**—Total bytes received by the WAP device.
- **Packets Transmitted**—Total packets transmitted by the WAP device.
- **Bytes Transmitted**—Total bytes transmitted by the WAP device.

- **Packets Receive Dropped**—Number of packets received by the WAP device that were dropped.
- **Bytes Receive Dropped**—Number of bytes received by the WAP device that were dropped.
- **Packets Transmit Dropped**—Number of packets transmitted by the WAP device that were dropped.
- **Bytes Transmit Dropped**—Number of bytes transmitted by the WAP device that were dropped.
- **Fragments Received**—Number of fragmented frames received by the WAP device.
- **Fragments Transmitted**—Number of fragmented frames sent by the WAP device.
- **Multicast Frames Received**—Count of MSDU frames received with the multicast bit set in the destination MAC address.
- **Multicast Frames Transmitted**—Count of successfully transmitted MSDU frames where the multicast bit is set in the destination MAC address.
- **Duplicate Frame Count**—Number of times a frame is received and the Sequence Control field indicates is a duplicate.
- **Failed Transmit Count**—Number of times an MSDU is not transmitted successfully due to transmit attempts exceeding either the short retry limit or the long retry limit.
- **Transmit Retry Count**—Number of times an MSDU is successfully transmitted after one or more retries.
- **Multiple Retry Count**—Number of times an MSDU is successfully transmitted after more than one retry.
- **RTS Success Count**—Count of CTS frames received in response to an RTS frame.
- **RTS Failure Count**—Count of CTS frames not received in response to an RTS frame.
- **ACK Failure Count**—Count of ACK frames not received when expected.
- **FCS Error Count**—Count of FCS errors detected in a received MPDU frame.

- **Frames Transmitted Count**—Count of each successfully transmitted MSDU.
- **WEP Undecryptable Count**—Number of frames discarded because they could not be decrypted by the radio. Frames can be discarded because the frame was not encrypted, or it was encrypted with a privacy option not supported by the WAP device.

You can click **Refresh** to refresh the screen and display the most current information.

Email Alert Status

The *Email Alert Status* page provides information about the email alerts sent based on the syslog messages generated in the WAP device. To view this page, click **Status and Statistics > Email Alert Status** in the navigation window.

This page displays these fields:

- **Email Alert Status**—The Email Alert operational status. The status is either Up or Down. The default is Down.
- **Number of Email Sent**—The total number of emails sent. The range is an unsigned integer of 32 bits. The default is 0.
- **Number of Email Failed**—The total number of email failures. The range is an unsigned integer of 32 bits. The default is 0.
- **Time Last Email Sent**—The day, date, and time when the last email was sent.

Log

The *Log* page displays a list of system events that generated a log entry, such as login attempts and configuration changes. The log is cleared upon a reboot and can be cleared by an administrator. Up to 512 events can be displayed. Older entries are removed from the list as needed to make room for new events.

To view this page, click **Status and Statistics > Log Status** in the navigation window.

This page displays these for each log entry:

- **Time Stamp**—The system time when the event occurred.
- **Severity**—Whether the event occurred due to an error (err) or is informational (info).
- **Service**—The software component associated with the event.
- **Description**—A description of the event.

You can click **Refresh** to refresh the screen and display the most current information.

You can click **Clear All** to clear all entries from the log.

3

Administration

This chapter describes how to configure global system settings and perform diagnostics.

It contains these Administration topics.

- System Settings
- User Accounts
- Time Settings
- Log Settings
- Email Alert
- HTTP/HTTPS Service
- Telnet/SSH Service
- Management Access Control
- Firmware Upgrade
- Download/Backup Configuration File
- Configuration Files Properties
- Copy/Save Configuration
- Reboot
- Discovery—Bonjour
- Packet Capture

System Settings

The *System Settings* page enables you to configure information that identifies the WAP device within the network.

To configure system settings:

STEP 1 Click **Administration** > **System Settings** in the navigation window.

STEP 2 Enter the parameters:

- **Host Name**—Administratively-assigned name for the WAP device. By convention, this is the fully-qualified domain name of the node. The default host name is "wap" concatenated with the last 6 hex digits of the MAC address of the WAP device. Host Name labels contain only letters, digits and hyphens. Host Name labels cannot begin or end with a hyphen. No other symbols, punctuation characters, or blank spaces are permitted.
- **System Contact**—A contact person for the WAP device.
- **System Location**—Description of the physical location of the WAP device.

STEP 3 Click **Save**. The changes are saved to the Running Configuration and the Startup Configuration.

User Accounts

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

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

You can use the *User Accounts* page configure up to five additional users and to change a user password.

Adding a User

To add a new user:

STEP 1 Click **Administration** > **User Accounts** in the navigation window.

The User Account Table displays the currently configured users. The user **cisco** is preconfigured in the system to have Read/Write privileges. This user cannot be deleted. However, you can change the password.

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

STEP 2 Click **Add**. A new row of text boxes displays.

STEP 3 Select the checkbox for the new user and click **Edit**.

STEP 4 Enter a **User Name** between 1 to 32 alphanumeric characters. Only numbers 0-9 and letters a-z (upper or lower) are allowed for user names.

STEP 5 Enter a **New Password** between 1 and 64 characters and then enter the same password in the **Confirm New Password** text box.

As you enter a password, the number and color of vertical bars changes to indicate 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 6 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

NOTE To delete a user, select the check box next to the user name and click **Delete**.

Changing a User Password

To change a user password:

STEP 1 Click **Administration** > **User Accounts** in the navigation window.

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

STEP 3 Enter a **New Password** between 1 and 64 characters and then enter the same password in the **Confirm New Password** text box.

As you enter a password, the number and color of vertical bars changes to indicate 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 **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

Time Settings

A system clock is used to provide a network-synchronized time-stamping service for software events such as message logs. You can configure the system clock manually or configure the WAP device as a Network Time Protocol (NTP) client that obtains the clock data from a server.

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

To display this page, click **Administration** > **Time Settings** in the navigation window.

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

To use NTP to have the WAP device automatically acquire its time settings:

STEP 1 For the System Clock Source field, select **Network Time Protocol (NTP)**.

STEP 2 Configure these parameters:

- **NTP Server**—Specify the IP address or domain name of an NTP server. A default NTP server is listed.
- **Time Zone**—Select the time zone for your location.

STEP 3 Select **Adjust Time for Daylight Savings** if daylight savings time is applicable to your time zone. When selected, configure these fields:

- **Daylight Savings Start**—Select which week, day, month, and time when daylight savings time starts.

- **Daylight Savings End**—Select which week, day, month, and time when daylight savings time ends.
- **Daylight Savings Offset**—Specify the number of minutes to move the clock forward when daylight savings time begins and backward when it ends.

STEP 4 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

To manually configure the time settings:

STEP 1 For the System Clock Source field, select **Manually**.

STEP 2 Configure these parameters:

- **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, such as 22:00:00 for 10 p.m.
- **Time Zone**—Select the time zone for your location.

STEP 3 Select **Adjust Time for Daylight Savings** if daylight savings time is applicable to your time zone. When selected, configure these fields:

- **Daylight Savings Start**—Select which week, day, month, and time when daylight savings time starts.
- **Daylight Savings End**—Select which week, day, month, and time when daylight savings time ends.
- **Daylight Savings Offset (minutes)**—Specify the number of minutes to move the clock forward when daylight savings time begins.

STEP 4 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

Log Settings

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

Configuring the Persistent Log

If the system unexpectedly reboots, 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 (non-volatile) memory and degrade network performance. You should only enable persistent logging to debug a problem. Make sure you disable persistent logging after you finish debugging the problem.

To configure persistent logging:

STEP 1 Click **Administration** > **Log Settings** in the navigation window.

STEP 2 Configure the parameters:

- **Persistence**—Click **Enable** to save system logs to nonvolatile memory so that the logs are kept when the WAP device reboots. Clear this field to save system logs to volatile memory. Logs in volatile memory are deleted when the system reboots.
- **Severity**—The minimum severity that an event must have for it to be written to the log in nonvolatile memory. For example, if you specify 2 (critical) then critical, alert and emergency events are logged to nonvolatile memory. Error messages with a severity level of 3–7 are written to volatile memory. The severity levels are as follows:
  - 0—Emergency
  - 1—Alert
  - 2—Critical
  - 3—Error
  - 4—Warning

- 5—Notice
- 6—Info
- 7—Debug

- **Depth**—You can store up to 512 messages in memory. When the number you configure in this field is reached, the oldest log event is overwritten by the newest log event.

STEP 3 Click **Save**. The changes are saved to the Running Configuration and the Startup Configuration.

Remote Log Server

The Kernel Log is a comprehensive list of system events (shown in the System Log) and kernel messages such as error conditions.

You cannot view kernel log messages directly from the Web interface. You must first setup a remote log server to receive and capture logs. Then you can configure the WAP device to log to the remote log server.

Remote log server collection for WAP device 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 Click **Administration** > **Log Settings** in the navigation window.

STEP 2 Configure the parameters:

- **Remote Log**—Enables the WAP to send log messages to a remote host. When disabled, all log messages are kept on the local system.
- **Server IPv4 Address/Name**—The IP address or DNS name of the remote log server. The IPv4 address should be in a form similar to xxx.xxx.xxx.xxx (192.0.2.10).
- **UDP Port**—The logical port number for the syslog process on the remote host. The default port is 514.

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

STEP 3 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

If you enabled a Remote Log host, clicking **Save** activates remote logging. The WAP device sends its kernel messages real-time for display to the remote log server monitor, a specified kernel log file, or other storage, depending on your configurations.

If you disabled a Remote Log host, clicking **Save** disables remote logging.

NOTE After new settings are saved, the corresponding processes may be stopped and restarted. When this happens, the WAP device may lose connectivity. We recommend that you change WAP device settings when it will least affect your wireless clients.

Email Alert

Use the email alert feature to send messages to the configured email addresses when particular system events occur.

The feature supports mail server configuration, message severity configuration, and up to three email address configurations to send urgent and non-urgent email alerts.

To configure the WAP to send email alerts:

STEP 1 Click **Administration** > **Email Alert** in the navigation window.

STEP 2 In the Global Configuration area, configure these parameters:

- **Admin Mode**—Enables the email alert feature globally.
- **From Email Address**—Email alert From Address configuration. The address is a 255 character string with only printable characters. The default is null.
- **Log Duration**—Configures how frequently a scheduled message is sent. The range is from 30 to 1440 minutes. The default is 30 minutes.

- **Scheduled Message Severity**—Log messages of this severity level or higher are grouped and sent periodically to the configuration email address. Select from these values: None, Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug. If set to None, then no scheduled severity messages are sent.
- **Urgent Message Severity**—Log messages of this severity level or higher are sent to the configured email address immediately. Possible values are: None, Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug. If set to None, then no urgent severity messages are sent. The default is Alert.

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

- **Server IPv4 Address/Name**—Configures the SMTP server IP address. The server address must be a valid IPv4 address or hostname. The IPv4 address should be in a form similar to xxx.xxx.xxx.xxx (192.0.2.10).
- **Data Encryption**—Configures the mode of security. Possible values are Open or TLSv1.
- **Port**—Configures the SMTP port. The range is a valid port number from 0 to 65535. The default is 25.
- **Username**—The username for authentication. The username is a 64-byte character string with all printable characters.
- **Password**—The password for authentication. The username is a 64-byte character string with all printable characters.

STEP 4 Configure the email addresses and subject line.

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

STEP 5 Click **Test Mail** to validate the configured email server credentials. The administrator can send a test email after the email server details are configured.

STEP 6 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

Email Alert Examples:

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

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

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           PriorityProcess Id          Message
Sep 8 03:48:25 info    login[1457]         root login on 'ttyp0'
Sep 8 03:48:26 info    mini_http-ssl[1175] Max concurrent connections of 20
reached
```

HTTP/HTTPS Service

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

Configuring HTTP and HTTPS Services

To configure HTTP and HTTP services:

STEP 1 Click **Administration** > **HTTP/HTTPS Service** in the navigation window.

STEP 2 Configure these Global Parameters:

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

  When a user logs on to the WAP device web interface, a session is created. This session is maintained until the user logs off or the session inactivity timer expires. The range is from 1 to 10 sessions. The default is 5. If the

maximum number of sessions is reached, the next user who attempts to log on to the configuration utility receives an error message about the session limit.

- **Session Timeout**—The maximum amount of time, in minutes, an inactive user remains logged on to the WAP device configuration utility. When the configured timeout is reached, the user is automatically logged off. The range is from 1 to 60 minutes. The default is 10 minutes.

STEP 3 Configure HTTP and HTTPS services:

- **HTTPS Server**—Enables access through secure HTTP. By default, HTTPS access is enabled. If you disable it, any current connections using that protocol are disconnected.
- **HTTPS Port**—The logical port number to use for HTTP connections, from 1025 to 65535. The default port number for HTTP connections is the well-known IANA port number 443.
- **HTTP Server**—Enables access through HTTP. By default, HTTP access is enabled. If you disable it, any current connections using that protocol are disconnected.
- **HTTP Port**—The logical port number to use for HTTP connections, from 1025 to 65535. The default port number for 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.

STEP 4 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

Managing SSL Certificates

To use 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.

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

In the Certificate File Status area, you can view whether a certificate currently exists on the WAP device, and this information about it:

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

If an SSL certificate (with a .pem extension) exists on the WAP device, you can download it to your computer as a backup. In the Download SSL Certificate (From Device to PC) area, select **HTTP** or **TFTP** for the **Download Method** and click **Download**.

- If you select HTTP, you will be prompted to confirm the download and then to browse to the location to save the file on your network.
- If you select TFTP, additional fields display to enable you to enter the File Name to assign to the downloaded file, and the TFTP server 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 Upload SSL Certificate (From PC to Device), select **HTTP** or **TFTP** for the **Upload Method**.

- For HTTP, browse to the network location, select the file, and click **Upload**.
- For TFTP, enter the **File Name** as it exists on the TFTP server and the **TFTP Server IPv4 Address**, then click **Upload**.

A confirmation displays to indicate that the upload was successful.

Telnet/SSH Service

You can enable management access through Telnet and SSH. The user names and passwords that you configure for HTTP/HTTPS access also apply to the Telnet and SSH services. These services are disabled by default.

To enable Telnet or SSH:

STEP 1 Click **Administration** > **Telnet/SSH Service** in the navigation window.

STEP 2 Select **Enable** for **Telnet** or **SSH**.

STEP 3 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

Management Access Control

You can create an Access Control List (ACL) that lists up to five IPv4 hosts and five IPv6 hosts that are authorized to access the WAP device management interface. If this feature is disabled, anyone can access the management interface from any network client by supplying the correct WAP device username and password.

If the management ACL is enabled, access through the Web, Telnet, SSH, and SNMP is restricted to the specified IP hosts.

CAUTION 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. It is highly recommend to give the Administrative computer a static IP address, so the address will not change over time.

To create an access list:

STEP 1 Click **Administration** > **Management Access Control** in the navigation window.

STEP 2 Select **Enable** for the **Management ACL Mode**.

STEP 3 Enter up to five IPv4 and five IPv6 addresses that you want to provide access to.

STEP 4 Verify the IP addresses are correct.

STEP 5 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

Firmware Upgrade

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

After you upload 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 access point retains the existing configuration information.

TFTP Upgrade

To upgrade the firmware on an access point using TFTP:

STEP 1 Click **Administration** > **Upgrade Firmware** in the navigation window.

The Product ID (PID), Vender ID (VID), and current Firmware Version display.

STEP 2 Select **TFTP** for **Transfer Method**.

STEP 3 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 will not work.

STEP 4 Enter the **TFTP Server IPv4 Address** and click **Upgrade**.

Uploading the new software may take several minutes. Do not refresh the page or navigate to another page while uploading the new software, or the software upload will be aborted. When the process is complete the access point will restart and resume normal operation.

STEP 5 To verify that the firmware upgrade completed successfully, log into the user interface and display the Upgrade Firmware page and view the active firmware version.

HTTP Upgrade

To upgrade using HTTP:

STEP 1 Select **HTTP** for **Transfer Method**.

STEP 2 If you know the name and path to the new file, enter it in the **Source File Name** field. Otherwise, click the **Browse** button 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 will not work.

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

Uploading the new software may take several minutes. Do not refresh the page or navigate to another page while uploading the new software, or the software upload will be aborted. When the process is complete the access point will restart and resume normal operation.

STEP 4 To verify that the firmware upgrade completed successfully, log into the user interface and display the Upgrade Firmware page and view the active firmware version.

Download/Backup Configuration File

The WAP configuration files are in XML format and contain all the information about the WAP device settings. You can backup (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 download it back to the access point to modify the configuration.

The WAP maintains these configuration files:

- **Running Configuration**—The current configuration, including any changes applied in the management sessions since the last reboot.
- **Startup Configuration**—The configuration file saved to flash memory.
- **Backup Configuration**—An additional configuration file saved on the WAP device for use as a backup.
- **Mirror Configuration**—If the Running Configuration is not modified for at least 24 hours, it is automatically saved to a Mirror Configuration file type, and a log message with severity *alert* is generated to indicate that a new mirror file is available. This feature allows the administrator to view the previous version of the configuration before it is saved to the Startup Configuration file type or to copy the Mirror Configuration file type to another configuration file type. If the WAP is rebooted, the Mirror Configuration is reset to the factory default parameters.

NOTE In addition to downloading and uploading these files to another system, you can copy them to different file types on the WAP device. See **Copy/Save Configuration, page 46**.

Backing Up a Configuration File

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

STEP 1 Click **Administration** > **Download/Backup Configuration File** in the navigation window.

STEP 2 Select **Via TFTP** or **Via HTTP/HTTPS** as the **Transfer Method**.

STEP 3 Select **Backup (AP to PC)** as the **Save Action**.

STEP 4 For a TFTP backup only, enter the **Destination File Name** with an .xml extension. Also include the path where the file is to be placed on the server, then enter the **TFTP Server IPv4 Address**.

STEP 5 For a TFTP backup only, enter the **TFTP Server IPv4 Address**.

STEP 6 Select which configuration file you want to back up:

- **Running Configuration**—Current configuration, including any changes applied in the current management session.
- **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 Running Configuration is not modified for at least 24 hours, it is automatically saved to the Mirror Configuration file type, and a log message with severity level **Alert** is generated to indicate that a new Mirror Configuration file is available. The Mirror Configuration file can be used when the WAP device has problems booting with the Startup or Backup Configuration file types. In such cases, the administrator can copy the Mirror Configuration to either the Startup or Backup Configuration file type and reboot.

STEP 7 Click **Save** to begin the backup. For HTTP backups, a window displays to enable you to browse to the desired location for saving the file.

Downloading a Configuration File

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

To download a configuration file to the WAP device:

STEP 1 Click **Administration** > **Download/Backup Configuration File** in the navigation window.

STEP 2 Select **Via TFTP** or **Via HTTP/HTTPS** as the **Transfer Method**.

STEP 3 Select **Download (PC to AP)** as the **Save Action**.

STEP 4 For a TFTP download only, enter the **Source File Name** with an .xml extension. Include the path (where the file exists on the server) and enter the **TFTP Server IPv4 Address**.

STEP 5 Select which configuration file on the WAP you want to be overwritten with the downloaded file: the **Startup Configuration** or the **Backup Configuration**.

If the downloaded file overwrites the Startup Configuration file, and the file passes a validity check, then the downloaded configuration will take effect the next time the WAP reboots.

STEP 6 Click **Save** to begin the upgrade or backup. For HTTP downloads, a window displays to enable you to browse to select the file to download. When the download is finished, a window displays indicating success.

CAUTION Ensure that power to the WAP 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.

Configuration Files Properties

The *Configuration Files Properties* page enables you to clear the Startup, Running, or Backup Configuration file. If you clear the Startup Configuration file, the Backup Configuration file will become active the next time that you reboot the WAP. The Running Configuration cannot be cleared.

To delete the Startup Configuration or Backup Configuration file:

STEP 1 Click **Administration** > **Configuration Files Properties** in the navigation window.

STEP 2 Select the **Startup Configuration**, **Backup Configuration**, or **Running Configuration** file type.

STEP 3 Click **Clear Files**.

Copy/Save Configuration

The *Copy/Save Configuration* page enables you to copy files within the WAP file system. For example, you can copy the Backup Configuration file to the Startup Configuration file type, so that it will be used the next time you boot up the WAP device.

To copy a file to another file type:

STEP 1 Click **Administration** > **Copy/Save Configuration** in the navigation window.

STEP 2 Select the **Source File Name**:

- **Running Configuration**—Current configuration, including any changes applied in the current management session.
- **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 Running Configuration is not modified for at least 24 hours, it is automatically saved to the Mirror Configuration file type, and a log message with severity level **Alert** is generated to indicate that a new Mirror Configuration file is available. The Mirror Configuration file can be used when the WAP device has problems booting with the Startup or Backup Configuration file types. In such cases, the administrator can copy the Mirror Configuration to either the Startup or Backup Configuration file type and reboot.

STEP 3 For the **Destination File Name**, select the file type to be overwritten with the file you are copying. (The running configuration cannot be overwritten.)

STEP 4 Click **Save** to begin the copy process.

When complete, a window displays the message, “Copy Operation Successful.”

Reboot

You can use the *Reboot* page reboot the WAP.

STEP 1 To reboot the WAP, click **Administration** > **Reboot** in the navigation window.

STEP 2 Select one of these options:

- **Reboot**—Reboots the WAP using Startup Configuration.
- **Reboot to Factory Default**—Reboots the WAP using the factory default configuration file. Any customized settings are lost.

A window appears to enable you to confirm or cancel the reboot. The current management session might be terminated.

STEP 3 Click **OK** to reboot.

Discovery—Bonjour

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

The WAP advertises these service types:

- **Cisco-specific device description** (csco-sb)—This service enables clients to discover Cisco WAP and other products deployed in small business networks.
- **Management user interfaces**—This service identifies the management interfaces available on the WAP (HTTP, Telnet, SSH, and SNMP).

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

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

Bonjour works in both IPv4 and IPv6 networks.

To enable the WAP device to be discovered through Bonjour:

STEP 1 Click **Administration** > **Discovery - Bonjour** in the navigation window.

STEP 2 Select **Enable**.

STEP 3 Click **Save**. Your changes are saved to the Startup Configuration.

Packet Capture

The wireless packet capture feature enables capturing and storing 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. Packet capture can operate in one of two methods:

- 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 tools such as Wireshark and OmniPeek.
- Remote capture method—Captured packets are redirected in real time to an external computer running the Wireshark tool.

The WAP device can capture these types of packets:

- 802.11 packets received and transmitted on radio interfaces. Packets captured on 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.

Click **Administration > Packet Capture** to display the *Packet Capture* page. From this page you can:

- Configure packet capture parameters.
- Start a local or remote packet capture.
- View the current packet capture status.
- Download a packet capture file.

Packet Capture Configuration

The Packet Capture Configuration area enables you to configure parameters and initiate a packet capture.

To configure packet capture settings:

STEP 1 Configure these parameters:

- **Capture Beacons**—Enables or disables the capturing of 802.11 beacons detected or transmitted by the radio.
- **Promiscuous Capture**—Enables or disables promiscuous mode when the capture is active.

  In promiscuous mode, the radio receives all traffic on the channel, including traffic that is not destined to this WAP device. While the radio is operating in promiscuous mode, it continues serving associated clients. Packets not destined to the WAP device are not forwarded.

  As soon as the capture is completed, the radio reverts to non-promiscuous mode operation.
- **Radio Client Filter**—Enables or disables the WLAN client filter to capture only frames that are transmitted to, or received from, a WLAN client with a specified MAC address.
- **Client Filter MAC Address**—The MAC address for WLAN client filtering.

  NOTE: The MAC filter is active only when capture is performed on an 802.11 interface.
- **Packet Capture Method**—Select one of these options:
  - **Local File**—Captured packets are stored in a file on the WAP device.
  - **Remote**—Captured packets are redirected in real time to an external computer running the Wireshark tool.

STEP 2 Depending on the selected method, refer to the steps in either of the below sections to continue.

NOTE Changes to packet capture configuration parameters take affect after packet capture is restarted. Modifying the parameters while the packet capture is running does not affect the current packet capture session. To begin using new parameter values, an existing packet capture session must be stopped and re-started.

Local Packet Capture

To initiate a local packet capture:

STEP 1 Ensure that **Local File** is selected for the **Packet Capture Method**.

STEP 2 Configure these parameters:

- **Capture Interface**—Types eligible for packet capture are:
  - radio1—802.11 traffic.
  - eth0—802.3 traffic on the Ethernet port.
  - wlan0—VAP0 traffic on radio 1.
  - vap*x* to vap*x*—Where *x* can be 0 through 7 VAP traffic, if configured for the Cisco WAP321. For the Cisco WAP121, *x* can be 0 to 3 VAP traffic.
  - brtrunk—Linux bridge interface in the WAP device.
- **Capture Duration**—The time duration in seconds for the capture. The range is from 10 to 3600.
- **Max Capture File Size**—The maximum allowed size for the capture file in KB. The range is from 64 to 4096.

STEP 3 Click **Save**. The changes are saved to the Running Configuration and the Startup Configuration.

STEP 4 Click **Start Capture**.

In Packet File Capture mode, the WAP device stores 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.

The Packet Capture Status area of the page shows the status of a packet capture, if one is active on the WAP device. The fields display:

- **Current Capture Status**—Whether packet capture is running or stopped.
- **Packet Capture Time**—Elapsed capture time.
- **Packet Capture File Size**—The current capture file size.

Click **Refresh** to display the latest data from the WAP device.

NOTE To stop a packet file capture, click **Stop Capture**.

Remote Packet Capture

The Remote Packet Capture feature enables you to specify a remote port as the destination 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 http://www.wireshark.org.

A Microsoft Windows computer running the Wireshark tool allows you to display, log, and analyze captured traffic. The remote packet capture facility is a standard feature of the Wireshark tool for Windows. Remote packet capture is not standard on the Linux version of Wireshark and the Linux version does not work with the WAP device.

When 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, these ports must be allowed to pass through the firewall. The firewall must also be configured to allow the Wireshark computer to initiate TCP connection to the WAP device.

To initiate a remote capture on a WAP device:

STEP 1 Click **Administration** > **Packet Capture**.

STEP 2 Enable **Promiscuous Capture**.

STEP 3 Select the **Remote** radio button.

STEP 4 Use the default port (2002), or if you are using a port other than the default, enter the desired port number used for connecting Wireshark to the WAP device.

STEP 5 Click **Save**.

STEP 6 Click **Start Capture**.

To initiate the Wireshark network analyzer tool for Microsoft Windows:

STEP 1 On the same computer, initiate the Wireshark tool.

STEP 2 In the menu, select **Capture** > **Options**. A pop-up appears.

STEP 3 At **Interface**, select **Remote**. A pop-up appears.

STEP 4 At **Host**, enter the IP address of the WAP device.

STEP 5 At **Port**, enter the port number of the WAP. 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 Depending on the interface from which you need to capture packets, select an interface for capture. At the Wireshark pop-up, next to the IP address, there is a pulldown list for you 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 WAP321, VAP1 ~ VAP7 traffic
`-- rpcap://[ 192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7`
At WAP121, VAP1 ~ VAP3 traffic
`-- rpcap://[ 192.168.1.220]:2002/wlan0vap1 ~ wlan0vap3`

You can trace up to four interfaces on the WAP device at the same time. However, you must start a separate Wireshark session for each interface. To initiate additional remote capture sessions, repeat the Wireshark configuration steps; no configuration needs to be done 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 after 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 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 where the Wireshark tool is located, the traffic can be sent on an Ethernet interface or one of the radios. To avoid a traffic flood caused by tracing the trace 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 the capture filter is automatically installed on the WAP device:

not portrange 58000-58004.

Enabling the packet capture feature impacts performance of the WAP device and can create a security issue (unauthorized clients may be able to connect to the WAP device and trace user data). The WAP device performance is negatively impacted even if there is no active Wireshark session with the WAP device. The performance is negatively impacted to a greater extent when packet capture is in progress.

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 the you must reenable it in order to resume capturing traffic. Packet capture parameters (other than mode) are saved in NVRAM.

In order to minimize performance impact on the WAP device while traffic capture is in progress, you should install capture filters to limit which traffic is sent to the Wireshark tool. When capturing 802.11 traffic, large portion of the captured frames tend to be beacons (typically sent every 100 ms by all APs). Although Wireshark

supports a display filter for beacon frames, it does not support a capture filter to prevent the WAP device from forwarding captured beacon packets to the Wireshark tool. In order to reduce the performance impact of capturing the 802.11 beacons, you can 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(S) 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 Select **Use TFTP to download the capture file**.

STEP 2 Enter the **TFTP Server Filename** 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 3 Specify a **TFTP Server IPv4 Address** in the field provided.

STEP 4 Click **Download**.

To download a packet capture file using HTTP:

STEP 1 Clear **Use TFTP to download the captured file**.

STEP 2 Click **Download**. A confirmation window displays.

STEP 3 Click **OK**. A dialog box displays to enable you to choose a network location to save the file.

4

LAN Settings

This chapter describes how to configure the port, network, and clock settings of the WAP devices.

It includes these topics:

- **Port Settings**
- **LAN Settings**

Port Settings

The *Port Settings* page enables you to view and configure settings for the port that physically connects the WAP device to a local area network.

To view and configure LAN settings:

STEP 1 Click **LAN** > **Port Settings** in the navigation area.

The Operational Status area displays the type of port used for the LAN port and the Link characteristics, as configured in the Administrative Settings area.

STEP 2 Enable or disable **Auto Negotiation**.

- When enabled, the port will negotiate 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.

STEP 3 If autonegotiation is disabled, select a **Port Speed** (10Mb/s or 100Mb/s) and the duplex mode (Half- or Full-duplex).

STEP 4 Enable or disable **Green Ethernet Mode** on the Cisco WAP321.

- Green Ethernet Mode is an auto power down mode that reduces chip power when the signal from a link partner is not present. Green Ethernet Mode works whether the port has auto-negotiation enabled or disabled.
- When Green Ethernet Mode is enabled, the WAP device automatically enters a low-power mode when energy on the line is lost, and it resumes normal operation when energy is detected.

STEP 5 Click **Save**. The settings are saved to the Running Configuration and the Startup Configuration.

LAN Settings

You can use the *LAN Settings* page to configure settings for the LAN interface, including static or dynamic IP address assignment and IPv6 functionality.

To configure LAN settings:

STEP 1 Click **LAN** > **LAN Settings** in the navigation area.

The page displays Global Settings, IPv4 Settings, and IPv6 Settings. The Global Settings area displays the MAC address of the LAN interface port. This field is read-only.

STEP 2 Configure these Global Settings:

- **Admit Only VLAN Tagged Frames**—Select to enable the forwarding of traffic that is received with no VLAN tag. Clear the checkbox if you want untagged traffic to be forwarded on the VLAN identified by the Port VLAN ID value.
- **Port VLAN ID**—This VLAN ID is used as the default VLAN for any traffic received on the LAN port that arrives without a VLAN tag. The WAP device supports one untagged VLAN on the LAN interface.

  VLAN 1 is the both default untagged VLAN and the default management VLAN. If you want to segregate management traffic from the untagged VLAN traffic, configure the new VLAN ID at your router, then use this new VLAN ID in your WAP device.
- **Management VLAN ID**—The VLAN associated with the IP address you use to access the WAP device. The default management VLAN ID is 1.

This VLAN is also the default untagged VLAN. If you already have a management VLAN configured on your network with a different VLAN ID, you must change the VLAN ID of the management VLAN on the WAP device.

STEP 3 Configure these IPv4 settings:

- **Connection Type**—By default, the DHCP client on the WAP121/WAP321 automatically broadcasts 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.

  Select one of these values from the list:

  - **DHCP**—The WAP device will acquire its IP address from a DHCP server on the LAN.
  - **Static IP**—You will manually configure the IPv4 address. The IPv4 address should be in a form similar to xxx.xxx.xxx.xxx (192.0.2.10).
- **Static IP Address, Subnet Mask, and Default Gateway**—If you elected to assign a static IP address, enter the IP information.
- **Domain Name Servers**—Select an option from the list:
  - **Dynamic**—The WAP device will acquire DNS server addresses from a DHCP server on the LAN.
  - **Manual**—You will manually configure one or more DNS server addresses. Enter up to two IP addresses in the text boxes provided.

STEP 4 Configure these IPv6 settings:

- **IPv6 Connection Type**—Configures how the WAP device obtains an IPv6 address:
  - **DHCPv6**—The IPv6 address will be assigned by a DHCPv6 server.
  - **Static IPv6**—You will 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 Administration Mode**—Enables IPv6 management access.
- **IPv6 Auto Configuration Administration Mode**—Enables IPv6 automatic address configuration on the WAP device.

  When enabled, the WAP device learns its IPv6 addresses and gateway by processing the Router Advertisements received on the LAN port. The WAP device can have multiple autoconfigured IPv6 addresses.

- **Static IPv6 Address**—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**—The prefix length of the static address, which is an integer in the range of 0 to 128.
- **IPv6 Autoconfigured Global Addresses**—If the WAP device has been assigned one or more IPv6 addresses automatically, the addresses are listed.
- **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.

STEP 5 Click **Save**. The settings are saved to the Running Configuration and the Startup Configuration.

NOTE After new settings are saved, the corresponding processes may be stopped and restarted. When this happens, the WAP device may lose connectivity. We recommend that you change WAP device settings when it will least affect your wireless clients.

5

Wireless Settings

This chapter describes how to configure properties of the wireless radio operation.

It includes these topics:

- Radio
- Rogue AP Detection
- Networks
- Scheduler
- Scheduler Association
- Bandwidth Utilization
- MAC Filtering
- WDS Bridge
- Work Group Bridge
- Quality of Service
- WPS Setup
- WPS Process

Radio

Radio settings directly control the behavior of the radio in the WAP device and its interaction with the physical medium; that is, how and what type of signal the WAP device emits.

To configure radio settings:

STEP 1 Click **Wireless** > **Radio** in the navigation window.

STEP 2 In the Global Settings area, configure the **TSPEC Violation Interval**—The time interval in seconds for the WAP device to report (through the system log and SNMP traps) associated clients that do not adhere to mandatory admission control procedures.

STEP 3 In the Basic Settings area, configure these settings:

- **Radio**—Turns on or off the radio interface.
- **MAC Address**—The Media Access Control (MAC) address for the interface. The MAC address is assigned by the manufacturer and cannot be changed.
- **Mode**—The IEEE 802.11 standard and frequency the radio uses.

  NOTE The modes available depend on the country code setting.

  Select one of these modes:

  - 802.11a—Only 802.11a clients can connect to the WAP device.
  - 802.11b/g—802.11b and 802.11g clients can connect to the WAP device.
  - 802.11a/n—802.11a clients and 802.11n clients operating in the 5-GHz frequency 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.
  - 5 GHz 802.11n—Only 802.11n clients operating in the 5-GHz frequency can connect to the WAP device.
  - 2.4 GHz 802.11n—Only 802.11n clients operating in the 2.4-GHz frequency can connect to the WAP device.

- **Channel Bandwidth** (802.11n modes only)—The 802.11n specification allows a 40 MHz-wide channel in addition to the legacy 20 MHz channel available with other modes. The 40 MHz channel enables higher data rates but leaves fewer channels available for use by other 2.4 GHz and 5 GHz devices.

  Set the field to 20 MHz to restrict the use of the channel bandwidth to a 20 MHz channel.

- **Primary Channel** (802.11n modes with 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.

  Select one of these options:

  - Upper—Set the Primary Channel as the upper 20 MHz channel in the 40 MHz band.
  - Lower—Set the Primary Channel as the lower 20 MHz channel in the 40 MHz band.

- **Channel**—The portion of the radio spectrum 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 no 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) or the International Telecommunication Union (ITU-R).

STEP 4 In the Advanced Settings area, configure these settings:

- **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 OFDM symbols. The guard interval prevents Inter-Symbol and Inter-Carrier Interference (ISI, ICI). The 802.11n mode allows for a reduction in this guard

interval from the a and g definition of 800 nanoseconds to 400 nanoseconds. Reducing the guard interval can yield a 10% improvement in data throughput.

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

Select one of these options:

- **Yes**—The WAP device transmits data using a 400 ns guard Interval when communicating with clients that also support the short guard interval.
- **No**—The WAP device transmits data using an 800 ns 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, these protection mechanisms are enabled (Auto). With protection enabled, protection mechanisms will be invoked if legacy devices are within range of the WAP device.

  You can disable (Off) these protection mechanisms; however, when protection is off, legacy clients or APs within range can be affected by 802.11n transmissions. Protection is also available when the mode is 802.11b/g. When protection is enabled in this mode, it protects 802.11b clients and APs from 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 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 value from 20 to 2000 milliseconds.

- **DTIM Period**—The Delivery Traffic Information Map (DTIM) period. Enter an integer from 1 to 255 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 pick-up.

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

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

- **Fragmentation Threshold**—The frame size threshold in bytes. The valid integer must be even and in the range of 256 to 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 you set, the fragmentation function 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, fragmentation is not used.

  Setting the threshold to the largest value (2,346 bytes) effectively disables fragmentation. Fragmentation plays no role when Aggregation is enabled.

  Fragmentation involves more overhead both because of the extra work of dividing up and reassembling of frames it requires, and because it increases message traffic on the network. However, fragmentation can help improve network performance and reliability if properly configured.

  Sending smaller frames (by using lower fragmentation threshold) might help with some interference problems; for example, with microwave ovens.

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

- **RTS Threshold**—The Request to Send (RTS) Threshold value. The valid integer range must be from 0 to 2347.

  The RTS threshold indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed.

  Changing the RTS threshold can help control traffic flow through the WAP device, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.

- **Maximum Associated Clients**—The maximum number of stations allowed to access this WAP device at any one time. You can enter an integer between 0 and 200.
- **Transmit Power**—A percentage value for the transmit power level for this WAP device.

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

  To increase capacity of the network, place APs closer together and reduce the value of the transmit power. This helps reduce overlap and interference among access points. A lower transmit power setting can also keep your network more secure because weaker wireless signals are less likely to propagate outside of the physical location of your network.
- **Fixed Multicast Rate**—The multicast traffic transmission rate the WAP device supports.
- **Legacy Rate Sets**—The transmission rate sets the WAP device supports and the basic rate sets the WAP device advertises:

  Rates are expressed in megabits per second.

  Supported Rate Sets indicate rates that the WAP device supports. You can check multiple rates (click a check box to select or de-select a rate). The WAP device will automatically choose the most efficient rate based on factors like error rates and distance of client stations from the WAP device.

  Basic Rate Sets indicate rates that the WAP device will advertise 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 an WAP device broadcast a subset of its supported rate sets.
- **MCS (Data Rate) Settings**—The Modulation and Coding Scheme (MCS) index values that the WAP device advertises. MCS can enhance throughput for 802.11n wireless clients.

  Select the check box below the MCS index number to enable it or clear it to disable the index.

  The WAP device supports MCS indexes 0 to 15. MSC index 15 allows for a maximum transmission rate of 300 Mbps. If no MCS index is selected, the radio will operate at MCS index 0, which allows for a maximum transmission rate of 15 Mbps.

The MCS settings can be configured only if the radio mode includes 802.11n support.

- **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 the Multicast/Broadcast Rate Limiting option is disabled. Until you enable Multicast/Broadcast Rate Limiting, these fields will be disabled:

- **Rate Limit**—The rate limit for multicast and broadcast traffic. The limit 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 the traffic 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.

- **TSPEC Mode**—Regulates the overall TSPEC mode on the WAP device. The options are:

  - **On** — The WAP device handles TSPEC requests according to the TSPEC settings you configure on the Radio page. Use this setting if the WAP device handles traffic from QoS-capable devices, such as a Wi-Fi CERTIFIED phone.

  - **Off** — The WAP device ignores TSPEC requests from client stations. Use this setting if you do not want to use TSPEC to give QoS-capable devices priority for time-sensitive traffic.

- **TSPEC Voice ACM Mode** —Regulates mandatory admission control (ACM) for the voice access category. 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 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 the WAP device attempts to transmit on the wireless medium using a voice AC to gain access.
- **TSPEC Video ACM Mode** —Regulates mandatory admission control for the video access category. 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.
- **TSPEC AP Inactivity Timeout** —The amount of time for a WAP device to detect an downlink TS as idle before deleting it. The valid integer range is from 0 to 120 seconds.
- **TSPEC Station Inactivity Timeout** —The amount of time for a WAP device to detect an uplink TS as idle before deleting it. The valid integer range is from 0 to 120 seconds.
- **TSPEC Legacy WMM Queue Map Mode** —Enables or disables the intermixing of legacy traffic on queues operating as ACM.

STEP 5 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

CAUTION After new settings are saved, the corresponding processes may be stopped and restarted. When this happens, the WAP device may lose connectivity. We recommend that you change WAP device settings when it will least affect your wireless clients.

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. Rogue access points pose a security threat because anyone with access to the premises can ignorantly or maliciously install an inexpensive wireless WAP device that can potentially allow unauthorized parties to access the network.

The *Rogue AP Detection* page provides real-time statistics for all APs detected by the WAP device in the vicinity of the network. If the AP listed as a rogue is legitimate, you can add it to the Known AP List.

NOTE The Detected Rogue AP List and Trusted AP List provide information that you can use to take further action. The AP does not have any control over rogue APs on the lists and cannot apply any security policies to APs detected through the RF scan.

To view information about other access points on the wireless network, click **Status and Statistics > Rogue AP Detection** in the navigation window.

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

Rogue AP detection can be enabled and disabled. To enable the radio to collect information about rogue APs, click **Enable** next to **AP Detection**. You can click **Refresh** to refresh the screen and display the most current information.

Information about detected and trusted rogue access points displays:

- **Action**—If the AP is in the Detected Rogue AP List, you can click **Trust** to move the AP from the to the Trusted AP List.

  If the AP is in the Trusted AP list, you can click **Untrust** to move the AP to the Detected Rogue AP List.

  NOTE The Detected Rogue AP List and Trusted AP List provide information. The WAP121/WAP321 does not have any control over the APs on the list and cannot apply any security policies to APs detected through the RF scan.

- **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).

  NOTE The Beacon Interval is set on the *Wireless > Radio* page.

- **Type**—The type of device:
  - AP indicates the rogue device is an AP that supports the IEEE 802.11 Wireless Networking Framework in Infrastructure Mode.
  - Ad hoc indicates a rogue station running in Ad hoc Mode. Stations set to ad hoc mode communicate with each other directly, without the use of a traditional AP. 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.

  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.
- **Privacy**—Indicates whether there is any security on the rogue device:
  - Off indicates that the Security mode on the rogue device is set to None (no security).
  - On indicates that the rogue device has some security in place.

  NOTE You can use the *Wireless > Networks* page to configure security on the AP.
- **WPA**—Whether WPA security is on or off for the rogue AP.
- **Band**—The IEEE 802.11 mode being used on the rogue AP. (For example, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.)

  The number shown indicates the mode according to the this map:
  - 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.

  The channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving.

  NOTE You can use the *Wireless > Radio* page to set the channel.
- **Rate**—The rate in megabits per second at which the rogue AP is currently transmitting.

  The current rate will always be one of the rates shown in Supported Rates.

- **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) displays.
- **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) rate sets 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 Wireless > Radio page.

To save the Trusted AP List to a file, click **Save**. The list contains the MAC addresses of all APs that have been added to the Known AP List. By default, the filename is *Rogue2.cfg*. You can use a text editor or Web browser to open the file and view its contents.

Use the Import AP List from a file feature to import a list of known APs from a saved list. The list might 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 will not be detected as a rogue.

To import an AP list from a file, use these steps:

STEP 1 Choose whether to replace the existing Trusted AP List or add the entries in the imported file to the Trusted AP List.

a. Select **Replace** to import the list and replace the contents of the Known AP List.

b. Select **Merge** to import the list and add the APs in the imported file to the APs currently displayed in the Known AP List.

STEP 2 Click **Browse** and choose the file to import.

The file that you import 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. Separate entries with a single space. For the AP to accept the file, it must contain only MAC addresses.

STEP 3 Click **Import**.

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

Networks

Virtual Access Points (VAPs) segment the wireless LAN into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. VAPs simulate multiple access points in one physical WAP device. Up to four VAPs are supported on the WAP121 and up to eight VAPs are supported on the WAP321.

Each VAP can be independently enabled or disabled, with the exception of VAP0. VAP0 is the physical radio interface and remains enabled as long as the radio is enabled. To disable operation of 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”. For all other VAPs, the default SSID is “Virtual Access Point x” where ‘x’ is the VAP number in the range of 1 to 4 for the WAP121 and 1 to 8 for the WAP321.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 printable characters plus the space (ASCII 0x20) are allowed, but these six characters are not:

?, ", $, [, \,], and +.

The allowable characters are:

ASCII 0x20, 0x21, 0x23, 0x25 through 0x2A, 0x2C through 0x3E, 0x40 through 0x5A, 0x5E through 0x7E.

In addition, these three characters cannot be the first character:

!, #, and ; (ASCII 0x21, 0x23, and 0x3B, respectively).

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, and the period "." (ASCII 0x2E) is also allowed.

VLAN IDs

Each VAP is associated with a VLAN, which is identified by a VLAN ID (VID). A VID can be any value from 1 to 4094, inclusive. The WAP121 supports five active VLANs (four for WLAN plus one management VLAN). The WAP321 supports nine active VLANs (eight for WLAN plus one management VLAN).

By default, the VID assigned to the management interface 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 Click **Wireless** > **Networks** in the navigation window.

STEP 2 Select the **Enabled** check box for the VAP you want to configure.

—Or—

If VAP0 is the only VAP configured on the system, and you want to add a VAP, click **Add**. Then, select the VAP and click **Edit**.

STEP 3 Configure the parameters:

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

  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 VLAN ID you enter in this field, 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 1–4094.

NOTE If you change the VLAN ID to a different ID than the current management VLAN ID, WLAN clients associated with this specific VAP cannot administer the device. Verify the configuration of the untagged and management VLAN IDs on the *LAN* page. For more information, see **LAN Settings, page 56**.

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

  NOTE: 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.

- **Broadcast SSID**—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 displayed in the list of available networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it is able to connect.

  Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect or monitor unencrypted traffic. 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 making it easy for clients to get a connection and where no sensitive information is available.

- **Security**—The type of authentication required for access to the VAP:
  - None
  - Static WEP
  - Dynamic WEP
  - WPA Personal
  - WPA Enterprise

  If you select a security mode other than None, additional fields appear. These fields are explained in **Configuring Security Settings, page 74**.

NOTE We recommend using WPA Personal or WPA Enterprise as your device's authentication type as it provides the stronger security protection. Use Static WEP or Dynamic WEP only for legacy wireless computers or devices that do not support WPA Personal/Enterprise. If you need to set security as Static WEP or Dynamic WEP, configure Radio as 802.11a or 802.11b/g mode (see **Radio, page 60**). The 802.11n mode restricts the use of Static or Dynamic WEP as your device's security mode.

- **MAC Filtering**—Whether the stations that can access this VAP are restricted to a configured global list of MAC addresses. You can select one of these types of MAC filtering:
  - **Disabled**: Do not use MAC filtering.
  - **Local**: Use the MAC Authentication list that you configure on the *MAC Filtering* page.
  - **RADIUS**: Use the MAC Authentication list on an external RADIUS server.
- **Channel Isolation**—Enables and disables station isolation.
  - When disabled, wireless clients can communicate with one another normally by sending traffic through the WAP device.
  - When enabled, the WAP device blocks communication between wireless clients on the same VAP. The WAP device still allows data traffic between its wireless clients and wired devices on the network, across a WDS link, and with other wireless clients associated with a different VAP, but not among wireless clients.
- **HTTP Redirect**—Enables or disables the redirecting of wireless clients to a custom Web page.

  When redirect mode is enabled, the user will be redirected to the URL you specify after the wireless client associates with a WAP device and the user opens a Web browser on the client to access the Internet.

  The custom Web page must be located on an external Web server and might contain information such as the company logo and network usage policy.

  NOTE: The wireless client is redirected to the external Web server only once while it is associated with the WAP device.
- **Redirect URL**—The URL where the Web browser is to be redirected after the wireless client associates with the WAP device and sends HTTP traffic.

STEP 4 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

CAUTION After new settings are saved, the corresponding processes may be stopped and restarted. When this happens, the WAP device may lose connectivity. We recommend that you change WAP device settings when it will least affect your wireless clients.

NOTE To delete a VAP, select the VAP and click **Delete**.

Configuring Security Settings

These sections describe the security settings that you configure, depending on your selection in the Security list on the *Networks* page.

None (Plain-text)

If you select **None** as your security mode, no further options are configurable on the WAP device. This mode means that any data transferred to and from the WAP device is not encrypted.This security mode can be useful during initial network configuration or for problem solving, but it is not recommended for regular use on the Internal network because it is not secure.

Static WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and access points on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

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

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

These parameters display for Static WEP configuration:

- **Transfer Key Index**—A key index list. Key indexes 1 through 4 are available. The default is 1.

  The Transfer Key Index indicates which WEP key the WAP device will use to encrypt the data it transmits.

- **Key Length**—The length of the key. Select one:
  - 64 bits
  - 128 bits
- **Key Type**—The key type. Select one:
  - ASCII
  - Hex
- **WEP Keys**—You can specify up to four WEP keys. In each text box, enter a string of characters for each key. The keys you enter depend on the key type selected:
  - ASCII—Includes upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.
  - Hex—Includes digits 0 to 9 and the letters A to F.

  Use the same number of characters for each key as specified in the Characters Required field. These are the RC4 WEP keys shared with the stations using the WAP device.

  Each client station must be configured to use one of these same WEP keys in the same slot as specified on the WAP device.
- **Characters Required:** The number of characters you enter into the WEP Key fields is determined by the Key length and Key type you select. For example, if you use 128-bit ASCII keys, you must enter 26 characters in the WEP key. The number of characters required updates automatically based on how you set Key Length and Key Type.
- **802.1X Authentication**—The authentication algorithm defines the method used to determine whether a client station is allowed to associate with WAP device when static WEP is the security mode.

  Specify the authentication algorithm you want to use by choosing one of these options:
  - **Open System** authentication allows any client station to associate with the WAP device whether that client station has the correct WEP key or not. This algorithm is also used in plaintext, IEEE 802.1X, and WPA modes. When the authentication algorithm is set to Open System, any client can associate with the WAP device.

NOTE Just because a client station is allowed to *associate* does not ensure it can exchange traffic with an WAP device. A station must have the correct WEP key to be able to successfully access and decrypt data from WAP device, and to transmit readable data to the WAP device.

- **Shared Key** authentication requires the client station to have the correct WEP key in order to associate with the WAP device. When the authentication algorithm is set to Shared Key, a station with an incorrect WEP key will not be able to associate with the WAP device.
- Both **Open System** and **Shared Key**. When you select both authentication algorithms, client stations configured to use WEP in shared key mode must have a valid WEP key in order to associate with the WAP device. Also, client stations configured to use WEP as an open system (shared key mode not enabled) will be able to associate with the WAP device even if they do not have the correct WEP key.

Static WEP Rules

If you use Static WEP, these rules apply:

- All client stations must have the Wireless LAN (WLAN) security set to WEP, and all clients must have one of the WEP keys specified on the WAP device in order to de-code AP-to-station data transmissions.
- The WAP device must have all keys used by clients for station-to-AP transmit so that it can de-code the station transmissions.
- The same key must occupy the same slot on all nodes (AP and clients). For example if the WAP device defines abc123 key as WEP key 3, then the client stations must define that same string as WEP key 3.
- Client stations can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)
- On some wireless client software, you can configure multiple WEP keys and define a client station “transfer key index”, and then set the stations to encrypt the data they transmit using different keys. This ensures that neighboring access points cannot decode each other’s transmissions.
- You cannot mix 64-bit and 128-bit WEP keys between the access point and its client stations.

Dynamic WEP

Dynamic WEP refers to the combination of 802.1x technology and the Extensible Authentication Protocol (EAP). With Dynamic WEP security, WEP keys are changed dynamically.

EAP messages are sent over an IEEE 802.11 wireless network using a protocol called EAP Encapsulation Over LANs (EAPOL). IEEE 802.1X provides dynamically-generated keys that are periodically refreshed. An RC4 stream cipher is used to encrypt the frame body and cyclic redundancy checking (CRC) of each 802.11 frame.

This mode requires the use of an external RADIUS server to authenticate users. The WAP device requires a RADIUS server that supports EAP, such as the Microsoft Internet Authentication Server. To work with Microsoft Windows clients, the authentication server must support Protected EAP (PEAP) and MSCHAP V2.

You can use any of a variety of authentication methods that the IEEE 802.1X mode supports, including certificates, Kerberos, and public key authentication. You must configure the client stations to use the same authentication method the WAP device uses.

These parameters display for Dynamic WEP configuration:

- **Use Global RADIUS Server Settings**—By default, each VAP uses the global RADIUS settings that you define for the WAP device (see **RADIUS Server, page 106**). However, you can configure each VAP to use a different set of RADIUS servers.

  To use the global RADIUS server settings, ensure the check box is selected.

  To use a separate RADIUS server for the VAP, clear the check box and enter the RADIUS server IP address and key in these fields:

- **Server IP Address Type**—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 for the address type you select in this field.

- **Server IP Address** or **Server IPv6 Address**—The address for the primary RADIUS server for this VAP.

  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 you specify.

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).

- **Server IP Address** or **Server IPv6 1–3**—Up to three IPv4 or IPv6 backup RADIUS server addresses.

  If authentication fails with the primary server, each configured backup server is tried in sequence.

- **Key**—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 you enter will be displayed as "*" characters.

- **Key 1–3**—The RADIUS key associated with the configured backup RADIUS servers. The server at RADIUS IP Address-1 uses RADIUS Key-1, RADIUS IP Address-2 uses RADIUS Key-2, and so on.

- **Enable RADIUS Accounting**—Enables tracking and measuring 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 administratively selecting 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 to this VAP.

  The default is 300. 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 to the VAP.

  The valid range is from 0 to 86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

WPA Personal

WPA Personal is a Wi-Fi Alliance IEEE 802.11i standard, which includes AES-CCMP and TKIP mechanisms. The Personal version of WPA employs 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 wireless clients that support the original WPA.

These parameters display for WPA Personal configuration:

- **WPA Versions**—The types of client stations you want to support:
  - **WPA**—The network has client stations that support the original WPA and none that support the newer WPA2.
  - **WPA2**—All client stations on the network support WPA2. This protocol version provides the best security per the IEEE 802.11i standard.

  If the network has a mix of clients, some of which support WPA2 and others which support only the original WPA, select both of the check boxes. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.
- **Cipher Suites**—The cipher suite you want to use:
  - TKIP
  - CCMP (AES)

  You can select either or both. Both TKIP and AES clients can associate with the WAP device. 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

  Clients not configured to use WPA Personal will not be able to associate with the WAP device.
- **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 upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.

- **Key Strength Meter**—The WAP device checks the key against complexity criteria such as how many different types of characters (uppercase, lowercase, numbers, and special characters) are used and how long the string is. If the WPA-PSK complexity check feature is enabled, the key will not be accepted unless it meets the minimum criteria. See **WPA-PSK Complexity, page 111** for information on configuring the complexity check.
- **Broadcast Key Refresh Rate**—The interval at which the broadcast (group) key is refreshed for clients associated to this VAP. The default is 300 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

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

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

These parameters display for WPA Enterprise configuration:

- **WPA Versions**—The types of client stations to be supported:
  - **WPA**—If all client stations on the network support the original WPA but none support the newer WPA2, then select WPA.
  - **WPA2**—If all client stations on the network support WPA2, we suggest using WPA2 which provides the best security per the IEEE 802.11i standard.
  - **WPA and WPA2**—If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select both WPA and WPA2. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.
- **Enable pre-authentication**—If for WPA Versions you select only WPA2 or both WPA and WPA2, you can enable pre-authentication for WPA2 clients.

  Click **Enable** pre-authentication if you want WPA2 wireless clients to send pre-authentication packet. The pre-authentication information will be relayed from the WAP device the client is currently using to the target WAP device. Enabling this feature can help speed up 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.

- **Cipher Suites**—The cipher suite you want to use:
  - TKIP
  - CCMP (AES)
  - TKIP and CCMP (AES)

  By default both TKIP and CCMP are selected. When both TKIP and CCMP are selected, 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
- **Use Global RADIUS Server Settings**—By default, each VAP uses the global RADIUS settings that you define for the WAP device (see **RADIUS Server, page 106**). However, you can configure each VAP to use a different set of RADIUS servers.

  To use the global RADIUS server settings, make sure the check box is selected.

  To use a separate RADIUS server for the VAP, clear the check box and enter the RADIUS server IP address and key in these fields:
- **Server IP Address Type**—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 for the address type you select in this field.
- **Server IP Address** or **Server IPv6 Address** —The address for the primary RADIUS server for this VAP.

  If the IPv4 RADIUS IP Address Type option is selected in the previous field, enter the IP address of the RADIUS server that all VAPs use by default, for example 192.168.10.23. If the IPv6 RADIUS IP Address Type option is selected, enter the IPv6 address of the primary global RADIUS server, for example 2001:DB8:1234::abcd.
- **Server IP Address** or **Server IPv6 Address 1–3**—Up to three IPv4 and/or IPv6 addresses to use as the backup RADIUS servers for this VAP. The field label is RADIUS IP Address when the IPv4 RADIUS IP Address Type option

is selected and RADIUS IPv6 Address when the IPv6 RADIUS IP Address Type option is selected.

If authentication fails with the primary server, each configured backup server is tried in sequence.

- **Key**—The RADIUS key is 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 you enter will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type.
- **Key 1–3**—The RADIUS key associated with the configured backup RADIUS servers. The server at RADIUS IP Address-1 uses RADIUS Key-1, RADIUS IP Address-2 uses RADIUS Key-2, and so on.
- **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 administratively selecting 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 to this VAP.

  The default is 300 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 to the VAP.

  The valid range is from 0 to 86400 seconds. A value of 0 indicates that the session key is not refreshed.

Scheduler

The Radio and VAP Scheduler allows you to configure a rule with a specific time interval for VAPs or radios to be operational, thereby automating the enabling or disabling of the VAPs and radio.

One way you can use this feature is to schedule the radio to operate only during the office working hours in order to achieve security and reduce power consumption. You can also use the Scheduler to allow access to VAPs for wireless clients only during specific times of day.

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.

Adding Scheduler Profiles

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

To view Scheduler status and add a Scheduler profile:

STEP 1 Click **Wireless** > **Scheduler** in the navigation window.

STEP 2 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 of the Scheduler. The range is Up or Down. The default is Down.
- **Reason**—The reason for the scheduler operational status. Possible values are:
  - IsActive—The scheduler is administratively enabled.
  - ConfigDown—Operational status is down because global configuration is disabled.
  - TimeNotSet—Time is not set on the WAP device either manually or through NTP.

STEP 3 To add a profile, enter a profile name in the **Scheduler Profile Configuration** text box and click **Add**. The profile name can be up to 32 alphanumeric characters.

Configuring Scheduler Rules

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 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 parameters (days of the week, hour, and minute) for the start time and the 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 rule for a profile:

STEP 1 Select the profile from the **Select a Profile Name** list.

STEP 2 Click **Add Rule**.

The new rule displays in the rule table.

STEP 3 Select the checkbox next to the rule name and click **Edit**.

STEP 4 From the **Day of the Week** menu, select 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**—The time when the radio or VAP will be operationally enabled. The time is in HH:MM 24-hour format. The range is <00-24>:<00-59>. The default is 00:00.
- **End Time**—The time when the radio or VAP will be operationally disabled. The time is in HH:MM 24-hour format. The range is <00-24>:<00-59>. The default is 00:00.

STEP 6 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

NOTE A Scheduler profile must be associated with a radio interface or a VAP interface to be in effect. See the *Scheduler Association* page.

NOTE To delete a rule, select the profile from the **Profile Name** column and click **Delete**.

Scheduler Association

The Scheduler profiles need to be associated with the WLAN interface or a VAP interface to be effective. By default, there are no Scheduler profiles created, hence no profile is associated to any radio or VAP.

Only one Scheduler profile can be associated with the WLAN interface or each VAP. A single profile can be associated to multiple VAPs. If the Scheduler profile associated with a VAP or the WLAN interface is deleted, then the association is removed.

To associate a Scheduler profile with the WLAN interface or a VAP:

STEP 1 Click **Wireless** > **Scheduler Association** in the navigation window.

STEP 2 For the WLAN interface or a VAP, select the profile from the **Create a Profile Name** list.

STEP 3 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

Bandwidth Utilization

Use the *Bandwidth Utilization* page to configure how much of the radio bandwidth can be used before the WAP device stops allowing new client associations. This feature is disabled by default.

To enable bandwidth utilization:

STEP 1 Click **Wireless** > **Bandwidth Utilization** in the navigation window.

STEP 2 Click **Enable** for the **Bandwidth Utilization** setting.

STEP 3 In the **Maximum Utilization Threshold** box, enter the percentage of network bandwidth utilization allowed on the radio before the WAP device stops accepting new client associations.

The default is 0, which means that all new associations will be allowed regardless of the utilization rate. The valid integer range is from 0 to 100.

STEP 4 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

NOTE After new settings are saved, the corresponding processes may be stopped and restarted. When this happens, the WAP device may lose connectivity. We recommend that you change WAP device settings when it will least affect your wireless clients.

MAC Filtering

Media Access Control (MAC) filtering can be used to exclude or allow only listed client stations to authenticate with the access point. MAC authentication is enabled and disabled per VAP on the *Networks* page. Depending on how the VAP is configured, the WAP device may refer to a MAC filter list stored on an external RADIUS server, or may refer a MAC filter list stored locally on the WAP device.

Configuring a MAC Filter List Locally on the WAP device

The *MAC Filtering* page enables you to configure a local list.

The WAP device supports one local MAC filter list only; that is, the same list applies to all VAPs that are enabled to use the local list. 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 MAC addresses can be added to the filter list.

To configure MAC filtering:

STEP 1 Click **Wireless** > **MAC Filtering** in the navigation window.

STEP 2 Select how the WAP device uses the filter list:

- **Allow only stations in the list**. Any station that is not in the Stations List is denied access to the network through the WAP device.
- **Block all stations in 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 MAC filtering list stored on the RADIUS server, if one exists.

STEP 3 In the **MAC Address** field, enter the MAC address to allow or block and click **Add**.

The MAC Address appears in the **Stations List**.

STEP 4 Continue entering MAC addresses until the list is complete, and then click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

NOTE: To remove a MAC Address from the Stations List, select it, then click **Remove**.

NOTE: After new settings are saved, the corresponding processes may be stopped and restarted. When this happens, the WAP device may lose connectivity. We recommend that you change WAP device settings when it will least affect your wireless clients.

Configuring MAC Authentication on the RADIUS Server

If one or more VAPs are configured to use a MAC filter stored on a RADIUS authentication server, 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 lookup a client MAC entry.	NOPASSWORD

WDS Bridge

The Wireless Distribution System (WDS) allows you to connect multiple WAP devices. With WDS, access points communicate with one another without wires in a standardized way. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required. 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 wireless clients and other repeaters. 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 client associations and communicates with the clients and other repeaters. 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 might 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. 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:

- WDS only works with Cisco WAP121 and Cisco WAP321 devices.
- When using WDS, be sure to configure WDS settings 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.
- Both WAP devices participating in a WDS link must be on the same Radio channel and using the same IEEE 802.11 mode. (See **Radio, page 60** for information on configuring the radio mode and channel.)
- If you use WPA encryption on the WDS link VAP0 must use WPA Personal or WPA Enterprise as the security mode.

To configure a WDS bridge:

STEP 1 Click **Wireless** > **WDS Bridge** in the navigation window.

STEP 2 Select **Enable** for **Spanning Tree Mode**. When enabled, STP helps prevent switching loops. STP is recommended if you configure WDS links.

STEP 3 Select **Enable** for **WDS Interface**.

STEP 4 Configure the remaining parameters:

- **Remote MAC Address**—Specify the MAC address of the destination WAP device; that is, the WAP device on the other end of the WDS link to which data will be sent or handed-off and from which data will be received.
- **Encryption**—The type of encryption to use on the WDS link. The options are none, WEP, and WPA Personal.

If you are unconcerned about 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 between Static WEP and WPA Personal. In WPA Personal mode, the WAP device uses WPA2-PSK with CCMP (AES) encryption over the WDS link.

NOTE: In order to configure WPA Personal on any WDS link, VAP0 must be configured for WPA Personal or WPA-Enterprise.

See **Configuring Security Settings, page 74** for more information about WEP and WPA Personal security settings.

STEP 5 Repeat these steps for up to three additional WDS interfaces.

STEP 6 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

CAUTION After new settings are saved, the corresponding processes may be stopped and restarted. When this happens, the WAP device may lose connectivity. We recommend that you change WAP device settings when it will least affect your wireless clients.

Work Group Bridge

The WAP device Work Group Bridge feature enables the WAP device to extend the accessibility of a remote network. In 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 BSS as an STA device while operating on another BSS as an WAP device device. When Work Group Bridge mode is enabled, then the WAP device supports only one BSS for wireless clients that associate with it, and another BSS to which the WAP device associates as a wireless client.

It is recommended that Work Group Bridge mode be used 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. The Work Group Bridge feature should be used ONLY when connecting to non-Cisco WAP121 or WAP321 devices. When the Work Group Bridge feature is enabled, the VAP 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 *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 to the WAP device's access point interface 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 wired interface should match that of the infrastructure client interface.

Work Group Bridge mode can be used as range extender to enable the 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.

NOTE Work Group Bridge mode currently supports only IPv4 traffic.

NOTE Work Group Bridge mode is not supported across a cluster.

To configure Work Group Bridge mode:

STEP 1 Click **Wireless** > **Work Group Bridge** in the navigation window.

STEP 2 Select **Enable** for the **Work Group Bridge Mode**.

STEP 3 Configure these parameters for the upstream interface and then the downstream interface:

- **SSID**—The 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 (it is disabled by default).

- **Broadcast SSID** (downstream only)—Select **On** if you want the downstream SSID to be broadcast. SSID Broadcast is enabled by default.
- **Security**—The type of security to use for authenticating as a client station on the upstream WAP device and for authenticating downstream client stations to the WAP device. Choices are:
  - **None**
  - **Static WEP**
  - **WPA Personal**
  - **WPA Enterprise** (Upstream only)

  Configure the infrastructure client interface with the same SSID and security settings as advertised by upstream WAP device. The infrastructure client interface will be associated to 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.

  In the downstream direction, clients associate to the access point interface.

  See **Configuring Security Settings, page 74** for information about WEP and WPA Personal security settings.
- **MAC Filtering** (downstream only)—Select one of these options:
  - **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.

  If you select Local or RADIUS, see **MAC Filtering, page 86** for instructions on creating the MAC filter list.
- **VLAN ID**—The VLAN associated with the BSS.

STEP 4 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

The associated downstream clients will now have connectivity to the upstream network.

Quality of Service

The Quality of Service (QoS) settings provide you with the ability to configure transmission queues for optimized throughput and better performance when handling differentiated wireless traffic, such as Voice-over-IP (VoIP), other types of audio, video, streaming media, and traditional IP data.

To configure QoS on the WAP device, you set parameters on the transmission queues for different types of wireless traffic and specifying minimum and maximum wait times (through contention windows) for transmission.

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

Station EDCA parameters affect traffic flowing from the client station to the WAP device.

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

To configure WAP device and Station EDCA parameters:

STEP 1 Click **Wireless** > **QoS** in the navigation window.

STEP 2 Select an option from the **EDCA Template** list:

- **WFA Defaults**—Populates the WAP device and Station EDCA parameters with WiFi Alliance default values, which are best for general, mixed traffic.
- **Optimized for Voice**—Populates the WAP device and 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, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
- Data 1 (Video)—High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
- Data 2 (Best Effort)—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
- Data 3 (Background)—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

To configure QoS on the WAP device:

STEP 3 Configure these parameters:

NOTE: The WAP EDCA and Station EDCA parameters are configurable only if you selected Custom in the previous step.

- **Arbitration Inter-Frame Space**—A wait time for 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 retry of a transmission.

  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 will be a number between 0 and the number specified here.

  If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window.

  Valid values for are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. 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 will continue until a maximum number of retries allowed is reached.

Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. This value must be higher than the value for the Minimum Contention Window.

- **Maximum Burst** (WAP only)—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.

- **Wi-Fi MultiMedia (WMM)**—Select **Enabled** to enable Wi-Fi MultiMedia (WMM) extensions. This 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).

- **TXOP Limit** (Station only)—The TXOP Limit is a station EDCA parameter and 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 Unified Access Point. The TXOP Limit maximum value is 65535.

- **No Acknowledgement**—Select **Enabled** to specify that the WAP device should not acknowledge frames with QosNoAck as the service class value.

- **Unscheduled Automatic Power Save Delivery**—Select **Enabled** to enable APSD, which is a power management method. APSD is recommended if VoIP phones access the network through the WAP device.

STEP 4 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

CAUTION After new settings are saved, the corresponding processes may be stopped and restarted. When this happens, the WAP device may lose connectivity. We recommend that you change WAP device settings when it will least affect your wireless clients.

WPS Setup

This section describes the Wi-Fi Protected Setup (WPS) protocol and its configuration on the WAP device. It contains these subsections:

- **WPS Overview**
- **Configuring WPS Settings**

WPS Overview

WPS is a standard that enables simple establishment of wireless networks without compromising network security. It relieves both the wireless client users and the WAP device administrators from having to know network names, keys, and various other cryptographic configuration options.

WPS facilitates network setup by allowing the administrator to use a push button or PIN mechanism to establish wireless networks, thereby avoiding the manual entry of network names (SSIDs) and wireless security parameters:

- **Push button**: The WPS button is either on the product or a clickable button on the user interface.
- **Personal Identification Number (PIN)**: The PIN either is located on a product label or can be viewed on product user interface.

WPS maintains network security during these simple steps by requiring both the users of new client devices and WLAN administrators to either have physical access to their respective devices or secure remote access to these devices.

Usage Scenarios

These are typical scenarios for using WPS:

- A user wishes to enroll a client station on a WPS-enabled WLAN. (The enrolling client device may detect the network, and prompt the user to enroll, although this is not necessary.) The user triggers the enrollment by pushing a button on the device. The WAP device's administrator then pushes a button on the WAP device. During a brief exchange of WPS protocol messages, the WAP device supplies the new client with a new security configuration through Extensible Authentication Protocol (EAP). The two devices disassociate, and then reassociate and authenticate with the new settings.
- A user wishes to enroll a client station on a WPS-enabled WLAN by supplying the WAP device administrator with the PIN of the client device. The administrator enters this PIN in the configuration utility of the WAP device and triggers the device enrollment. The new enrollee and the WAP device exchange WPS messages, including a new security configuration, disassociate, reassociate, and authenticate.
- A WAP device administrator purchases a new WAP device that has been certified by the Wi-Fi Alliance to be compliant with WPS version 2.0, and wishes to add the WAP device to an existing (wired or wireless) network. The administrator turns on the WAP device, and then accesses a network host that supports the WPS registration protocol. The administrator enters the WAP device's pin in the configuration utility of this "external registrar," and triggers the WPS registration process. (On a wired LAN, the WPS protocol messages are transported through Universal Plug and Play, or UPnP, protocol.) The host registers the WAP as a new network device and configures the WAP with new security settings.
- A WAP device administrator has just added a new WAP device to an existing (wireless or wired) network through WPS, and wishes to grant network access to a new client device. The device is enrolled through either the "PIN" or Push-Button Control (PBC) methods described above, but this time the device enrolls with the external registrar, with the WAP device acting solely as a proxy.
- A wireless device that does not support WPS must join the WPS-enabled WLAN. The administrator, who cannot use WPS in this case, instead manually configures the device with the SSID, public shared key, and cryptography modes of the WPS-enabled WAP device. The device joins the network.

The PIN is either an eight-digit number that uses its last digit as a checksum value, or a four-digit number with no checksum. Each of these numbers may contain leading zeroes.

WPS Roles

The WPS standard assigns specific roles to the various components in its architecture:

- **Enrollee**—A device that can join the wireless network.
- **AP**—A device that provides wireless access to the network.
- **Registrar**—An entity that issues security credentials to enrollees and configures APs.

The WAP devices act as AP devices and support a built-in registrar. They do not function as an enrollee.

Enabling and disabling WPS on a VAP

The administrator can enable or disable WPS on only one VAP. WPS is operational only if this VAP meets these conditions:

- The WAP device is configured to broadcast the VAP SSID.
- MAC address filtering is disabled on the VAP.
- WEP encryption is disabled on the VAP.
- The VAP is configured to use either WPA-Personal security or none. If WPA2-PSK encryption mode is enabled, then an valid pre-shared key (PSK) must be configured and CCMP (AES) encryption must be enabled.
- The VAP is operationally enabled.

WPS is operationally disabled on the VAP if any of these conditions are not met.

NOTE Disabling WPS on a VAP does not cause disassociation of any clients previously authenticated through WPS on that VAP

External and Internal Registration

It is not necessary for the WAP devices to handle the registration of clients on the network themselves. The WAP device can either use its built-in registrar, or act as a proxy for an external registrar. The external registrar may be accessed through the wired or wireless LAN. An external registrar may also configure the SSID, encryption mode, and public shared key of a WPS-enabled BSS. This capability is very useful for "out-of-box" deployments; that is, when an administrator simply attaches a new WAP device to a LAN for the first time.

If the WAP device is using a built-in registrar, it enrolls new clients using the configuration of the VAP associated with the WPS service, whether this configuration was configured directly on the WAP device or acquired by an external registrar through WPS.

Client Enrollment

Push-button Control

The WAP device enrolls 802.11 clients through WPS by one of two methods: the Push-Button Control (PBC) method, or the Personal Identification Number (PIN) method.

Using the PBC method, when the user of a prospective client pushes a button on the enrolling device, the administrator of the WAP device with an enabled built-in registrar pushes a similar (hardware or software) button. This sequence begins enrollment process, and the client device joins the network. Although the Cisco WAP devices do not support an actual hardware button, the administrator can initiate the enrollment for a particular VAP using a "software button" in the web-based configuration utility.

NOTE There is no defined order in which the buttons on the client device and WAP device must be pressed. Either device can initiate the enrollment. However, if the software button on the WAP device is pressed, and no client attempts to enroll after 120 seconds, the WAP device terminates the pending WPS enrollment transaction.

PIN Control

A client may also enroll with a registrar by using a PIN. For example, the WAP device administrator may start an enrollment transaction for a particular VAP by entering the PIN of a client. When the client detects the WPS-enabled device, the user can then supply its PIN to the WAP device to continue the enrollment process. After the WPS protocol has completed, the client securely joins the network. The client can also initiate this process.

As with the PBC method, if the WAP device begins the enrollment transaction and no client attempts to enroll after 120 seconds, the WAP device terminates the pending transaction.

Optional Use of Built-In Registrar

Although the WAP device supports a built-in registrar for WPS, its use is optional. After an external registrar has configured the WAP device, the WAP device acts as a proxy for that external registrar, regardless if the WAP device's built-in registrar is enabled (it is enabled by default).

Lockdown Capability

Each WAP device stores a WPS-compatible device PIN in nonvolatile RAM. WPS requires this PIN if an administrator wants to allow an unconfigured WAP device (that is, one with only factory defaults, including WPS being enabled on a VAP) to join a network. In this "out-of-box" scenario, the administrator obtains the PIN value from the configuration utility of the WAP device.

The administrator may wish to change the PIN if network integrity has been compromised in some way. The WAP device provides a method for generating a new PIN and storing this value in NVRAM. In the event that the value in NVRAM is corrupted, erased, or missing, a new PIN is generated by the WAP device and stored in NVRAM.

The PIN method of enrollment is potentially vulnerable by way of "brute force" attacks. A network intruder could try to pose as an external registrar on the wireless LAN and attempt to derive the WAP device's PIN value by exhaustively applying WPS-compliant PINs. To address this vulnerability, in the event that a registrar fails to supply a correct PIN in three attempts within 60 seconds, the WAP device prohibits any further attempts by an external registrar to register the WAP device on the WPS-enabled VAP for 60 seconds. However, wireless client stations may enroll with the WAP device's built-in registrar, if enabled, during this "lockdown" period. The WAP device also continues to provide proxy services for enrollment requests to external registrars.

The WAP device adds an additional security mechanism for protecting its device PIN. After the WAP device has completed registration with an external registrar, and the resulting WPS transaction has concluded, the device PIN is automatically regenerated.

VAP Configuration Changes

The WPS protocol on a WPS-enabled VAP may configure these parameters:

- Network SSID
- Key management options (WPA-PSK, or WPA-PSK and WPA2-PSK)
- Cryptography options (CCMP/AES, or TKIP and CCMP/AES)
- Network (public shared) key

If a VAP is enabled for WPS, these configuration parameters are subject to change, and are persistent between reboots of the WAP device.

External Registration

The WAP device supports the registration with WPS External Registrars (ER) on the wired and wireless LAN. On the WLAN, external registrars advertise their capabilities within WPS-specific Information Elements (IEs) of their beacon frames; on the wired LAN, external registrars announce their presence through UPnP.

WPS v2.0 does not require registration with an ER to be done explicitly through the WAP device's user interface. The WAP device administrator can register the WAP device with an ER by:

1. Entering the ER's PIN on the WAP device.
2. Entering the WAP device's PIN on the user interface of the ER.

NOTE The registration process can also configure the WAP device as specified in **VAP Configuration Changes, page 101** if the WAP device has declared within the WPS-specific IEs of its beacon frames or UPnP messages that it requires such configuration.

The WAP device is capable of serving as a proxy for up to three external registrars simultaneously.

Exclusive Operation of WPS Transactions

Any one VAP on the WAP device can be enabled for WPS. At most, one WPS transaction (for example, enrollment and association of an 802.11 client) can be in progress at a time on the WAP device. The WAP device administrator can terminate the transaction in progress from the web-based configuration utility. The configuration of the VAP, however, should not be changed during the transaction; nor should the VAP be changed during the authentication process. This restriction is recommended but not enforced on the WAP device.

Backward Compatibility with WPS Version 1.0

Although the WAP121 supports WPS version 2.0, the WAP device interoperates with enrollees and registrars that are certified by the Wi-Fi Alliance to conform to version 1.0 of the WPS protocol.

Configuring WPS Settings

You can use the *WPS Setup* page to enable the WAP device as a WPS-capable device and configure basic settings. When you are ready to use the feature to enroll a new device or add the WAP device to a WPS-enabled network, use the *WPS Process* page.

CAUTION For security reasons, it is recommended, but not required, that you use an HTTPS connection to the web-based configuration utility when configuring WPS.

To configure the WAP device as a WPS-capable device:

STEP 1 Click **Wireless** > **WPS Setup** in the navigation window.

The *WPS Setup* page shows global parameters and status, and parameters and status of the WPS instance. An instance is an implementation of WPS that is associated with a VAP on the network. The WAP device supports one instance only.

STEP 2 Configure the global parameters:

- **Supported WPS Version**—The WPS protocol version that the WAP device supports.
- **WPS Device Name**—A default device name displays. You can assign a different name of up to 32 characters, including spaces and special characters.
- **WPS Global Operational Status**—Whether the WPS protocol is enabled or disabled on the WAP device. It is enabled by default.
- **WPS Device PIN**—A system-generated eight-digit WPS PIN for the WAP device. The administrator may use this generated PIN to register the WAP device with an external registrar.

  You can click **Generate** to generate a new PIN. This is advisable if network integrity has been compromised.

STEP 3 Configure the WPS instance parameters:

- **WPS Instance ID**—An identifier for the instance. As there is only one instance, the only option is wps1.
- **WPS Mode**—Enables or disables the instance.
- **WPS VAP**—The VAP associated with this WPS instance.
- **WPS Built-in Registrar**—Select to enable the built-in registrar function. When enabled, enrollees (typically WLAN clients) can register with the WAP device. When disabled, the registrar functionality in the WAP device is turned off and the enrollee needs to register with another registrar on the network. In this case, another device on the network acts as the registrar and the WAP device serves as a proxy for forwarding client registration requests and the registrar's responses.
- **WPS Configuration State**—Whether the VAP will be configured from the external registrar as a part of WPS process. It can be set to one of these values:
  - **Unconfigured**—VAP settings will be configured using WPS, after which the state will be change to Configured.
  - **Configured**—VAP settings will not be configured by the external registrar and will retain the existing configuration.

STEP 4 Click **Update**. The changes are saved to the Running Configuration and to the Startup Configuration.

The operational status of the instance and the reason for that status also display. See **Enabling and disabling WPS on a VAP, page 98** for information about conditions that may cause the instance to be disabled.

NOTE The Instance Status area displays the **WPS Operational Status** as Enabled or Disabled. You can click **Refresh** to update the page with the most recent status information.

WPS Process

You can use the *WPS Process* page to use WPA to enroll a client station on the network. You can enroll a client using a pin or using the push button method, if supported on the client station.

Enrolling a Client Using the PIN Method

To enroll a client station using the PIN method:

STEP 1 Obtain the PIN from the client device. The PIN may be printed on the hardware itself, or may be obtained from the device's software interface.

STEP 2 Click **Wireless** > **WPS Process** in the navigation window.

STEP 3 Enter the client's PIN in the **PIN Enrollment** text box and click **Start**.

STEP 4 Within two minutes, enter the WAP device's pin on the client station's software interface. The WAP device's pin is configured on the **WPS Setup** page.

When you enter the PIN on the client device, the WPS Operational Status changes to Adding Enrollee. When the enrollment process is complete, the WPS Operational Status changes to Ready and the Transaction Status changes to Success.

NOTE This enrollment sequence may also work in reverse; that is, you may be able to initiate the process on the client station by entering the WAP device's pin, and then entering the client's PIN on the WAP device.

When the client is enrolled, either the WAP device's built-in registrar or the external registrar on the network proceeds to configure the client with the SSID, encryption mode, and public shared key of a WPS-enabled BSS.

Enrolling a Client Using the Push Button Method

To enroll a client station using the push method:

STEP 1 Click **Start** next to **PBC Enrollment**.

STEP 2 Push the hardware button on the client station.

NOTE You can alternatively initiate this process on the client station, and then click the PBC Enrollment Start button on the WAP device.

When you push the button on the client station, the WPS Operational Status changes to Adding Enrollee. When the enrollment process is complete, the WPS Operational Status changes to Ready and the Transaction Status changes to Success.

When the client is enrolled, either the WAP device's built-in registrar or the external registrar on the network proceeds to configure the client with the SSID, encryption mode, and public shared key of a WPS-enabled BSS.

Viewing Instance Summary Information

This information displays for WPS instance:

- **WPS Radio**
- **WPS VAP**
- **SSID**
- **Security**

If the WPS Configuration State field on the WPS Setup page is set to Unconfigured, then the SSID and Security values are configured by the external registrar. If the field is set to Configured, then these values are configured by the administrator.

NOTE You can click **Refresh** to update the page with the most recent status information.

6

System Security

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

It contains these topics.

- **RADIUS Server**
- **802.1X Supplicant**
- **Password Complexity**
- **WPA-PSK Complexity**

RADIUS Server

Several features require communication with a RADIUS authentication server. For example, when you configure Virtual Access Points (VAPs) on the WAP, you can configure security methods that control wireless client access (see **Radio, page 60**). The Dynamic WEP and WPA Enterprise security methods use an external RADIUS server to authenticate clients. The MAC address filtering feature, where client access is restricted to a list, may also be configured to use a RADIUS server to control access. The Captive Portal feature also uses RADIUS to authenticate clients.

You can 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 a primary while the others act as 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 the *Networks* page.

To configure global RADIUS servers:

STEP 1 Click **Security** > **RADIUS Server** in the navigation window.

STEP 2 Enter the parameters:

- **Server IP Address Type**—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 of the address type you select in this field.

- **Server IP Address-1** or **Server IPv6 Address-1**—The addresses for the primary global RADIUS server.

  When the first wireless client tries to authenticate with the WAP device, the 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** through **4)** or **Server IPv6 Address-(2** through **4)**—Up to three backup IPv4 or IPv6 RADIUS server addresses.

  If authentication fails with the primary server, each configured backup server is tried in sequence.

- **Key-1**—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 you enter will be displayed as "*" characters.

- **Key-(2** through **4)**—The RADIUS key associated with the configured backup RADIUS servers. The server at RADIUS IP Address-2 uses RADIUS Key-2, RADIUS IP Address-3 uses RADIUS Key-3, and so on.

- **Enable RADIUS Accounting**—Enables tracking and measuring 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.

STEP 3 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

802.1X Supplicant

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

On 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.

The *802.1X Supplicant* page is divided into three areas: Supplicant Configuration, Certificate File Status, and Certificate File Upload.

The Supplicant Configuration area enables you to configure the 802.1X operational status and basic settings.

STEP 1 Click **System Security** > **802.1X Supplicant** in the navigation window.

STEP 2 Enter the parameters:

- **Administrative Mode**—Enables the 802.1X supplicant functionality.
- **EAP Method**—The algorithm to be used for encrypting authentication user names and passwords.
  - **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**—The WAP device uses this username when responding to requests from an 802.1X authenticator. The user name can be 1 to 64 characters long. ASCII-printable characters are allowed, which includes upper and lower case alphabetic letters, numeric digits, and all special characters except quotation marks (“).

- **Password**—The WAP device uses this MD5 password when responding to requests from an 802.1X authenticator. The password can be 1 to 64 characters in length. ASCII-printable characters are allowed, which includes upper and lower case letters, numbers, and all special characters except quotation marks (“).

STEP 3 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

NOTE After new settings are saved, the corresponding processes may be stopped and restarted. When this happens, the WAP device may lose connectivity. We recommend that you change WAP device settings when it will least affect your wireless clients.

The Certificate File Status area shows whether a current certificate exists:

- **Certificate File Present**—Indicates if the HTTP SSL Certificate file is present. The field shows Yes if it is present. The default setting is No.
- **Certificate Expiration Date**—Indicates when the HTTP SSL Certificate file will expire. The range is a valid date.

The Certificate File Upload area enables you to upload a certificate file to the WAP:

STEP 1 Select either **HTTP** or **TFTP** as the **Transfer Method**.

STEP 2 If you selected HTTP, click **Browse** to select the file.

NOTE: To configure the HTTP and HTTPS server settings, see **HTTP/HTTPS Service, page 37**.

If you selected TFTP, enter **Filename** and the **TFTP Server IPv4 Address**.

STEP 3 Click **Upload**.

A confirmation window displays, followed by a progress bar to indicate the status of the upload.

Password Complexity

You can configure complexity requirements for passwords used to access the WAP device management interfaces. Complex passwords increase security.

To configure password complexity requirements:

STEP 1 Click **Security** > **Password Complexity** in the navigation window.

STEP 2 For the **Password Complexity** setting, select **Enable**.

STEP 3 Configure the parameters:

- **Password Minimum Character Class**—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.
- **Password Different From Current**—Select to have users enter a different password when their current password expires. If not selected, users can reenter the previous password when their current password expires.
- **Maximum Password Length**—The maximum password character length is a range from 64 to 80. 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**—Select to have passwords expire after a configured time period.
- **Password Aging Time**—The number of days before a newly created password expires, from 1 to 365. The default is 180 days.

STEP 4 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

WPA-PSK Complexity

When you configure 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 for any VAP, you can use the *WPA-PSK Complexity* page to configure complexity requirements for the key used in the authentication process. More complex keys provide increased security.

To configure WPA-PSK complexity:

STEP 1 Click **Security** > **WPA-PSK Complexity** in the navigation window.

STEP 2 Click **Enable** for the **WPA-PSK Complexity** setting to enable the WAP device to check WPA-PSK keys against the criteria you configure. If you clear the checkbox, none of these settings will be used.

STEP 3 Configure the parameters:

- **WPA-PSK Minimum Character Class**—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.
- **WPA-PSK Different From Current**—Select one of these options:
  - **Enable**—Users must configure a different key after their current key expires.
  - **Disable**— Users can use the old or previous key after their current key expires.
- **Maximum WPA-PSK Length**—The maximum key length in number of characters is from 32 to 64. The default is 63.
- **Minimum WPA-PSK Length**—The minimum key length in number of characters is from 8 to 16. The default is 8. Select the checkbox to make the field editable and to activate this requirement.

STEP 4 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

7

Client Quality of Service

This chapter provides an overview of Client Quality of Service (QoS) and explains the QoS features available from the Client QoS menu.

- **ACLs**
- **Class Map**
- **Policy Map**
- **Client QoS Association**
- **Client QoS Status**

ACLs

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.

IPv4 and IPv6 ACLs

IP ACLs classify traffic for Layers 3 and 4.

Each ACL is a set of up to 10 rules applied to traffic sent from a wireless client or to be received by a wireless client. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network. Rules can be based on various criteria and may apply to one ore more fields within a packet, such as the source or destination IP address, the source or destination port, or the protocol carried in the packet.

NOTE There is an implicit deny at the end of every Rule created. To avoid deny all, it is strongly recommended to add a permit rule within 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 or exits the WAP device port (depending on whether the ACL is applied in the up or down direction), 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.

Configuring ACLs

Configure ACLs and rules on the *ACL Configuration* page, and then apply the rules to a specified VAP.

The steps below give a general description of how to configure ACLs:

STEP 1 Click **Client QoS** > **ACL** in the navigation window.

STEP 2 Specify a name for the ACL.

STEP 3 Select the type of ACL to add.

STEP 4 Add the ACL

STEP 5 Add new rules to the ACL.

STEP 6 Configure the match criteria for the rules.

STEP 7 Use the *Client QoS Association* page to apply the ACL to one or more VAPs.

The steps below give a detailed description of how to configure ACLs:

STEP 1 Click **Client QoS** > **ACL** in the navigation window.

STEP 2 Enter these parameters to create a new ACL:

- **ACL Name**—A name to identify the ACL. The name can contain from 1 to 31 alphanumeric characters. Spaces are not allowed.
- **ACL Type**—The type of ACL to configure:
  - IPv4
  - IPv6
  - MAC

IPv4 and IPv6 ACLs control access to network resources based on Layer 3 and Layer 4 criteria. MAC ACLs control access based on Layer 2 criteria.

STEP 3 Click **Add ACL**.

The page displays additional fields for configuring the ACL.

STEP 4 Configure the rule parameters:

- **ACL Name - ACL Type**—The ACL to configure with the new rule. The list contains all ACLs added in the ACL Configuration section.
- **Rule**—The action to be taken:
  - Select **New Rule** to configure a new rule for the selected ACL.
  - If rules already exist (even if created for use with other ACLs), you can select the rule number to add the rule to the selected ACL or to modify the rule.

  When an ACL has multiple rules, the rules are applied to the packet or frame in the order in which you add them to the ACL. There is an implicit deny all rule as the final rule.
- **Action**—Whether the ACL rule permits or denies an action.

  When you select Permit, the rule allows all traffic that meets the rule criteria to enter or exit the WAP device (depending on the ACL direction you select). Traffic that does not meet the criteria is dropped.

  When you select Deny, the rule blocks all traffic that meets the rule criteria from entering or exiting the WAP device (depending on the ACL direction you select). Traffic that does not meet the criteria is forwarded unless this rule is the final rule. Because there is an implicit deny all rule at the end of every ACL, traffic that is not explicitly permitted is dropped.
- **Match Every Packet**—If selected, the rule, which either has a permit or deny action, will match the frame or packet regardless of its contents.

  If you select this field, you cannot configure any additional match criteria. The Match Every option is selected by default for a new rule. You must clear the option to configure other match fields.

For IPv4 ACLs, configure these parameters:

- **Protocol**—The Protocol field to use an L3 or L4 protocol match condition based on the value of the IP Protocol field in IPv4 packets or the Next Header field of IPv6 packets.

If you select the checkbox, select one of these options:

- **Select From List**—Select one of these protocols: IP, ICMP, IGMP, TCP, or UDP.
- **Match to Value**—Enter a standard IANA-assigned protocol ID from 0 to 255. Choose this method to identify a protocol not listed by name in the Select From List.

- **Source IP Address**—Requires a packet's source IP address to match the address listed here. Enter an IP address in the appropriate field to apply this criteria.
- **Wild Card Mask**—The source IP address wildcard mask.

  The wild card masks 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 wildcard of 0.0.0.0 indicates that all of the bits are important. This field is required when Source IP Address is checked.

  A wild card mask is, in essence, the inverse of a subnet mask. For example, to match the criteria to a single host address, use a wildcard 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.

  If you select this checkbox, choose the port name or enter the port number.

  - **Select From List**—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.
  - **Match to Port**—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:

    0–1023—Well Known Ports

    1024–49151—Registered Ports

    49152–65535—Dynamic and/or Private Ports
- **Destination IP Address**—Requires a packet's destination IP address to match the address listed here. Enter an IP address in the appropriate field to apply this criteria.

- **Wild Card Mask**—The destination IP address wildcard mask.

  The wild card masks 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 wildcard of 0.0.0.0 indicates that all of the bits are important. This field is required when Source IP Address is selected.

  A wild card mask is in essence the inverse of a subnet mask. For example, To match the criteria to a single host address, use a wildcard 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.

  If you select this checkbox, choose the port name or enter the port number.

  - **Select From List**—Select 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.

  - **Match to Port**—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:

    0–1023—Well Known Ports

    1024–49151—Registered Ports

    49152–65535—Dynamic and/or Private Ports

- **IP DSCP**—Matches packets based on their IP DSCP value.

  If you select this checkbox, choose one of these options as the match criteria:

  - **Select From List**—DSCP Assured Forwarding (AS), Class of Service (CS) or Expedited Forwarding (EF) values.

  - **Match to Value**—A custom DSCP value, from 0 to 63.

- **IP Precedence**—Matches packets based on their IP Precedence value. If you select this checkbox, enter an IP Precedence value from 0 to 7.

- **IP TOS Bits**—Specifies a value to use the packet's Type of Service bits in the IP header as match criteria.

The IP TOS field in a packet is defined as all eight bits of the Service Type octet in the IP header. The TOS Bits value is a two-digit hexadecimal number from 00 to ff.

The high-order three bits represent the IP precedence value. The high-order six bits represent the IP Differentiated Services Code Point (DSCP) value.

- **IP TOS Mask**—Enter an IP TOS mask value to identify the bit positions in the TOS Bits value that are used for comparison against the IP TOS field in a packet.

  The TOS Mask value is a two-digit hexadecimal number from 00 to ff, representing an inverted (that is, wildcard) mask. The zero-valued bits in the TOS Mask denote the bit positions in the TOS Bits value that are used for comparison against the IP TOS field of a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a TOS Bits value of 0 and a TOS Mask of 00. This is an optional configuration.

For IPv6 ACLs, configure these parameters:

- **Protocol**—Select the Protocol field to use an L3 or L4 protocol match condition based on the value of the IP Protocol field in IPv4 packets or the Next Header field of IPv6 packets.

  If you select the field, choose the protocol to match by keyword or protocol ID.

- **Source IPv6 Address**—Select this field to require a packet's source IPv6 address to match the address listed here. Enter an IPv6 address in the appropriate field to apply this criteria.

- **Source IPv6 Prefix Length**—Enter the prefix length of the source IPv6 address.

- **Source Port**—Select this option to include a source port in the match condition for the rule. The source port is identified in the datagram header.

  If you select this checkbox, choose the port name or enter the port number.

- **Destination IPv6 Address**—Select this field to require a packet's destination IPv6 address to match the address listed here. Enter an IPv6 address in the appropriate field to apply this criteria.

- **Destination IPv6 Prefix Length**—Enter the prefix length of the destination IPv6 address.

- **Destination Port**—Select this option to include a destination port in the match condition for the rule. The destination port is identified in the datagram header.

  If you select this checkbox, choose the port name or enter the port number.

- **IPv6 Flow Label**—Flow label is 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 1048575).

- **IP DSCP**—Matches packets based on their IP DSCP value.

  If you select this checkbox, choose one of these options as the match criteria:

  - **Select From List**—DSCP Assured Forwarding (AS), Class of Service (CS) or Expedited Forwarding (EF) values.

  - **Match to Value**—A custom DSCP value, from 0 to 63.

For a MAC ACL, configure these parameters:

- **EtherType**—Select the EtherType field to compare the match criteria against the value in the header of an Ethernet frame.

  Select an EtherType keyword or enter an EtherType value to specify the match criteria.

  - **Select from List**—Select one of these protocol types: appletalk, arp, ipv4, ipv6, ipx, netbios, pppoe.

  - **Match to Value**—Enter a custom protocol identifier to which packets are matched. The value is a four-digit hexadecimal number in the range of 0600–FFFF.

- **Class of Service**—Select this field and enter an 802.1p user priority to compare against an Ethernet frame.

  The valid range is from 0 to 7. This field is located in the first/only 802.1Q VLAN tag.

- **Source MAC Address**—Select this field and enter the source MAC address to compare against an Ethernet frame.

- **Source MAC Mask**—Select this field and enter the source MAC address mask specifying which bits in the source MAC to compare against an Ethernet frame.

A 0 indicates that the address bit is significant, and an f indicates that the address bit is to be ignored. A MAC mask of 00:00:00:00:00:00 matches a single MAC address.

- **Destination MAC Address**—Select this field and enter the destination MAC address to compare against an Ethernet frame.
- **Destination MAC Mask**—Enter the destination MAC address mask specifying which bits in the destination MAC to compare against an Ethernet frame.

  A 0 indicates that the address bit is significant, and an f indicates that the address bit is to be ignored. A MAC mask of 00:00:00:00:00:00 matches a single MAC address.
- **VLAN ID**—Select this field and enter the specific VLAN ID to compare against an Ethernet frame.

  This field is located in the first/only 802.1Q VLAN tag.

STEP 5 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

NOTE: To delete an ACL, ensure that it is selected in the **ACL Name-ACL Type** list, select **Delete ACL**, and click **Save**.

Class Map

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

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 policy maps that give precedence over other traffic.

You can use the *Class Map* page to define classes of traffic. Use the *Policy Map* page to define policies and associate class maps to them.

Adding a Class Map

To add a class map:

STEP 1 Click **Client QoS** > **Class Map** in the navigation window.

STEP 2 Enter a **Class Map Name**.

STEP 3 Select a value from the **Match Layer 3 Protocol** list:

- **IPv4**—The class map applies only to IPv4 traffic on the WAP device.
- **IPv6**—The class map applies only to IPv6 traffic on the WAP device.

The Class Map page displays with additional fields, depending on the layer 3 protocol selected:

Use the fields in the Match Criteria Configuration area to match packets to a class. Select the check box for each field to be used as a criterion for a class and enter data in the related field. You can have multiple match criteria in a class.

The match criteria fields that are available depend on whether the class map is an IPv4 or IPv6 class map.

Defining a Class Map

To configure a class map:

STEP 1 Select the class map from the **Class Map Name** list.

STEP 2 Configure the parameters (parameters that display only for IPv4 or IPv6 class maps are noted):

- **Match Every Packet**—The match condition is true to all the parameters in an L3 packet.

When selected, all L3 packets will match an Match Every match condition.

- **Protocol**—Use an L3 or L4 protocol match condition based on the value of the IP Protocol field in IPv4 packets or the Next Header field of IPv6 packets.

  If you select the field, choose the protocol to match by keyword or enter a protocol ID.

  - **Select From List**—Match the selected protocol: IP, ICMP, IPv6, ICMPv6, IGMP, TCP, UDP.
  - **Match to Value**—Match 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 IP Address** or **Source IPv6 Address**—Requires a packet's source IP address to match the address listed here. Select the checkbox and enter an IP address in the text box.

- **Source IP Mask** (IPv4 only)—The source IP 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 a 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.

- **Source IPv6 Prefix Length** (IPv6 only)—The prefix length of the source IPv6 address.

- **Destination IP Address** or **Destination IPv6 Address**—Requires a packet's destination IP address to match the address listed here. Enter an IP address in the appropriate field to apply this criteria.

- **Destination IP Mask** (IPv4 only)—The destination IP 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 a 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 IPv6 Prefix Length** (IPv6 only)—The prefix length of the destination IPv6 address.
- **IPv6 Flow Label** (IPv6 only)—A 20-bit number that is unique to an IPv6 packet. It is used by end stations to signify quality-of-service handling in routers (range 0 to 1048575).
- **IP DSCP**—See description under Service Type fields below.
- **Source Port**—Includes a source port in the match condition for the rule. The source port is identified in the datagram header.

  If you select the field, choose the port name or enter the port number.

  - **Select From List**—Matches a keyword associated with the source port: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.

    Each of these keywords translates into its equivalent port number.

  - **Match to Port**—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:

    0–1023—Well Known Ports

    1024–49151—Registered Ports

    49152–65535—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.

  If you select this field, choose the port name or enter the port number.

  - **Select From List**—Matches the destination port in the datagram header with the selected keyword: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.

    Each of these keywords translates into its equivalent port number.

  - **Match to Port**—Matches the destination port in the datagram header with an IANA port number that you specify. The port range is from 0 to 65535 and includes three different types of ports:

0–1023—Well Known Ports

1024–49151—Registered Ports

49152–65535—Dynamic and/or Private Ports

- **EtherType**—Compares the match criteria against the value in the header of an Ethernet frame.

  Select an EtherType keyword or enter an EtherType value to specify the match criteria.

  - **Select from List**—Matches the Ethertype in the datagram header with the selected protocol types: appletalk, arp, ipv4, ipv6, ipx, netbios, pppoe.
  - **Match to Value**—Matches the Ethertype in the datagram header with a custom protocol identifier that you specify. The value can be a four-digit hexadecimal number in the range of 0600–FFFF.

- **Class of Service**—A class of service 802.1p user priority value to be matched for the packets. The valid range is from 0 to 7.
- **Source MAC Address**—A source MAC address to compare against an Ethernet frame.
- **Source MAC Mask**—The source MAC address mask specifying which bits in the destination MAC to compare against an Ethernet frame.

  An f indicates that the address bit is significant, and a 0 indicates that the address bit is to be ignored. A MAC mask of ff:ff:ff:ff:ff:ff matches a single MAC address.

- **Destination MAC Address**—The destination MAC address to compare against an Ethernet frame.
- **Destination MAC Mask**—The destination MAC address mask specifying which bits in the destination MAC to compare against an Ethernet frame.

  An f indicates that the address bit is significant, and a 0 indicates that the address bit is to be ignored. A MAC mask of ff:ff:ff:ff:ff:ff matches a single MAC address.

- **VLAN ID**—A VLAN ID to be matched for packets. The VLAN ID range is from 0 to 4095.

The Service Type fields below display for IPv4 only. You can specify one type of service to use in matching packets to class criteria.

- **IP DSCP**—A differentiated services code point (DSCP) value to use as a match criteria:
  - **Select from List**—A list of DSCP types.
  - **Match to Value**—A DSCP value that you specify, from 0 to 63.
- **IP Precedence** (IPv4 only)—Matches the packet's IP Precedence value to the class criteria IP Precedence value. The IP Precedence range is from 0 to 7.
- **IP TOS Bits** (IPv4 only)—Uses the packet's Type of Service bits in the IP header as match criteria.

  The TOS bit value ranges between (00–FF). The high-order three bits represent the IP precedence value. The high-order six bits represent the IP Differentiated Services Code Point (DSCP) value.

STEP 3 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

NOTE: To delete a class map, select it in the **Class Map Name** list and click **Delete**. The class map cannot be deleted if it is already attached to a policy.

Policy Map

Packets are classified and processed based on defined criteria. The classification criteria is defined by a class on the *Class Map* page. The processing is defined by a policy's 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 supports up to 50 Policy Maps. A Policy Map can contain up to 10 Class Maps.

To add and configure a policy map:

STEP 1 Click **Client QoS** > **Policy Map** in the navigation window.

STEP 2 Enter a **Policy Map Name** and click **Add Policy Map**.

The page redisplays with additional fields for configuring the policy map.

STEP 3 In the Policy Class Definition area, ensure the newly created policy map displays in the **Policy Map Name** list.

STEP 4 In the **Class Map Name** list, select the class map to apply this policy.

STEP 5 Configure the parameters:

- **Police Simple**—Establishes the traffic policing style for the class. The simple form of the policing style uses a single data rate and burst size, resulting in two outcomes: conform and nonconform. If you select this field, configure one of these fields:
  - **Committed Rate**—The committed rate, in Kbps, to which traffic must conform. The range is from 1 to 4294967295 Kbps.
  - **Committed Burst**—The committed burst size, in bytes, to which traffic must conform. The range is from 1 to 64000 bytes.
- **Send**—Specifies that all packets for the associated traffic stream are to be forwarded if the class map criteria is met.
- **Drop**—Specifies that all packets for the associated traffic stream are to be dropped if the class map criteria is met.
- **Mark Class of Service**—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.
- **Mark IP DSCP**—Marks all packets for the associated traffic stream with the IP DSCP value you select from the list or specify.
  - **Select from List**—A list of DSCP types.
  - **Match to Value**—A DSCP value that you specify. The value is an integer between 0 to 63.
- **Mark 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.
- **Disassociate Class Map**—Removes the class selected in the Class Map Name list from the policy selected in the Policy Map Name list.
- **Member Classes**—Lists all DiffServ classes currently defined as members of the selected policy. If no class is associated with the policy, the field is empty.

STEP 6 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

NOTE: To delete a policy map, select it in the **Policy Map Name** list and click **Delete**.

Client QoS Association

The *Client QoS Association* page provides additional control over certain QoS aspects of wireless clients that connect to the network, such as the amount of bandwidth an individual client is allowed to send and receive. To control general categories of traffic, such as HTTP traffic or traffic from a specific subnet, you can configure ACLs and assign them to one or more VAPs.

In addition to controlling general traffic categories, Client QoS allows you to configure per-client conditioning of various micro-flows through Differentiated Services (DiffServ). DiffServ policies are a useful tool for establishing general micro-flow 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 client QoS association parameters:

STEP 1 Click **Client QoS** > **Client QoS Association** in the navigation window.

STEP 2 Select **Enable** for the **Client QoS Global Admin Mode** to globally enable this feature.

STEP 3 From the VAP list, select the VAP on which you want to configure client QoS parameters.

STEP 4 Configure these parameters for the selected VAP:

- **Client QoS Mode**—Select **Enable** to enable client QoS functionality on the selected VAP.
- **Bandwidth Limit Down**—The maximum allowed transmission rate from the WAP device to the client in bits per second (bps). The valid range is from 0 to 4294967295 bps.
- **Bandwidth Limit Up**—The maximum allowed transmission rate from the client to the WAP device in bits per second (bps). The valid range is from 0 to 4294967295 bps.

- **ACL Type Down**—The type of ACL to apply to traffic in the outbound (WAP device-to-client) direction, which can be one of these options:
  - IPv4—The ACL examines IPv4 packets for matches to ACL rules.
  - IPv6—The ACL examines IPv6 packets for matches to ACL rules.
  - MAC—The ACL examines layer 2 frames for matches to ACL rules.
- **ACL Name Down**—The name of the ACL applied to traffic in the outbound direction.

  After switching the packet or frame to the outbound interface, the ACL's rules are checked for a match. The packet or frame is transmitted if it is permitted and discarded if it is denied.
- **ACL Type Up**—The type of ACL that is applied to traffic in the inbound (client-to-WAP) direction, which can be one of these options:
  - IPv4—The ACL examines IPv4 packets for matches to ACL rules.
  - IPv6—The ACL examines IPv6 packets for matches to ACL rules.
  - MAC—The ACL examines layer 2 frames for matches to ACL rules.
- **ACL Name Up**—The name of the ACL applied to traffic entering the WAP device in the inbound direction.

  When a packet or frame is received by the WAP device, the ACL's rules are checked for a match. The packet or frame is processed if it is permitted and discarded if it is denied.
- **DiffServ Policy Down**—The name of the DiffServ policy applied to traffic from the WAP device in the outbound (WAP-to-client) direction.
- **DiffServ Policy Up**—The name of the DiffServ policy applied to traffic sent to the WAP device in the inbound (client-to-WAP) direction.

STEP 5 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

Client QoS Status

The *Client QoS Status* page shows the client QoS settings that are applied to each client currently associated with the WAP device.

To display this page, click **Client QoS** > **Client QoS Status** in the navigation window.

These fields display:

- **Station**—The Station menu contains the MAC address of each client currently associated with the WAP device. To view the QoS settings applied to a client, select its MAC address from the list.
- **Global QoS Mode**—Whether QoS is enabled globally on the WAP device. This status is configured on the *Client QoS Association* page.
- **Client QoS Mode**—Whether QoS is enabled on the client's associated VAP. This status is configured on the *Client QoS Association* page.
- **Bandwidth Limit Down**—The maximum allowed transmission rate from the WAP device to the client in bits per second (bps). The valid range is from 0 to 4294967295 bps.
- **Bandwidth Limit Up**—The maximum allowed transmission rate from the client to the WAP device in bits per second (bps). The valid range is from 0 to 4294967295 bps.
- **ACL Type Up**—The type of ACL that is applied to traffic in the inbound (client-to-WAP) direction, which can be one of these options:
  - IPv4: The ACL examines IPv4 packets for matches to ACL rules.
  - IPv6: The ACL examines IPv6 packets for matches to ACL rules.
  - MAC: The ACL examines layer 2 frames for matches to ACL rules.
- **ACL Name Up**—The name of the ACL applied to traffic entering the WAP in the inbound direction. When a packet or frame is received by the WAP, the ACL rules are checked for a match. The packet or frame is processed if it is permitted and discarded if it is denied.

- **ACL Type Down**—The type of ACL to apply to traffic in the outbound (WAP-to-client) direction, which can be one of these options:
  - IPv4: The ACL examines IPv4 packets for matches to ACL rules.
  - IPv6: The ACL examines IPv6 packets for matches to ACL rules.
  - MAC: The ACL examines layer 2 frames for matches to ACL rules.
- **ACL Name Down**—The name of the ACL applied to traffic in the outbound direction. After switching the packet or frame to the outbound interface, the ACL rules are checked for a match. The packet or frame is transmitted if it is permitted and discarded if it is denied.
- **DiffServ Policy Up**—The name of the DiffServ policy applied to traffic sent to the WAP device in the inbound (client-to-WAP) direction.
- **DiffServ Policy Down**—The name of the DiffServ policy applied to traffic from the WAP device in the outbound (WAP-to-client) direction.

8

Simple Network Management Protocol

This chapter describes how to configure the Simple Network Management Protocol (SNMP) to perform configuration and statistics gathering tasks.

It contains these topics:

- SNMP Overview
- General SNMP Settings
- SNMP Views
- SNMP Groups
- SNMP Users
- SNMP Targets

SNMP Overview

SNMP defines a standard for recording, storing, and sharing information about network devices. SNMP facilitates network management, troubleshooting, and maintenance.

The WAP device supports SNMP versions 1, 2, and 3. Unless specifically noted, all configuration parameters apply to SNMPv1 and SNMPv2c only. Key components of any SNMP-managed network are managed devices, SNMP agents, and a management system. The agents store data about their devices in Management Information Bases (MIBs) and return this data to the SNMP manager when requested. Managed devices can be network nodes such as WAP devices, routers, switches, bridges, hubs, servers, or printers.

The WAP device can function as an SNMP managed device for seamless integration into network management systems.

General SNMP Settings

You can use the General page to enable SNMP and configure basic protocol settings.

To configure general SNMP settings:

STEP 1 Click **SNMP** > **General** in the navigation window.

STEP 2 Select **Enabled** for the **SNMP** setting. SNMP is disabled by default.

STEP 3 Configure the parameters:

- **Read-only Community Name**—A read-only community name for SNMPv2 access. The valid range is 1 to 256 characters.

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

  The community name can accept alphanumeric and special characters.

- **UDP Port**—By default an SNMP agent only listens to requests from port 161. However, you can configure this so that the agent listens to requests on another port. The valid range is from 1025 to 65535.

- **Read-write Community Name**—Sets a read-write community name to be used for SNMP Set requests. The valid range is from 1 to 256 characters.

  Setting a community name is similar to setting a password. Only requests from the machines that identify themselves with this community name will be accepted.

  The community name can be in any alphanumeric format.

- **Management Station**—Determines which stations can access the WAP device through SNMP: Select one of these options:

  - **All**—The set of stations that can access the WAP device through SNMP is not restricted.

  - **User Defined**—Restricts the source of permitted SNMP requests to those specified in these lists:

- **NMS Hostname, IPv4 Address/Name**—The IPv4 IP address, DNS hostname, or subnet of the machines that can execute get and set requests to the managed devices. The valid range is from 1 to 256 characters.

  As with community names, this provides a level of security on SNMP settings. The SNMP agent will only accept requests from the IP address, hostname, or subnet specified here.

  To specify a subnet, enter one or more subnetwork address ranges in the form `address/mask_length` where *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`.

  The address range is used to specify the subnet of the designated NMS. Only machines with IP addresses in this range are permitted to execute, get, and set requests on the managed device. Given the example above, the machines with addresses from `192.168.1.1` through `192.168.1.254` can execute SNMP commands on the device. (The address identified by suffix .0 in a subnetwork range is always reserved for the subnet address, and the address identified by .255 in the range is always reserved for the broadcast address).

  As another example, if you enter a range of `10.10.1.128/25` machines with IP addresses from `10.10.1.129` through `10.10.1.254` can execute SNMP requests on managed devices. In this example, `10.10.1.128` is the network address and `10.10.1.255` is the broadcast address. 126 addresses would be designated.

- **NMS IPv6 Address/Name**—The IPv6 IP address, DNS hostname, or subnet of the machines 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). The valid range is from 1 to 253 characters.

- **Trap Community Name**—A global community string associated with SNMP traps. Traps sent from the device will provide this string as a community name. The valid range is from 1 to 60 characters, in alphanumeric format and can include special characters.

- **Trap Destination Table**—A list of up to three IP addresses or hostnames to receive SNMP traps. The valid range is from 1 to 63 characters. Select the checkbox and choose a **Host Type** (IPv4 or IPv6) before adding the **IP Address/Hostname**.

An example of a DNS hostname is: `snmptraps.foo.com`. Since 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 hostnames. Ensure you select the **Enabled** check box and select the appropriate Host Type.

STEP 4 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

NOTE After new settings are saved, the corresponding processes may be stopped and restarted. When this happens, the WAP device may lose connectivity. We recommend that you change WAP device settings when it will least affect your wireless clients.

SNMP Views

An 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.

These notes summarize some critical guidelines regarding 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 configure an SNMP view:

STEP 1 Click **SNMP** > **Views** in the navigation window.

STEP 2 Configure the parameters:

- **View Name**—A name that identifies the MIB view. View names can contain up to 32 alphanumeric characters.

- **Type**—Whether to include or exclude the view subtree or family of subtrees from the MIB view.
- **OID**—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**—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 . (period) or : (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 **Add**, and then click **Save**. The view is added to the SNMPv3 Views list and your changes are saved to the Running Configuration and to the Startup Configuration.

NOTE To remove a view, select the view in the list and click **Remove**.

SNMP Groups

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 Management Objects (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 an MD5 key/password for authentication and a DES key/password for encryption. Both the MD5 and DES key/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 an MD5 key/password for authentication and a DES key/password for encryption. Both the MD5 and DES key/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.

NOTE The WAP Device supports a maximum of eight groups.

To add an SNMP group:

STEP 1 Click **SNMP** > **Groups** in the navigation window.

STEP 2 Configure the parameters:

- **Name**—A name that identifies the group. The default group names are RO and RW.

  Group names can contain up to 32 alphanumeric characters.

- **Security Level**—Sets the security level for the group, which can be one of these options:

  - **noAuthentication-noPrivacy**—No authentication and no data encryption (no security).

  - **Authentication-noPrivacy**—Authentication, but no data encryption. With this security level, users send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption.

  - **Authentication-Privacy**—Authentication and data encryption. With this security level, users send an MD5 key/password for authentication and a DES key/password for encryption.

    For groups that require authentication, encryption, or both, you must define the MD5 and DES key/passwords on the *SNMP Users* page.

- **Write Views**—The write access to MIBs for the group, which can be one of these options:

  - **write-all**—The group can create, alter, and delete MIBs.

  - **write-none**—The group cannot create, alter, or delete MIBS.

- **Read Views**—The read access to MIBs for the group:
  - **view-all**—The group is allowed to view and read all MIBs.
  - **view-none**—The group cannot view or read MIBs.

STEP 3 Click **Add**, and then click **Save**. The group is added to the SNMPv3 Groups list and your changes are saved to the Running Configuration and to the Startup Configuration.

NOTE To remove a group, select the group in the list and click **Remove**.

SNMP Users

You can use the *SNMP Users* page to define users, associate a security level to each user, and configure security keys per-user.

Each user is mapped to an SNMPv3 group, either from the predefined or user-defined groups, and, optionally, is configured for authentication and encryption. For authentication, only the MD5 type is supported. For encryption, only the DES type is supported. There are no default SNMPv3 users on the WAP Device, and you can add up to eight users.

To add SNMP users:

STEP 1 Click **SNMP** > **Users** in the navigation window.

STEP 2 Configure the parameters:

- **Name**—A name that identifies the SNMPv3 user. User names can contain up to 32 alphanumeric characters.
- **Group**—The group that the user is mapped to. The default groups are RWAuth, RWPriv, and RO. You can define additional groups on the *SNMP Groups* page.
- **Authentication Type**—The type of authentication to use on SNMPv3 requests from the user, which can be one of these options:
  - **MD5**—Require MD5 authentication on SNMP requests from the user.
  - **None**—SNMPv3 requests from this user require no authentication.

- **Authentication Key**—(If you specify MD5 as the authentication type) A password to enable the SNMP agent to authenticate requests sent by the user. The password must be between 8 and 32 characters in length.
- **Encryption Type**—The type of privacy to use on SNMP requests from the user, which can be one of these options:
  - **DES**—Use DES encryption on SNMPv3 requests from the user.
  - **None**—SNMPv3 requests from this user require no privacy.
- **Encryption Key**—(If you specify DES as the privacy type) A key to use to encrypt the SNMP requests. The key must be between 8 and 32 characters in length.

STEP 3 Click **Add**, and then click **Save**. The user is added to the SNMPv3 Users list and your changes are saved to the Running Configuration and to the Startup Configuration.

NOTE To remove a user, select the user in the list and click **Remove**.

SNMP Targets

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

NOTE SNMPv3 user configuration (see **SNMP Users, page 136**) should be completed before configuring SNMPv3 targets.

NOTE The WAP Device supports a maximum of eight targets.

To add SNMP targets:

STEP 1 Click **SNMP** > **Targets** in the navigation window.

STEP 2 Configure the parameters:

IPv4/IPv6 Address—Enter the IP address of the remote SNMP manager to receive the target. 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).

- **Port**—Enter the UDP port to use for sending SNMPv3 targets.
- **Users**—Enter the name of the SNMP user to associate with the target. To configure SNMP users, see “Configuring SNMP Users” on page 125.
- **SNMPv3 Targets**—This field shows the SNMPv3 Targets on the WAP Device. To remove a target, select it and click **Remove**.

STEP 3 Click **Add**, and then click **Save**. The user is added to the SNMPv3 Targets list and your changes are saved to the Running Configuration and to the Startup Configuration.

NOTE To remove a user, select the user in the list and click **Remove**.

9

Captive Portal

This chapter describes the Captive Portal (CP) feature, which allows you to block wireless clients from accessing the network until user verification has been established. You can configure CP verification to allow access for both guest and authenticated users.

NOTE The Captive Portal feature is available only on the Cisco WAP321 device.

Authenticated users must be validated against a database of authorized Captive Portal groups or users before access is granted. The database can be stored locally on the WAP device or on a RADIUS server.

Captive Portal consists of two CP instances. Each instance can be configured independently, with different verification methods for each VAP or SSID. Cisco WAP321 devices operate concurrently with some VAPs configured for CP authentication and other VAPs configured for normal wireless authentication methods, such as WPA or WPA Enterprise.

This chapter includes these topics:

Global Captive Portal Configuration

You can use the Global CP Configuration page to control the administrative state of the CP feature and configure global settings that affect all captive portal instances configured on the WAP device.

To configure CP Global settings:

STEP 1 Click **Captive Portal** > **Global Configuration** in the navigation window.

STEP 2 Configure the parameters:

- **Captive Portal Mode**—Enables CP operation on the WAP device.
- **Authentication Timeout**—To access the network through a portal, the client must first enter authentication information on an authentication Web page. This field specifies the number of seconds the WAP device keeps an authentication session open with the associated wireless client. If the client fails to enter authentication credentials within the timeout period allowed, the client needs to refresh the Web authentication page, or reconnect to the wireless network. The default authentication timeout is 300 seconds.
- **Additional HTTP Port**—HTTP traffic uses port 80, but you can configure an additional port for HTTP traffic. Enter a port number between 0-65535. Port number 80 or 443 cannot be used, and the HTTP and HTTPs ports cannot be the same.
- **Additional HTTPS Port**—HTTP traffic over SSL (HTTPS) uses port 443, but you can configure an additional port for HTTPS traffic. Enter a port number between 0-65535. Port number 80 or 443 cannot be used, and the HTTP and HTTPs ports cannot be the same.

These fields display nonconfigurable CP information:

- **Instance Count**—The number of CP instances currently configured on the WAP device. Up to two instances can be configured.
- **Group Count**—The number of CP groups currently configured on the WAP device. Up to two groups can be configured. Default Group exists by default and cannot be deleted.
- **User Count**—The number of CP users currently configured on the WAP device. Up to 128 users can be configured.

STEP 3 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

Instance Configuration

You can create up to two Captive Portal instances; each CP instance is a defined set of instance parameters. Instances can be associated with one or more VAPs. Different instances can be configured to respond differently to users as they attempt to access the associated VAP.

To create a CP instance and configure its settings:

STEP 1 Click **Captive Portal** > **Instance Configuration** in the navigation window.

STEP 2 Ensure that **Create** is selected from the **Captive Port Instances** list.

STEP 3 Enter an **Instance Name** from 1 to 32 alphanumeric characters and click **Save**.

STEP 4 Select the instance name from the **Captive Port Instances** list.

The Captive Portal Instance Parameters fields redisplay, with additional options.

STEP 5 Configure the parameters:

- **Instance ID**—The instance ID. This field is non-configurable.
- **Administrative Mode**—Enables and disables the CP instance.
- **Protocol**—Specifies 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.
- **Verification**—The authentication method for CP to use to verify clients:
  - **Guest**—The user does not need to be authenticated by a database.
  - **Local**—The WAP device uses a local database to authenticated users.

  - **RADIUS**—The WAP device uses a database on a remote RADIUS server to authenticate users.

- **Redirect**—Specifies that CP should redirect the newly authenticated client to the configured URL. If this option is clear, the user sees the locale-specific welcome page after a successful verification.
- **Redirect URL**—Enter the URL (including http://) to which the newly authenticated client is redirected if the URL Redirect Mode is enabled. The range is from 0 to 256 characters.
- **Away Timeout**—The amount of time a user can remain idle before automatically being logged out. If the value is set to 0, the timeout is not enforced. The range is from 0 to 1440 minutes. The default value is 60 minutes.
- **Session Timeout**—The amount of time to wait before terminating a session. A user is logged out after the session timeout is reached. If the value is set to 0, the timeout is not enforced. The range is from 0 to 1440 minutes. The default value is 0.
- **User Up Rate**—The maximum upload speed, in megabits per second, that a client can transmit traffic when using the captive portal. This setting limits the bandwidth at which the client can send data into the network. The range is from 0 to 300 Mbps. The default value is 0.
- **User Down Rate**—The maximum download speed, in megabits per second, that a client can receive traffic when using the captive portal. This setting limits the bandwidth at which the client can receive data from the network. The range is from 0 to 300 Mbps. The default value is 0.
- **User Group Name**—If the Verification Mode is Local or RADIUS, assigns an existing User Group to the CP instance. All users who belong to the group are permitted to access the network through this portal.
- **RADIUS IP Network**—Choose if the WAP RADIUS client will use the configured IPv4 or IPv6 RADIUS server addresses.
- **Global RADIUS**—If the Verification Mode is RADIUS, select to specify that the default Global RADIUS server list is used to authenticating clients. (See **RADIUS Server, page 106** for information about configuring the global RADIUS servers.) If you want the CP feature to use a different set of RADIUS servers, clear this setting and configure the servers in the fields on this page.
- **RADIUS Accounting**—Enables tracking and measuring the resources a particular user has consumed, such as system time and amount of data transmitted and received.

If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers, and for globally or locally configured servers.

RADIUS IP—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 authentication requests are sent to the address you specify.

- **Radius Backup IP 1–3**—Up to three IPv4 or IPv6 backup RADIUS server addresses.

  If authentication fails with the primary server, each configured backup server is tried in sequence.

- **RADIUS Current**—Enables selecting administratively 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.

- **RADIUS Key**—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 you enter will be displayed as "*" characters.

- **RADIUS Backup Key 1–3**—The RADIUS key associated with the configured backup RADIUS servers. The server at RADIUS IP Address-1 uses RADIUS Key-1, RADIUS IP Address-2 uses RADIUS Key-2, and so on.

- **Locale Count**—The number of locales associated with the instance. You can create and assign up to three different locales to each CP instance from the *Web Customization* page.

- **Delete Instance**—Deletes the current instance.

STEP 6 Click **Save**. You changes are saved to the Running Configuration.

Instance Association

You can use the *Instance Association* page to associate a CP instance to a VAP. The associated CP instance settings will apply to users who attempt to authenticate on the VAP.

To associate an instance to a VAP:

STEP 1 Click **Captive Portal** > **Instance Association** in the navigation window.

STEP 2 Select the instance name for each VAP you want to associate an instance to.

STEP 3 Click **Save**. Your change are saved to the Running Configuration.

Upload Binary Files

When users initiate access to a VAP that is associated to a captive portal instance, an authentication page displays. You can customize this page with your own logo and other graphics. You can use the *Upload Binary Files* page to upload these graphics to the WAP device.

Up to 18 images can be uploaded (assuming six locales and each locale can have three images).

To upload binary graphic files to the WAP device:

STEP 1 Create or identify custom graphics to replace the default graphics, as shown in this table:

Image Type	Use	Default Width x Height
Logo	Displays at top left of page to provide branding information.	168 × 78 pixels
Account	Displays above the login field to depict an authenticated login.	295 × 55 pixels
Background	Displays in the page background.	10 × 800 pixels

Images will be resized to fit the specified dimensions. For best results, the logo and account images should be similar in proportion to the default images.

All images must be 5 kilobytes or smaller and must be in GIF or JPG format.

STEP 2 Click **Captive Portal** > **Upload Binary Files** in the navigation window.

STEP 3 Click **Browse** next to **Upload Web Customization Image** to select the file from your computer or network.

STEP 4 Click **Upload**.

STEP 5 Go to the *Web Customization* page to apply an uploaded graphic to a CP web page.

NOTE: To delete an image, select it from the **Delete Web Customization Image** list and click **Delete**.

Web Customization

When users initiate access to a VAP that is associated to a captive portal instance, an authentication page displays. You can use the *Web Customization* page to create unique pages for different locales on your network, and to customize the textual and graphic elements of the pages.

To create and customize a CP authentication page:

STEP 1 Click **Captive Portal** > **Web Customization** in the navigation window.

STEP 2 Select **Create** from the **Captive Portal Web Locale** list.

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

STEP 3 Enter a **Web Locale Name** to assign to the page. The name can be from 1 to 32 alphanumeric characters.

STEP 4 From the **Captive Portal Instances** list, select the CP instance that this locale is associated with.

You can associate multiple locales with an instance. When a user attempts to access a particular VAP that is associated with a CP instance, the locales that are associated with that instance display as links on the authentication page. The user can select a link to switch to that locale.

STEP 5 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

STEP 6 From the **Captive Portal Web Locale** list, select the locale you created.

The page displays additional fields for modifying the locale. The **Locale ID** and **Instance Name** fields cannot be edited. The editable fields are populated with default values.

STEP 7 Configure the parameters:

- **Background Image Name**—The image to display as the page background. If you uploaded a custom background image to the WAP device, you can select it from the list.
- **Logo Image Name**—The image file to display on the top left corner of the page. This image is used for branding purposes, such as the company logo. If you uploaded a custom logo image to the WAP device, you can select it from the list.

- **Foreground color**—The HTML code for the foreground color in 6-digit hexadecimal format. The range is from 1 to 32 characters. The default is #999999.
- **Background color**—The HTML code for the background color in 6-digit hexadecimal format. The range is from 1 to 32 characters. The default is #BFBFBF.
- **Separator**—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 #BFBFBF. The default is #BFBFBF.
- **Locale Label**—A descriptive label for the locale, from 1 to 32 characters. The default is *English*.
- **Locale**—An abbreviation for the locale, from 1 to 32 characters. The default is *en*.
- **Account Image**—The image file to display above the login field to depict an authenticated login.
- **Account Label**—The text that instructs the user to enter a user name. The range is from 0 to 32 characters.
- **User Label**—The label for the user name text box. The range is from 0 to 32 characters.
- **Password Label**—The label for the user password text box. The range is from 0 to 64 characters.
- **Button Label**—The label on the button users click to submit their user name/password for authentication. The range is from 2 to 32 characters. The default is Connect.
- **Fonts**—The name of the font to use for all text on the CP page. You can enter multiple font names, each separated by a comma. If the first font is not available on the client system, the next font will be used, and so on. For font names that have spaces, surround the entire name in quotes. The range is from 1 to 512 characters. The default is MS UI Gothic, arial, sans-serif.
- **Browser Title**—The text to display in the browser title bar. The range is from 1 to 128 characters. The default is Captive Portal.
- **Browser Content**—The text that displays 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.

- **Content**—The instructive text that displays in the page body below the user name and password text boxes. The range is from 0 to 256 characters. The default is: To start using this service, enter your credentials and click the connect button.
- **Acceptance Use Policy**—The text that appears in the Acceptance Use Policy box. The range is from 0 to 8192 characters. The default is: Acceptance Use Policy.
- **Accept Label**—The text that instructs users to select the check box to acknowledge reading and accepting the Acceptance Use Policy. The range is from 0 to 128 characters. The default is: Check here to indicate that you have read and accepted the Acceptance Use Policy.
- **No Accept Text**—The text that displays 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. The default is: Error: You must acknowledge the Acceptance Use Policy before connecting!
- **Work In Progress Text**—The text that displays during authentication. The range is from 1 to 128 characters. The default is: Connecting, please be patient....
- **Denied Text**—The text that displays when a user fails authentication. The range is from 1 to 128 characters. The default is: Error: Invalid Credentials, please try again!
- **Resource Text**—The text that displays when the authenticator is unavailable. The range is from 1 to 128 characters. The default is: Error: Limited Resources, please reconnect and try again later.
- **Timeout Text**—The text that displays when the authenticator has not replied in the configured time frame. The range is from 1 to 128 characters. The default is: Error: Timed Out, please reconnect and try again!
- **Welcome Title**—The text that displays when the client has authenticated to the VAP. The range is from 1 to 128 characters. The default is: Congratulations!
- **Welcome Content**—The text that displays when the client has connected to the network. The range is from 0 to 256 characters. The default is: You are now authorized and connected to the network.
- **Delete Locale**—Deletes the current locale.

STEP 8 Click **Save**. Your changes are saved to the Running Configuration and the Startup Configuration.

You can use the *Web Customization Preview* page view the updated page.

Web Customization Preview

Use the *Web Customization Preview* page to view a locale page that you have modified.

To preview a customized page:

STEP 1 Click **Captive Portal** > **Web Customization Preview** in the navigation window.

STEP 2 Select the locale you want to preview from the **Captive Portal Web Locale** list.

The page for the locale displays in the Captive Portal Web Locale Parameters Preview area.

Local Groups

Each local user is assigned to a user group. Each 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. You can create up to two additional user groups.

To add local user groups:

STEP 1 Click **Captive Portal** > **Local Groups** in the navigation window.

STEP 2 Enter a **Group Name** and click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

NOTE: To delete a group, select it in the **Captive Portal Groups** list, select the **Delete Group** check box, and click **Save**.

Local Users

You can configure a captive portal instance to accommodate either guest users and authorized users. Guest users do not have assigned user names and passwords.

Authorized users provide a valid user name and password that must first be validated against a local database or RADIUS server. Authorized users are typically assigned to a CP instance that is associated with a different VAP than guest users.

You can use the *Local Users* page to configure up to 128 authorized users in the local database.

To add and configure a local user:

STEP 1 Click **Captive Portal** > **Local Users** in the navigation window.

STEP 2 Enter a **User Name** and click **Save**.

The page displays additional fields for configuring the user.

STEP 3 Enter the parameters:

- **User Password**—Enter the user's password, from 8 to 64 alphanumeric and special characters. A user enter must enter the password to log into the network through the Captive Portal.
- **Away Timeout**—The period of time after which the user is logged out if there is no activity. The range is from 1 to 1440 minutes. The default is 0.
- **Group Name**—The assigned user group. Each CP instance is configured to support a particular group of users.
- **Maximum Bandwidth Up**—The maximum upload speed, in megabits per second, that a client can transmit traffic when using the captive portal. This setting limits the client's bandwidth used to send data into the network. The range is from 0 to 300 Mbps. The default is 0.
- **Maximum Bandwidth Down**—The maximum download speed, in megabits per second, that a client can receive traffic when using the captive portal. This setting limits the client's bandwidth used to receive data from the network. The range is from 0 to 300 Mbps. The default is 0.
- **Delete User**—Deletes the current user.

STEP 4 Click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

Authenticated Clients

The *Authenticated Clients* page provides information about clients that have authenticated on any Captive Portal instance.

To view the list of authenticated clients, click **Captive Portal** > **Authenticated Clients** in the navigation window.

These fields display:

- **MAC Address**—The MAC address of the client.
- **IP Address**—The IP address of the client.
- **User Name**—The client's Captive Portal user name.
- **Protocol**—The protocol 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 authenticated users.
  - **RADIUS**—The WAP device uses a database on a remote RADIUS server to authenticate users.
- **VAP ID**—The VAP that the user is associated with.
- **Radio ID**—The ID of the radio. Because the WAP321 has a single radio, this field always displays Radio1.
- **Captive Portal ID**—The ID of the Captive Portal instance to which the user is associated.
- **Session Timeout**—The time that has elapsed since the user authenticated on Captive Portal.
- **Away Timeout**—The time that has elapsed since the last user activity.

- **Initial URL Request**—The URL that the user initially attempted to access.
- **Received Packets**—The number of IP packets received by the WAP device from the user station.
- **Transmitted Packets**—The number of IP packets transmitted from the WAP device to the user station.
- **Received Bytes**—The number of bytes received by the WAP device from the user station.
- **Transmitted Bytes**—The number of bytes transmitted from the WAP device to the user station.

You can click **Refresh** to show the latest data from the WAP device.

Failed Authentication Clients

The *Failed Authenticated Clients* page lists information about clients that attempted to authenticate on a Captive Portal and failed.

To view a list of clients who failed authentication, click **Captive Portal** > **Failed Authentication Clients** in the navigation window.

These fields display:

- **MAC Address**—The MAC address of the client.
- **IP Address**—The IP address of the client.
- **User Name**—The client's Captive Portal user name.
- **Verification**—The method the client attempted to use to authenticate 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 authenticated users.
  - **RADIUS**—The WAP device uses a database on a remote RADIUS server to authenticate users.
- **VAP ID**—The VAP that the user is associated with.
- **Radio ID**—The ID of the radio. Because the WAP321 has a single radio, this field always displays Radio1.

- **Captive Portal ID**—The ID of the Captive Portal instance to which the user is associated.
- **Failure Time**—The time that the authentication failure occurred. A timestamp is included that shows the time of the failure.

You can click **Refresh** to show the latest data from the WAP device.

A

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the Cisco WAP121 and WAP321 Access Point.

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Cisco Small Business Firmware Downloads	www.cisco.com/go/smallbizfirmware Select a link to download firmware for Cisco Small Business Products. No login is required. Downloads for all other Cisco Small Business products, including Network Storage Systems, are available in the Download area on Cisco.com at www.cisco.com/go/software (registration/login required).
Cisco Small Business Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Product Documentation	
Cisco Small Business WAP121 and WAP321 Wireless-N Access Point with PoE Quick Start Guide and Administration Guide	http://www.cisco.com/go/100_wap_resources or http://www.cisco.com/go/300_wap_resources

Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb