283935

ADMINISTRATION GUIDE

Cisco Small Business

WAP121 Wireless-N Access Point with PoE

and

WAP321 Wireless-N Selectable-Band Access Point with PoE

78-20373-02

Contents

1

Getting Started

This chapter provides an introduction to the Wireless Access Point (WAP) devices web-based configuration utility, and includes these topics:

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 Domain Name System (DNS) 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. Select **Tools > Internet Options** and then select the **Security** tab. Select **Local Intranet** and select **Sites**. Select **Advanced** and then select **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 configuration utility:

STEP 1 Open a web browser.

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, go to cisco.com and enter www.cisco.com/go/findit.
- For further instructions on how to locate the IP address of your WAP device, see the WAP device Quick Start Guide.

STEP 2 Enter the user name and password. The factory default user name is **cisco** and the default password is **cisco**.

STEP 3 Click **Log In**. The Access Point Setup 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** for instructions on using the wizard.

Logging Out

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

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

Using the Access Point Setup Wizard

The first time that you log into the WAP device (or after it has been reset to the factory default settings), the Access Point Setup Wizard appears 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 appears. You can then change the default password for logging in. For all other settings, the factory default configurations apply.

You must log in again after changing your password.

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

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 **VLAN and IPv4 Address Settings**.

STEP 3 Click **Next**. The Single Point Setup — Set a Cluster window appears. For a description of Single Point Setup, see **Single Point Setup**.

STEP 4 To create a new Single Point Setup of WAP devices, select **Create a New Cluster** and specify a **New Cluster Name**. When you configure your devices with the same cluster name and enable Single Point Setup mode on other WAP devices, they automatically join the group.

If you already have a cluster on your network, you can add this device to it by clicking **Join an Existing Cluster**, and then entering the **Existing Cluster Name**.

If you do not want this device to participate in a Single Point Setup at this time, click **Do not Enable Single Point Setup**.

(Optional) You can enter text in the AP Location field to note the physical location of the WAP device.

STEP 5 Click **Next**. The Configure Device - Set System Date and Time window appears.

STEP 6 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**.

STEP 7 Click **Next**. The Enable Security - Set Password window appears.

STEP 8 Enter a **New Password** and enter it again in the **Confirm Password** text box. For more information about passwords, see **User Accounts**.

NOTE You can uncheck the Password Complexity box if you wish to disable the password security rules. However, we strongly recommend keeping the password security rules enabled.

STEP 9 Click **Next**. The Enable Security - Name Your Wireless Network window appears.

STEP 10 Enter a **Network Name**. This name serves as the SSID for the default wireless network.

STEP 11 Click **Next**. The Enable Security - Secure Your Wireless Network window appears.

STEP 12 Choose a security encryption type and enter a security key. For a description of these options, see **System Security**.

STEP 13 Click **Next**. The Wizard displays the Enable Security- Assign the VLAN ID For Your Wireless Network window.

STEP 14 Enter a VLAN ID for traffic received on the wireless network.

It is suggested that you assign a different VLAN ID from the default (1) to wireless traffic, in order to segregate it from management traffic on VLAN 1.

STEP 15 Click **Next**.

For the WAP121 device, the Wizard displays the Summary - Confirm Your Settings window. Skip to **STEP 24**.

For the WAP321 device, the Wizard displays the Enable Captive Portal - Create Your Guest Network window.

STEP 16 Select whether or not to set up an authentication method for guests on your network (WAP321 only), and click **Next**.

If you click **No**, skip to **STEP 24**.

If you click **Yes**, the Wizard displays the Enable Captive Portal - Name Your Guest Network window.

STEP 17 Specify a **Guest Network Name**.

STEP 18 Click **Next**. The Wizard displays the Enable Captive Portal - Secure Your Guest Network window.

STEP 19 Choose a security encryption type for the guest network and enter a security key. For a description of these options, see **System Security**.

STEP 20 Click **Next**. The Wizard displays the Enable Captive Portal - Assign the VLAN ID window.

STEP 21 Specify a VLAN ID for the guest network. The guest network VLAN ID should be different from the management VLAN ID.

STEP 22 Click **Next**. The Wizard displays the Enable Captive Portal - Enable Redirect URL window.

STEP 23 Select **Enable Redirect URL** and specify a fully qualified domain name or IP address in the Redirect URL field (including http://). If specified, guest network users are redirected to the specified URL after authenticating.

STEP 24 Click **Next**. The Wizard displays the Summary - Confirm Your Settings window.

STEP 25 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 26 If they are correct, click **Submit**. Your WAP setup settings are saved and a confirmation window appears.

STEP 27 Click **Finish**. The Getting Started window appears.

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 configuration utility.

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
	Run WPS	WPS Setup
	Configure Single Point Setup	Single Point Setup
Device Status	System Summary	System Summary
	Wireless Status	Network Interfaces
Quick Access	Change Account Password	User Accounts
	Upgrade Device Firmware	Upgrade Firmware
	Backup/Restore Configuration	Download/Backup Configuration File
Other Resources	Support	A link to the Cisco WAP support site.
	Forums	A link to the Cisco Support Community site.
	Wireless Planning Tool	A link to Fluke networks AirMagnet Planner for Cisco Small Business.

Window Navigation

This section describes the features of the configuration utility.

Configuration Utility Header

The Configuration Utility header contains standard information and appears 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 configuration utility.
About	Click to show the WAP device type and version number.
Help	Click to show the online help. The online help is designed to be viewed with browsers using UTF-8 encoding. If the online help shows errant characters, verify that the encoding settings on your browser are set to UTF-8.

Navigation Pane

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

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 startup configuration.

2

Status and Statistics

This chapter describes how to display status and statistics and contains these topics:

- System Summary
- Network Interfaces
- Traffic Statistics
- WorkGroup Bridge Transmit/Receive
- Associated Clients
- TSPEC Client Associations
- TSPEC Status and Statistics
- TSPEC AP Statistics
- Radio Statistics
- Email Alert Status
- Log

System Summary

The System Summary page shows basic information such as the hardware model description, software version, and the time that has elapsed since the last reboot.

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

The System Summary page shows this information:

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

- **Serial Number**—The serial number of the Cisco WAP device.
- **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.
- **Power Source**—The system may be powered by a power adapter, or may be receiving power-over-Ethernet from PoE power-sourcing equipment (PSE).

The TCP/UDP Service table shows 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 appear 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 the role of each device 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 show the most current information.

Network Interfaces

Use the Network Interfaces page to show configuration and status information about the wired and wireless interfaces. To show the Network Interfaces page, select **Status and Statistics** > **Network Interface** in the navigation pane.

The Network Interfaces page shows this information:

- **LAN Status**—These settings apply to the internal interface. For the WAP321, the information indicates whether or not Green Ethernet mode is enabled.

  To change any of these settings, click the **Edit** link. After you click Edit, you are redirected to the VLAN and IPv4 Address Settings page. See **VLAN and IPv4 Address Settings** for descriptions of these fields.

- **Radio Status**—These settings include the Wireless Radio mode (Enabled or Disabled), the MAC address associated with the 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** for descriptions of these fields.

- **Interface Status**—This table lists status information for each Virtual Access Point (VAP) and on each Wireless Distribution System (WDS) interface.

  If the VAP has been configured, the table lists the SSID, the administrative status (up or down), the MAC address of the radio interface, the VLAN ID, the name of any associated scheduler profile, and the current state (active or inactive). The state indicates whether the VAP is exchanging data with a client.

You can click **Refresh** to refresh the screen and show 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, the Virtual Access Points (VAPs), and any WDS 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 show the Traffic Statistics page, select **Status and Statistics** > **Traffic Statistics** in the navigation pane.

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

- **Network Interface**—Name of the Ethernet interface and each VAP and WDS interface.

  Each VAP interface name is followed by its SSID in parentheses.
- **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 show the most current information.

WorkGroup Bridge Transmit/Receive

The WorkGroup Bridge Transmit/Receive page shows packet and byte counts for traffic between stations on a WorkGroup Bridge. For information on configuring WorkGroup Bridges, see **WorkGroup Bridge**.

To show the WorkGroup Bridge Transmit/Receive page, select **Status and Statistics** > **WorkGroup Bridge** in the navigation pane.

Each network interface that is configured as a WorkGroup Bridge interface shows these fields:

- **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**.
- **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**.

Additional information appears 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 show 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 show the Associated Clients page, select **Status and Statistics** > **Associated Clients** in the navigation pane.

The associated stations are shown 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.
- **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 appears as expected; that is, if a client shows as authenticated to the WAP device, it is able to transmit and receive data. (The reason why is that 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 appear as authenticated (through IEEE 802.11 security) although it is not actually authenticated through the second layer of security.

- **From Station/To Station**—For the From Station, the counters indicate the packets or bytes received by the wireless client. For the To Station, the 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 show the most current information.

TSPEC Client Associations

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

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, select **Status and Statistics > TSPEC Client Associations** in the navigation pane.

The TSPEC Client Associations page shows this information:

Status and Statistics:

- **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 to 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 Interface**—Radio interface used by the client.
- **Station**—Client station MAC address.
- **TS Identifier**—TSPEC Traffic Session Identifier (range 0 to 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.
  - **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.
  - **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 show 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, select **Status and Statistics > TSPEC Status and Statistics** in the navigation pane.

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 Status 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 appear 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 appear 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 show 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 the TSPEC AP Statistics page, select **Status and Statistics > TSPEC AP Statistics** in the navigation pane.

- **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 show the most current information.

Radio Statistics

You can use the Radio Statistics page to show packet-level and byte-level statistics for the wireless radio interface. To view the Radio Statistics page, select **Status and Statistics > Radio Statistics** in the navigation pane.

- **Packets Received**—Total packets received by the WAP device.
- **Packets Transmitted**—Total packets transmitted by the WAP device.
- **Bytes Received**—Total bytes received 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.
- **Packets Transmit Dropped**—Number of packets transmitted by the WAP device that were dropped.
- **Bytes Receive Dropped**—Number of bytes received 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 was set in the destination MAC address.
- **Duplicate Frame Count**—Number of times a frame was received and the Sequence Control field indicates it was a duplicate.
- **Failed Transmit Count**—Number of times an MSDU was not transmitted successfully due to transmit attempts exceeding either the short retry limit or the long retry limit.

- **FCS Error Count**—Count of FCS errors detected in a received MPDU frame.
- **Transmit Retry Count**—Number of times an MSDU is successfully transmitted after one or more retries.
- **ACK Failure Count**—Count of ACK frames not received when expected.
- **RTS Failure Count**—Count of CTS frames not received in response to an RTS frame.
- **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.
- **RTS Success Count**—Count of CTS frames received in response to an RTS frame.
- **Multiple Retry Count**—Number of times an MSDU is successfully transmitted after more than one retry.
- **Frames Transmitted Count**—Count of each successfully transmitted MSDU.

You can click **Refresh** to refresh the screen and show 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 the Email Alert Status page, select **Status and Statistics > Email Alert Status** in the navigation pane.

- **Email Alert Status**—The Email Alert configured status. The status is either Enabled or Disabled. The default is Disabled.
- **Number of Emails Sent**—The total number of emails sent. The range is an unsigned integer of 32 bits. The default is 0.
- **Number of Emails 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 shows 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 shown. Older entries are removed from the list as needed to make room for new events.

To view the Log page, select **Status and Statistics > Log Status** in the navigation pane.

- **Time Stamp**—The system time when the event occurred.
- **Severity**—Whether the event is 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 show 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 topics:

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

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 Select **Administration** > **System Settings** in the navigation pane.

STEP 2 Enter the parameters:

- **Host Name**—Administratively assigned name for the WAP device. By convention, the name 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 can 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. The Host Name can be 1 to 63 characters long.
- **System Contact**—A contact person for the WAP device. The System Contact can be 0 to 255 characters long and can include spaces and special characters.
- **System Location**—Description of the physical location of the WAP device. The System Location can be 0 to 255 characters long and can include spaces and special characters.

STEP 3 Click **Save**. The changes are saved to 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 to configure up to four additional users and to change a user password.

Adding a User

To add a new user:

STEP 1 Select **Administration** > **User Accounts** in the navigation pane.

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

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

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

STEP 3 Check the box for the new user and select **Edit**.

STEP 4 Enter a **User Name** between 1 to 32 alphanumeric characters. Only numbers 0 to 9 and letters a to 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 Startup Configuration.

NOTE To delete a user, select the check box next to the user name and select **Delete**. To save your deletion permanently, select **Save** when complete.

Changing a User Password

To change a user password:

STEP 1 Select **Administration** > **User Accounts** in the navigation pane.

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

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

STEP 3 Enter a **New Password** between 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 Startup Configuration.

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

Time Settings

A system clock provides 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 device is configured to obtain its time from a predefined list of NTP servers.

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

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/IPv4/IPv6 Address Name**—Specify the IPv4 address, IPv6 address, or hostname of an NTP server. A default NTP server is listed.

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

- **Time Zone**—Select the time zone for your location.

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

- **Daylight Savings End**—Select the 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 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 (nonvolatile) memory and degrade network performance. Only enable persistent logging to debug a problem. Make sure that you disable persistent logging after you finish debugging the problem.

To configure persistent logging:

STEP 1 Select **Administration** > **Log Settings** in the navigation pane.

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. You can save up to 128 log messages in the nonvolatile memory. When the limit of 128 is reached, the oldest log message is overwritten by the newest message. Clear this field to save system logs to volatile memory. Logs in volatile memory are deleted when the system reboots.

- **Severity**—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 to 7 are written to volatile memory.
- **Depth**—The maximum number of messages, up to 512, that can be stored in volatile memory. When the number you configure in this field is reached, the oldest log event is overwritten by the newest log event. Note that the maximum number of log messages that can be stored in nonvolatile memory (the persistent log) is 128, which is not configurable.

STEP 3 Click **Save**. The changes are saved to 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 set up 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 Select **Administration** > **Log Settings** in the navigation pane.

STEP 2 Configure the parameters:

- **Remote Log**—Enables the WAP device to send log messages to a remote host. When disabled, all log messages are kept on the local system.
- **Server IPv4/IPv6 Address/Name**—The IPv4 or IPv6 address, or the hostname of the remote log server.

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

- **UDP Port**—The logical port number for the syslog process on the remote host. The range is from 1 to 65535. The default port is 514.

  Using the default port is recommended. If you 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 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 a loss of connectivity 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.

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

To configure the WAP device to send email alerts:

STEP 1 Select **Administration** > **Email Alert** in the navigation pane.

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

- **Administrative Mode**—Choose to enable the email alert feature globally.
- **From Email Address**—Enter the address to show as the sender of the email. The address is a 255 character string with only printable characters. No address is configured by default.
- **Log Duration**—Choose the frequency at which scheduled messages are 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 to the configuration email address at the frequency specified by the Log Duration. Select from these values: None, Emergency, Alert, Critical, Error, Warning, Notice, Info, and Debug. If set to None, then no scheduled severity messages are sent. The default severity is Warning.
- **Urgent Message Severity**—Log messages of this severity level or higher are sent to the configured email address immediately. Select from these values: None, Emergency, Alert, Critical, Error, Warning, Notice, Info, and 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**—Enter the IP address or hostname of the outgoing SMTP server. (You can check with your email provider for the hostname.) 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).

  A hostname can consist of one or more labels, which are sets of up to 63 alphanumeric characters. If a hostname includes multiple labels, each is separated by a period (.). The entire series of labels and periods can be up to 253 characters long.
- **Data Encryption**—Enter the mode of security for the outbound email alert. The alert can be sent using secure TLS protocol or the default Open protocol. Using secure TLSv1 protocol can prevent eavesdropping and tampering during the communication across the public network.
- **Port**—Enter the SMTP port number to use for outbound emails. The range is a valid port number from 0 to 65535. The default port is 465. The port generally depends on the mode used by the email provider.

- **Username**—Enter the username for the email account that will be used to send these emails. Typically (but not always) the username is the full email address including the domain (such as Name@example.com). The specified account will be used as the email address of the sender. The username can be from 1 to 64 alphanumeric characters.
- **Password**—Enter the password for the email account that will be used to send these emails. The password can be from 1 to 64 characters.

STEP 4 Configure the email addresses and subject line.

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

STEP 5 Click **Test Mail** to send a test email to validate the configured email account.

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

Email Alert Examples

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

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

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

Yahoo! Mail
Yahoo requires using a paid account for this type of service. Yahoo
recommends the following settings:
Data Encryption: TLSv1
SMTP Server: plus.smtp.mail.yahoo.com
```

```
SMTP Port: 465 or 587
Username: Your email address, without the domain name such as myName (without
@yahoo.com)
Password: Your Yahoo account password
```

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

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

TIME           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 is used for secure management sessions, you also use the HTTP/HTTPS Service page to manage the required SSL certificates.

Configuring HTTP and HTTPS Services

To configure HTTP and HTTP services:

STEP 1 Select **Administration** > **HTTP/HTTPS Service** in the navigation pane.

STEP 2 Configure these Global Settings:

- **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 configuration utility, a session is created. This session is maintained until the user logs off or the Session Timeout expires. The range is from 1 to 10 sessions. The default is 5. If the maximum number of sessions 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:

- **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.
- **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.
- **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 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 device has acquired an IP address to ensure that the common name for the certificate matches the IP address of the WAP device. Generating a new SSL certificate restarts the secure web server. The secure connection does not work until the new certificate is accepted on the browser.

In the Certificate File Status area, you can view whether a certificate currently exists on the WAP device, and view 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 are 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 appear to enable you to enter the File Name to assign to the downloaded file, and enter 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) area, 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**. The filename cannot contain the following characters: spaces, <, >, |, \, : , (,), &, ; , #, ? , *, and two or more successive periods.

A confirmation appears when the upload was successful.

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 configuration utility. If this feature is disabled, anyone can access the configuration utility from any network client by supplying the correct WAP device username and password.

If the management ACL is enabled, access through the web 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 does not change over time.

To create an access list:

STEP 1 Select **Administration** > **Management Access Control** in the navigation pane.

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

STEP 3 Enter up to five IPv4 and five IPv6 addresses that will be allowed access.

STEP 4 Verify the IP addresses are correct.

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

Upgrade Firmware

As new versions of the WAP device firmware become available, you can upgrade the firmware on your devices to take advantage of new features and enhancements. The WAP device 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 Select **Administration** > **Update Firmware** in the navigation pane.

The Product ID (PID) and active and inactive firmware versions appear.

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 do not work.

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

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 is aborted. When the process is complete the access point restarts and resumes 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 do 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 is aborted. When the process is complete, the access point restarts and resumes normal operation.

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

Firmware Recovery

The WAP device has a firmware recovery feature that enables the restoration of a valid image on the WAP device after a failed download. If the power goes down during an image download, the WAP device might not be able to boot. In this event, although the image is not usable, the boot loader file that loads the firmware image from flash memory to RAM should continue to be functional. An HTTP server is embedded in the boot loader file, enabling the administrator to connect to the WAP device over the LAN port and use a web browser to download and install a new firmware image.

The WAP device enters the HTTP firmware recovery mode when it is booted and the boot loader cannot find a valid image in flash memory. In this mode, the boot loader sets the internal network port to the following static IP address:

- IP Address: 192.168.1.254
- Network Mask: 255.255.255.0
- Default Gateway: 192.168.1.1

An HTTP server starts and listens for client connections on port 80.

NOTE The Firmware Recovery page is shown in the web-based configuration utility only when an image needs to be restored.

To use this feature to download a new firmware image:

STEP 1 Directly connect a PC to the LAN port.

STEP 2 Configure the IP address and mask on the management PC to be in the same subnet as the switch.

NOTE You can access the system across a network if the default gateway IP address is 192.168.1.1.

STEP 3 Open a web browser and enter the IP address of the switch in the address bar (192.168.1.254).

NOTE The HTTP firmware recovery features support the following browsers:

- Firefox 3.0 and later versions
- Internet Explorer 6 and later versions

A Firmware Recovery page appears. No authentication is required.

The web page shows the PIC VID (product ID and vendor ID), serial number, and MAC address of the WAP device.

STEP 4 Select **Browse** and select a valid firmware image to download.

A progress bar appears while the file is downloading. The following message appears upon a successful download:

100% Complete
File downloaded successfully. Please wait while the file is being written to flash. System will automatically reboot.

The file selected by administrator is downloaded to RAM and is validated for the following conditions:

- The CRC of the file is good.
- The STK file is built for this platform.
- The STK file size is within the partition limits (4.5 MB is reserved for this file).

If these conditions are met, the file is written to flash memory and the system is rebooted using the new firmware.

If any of these checks fail, the image is not written to flash memory and the recovery process is stopped. You can restart the recovery process with a correct image file.

If the transfer is aborted because the browser window is refreshed or closed, the session is cleared and the session times out immediately. If the transfer is aborted because the network is unreachable, the session times out after 45 seconds. After the session times out, you can begin the recovery process again.

Download/Backup Configuration File

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

The WAP device maintains these configuration files:

- **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 Startup Configuration is not modified for at least 24 hours, it is automatically saved to a Mirror Configuration file. The Mirror Configuration file is a snapshot of a past Startup Configuration. The Mirror Configuration is preserved across factory resets, so it can be used to recover a system configuration after a factory reset by copying the Mirror Configuration to the Startup Configuration.

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**.

Backing Up a Configuration File

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

STEP 1 Select **Administration** > **Download/Backup Configuration File** in the navigation pane.

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 and then enter the **TFTP Server IPv4 Address**.

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

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

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

- **Startup Configuration**—Configuration file type used when the WAP device last booted. This does not include any configuration changes applied but not yet saved to the WAP device.
- **Backup Configuration**—Backup configuration file type saved on the WAP device.
- **Mirror Configuration**—If the Startup Configuration is not modified for at least 24 hours, it is automatically saved to a Mirror Configuration file. The Mirror Configuration file is a snapshot of a past Startup Configuration. The Mirror Configuration is preserved across factory resets, so it can be used to recover a system configuration after a factory reset by copying the Mirror Configuration to the Startup Configuration.

STEP 7 Click **Save** to begin the backup. For HTTP backups, a window appears 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 device to update the configuration or to restore the WAP device to a previously backed-up configuration.

To download a configuration file to the WAP device:

STEP 1 Select **Administration** > **Download/Backup Configuration File** in the navigation pane.

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**.

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

STEP 5 Select which configuration file on the WAP device that you want replaced 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 takes effect the next time the WAP device reboots.

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

CAUTION Ensure that power to the WAP device remains uninterrupted while the configuration file is downloading. If a power failure occurs while downloading the configuration file, the file is lost and the process must be restarted.

Configuration Files Properties

The Configuration Files Properties page enables you to clear the Startup or Backup Configuration file. If you clear the Startup Configuration file, the Backup Configuration file becomes active the next time that you reboot the WAP device.

To delete the Startup Configuration or Backup Configuration file:

STEP 1 Select **Administration** > **Configuration Files Properties** in the navigation pane.

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

STEP 3 Click **Clear Files**.

Copy/Save Configuration

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

To copy a file to another file type:

STEP 1 Select **Administration** > **Copy/Save Configuration** in the navigation pane.

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

- **Startup Configuration**—Configuration file type used when the WAP device last booted. This does not include any configuration changes applied but not yet saved to the WAP device.
- **Backup Configuration**—Backup configuration file type saved on the WAP device.
- **Mirror Configuration**—If the Startup Configuration is not modified for at least 24 hours, it is automatically saved to a Mirror Configuration file. The Mirror Configuration file is a snapshot of a past Startup Configuration. The Mirror Configuration is preserved across factory resets, so it can be used to recover a system configuration after a factory reset by copying the Mirror Configuration to the Startup Configuration.

STEP 3 For the **Destination File Name**, select the file type to be replaced with the file you are copying.

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

When complete, a window shows the message, Copy Operation Successful.

Reboot

You can use the Reboot page reboot the WAP device.

STEP 1 To reboot the WAP, select **Administration** > **Reboot** in the navigation pane.

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

The WAP device advertises these service types:

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

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

A system administrator can use an installed Internet 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 Select **Administration** > **Discovery - Bonjour** in the navigation pane.

STEP 2 Select **Enable**.

STEP 3 Click **Save**. The 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. There are two methods of packet capture:

- Local capture method— Captured packets are stored in a file on the WAP device. The WAP device can transfer the file to a TFTP server. The file is

formatted in pcap format and can be examined using 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 show the Packet Capture page. From the Packet Capture 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 nonpromiscuous 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**—Specifies the MAC address for WLAN client filtering.

  NOTE The MAC filter is active only when a 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 the Local Packet Capture or Remote Packet Capture section 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 restarted.

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**—Enter a capture interface type for packet capture:
  - **radio1**—802.11 traffic on the radio interface.
  - **eth0**—802.3 traffic on the Ethernet port.
  - **VAP0**—VAP0 traffic.
  - **VAP1** to **VAP15**, if configured—Traffic on the specified VAP.

- **brtrunk**—Linux bridge interface in the WAP device.

- **Capture Duration**—Enter the time duration in seconds for the capture. The range is from 10 to 3600. The default is 60.
- **Max Capture File Size**—Enter the maximum allowed size for the capture file in KB. The range is from 64 to 4096. The default is 1024.

STEP 3 Click **Save**. The changes are saved to 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.

- **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 show 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. 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, the traffic for these ports must be allowed to pass through the firewall. The firewall must also be configured to allow the Wireshark computer to initiate a 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 For the **Packet Capture Method**, select **Remote**.

STEP 4 For the **Remote Capture Port**, 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. The port range is from 1025 to 65530.

STEP 5 If you want to save the settings for use at another time, click **Save**. (The selection of **Remote** as the **Packet Capture Method** is not saved, however.)

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 popup window appears.

STEP 3 At **Interface**, select **Remote**. A popup window 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 Select the interface from which you need to capture packets. At the Wireshark popup window, next to the IP address, there is a pull-down 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 WAP321, 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 number greater than 1024.

When you are capturing traffic on the radio interface, you can disable beacon capture, but other 802.11 control frames are still sent to Wireshark. You can set up a display filter to show only:

- Data frames in the trace
- Traffic on specific Basic Service Set IDs (BSSIDs)
- Traffic between two clients

Some examples of useful display filters are:

- Exclude beacons and ACK/RTS/CTS frames:

  !(wlan.fc.type_subtype == 8 || wlan.fc.type == 1)

- Data frames only:

  wlan.fc.type == 2

- Traffic on a specific BSSID:

  wlan.bssid == 00:02:bc:00:17:d0

- All traffic to and from a specific client:

  wlan.addr == 00:00:e8:4e:5f:8e

In remote capture mode, traffic is sent to the computer running Wireshark through one of the network interfaces. Depending on the location of the Wireshark tool, the traffic can be sent on an Ethernet interface or one of the radios. To avoid a traffic flood caused by tracing the packets, the WAP device automatically installs a capture filter to filter out all packets destined to the Wireshark application. For example, if the Wireshark IP port is configured to be 58000, then this capture filter is automatically installed on the WAP device:

not portrange 58000-58004

Due to performance and security issues, the packet capture mode is not saved in NVRAM on the WAP device; if the WAP device resets, the capture mode is disabled and then you must reenable it to resume capturing traffic. Packet capture parameters (other than mode) are saved in NVRAM.

Enabling the packet capture feature can create a security issue: Unauthorized clients may be able to connect to the WAP device and trace user data. The performance of the WAP device also is negatively impacted during packet capture, and this impact continues to a lesser extent even when there is no active Wireshark session. To minimize the performance impact on the WAP device during traffic capture, install capture filters to limit which traffic is sent to the Wireshark tool. When capturing 802.11 traffic, a large portion of the captured frames tends 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. To reduce the performance impact of capturing the 802.11 beacons, disable the capture beacons mode.

Packet Capture File Download

You can download a capture file by TFTP to a configured TFTP server, or by HTTP(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 appears.

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

Support Information

The Support Information page enables you to download a text file that contains detailed configuration information about the AP. The file includes software and hardware version information, MAC and IP addresses, the administrative and operational status of features, user-configured settings, traffic statistics, and more. You can provide the text file to technical support personnel to assist them in troubleshooting problems.

To show the Support Information page, select **Administration > Support Information** in the navigation pane.

Click **Download** to generate the file based on current system settings. After a short pause, a window appears to enable you to save the file to your computer.

4

LAN

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

It includes these topics:

- **Port Settings**
- **VLAN and IPv4 Address Settings**
- **IPv6 Addresses**

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 Select **LAN** > **Port Settings** in the navigation area.

The Operational Status area shows the type of port used for the LAN port and the Link characteristics, as configured in the Administrative Settings area. If the settings change through configuration or auto negotiation, you can click **Refresh** to show the latest settings.

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

- When enabled, the port negotiates with its link partner to set the fastest link speed and duplex mode available.
- When disabled, you can manually configure the port speed and duplex mode.

STEP 3 If autonegotiation is disabled, select a **Port Speed** (10/100 Mb/s for the WAP121, and 10/100/1000 Mb/s for the WAP321) and the duplex mode (Half- or Full-duplex).

STEP 4 Enable or disable **Green Ethernet Mode** (WAP321 only).

- 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 changes are saved to the Startup Configuration.

VLAN and IPv4 Address Settings

You can use the VLAN and IPv4 Address Settings page to configure settings for the LAN interface, including static or dynamic IPv4 address assignment.

To configure LAN settings:

STEP 1 Select **LAN** > **VLAN and IPv4 Address** in the navigation area.

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

STEP 2 Configure these Global Settings:

- **Untagged VLAN**—Enables or disables VLAN tagging. When enabled (the default), all traffic is tagged with a VLAN ID.

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

- **Untagged VLAN ID**—Specifies a number between 1 and 4094 for the untagged VLAN ID. The default is 1. Traffic on the VLAN that you specify in this field is not be tagged with a VLAN ID when forwarded to the network.

  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, and then use this new VLAN ID on your WAP device.

- **Management VLAN ID**—The VLAN associated with the IP address you use to access the WAP device. Provide a number between 1 and 4094 for the Management VLAN ID. The default 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 Cisco WAP121 and 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 acquires its IP address from a DHCP server on the LAN.
  - **Static IP**—You 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 acquires DNS server addresses from a DHCP server on the LAN.
  - **Manual**—You manually configure one or more DNS server addresses. Enter up to two IP addresses in the text boxes.

STEP 4 Click **Save**. The changes are saved 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 a loss of connectivity will least affect your wireless clients.

IPv6 Addresses

You can use the IPv6 Addresses page to configure the WAP device to use IPv6 addresses.

To configure IPv6 address settings:

STEP 1 Select **LAN** > **IPv6 Addresses** in the navigation area.

STEP 2 Configure the following settings:

- **IPv6 Connection Type**—Choose how the WAP device obtains an IPv6 address:
  - **DHCPv6**—The IPv6 address is assigned by a DHCPv6 server.
  - **Static IPv6**—You 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. The default is 0.
- **Static IPv6 Address Status**—One of the following values appears:
  - **Operational**—The IP address has been verified as unique on the LAN and is usable on the interface.
  - **Tentative**—The WAP device initiates a duplicate address detection (DAD) process automatically when a static IP address is assigned. An IPv6 address is in the tentative state while it is being verified as unique on the network. While in this state, the IPv6 address cannot be used to transmit or receive ordinary traffic.
  - **Blank (no value)**—No IP address is assigned or the assigned address is not operational.
- **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.
- **IPv6 DNS Nameservers**—Select one of the following values:
  - **Dynamic**—The DNS name servers are learned dynamically through DHCPv6.
  - **Manual**—You specify up to two IPv6 DNS name servers in the fields provided.

STEP 3 Click **Save**. The changes are saved 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 a loss of connectivity will least affect your wireless clients.

5

Wireless

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
- WorkGroup 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 Select **Wireless** > **Radio** in the navigation pane.

STEP 2 In the Global Settings area, configure the **TSPEC Violation Interval**, which is the time interval in seconds for the WAP device to report associated clients that do not adhere to mandatory admission control procedures. The reporting occurs through the system log and SNMP traps. Enter a time from 0 to 900 seconds. The default is 300 seconds.

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

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

- **Radio**—Turns on or off the radio interface. By default, the radio is off.
- **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. Select one of the available 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**—The 802.11n specification allows a coexisting 20/40 MHz channel in addition to the legacy 20 MHz channel available with other modes. The 20/40 MHz channel enables higher data rates but leaves fewer channels available for use by other 2.4 GHz and 5 GHz devices.

  By default, when the radio mode includes 802.11n, the channel bandwidth is set to 20/40 MHz to enable both channel widths. 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 20/40 MHz bandwidth only)—A 40 MHz channel can be considered to consist of two 20 MHz channels that are contiguous in the frequency domain. These two 20 MHz channels are often referred to as the Primary and Secondary channels. The Primary Channel is used for 802.11n clients that support only a 20 MHz channel bandwidth and for legacy clients.

  Select one of these options:

  - **Upper**—Sets the Primary Channel as the upper 20 MHz channel in the 40 MHz band.
  - **Lower**—Sets the Primary Channel as the lower 20 MHz channel in the 40 MHz band. Lower is the default selection.

- **Channel**—The portion of the radio spectrum the radio uses for transmitting and receiving.

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

  Each mode offers a number of channels, depending on how the spectrum is licensed by national and transnational authorities such as the Federal Communications Commission (FCC) 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 percent 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-nanosecond guard Interval when communicating with clients that also support the short guard interval. Yes is the default selection.

- **No**—The WAP device transmits data using an 800-nanosecond guard interval.

- **Protection**—The protection feature contains rules to guarantee that 802.11 transmissions do not cause interference with legacy stations or applications. By default, protection is enabled (Auto). With protection enabled, protection is invoked if legacy devices are within range of the WAP device.

  You can disable protection (Off); however, legacy clients or WAP devices 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 WAP devices 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 from 20 to 2000 milliseconds. The default is 100 milliseconds.

- **DTIM Period**—The Delivery Traffic Information Map (DTIM) period. Enter an integer from 1 to 255 beacons. The default is 2 beacons.

  The DTIM message is an element included in some Beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the WAP device awaiting pickup.

  The DTIM period 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 check for buffered data on the WAP device at every beacon. If you set this field to 10, clients 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 default is 2346.

  The fragmentation threshold is a way of limiting the size of packets (frames) transmitted over the network. If a packet exceeds the fragmentation threshold 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, which is the default) effectively disables fragmentation.

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 default is 2347 octets.

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

  Changing the RTS threshold can help control traffic flow through the WAP device, especially one with a lot of clients. If you specify a low threshold value, RTS packets are sent more frequently, which consumes more bandwidth and reduces the throughput of the packet. However, sending more RTS packets can help the network recover from interference or collisions that might occur on a busy network, or on a network experiencing electromagnetic interference.

- **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. The default is 200 stations.

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

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

  To increase the capacity of the network, place WAP devices 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.

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

- **Fixed Multicast Rate**—The transmission rate in Mbps for broadcast and multicast packets. This setting can be useful in an environment where wireless multicast video streaming occurs, provided the wireless clients are capable of handling the configured rate.

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

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

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

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

- **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.

  Check the box below the MCS index number to enable it or uncheck it to disable the index. You cannot disable all indexes at the same time.

  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 operates 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 are 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 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. By default, TSPEC mode is off. 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. By default, TSPEC Voice ACM mode is off. The options are:
  - **On**—A station is required to send a TSPEC request for bandwidth to the WAP device before sending or receiving a voice traffic stream. The WAP device responds with the result of the request, which includes the allotted medium time if the TSPEC was admitted.
  - **Off**—A station can send and receive 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. The default limit is 20 percent of total traffic.
- **TSPEC Video ACM Mode** —Regulates mandatory admission control for the video access category. By default, TSPEC Video ACM mode is off. The options are:

  - **On** — A station is required to send a TSPEC request for bandwidth to the WAP device before sending or receiving a video traffic stream. The WAP device responds with the result of the request, which includes the allotted medium time if the TSPEC was admitted.
  - **Off** — A station can send and receive video priority traffic without requiring an admitted TSPEC; the WAP device ignores video TSPEC requests from client stations.

- **TSPEC Video ACM Limit**—The upper limit on the amount of traffic that the WAP device attempts to transmit on the wireless medium using a video AC to gain access. The default limit is 15 percent of total traffic.
- **TSPEC AP Inactivity Timeout**—The amount of time for a WAP device to detect a downlink traffic specification as idle before deleting it. The valid integer range is from 0 to 120 seconds and the default is 30 seconds.
- **TSPEC Station Inactivity Timeout**—The amount of time for a WAP device to detect an uplink traffic specification as idle before deleting it. The valid integer range is from 0 to 120 seconds and the default is 30 seconds.
- **TSPEC Legacy WMM Queue Map Mode**—Enables or disables the intermixing of legacy traffic on queues operating as ACM. By default, this mode is off.

STEP 5 Click **Save**. The changes are saved 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 a loss of connectivity 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 WAP device performs an RF scan on all channels to detect all APs in the vicinity of the network. If rogue APs are detected, they are shown on the Rogue AP Detection page. If an AP listed as a rogue is legitimate, 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.

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

Viewing the Rogue AP List

Rogue AP detection can be enabled and disabled. To enable the radio to collect information about rogue APs, click **Enable** next to **AP Detection** and then click **Save**.

Information about detected and trusted rogue access points appears. You can click **Refresh** to refresh the screen and show the most current information:

- **Action**—If the AP is in the Detected Rogue AP List, you can click **Trust** to move the AP 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 WAP device 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 **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 **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:

  - 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 **Radio** page to set the channel.

- **Rate**—The rate in megabits per second at which the rogue AP is currently transmitting.

  The current rate is always one of the rates shown in 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) appears.

- **Beacons**—The total number of beacons received from the rogue AP since it was first discovered.
- **Last Beacon**—The date and time of the last beacon received from the rogue AP.
- **Rates**—Supported and basic (advertised) 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 **Radio** page.

Creating and Saving a Trusted AP List

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

STEP 1 In the Detected Rogue AP List, click **Trust** for APs that are known to you. The Trusted APs move to the Trusted AP List.

STEP 2 In the Download/Backup Trusted AP List area, select **Backup (AP to PC)**.

STEP 3 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.

Importing a Trusted AP List

You can 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 is not detected as a rogue.

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

STEP 1 In the Download/Backup Trusted AP List area, select **Download (PC to AP)**.

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. You must separate entries with a single space. For the AP to accept the file, it must contain only MAC addresses.

STEP 3 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 shown in the Known AP List.

STEP 4 Click **Save**.

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. Every additional VAP created has a blank SSID name. The SSIDs for all VAPs can be configured to other values.

The SSID can be any alphanumeric, case-sensitive entry from 2 to 32 characters. The 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 configuration utility for the WAP device is 1, which is also the default untagged VID. If the management VID is the same as the VID assigned to a VAP, then the WLAN clients associated with this specific VAP can administer the WAP device. If needed, an access control list (ACL) can be created to disable administration from WLAN clients.

Configuring VAPs

To configure VAPs:

STEP 1 Select **Wireless** > **Networks** in the navigation pane.

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.

CAUTION Be sure to enter a VLAN ID that is properly configured on the network. Network problems can result if the VAP associates wireless clients with an improperly configured VLAN.
When a wireless client connects to the WAP device by using this VAP, the WAP device tags all traffic from the wireless client with the 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 from 1 to 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 **VLAN and IPv4 Address Settings**.

- **SSID Name**—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 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 shown in the list of available networks on a client station. Instead, you must enter the exact network name manually into the wireless connection utility on the client so that it can connect.

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

- **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**.

NOTE We recommend using WPA Personal or WPA Enterprise as the authentication type as it provides 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**). The 802.11n mode restricts the use of Static or Dynamic WEP as the security mode.

- **MAC Filtering**—Specifies 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.

STEP 4 Click **Save**. The changes are saved 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 a loss of connectivity will least affect your wireless clients.

NOTE To delete a VAP, select the VAP and click **Delete**. To save your deletion permanently, click **Save** when complete.

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 additional security settings 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 configure Static WEP:

- **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 uses 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 uppercase and lowercase 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 the 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 the 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 cannot 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) can 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 decode AP-to-station data transmissions.
- The WAP device must have all keys used by clients for station-to-AP transmit so that it can decode 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 using the same key 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 other access point 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 configure Dynamic WEP:

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

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

  To use a separate RADIUS server for the VAP, uncheck 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 1** or **Server IPv6 Address 1**—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 2** to **4** or **Server IPv6 Address 2** to **4**—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 is shown as asterisks.

- **Key 2** to **Key 4**—The RADIUS key associated with the configured backup RADIUS servers. The server at **Server IP (IPv6) Address 2** uses **Key 2**, the server at **Server IP (IPv6) Address 3** uses **Key 3**, and so on.

- **Enable RADIUS Accounting**—Enables tracking and measuring of 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 with 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 with 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 encryption. The Personal version of WPA uses a pre-shared key (PSK) instead of using IEEE 802.1X and EAP as is used in the Enterprise WPA security mode. The PSK is used for an initial check of credentials only. WPA Personal is also referred to as WPA-PSK.

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

These parameters configure WPA Personal:

- **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 in place 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 are not 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 uppercase and lowercase 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 and lowercase alphabetic letters, numbers, and special characters) are used and how long the string is. If the WPA-PSK complexity check feature is enabled, the key is not accepted unless it meets the minimum criteria. See **WPA-PSK Complexity** for information on configuring the complexity check.
- **Broadcast Key Refresh Rate**—The interval at which the broadcast (group) key is refreshed for clients associated with this VAP. The default is 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 encryption. 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 configure WPA Enterprise:

- **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, and 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 setting lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, in place of some security.
- **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 packets. The pre-authentication information is relayed from the WAP device that the client is currently using to the target WAP device. Enabling this feature can help speed up 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**). 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, uncheck the 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 that you select in this field.

- **Server IP Address 1** or **Server IPv6 Address 1**—The address for the primary RADIUS server for this VAP.

  If **IPv4** is selected as the **Server IP Address Type**, enter the IP address of the RADIUS server that all VAPs use by default, for example, 192.168.10.23. If **IPv6** is selected, enter the IPv6 address of the primary global RADIUS server, for example, 2001:DB8:1234::abcd.

- **Server IP Address 2** to **4** or **Server IPv6 Address 2** to **4**—Up to three IPv4 and/or IPv6 addresses to use as the backup RADIUS servers for this VAP.

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

- **Key 1**—The shared secret key for the global RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive, and you must configure the same key on the WAP device and on your RADIUS server. The text you enter is shown as asterisks to prevent others from seeing the RADIUS key as you type.

- **Key 2** to **Key 4**—The RADIUS key associated with the configured backup RADIUS servers. The server at **Server IP (IPv6) Address 2** uses **Key 2**, the server at **Server IP (IPv6) Address 3** uses **Key 3**, 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 the administrative selection of the active RADIUS server, rather than having the WAP device attempt to contact each configured server in sequence and choose the first server that is up.

  Broadcast Key Refresh Rate—The interval at which the broadcast (group) key is refreshed for clients associated with this VAP.

  The default is 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 with 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, which automates 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 Select **Wireless** > **Scheduler** in the navigation pane.

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 shows in the rule table.

STEP 3 Check the box next to the **Profile 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 is operationally enabled. The time is in HH:MM 24-hour format. The range is <00-23>:<00-59>. The default is 00:00.
- End Time—The time when the radio or VAP is operationally disabled. The time is in HH:MM 24-hour format. The range is <00-23>:<00-59>. The default is 00:00.

STEP 6 Click **Save**. The changes are saved 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, and no profile is associated with any radio or VAP.

Only one Scheduler profile can be associated with the WLAN interface or each VAP. A single profile can be associated with 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 Select **Wireless** > **Scheduler Association** in the navigation pane.

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

The **Interface Operational Status** column shows whether the interface is currently enabled or disabled.

STEP 3 Click **Save**. The changes are saved 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 Select **Wireless** > **Bandwidth Utilization** in the navigation pane.

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 valid integer range is from 0 to 100 percent. The default is 70 percent. When set to 0, all new associations are allowed regardless of the utilization rate.

STEP 4 Click **Save**. The changes are saved 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 a loss of connectivity 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 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 Select **Wireless** > **MAC Filtering** in the navigation pane.

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 Startup Configuration.

NOTE To remove a MAC address from the Stations List, select it and 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 a loss of connectivity 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.

RADIUS Server Attribute	Description	Value
User-Password (2)	A fixed global password used to look up a client MAC entry.	NOPASSWORD

WDS Bridge

The Wireless Distribution System (WDS) allows you to connect multiple WAP121 and WAP321 devices. With WDS, access points communicate with one another without wires. 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.
- All Cisco WAP devices participating in a WDS link must have the following identical settings:

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

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

See **Radio** (Basic Settings) for information on configuring these settings.

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

To configure a WDS bridge:

STEP 1 Select **Wireless** > **WDS Bridge** in the navigation pane.

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**—Specifies the MAC address of the destination WAP device; that is, the WAP device on the other end of the WDS link to which data is sent or handed-off and from which data is received.

TIP You can find the MAC address on the Status and Statistics > Network Interface page.

- **Encryption**—The type of encryption to use on the WDS link; it does not have to match the VAP you are bridging. The WDS Encryption settings are unique to the WDS bridge. 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. See **WEP on WDS Links** or **WPA/PSK on WDS Links** following this procedure for more information about encryption options.

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

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

STEP 7 Replicate this procedure on the other device or devices connecting to the bridge.

TIP You can verify that the bridge link is up by going to the Status and Statistics > Network Interface page. In the Interface Status table, the WLAN0:WDS(x) status should state Up.

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 a loss of connectivity will least affect your wireless clients.

WEP on WDS Links

These additional fields appear when you select WEP as the encryption type.

- **Key Length**—If WEP is enabled, specify the length of the WEP key as **64 bits** or **128 bits**.
- **Key Type**—If WEP is enabled, specify the WEP key type: **ASCII** or **Hex**.
- **WEP Key**—If you selected **ASCII**, enter any combination of 0 to 9, a to z, and A to Z. If you selected **Hex**, enter hexadecimal digits (any combination of 0 to 9 and a to f or A to F). These are the RC4 encryption keys shared with the stations using the WAP device.

  Note that the required number of characters is indicated to the right of the field and changes based on your selections in the **Key Type** and **Key Length** fields.

WPA/PSK on WDS Links

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

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

  The WDS ID can be any alphanumeric combination.

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

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

WorkGroup Bridge

The WAP device WorkGroup Bridge feature enables the WAP device to extend the accessibility of a remote network. In WorkGroup 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 WorkGroup Bridge mode.

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

It is recommended that WorkGroup 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 WorkGroup Bridge solution. Use WDS if you are bridging Cisco WAP121 and WAP321 devices. If you are not, then consider WorkGroup Bridge. When the WorkGroup Bridge feature is enabled, the VAP configurations are not applied; only the WorkGroup Bridge configuration is applied.

NOTE The WDS feature does not work when the WorkGroup Bridge mode is enabled on the WAP device.

In WorkGroup 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 with the access point interface of the device, can access the network connected by the infrastructure client interface. To allow the bridging of packets, the VLAN configuration for the access point interface and wired interface should match that of the infrastructure client interface.

WorkGroup 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.

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

- All WAP devices participating in WorkGroup Bridge must have the following identical settings:
  - Radio
  - IEEE 802.11 Mode
  - Channel Bandwidth
  - Channel (Auto is not recommended)

  See **Radio** (Basic Settings) for information on configuring these settings.
- WorkGroup Bridge mode currently supports only IPv4 traffic.
- WorkGroup Bridge mode is not supported across a Single Point Setup.

To configure WorkGroup Bridge mode:

STEP 1 Select **Wireless** > **WorkGroup Bridge** in the navigation pane.

STEP 2 Select **Enable** for the **WorkGroup Bridge Mode**.

STEP 3 Configure these parameters for the Infrastructure Client Interface (upstream):

- **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 (which is also disabled by default).

- **Security**—The type of security to use for authenticating as a client station on the upstream WAP device. Choices are:
  - **None**
  - **Static WEP**
  - **WPA Personal**
  - **WPA Enterprise**

  See **Configuring Security Settings** for information about WEP and WPA Personal security settings.
- **VLAN ID**—The VLAN associated with the BSS.

  NOTE The Infrastructure Client Interface will be associated with the upstream WAP device with the configured credentials. The WAP device may obtain its IP address from a DHCP server on the upstream link. Alternatively, you can assign a static IP address. The **Connection Status** field indicates whether the WAP is connected to the upstream WAP device. You can click the **Refresh** button at the top of the page to view the latest connection status.

STEP 4 Configure the following additional fields for the Access Point Interface:

- **Status**—Select **Enable** for the Access Point Interface.
- **SSID**—The SSID for the Access Point Interface does not need to be the same as the Infrastructure Client SSID. However, if attempting to support a roaming type of scenario, the SSID and security must be the same.
- **SSID Broadcast**—Select if you want the downstream SSID to be broadcast. SSID Broadcast is enabled by default.
- **Security**—The type of security to use for authenticating. Choices are:
  - **None**
  - **Static WEP**
  - **WPA Personal**
- **MAC Filtering**—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** for instructions on creating the MAC filter list.

- **VLAN ID**—Configure the Access Point Interface with the same VLAN ID as advertised on the Infrastructure Client Interface.

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

The associated downstream clients 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 specify 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 affects the QoS provided.

To configure WAP device and Station EDCA parameters:

STEP 1 Select **Wireless** > **QoS** in the navigation pane.

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).

STEP 3 Configure the following EDCA and Station EDCA parameters:

NOTE These 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 is a number between 0 and the number specified here.

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

Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 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 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 **Enable** to enable Wi-Fi MultiMedia (WMM) extensions. This field is enabled by default. With WMM enabled, QoS prioritization and coordination of wireless medium access is on. With WMM enabled, QoS settings on the WAP device control downstream traffic flowing from the WAP device to client station (AP EDCA parameters) and the upstream traffic flowing from the station to the AP (station EDCA parameters).

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

- **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 WAP device. The TXOP Limit maximum value is 65535.

STEP 4 Configure the following additional settings:

- **No Acknowledgement**—Select **Enable** to specify that the WAP device should not acknowledge frames with QosNoAck as the service class value.
- **Unscheduled Automatic Power Save Delivery**—Select **Enable** to enable APSD, which is a power management method. APSD is recommended if VoIP phones access the network through the WAP device.

STEP 5 Click **Save**. The changes are saved 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 a loss of connectivity 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.

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 to establish wireless networks, which avoids 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 can be viewed in the product user interface.

WPS maintains network security by requiring both the users of new client devices and WLAN administrators to have either 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 client 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 PIN of the WAP device 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 a 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.

The PBC method is when the user of a prospective client pushes a button on the enrolling device, and the administrator of the WAP device with an enabled built-in registrar pushes a similar (hardware or software) button. This sequence begins the 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 built-in registrar of the WAP device 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 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. If 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 PIN value of the WAP device 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 with the WAP device on the WPS-enabled VAP for 60 seconds. The lockdown duration increases upon subsequent failures, up to a maximum of 64 minutes. The WAP devices registration functionality goes into permanent lockdown after the 10th consecutive failed attempt. Reset the device to restart the registration functionality.

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 has an additional security features 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 can configure the following parameters for a WPS-enabled VAP on a WAP device:

- 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 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 through the user interface. The administrator can register the WAP device with an ER by:

STEP 1 Entering the ER PIN on the WAP device.

STEP 2 Entering the WAP device PIN on the user interface of the ER.

NOTE The registration process can also configure the WAP device as specified in the VAP Configuration Changes section, 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 can serve 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 WAP devices support 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 Select **Wireless** > **WPS Setup** in the navigation pane.

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**—Provides a default device name. You can assign a different name from 1 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. Generating a new pin 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**—Enables 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 responses of the registrar.
- **WPS Configuration State**—Specifies if 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 are configured using WPS, after which the state will be change to Configured.
  - **Configured**—VAP settings are not configured by the external registrar and will retain the existing configuration.

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

The operational status of the instance and the reason for that status appears. See Enabling or Disabling WPS on a VAP for information about conditions that may cause the instance to be disabled.

Instance Status

The Instance Status area shows the following information about the selected WPS instance:

- **WPS Operational Status**—Whether or not the WPS instance is operational.
- **AP Lockdown Status**—Whether the AP is in lockdown mode, in which external registrars are blocked from registering with the AP. When in lockdown status, this field reports the start time of the lockdown, whether it is temporary or permanent, and if temporary, the duration of the lockdown period. When not in lockdown mode, the status appears as **Disabled**.
- **Failed Attempts with Invalid PIN**—The number of times an external registrar has tried and failed to register with the WAP device.

When in lockdown status, the following fields appear:

- **AP Lockdown Duration**—The duration in minutes for which the WAP is locked. When the WAP is permanently locked, this value is set to –1.
- **AP Lockdown Timestamp**—The time when the WAP device was locked.

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 software interface of the device.

STEP 2 Select **Wireless** > **WPS Process** in the navigation pane.

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

STEP 4 Within two minutes, enter the WAP pin on the software interface of the client device. The WAP 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.

When the client is enrolled, either the built-in registrar of the WAP device 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.

CAUTION 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 pin of the WAP device. However, this method is **not recommended** for security reasons, as it enables the client to configure the SSID and security settings on the AP. The administrator should only share the PIN with trusted devices.

Enrolling a Client Using the Push Button Method

To enroll a client station using the push button 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 built-in registrar of the WAP device 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 Status Information

The Instance Status section shows the following information about the WPS instance selected in the **WPS Instance ID** list:

- **WPS Status**—Whether the selected WPS instance is enabled or disabled.
- **WPS Configuration State**—Whether the VAP will be configured from the external registrar as a part of the WPS process.
- **Transaction Status**—The status of the last WPS transaction. The possible values are None, Success, WPS Message Error, and Timed Out.
- **WPS Operational Status**—The status of the current or most recent WPS transaction. The possible values are Disabled, Ready, Configuring, Proxying, and Adding Enrollee. When no WPS transactions have occurred since WPS was enabled, Ready appears.
- **AP Lockdown Status**—Whether the instance is currently in lockdown state.
- **Failed Attempts with Invalid PIN**—The number of times an attempt at authenticating an external registrar has failed due to an invalid password.

Viewing Instance Summary Information

This information appears 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 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 device, you can configure security methods that control wireless client access (see the **Radio** page). 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 Select **Security** > **RADIUS Server** in the navigation pane.

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 from 1 to 64 standard alphanumeric and special characters. The key is case sensitive and must match the key configured on the RADIUS server. The text you enter appears as asterisks.

- **Key (2** through **4)**—The RADIUS key associated with the configured backup RADIUS servers. The server at **Server IP (IPv6) Address 2** uses **Key 2**, the server at **Server IP (IPv6) Address-3** uses **Key 3**, and so on.

- **Enable RADIUS Accounting**—Enables tracking and measuring of 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 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 Select **System Security** > **802.1X Supplicant** in the navigation pane.

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 username can be 1 to 64 characters long. ASCII-printable characters are allowed, which includes uppercase and lowercase 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 uppercase and lowercase alphabetic letters, numeric digits, and all special characters except quotation marks.

STEP 3 Click **Save**. The changes are saved 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 a loss of connectivity will least affect your wireless clients.

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

- **Certificate File Present**—Indicates whether 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 device:

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**.

If you selected TFTP, enter the **Filename** and the **TFTP Server IPv4 Address**. The filename cannot contain the following characters: spaces, <, >, |, \, : , (,), &, ; , #, ? , *, and two or more successive periods.

STEP 3 Click **Upload**.

A confirmation window appears, 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 configuration utility. Complex passwords increase security.

To configure password complexity requirements:

STEP 1 Select **Security** > **Password Complexity** in the navigation pane.

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 same password when it 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 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 Select **Security** > **WPA-PSK Complexity** in the navigation pane.

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 uncheck the box, none of these settings are used. WPA-PSK Complexity is disabled by default.

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. Three is the default.
- **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 63. 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. Check the box to make the field editable and to activate this requirement.

STEP 4 Click **Save**. The changes are saved 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. It contains these topics:

- Client QoS Global Settings
- ACL
- Class Map
- Policy Map
- Client QoS Association
- Client QoS Status

Client QoS Global Settings

You can use the Client QoS Global Settings page to enable or disable quality of service functionality on the WAP device.

If you disable **Client QoS Mode**, all ACLs, rate limiting, and DiffServ configurations are globally disabled.

If you enable this mode, you can also enable or disable Client QoS mode on particular VAPs. See the **Client QoS Mode** setting on the *Client QoS Association* page.

ACL

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 or received by the WAP device. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network. Rules can be based on various criteria and may apply to one or more fields within a packet, such as the source or destination IP address, the source or destination port, or the protocol carried in the packet.

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.

These steps give a general description of how to configure ACLs:

STEP 1 Select **Client QoS** > **ACL** in the navigation pane.

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.

These steps give a detailed description of how to configure ACLs:

STEP 1 Select **Client QoS** > **ACL** in the navigation pane.

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 and special 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 shows 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, matches the frame or packet regardless of its contents.

  If you select this field, you cannot configure any additional match criteria. The Match Every Packet 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 Layer 3 or Layer 4 protocol match condition based on the value of the IP Protocol field in IPv4 packets or the Next Header field in IPv6 packets.

  If you select Protocol, 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 wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all bits are important. This field is required when Source IP Address is checked.

  A wildcard mask is basically 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 wildcard 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 Source Port, 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 to 1023—Well Known Ports

  1024 to 49151—Registered Ports

  49152 to 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 wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all bits are important. This field is required when Source IP Address is selected.

  A wildcard mask is basically 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 wildcard 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 the Destination Port, 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 to 1023—Well-Known Ports

    1024 to 49151—Registered Ports

49152 to 65535—Dynamic and/or Private Ports

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

  If you select IP DSCP, 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 selected, 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 IP 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 IP TOS Bits value that are used for comparison against the IP TOS field in a packet.

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

For IPv6 ACLs, configure these parameters:

- **Protocol**—Select the Protocol field to use a Layer 3 or Layer 4 protocol match condition based on the value of the IP Protocol field in IPv4 packets or the Next Header field in IPv6 packets.

  If you select this 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 selected, 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 selected, choose the port name or enter the port number.
- **IPv6 Flow Label**—A 20-bit number that is unique to an IPv6 packet. It is used by end stations to signify QoS handling in routers (range 0 to 1048575).
- **IP DSCP**—Matches packets based on their IP DSCP value. If selected, 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 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 to 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.

  For each bit position in the MAC mask, a 0 indicates that the corresponding address bit is significant and a 1 indicates that the address bit is ignored. For example, to check only the first four octets of a MAC address, a MAC mask of 00:00:00:00:ff:ff is used. A MAC mask of 00:00:00:00:00:00 checks all address bits and is used to match a single MAC address.
- **Destination MAC Address**—Select this field and enter the destination MAC address to compare against an Ethernet frame.
- **Destination MAC Mask**—Enter the destination MAC address mask to specify which bits in the destination MAC to compare against an Ethernet frame.

  For each bit position in the MAC mask, a 0 indicates that the corresponding address bit is significant and a 1 indicates that the address bit is ignored. For example, to check only the first four octets of a MAC address, a MAC mask of 00:00:00:00:ff:ff is used. A MAC mask of 00:00:00:00:00:00 checks all address bits and is used to match a single MAC address.
- **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 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 a 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 Select **Client QoS** > **Class Map** in the navigation pane.

STEP 2 Enter a **Class Map Name**. The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

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 appears 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 appear only for IPv4 or IPv6 class maps are noted):

- **Match Every Packet**—The match condition is true to all the parameters in a Layer 3 packet.

  When selected, all Layer 3 packets will match the condition.

- **Protocol**—Use a Layer 3 or Layer 4 protocol match condition based on the value of the IP Protocol field in IPv4 packets or the Next Header field in IPv6 packets.

  If you select this 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. Check the box and enter an IP address.

- **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 wildcard 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 wildcard 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 QoS handling in routers (range 0 to 1048575).
- **IP DSCP**—See description under Service Type fields.
- **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 to 1023—Well-Known Ports

1024 to 49151—Registered Ports

49152 to 65535—Dynamic and/or Private Ports

- **Destination Port**—Includes a destination port in the match condition for the rule. The destination port is identified in the datagram header.

  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 to 1023—Well Known Ports

    1024 to 49151—Registered Ports

    49152 to 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 to 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.

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

- **Destination MAC Address**—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.

  For each bit position in the MAC mask, a 0 indicates that the corresponding address bit is significant and a 1 indicates that the address bit is ignored. For example, to check only the first four octets of a MAC address, a MAC mask of 00:00:00:00:ff:ff is used. A MAC mask of 00:00:00:00:00:00 checks all address bits and is used to match a single MAC address.
- **VLAN ID**—A VLAN ID to be matched for packets. The VLAN ID range is from 0 to 4095.

The following Service Type fields show 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 criterion:
  - **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 IP TOS bit value ranges between (00 to FF). The high-order three bits represent the IP Precedence value. The high-order six bits represent the IP Differentiated Services Code Point (DSCP) value.

STEP 3 Click **Save**. The changes are saved 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 Select **Client QoS** > **Policy Map** in the navigation pane.

STEP 2 Enter a **Policy Map Name** The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

STEP 3 Click **Add Policy Map**. The page refreshes with additional fields for configuring the policy map.

STEP 4 In the Policy Class Definition area, ensure that the newly created policy map shows in the **Policy Map Name** list.

STEP 5 In the **Class Map Name** list, select the class map to apply this policy.

STEP 6 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 1000000 Kbps.
  - **Committed Burst**—The committed burst size, in bytes, to which traffic must conform. The range is from 1 to 204800000 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 7 Click **Save**. The changes are saved 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 Select **Client QoS** > **Client QoS Association** in the navigation pane.

STEP 2 From the VAP list, select the VAP on which you want to configure client QoS parameters.

STEP 3 Select **Enable** for the **Client QoS Global** to enable this feature.

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 300 Mbps.
- **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 300 Mbps.
- **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 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 show the Client QoS Status page, select **Client QoS** > **Client QoS Status** in the navigation pane.

Use these fields to configure Client QoS Status:

- **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 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
- Views
- Groups
- Users
- 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 Select **SNMP** > **General** in the navigation pane.

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

STEP 3 Specify a **UDP Port** for SNMP traffic.

By default, an SNMP agent listens only to requests from port 161. However, you can configure this so that the agent listens to requests on a different port. The valid range is from 1025 to 65535.

STEP 4 Configure the SNMPv2 settings:

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

  The community name acts as a simple authentication feature to restrict the 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.

- **Read-write Community**—A read-write community name to be used for SNMP set requests. The valid range is from 1 to 256 alphanumeric and special characters.

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

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

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

  - **User Defined**—The set of permitted SNMP requests is restricted to those specified.

- **NMS, IPv4 Address/Name**—The IPv4 IP address, DNS hostname, or subnet of the network management system (NMS), or the set of machines that can execute get and set requests to the managed devices.

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

As with community names, this setting provides a level of security on SNMP settings. The SNMP agent only accepts 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. A total of 126 addresses would be designated.

- **NMS IPv6 Address/Name**—The IPv6 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).

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

STEP 5 Configure the SNMPv2 trap settings:

- **Trap Community**—A global community string associated with SNMP traps. Traps sent from the device provide this string as a community name. The valid range is from 1 to 60 alphanumeric and special characters.

- **Trap Destination Table**—A list of up to three IP addresses or hostnames to receive SNMP traps. Check the box and choose a **Host IP Address Type** (IPv4 or IPv6) before adding the **Hostname/IP Address**.

  An example of a DNS hostname is snmptraps.foo.com. Because 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 that you select the **Enabled** check box and select the appropriate **Host IP Address Type**.

  Also see the note about hostnames in the preceding step.

STEP 6 Click **Save**. The changes are saved 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 a loss of connectivity will least affect your wireless clients.

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 add and configure an SNMP view:

STEP 1 Select **SNMP** > **Views** in the navigation pane.

STEP 2 Click **Add** to create a new row in the SNMPv3 Views table.

STEP 3 Check the box in the new row and click **Edit**:

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

  For example, the system subtree is specified by the OID string .1.3.6.1.2.1.1.
- **Mask**—Enter an OID mask. The mask is 47 characters in length. The format of the OID mask is xx.xx.xx (.)... or xx:xx:xx.... (:) and is 16 octets in length. Each octet is two hexadecimal characters separated by either a period (.) or a colon (:). Only hex characters are accepted in this field.

  For example, OID mask FA.80 is 11111010.10000000.

  A family mask is used to define a family of view subtrees. The family mask indicates which subidentifiers 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 4 Click **Save**. The view is added to the SNMPv3 Views list and your changes are saved to the Startup Configuration.

NOTE To remove a view, select the view in the list and click **Delete**.

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 Information Bases (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 and configure an SNMP group:

STEP 1 Select **SNMP** > **Groups** in the navigation pane.

STEP 2 Click **Add** to create a new row in the SNMPv3 Groups table.

STEP 3 Check the box for the new group and click **Edit**.

STEP 4 Configure the parameters:

- **Group 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 5 Click **Save**. The group is added to the SNMPv3 Groups list and your changes are saved to the Startup Configuration.

NOTE To remove a group, select the group in the list and click **Delete**.

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 Select **SNMP** > **Users** in the navigation pane.

STEP 2 Click **Add** to create a new row in the SNMPv3 Users table.

STEP 3 Check the box in the new row and click **Edit**.

STEP 4 Configure the parameters:

- **User 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 Pass Phrase**—(If you specify MD5 as the Authentication Type) A pass phrase to enable the SNMP agent to authenticate requests sent by the user. The pass phrase 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 Pass Phrase**—(If you specify DES as the privacy type) A pass phrase to use to encrypt the SNMP requests. The pass phrase must be between 8 and 32 characters in length.

STEP 5 Click **Save**. The user is added to the SNMPv3 Users list and your changes are saved to the Startup Configuration.

NOTE To remove a user, select the user in the list and click **Delete**.

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 the **Users** page) should be completed before configuring SNMPv3 targets.

NOTE The WAP device supports a maximum of eight targets.

To add SNMP targets:

STEP 1 Select **SNMP** > **Targets** in the navigation pane.

STEP 2 Click **Add**. A new row is created in the table.

STEP 3 Check the box in the new row and click **Edit**.

STEP 4 Configure the parameters:

- **IP Address**—Enter the IPv4 address of the remote SNMP manager to receive the target.
- **UDP 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 the **Users** page.

STEP 5 Click **Save**. The user is added to the SNMPv3 Targets list and your changes are saved to the Startup Configuration.

NOTE To remove an SMMP target, select the user in the list and click **Delete**.

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:

- **Captive Portal Global Configuration**
- **Instance Configuration**
- **Instance Association**
- **Web Portal Customization**
- **Local Groups**
- **Local Users**
- **Authenticated Clients**
- **Failed Authentication Clients**

Captive Portal Global 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 Select **Captive Portal** > **Global Configuration** in the navigation pane.

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 may need to refresh the web authentication page. The default authentication timeout is 300 seconds. The range is from 60 to 600 seconds.
- **Additional HTTP Port**—HTTP traffic uses the HTTP management port, which is 80 by default. You can configure an additional port for HTTP traffic. Enter a port number between 1025 and 65535, or 80. The HTTP and HTTPs ports cannot be the same.
- **Additional HTTPS Port**—HTTP traffic over SSL (HTTPS) uses the HTTPS management port, which is 443 by default. You can configure an additional port for HTTPS traffic. Enter port number between 1025 and 65535, or 443. The HTTP and HTTPs ports cannot be the same.

The Captive Portal Configuration Counters area shows read-only 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 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.

NOTE Before you create an instance, review these bullets first:

- Do you need to add a new VAP? If yes, go to **Networks** to add a VAP.
- Do you need to add a new group? If yes, go to **Local Groups** to add a group.
- Do you need to add a new user? If yes, go to **Local Users** to add a user.

To create a CP instance and configure its settings:

STEP 1 Select **Captive Portal** > **Instance Configuration** in the navigation pane.

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 reappear with additional options.

STEP 5 Configure the parameters:

- **Instance ID**—The instance ID. This field is nonconfigurable.
- **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 remains in the CP authenticated client list after the client disassociates from the WAP. If the time specified in this field expires before the client attempts to reauthenticate, the client entry is removed from the authenticated client list. The range is from 0 to 1440 minutes. The default value is 60 minutes.

  NOTE An away timeout value is also configured for each user. See the **Local Users** page. The away timeout value set on the Local Users page has precedence over the value configured here, unless the value is set to 0 (the default). A value of 0 indicates to use the instance timeout value.
- **Session Timeout**—The time remaining, in seconds, for the CP session to be valid. After the time reaches zero, the client is deauthenticated. The range is from 0 to 1440 minutes. The default value is 0.
- **Maximum Bandwidth Upstream**—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.
- **Maximum Bandwidth Downstream**—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 uses the configured IPv4 or IPv6 RADIUS server addresses.

- **Global RADIUS**—If the Verification Mode is RADIUS, select this option to the default Global RADIUS server list to authenticate clients. (See **RADIUS Server** for information about configuring the global RADIUS servers.) If you want the CP feature to use a different set of RADIUS servers, uncheck the box and configure the servers in the fields on this page.
- **RADIUS Accounting**—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, all backup servers, and globally or locally configured servers.
- **Server IP Address 1 or Server IPv6 Address 1**—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 specified address.
- **Server IP Address (2** through **4)** or **Server IPv6 Address (2** through **4)**—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 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 is shown as asterisks.
- **Key 2 to 4**—The RADIUS key associated with the configured backup RADIUS servers. The server at Server IP Address 1 uses Key 1, Server IP Address 2 uses Key 2, and so on.
- **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**. Your changes are saved to the Startup Configuration.

Instance Association

Once you create an instance, you can use the Instance Association page to associate a CP instance to a VAP. The associated CP instance settings applies to users who attempt to authenticate on the VAP.

To associate an instance to a VAP:

STEP 1 Select **Captive Portal** > **Instance Association** in the navigation pane.

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 Startup Configuration.

Web Portal Customization

Once your CP instance is associated with a VAP, you need to create a locale (an authentication web page) and map it to the CP instance. When a user accesses a VAP that is associated with a captive portal instance, the user sees an authentication page. You use the Web Portal Customization page to create unique pages for different locales on your network, and to customize the text and images on the pages.

To create and customize a CP authentication page:

STEP 1 Select **Captive Portal > Web Portal Customization** in the navigation pane.

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 show 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 Startup Configuration.

STEP 6 From the **Captive Portal Web Locale** list, select the locale you created.

The page shows 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 show as the page background. You can click **Upload/Delete Custom Image** to upload images for Captive Portal instances. See Uploading and Deleting Images.
- **Logo Image Name**—The image file to show 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.
- **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 show 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 1 to 32 characters.
- **User Label**—The label for the user name text box. The range is from 1 to 32 characters.
- **Password Label**—The label for the user password text box. The range is from 1 to 64 characters.
- **Button Label**—The label on the button that 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 is 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 show in the browser title bar. The range is from 1 to 128 characters. The default is Captive Portal.
- **Browser Content**—The text that shows 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 shows in the page body below the user name and password text boxes. The range is from 1 to 256 characters. The default is To start using this service, enter your credentials and click the connect button.
- **Acceptance Use Policy**—The text that appears in the Acceptance Use Policy box. The range is from 1 to 4096 characters. The default is Acceptance Use Policy.
- **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 1 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 shows 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 shows during authentication. The range is from 1 to 128 characters. The default is Connecting, please be patient....
- **Denied Text**—The text that shows when a user fails authentication. The range is from 1 to 128 characters. The default is Error Invalid Credentials, please try again!
- **Welcome Title**—The text that shows 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 shows when the client has connected to the network. The range is from 1 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 Startup Configuration.

STEP 9 Click **Preview** to view the updated page.

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

Uploading and Deleting Images

When users initiate access to a VAP that is associated with a captive portal instance, an authentication page appears. You can customize the authentication page with your own logo or other images.

Up to 18 images can be uploaded (assuming six locales, with each locale having three images). All images must be 5 kilobytes or smaller and must be in GIF or JPG format.

Images are resized to fit the specified dimensions. For best results, your logo and account images should be similar in proportion to the default images, as follows:

Image Type	Use	Default Width by Height
Background	Shows as the page background.	10 by 800 pixels

Image Type	Use	Default Width by Height
Logo	Shows at top left of page to provide branding information.	168 by 78 pixels
Account	Shows above the login field to depict an authenticated login.	295 by 55 pixels

To upload binary graphic files to the WAP device:

STEP 1 On the Web Portal Customization page, click **Upload/Delete Custom Image** next to the **Background Image Name**, **Logo Image Name**, or **Account Image** fields.

The Web Portal Custom Image page appears.

STEP 2 Browse to select the image.

STEP 3 Click **Upload**.

STEP 4 Click **Back** to return to the Web Portal Custom Image page.

STEP 5 Select the **Captive Portal Web Locale** you want to configure.

STEP 6 For the **Background Image Name**, **Logo Image Name**, or **Account Image** fields, select the newly uploaded image.

STEP 7 Click **Save**.

NOTE To delete an image, on the Web Portal Custom Image page, select it from the **Delete Web Customization Image** list and click **Delete**. You cannot delete the default images.

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 Select **Captive Portal** > **Local Groups** in the navigation pane.

STEP 2 Enter a **Group Name** and click **Save**. The changes are saved 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 Select **Captive Portal** > **Local Users** in the navigation pane.

STEP 2 Enter a **User Name** and click **Save**.

Additional fields appear to configure the user.

STEP 3 Enter the parameters:

- **User Password**—Enter the 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.
- **Show Password as Clear Text**—When enabled, the text you type is visible. When disabled, the text is not masked as you enter it.
- **Away Timeout**—The period of time a user remains in the CP authenticated client list after the client disassociates from the AP. If the time specified in this field expires before the client attempts to reauthenticate, the client entry is removed from the authenticated client list. The range is from 0 to 1440

minutes. The default value is 60. The timeout value configured here has precedence over the value configured for the captive portal instance, unless the user value is set to 0. When set to 0, the timeout value configured for the CP instance is used.

- **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 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 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 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, select **Captive Portal** > **Authenticated Clients** in the navigation pane.

- **MAC Address**—The MAC address of the client.
- **IP Address**—The IP address of the client.
- **User Name**—The Captive Portal user name of the client.
- **Protocol**—The protocol 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 shows Radio1.
- **Captive Portal ID**—The ID of the Captive Portal instance to which the user is associated.
- **Session Timeout**—The time remaining, in seconds, for the CP session to be valid. After the time reaches zero, the client is deauthenticated.
- **Away Timeout**—The time remaining, in seconds, for the client entry to be valid. The timer starts when the client dissociates from the CP. After the time reaches zero, the client is deauthenticated.
- **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, select **Captive Portal** > **Failed Authentication Clients** in the navigation pane.

- **MAC Address**—The MAC address of the client.
- **IP Address**—The IP address of the client.
- **User Name**—The Captive Portal user name of the client.

- **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 shows 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.

10

Single Point Setup

This chapter describes how to configure Single Point Setup over multiple WAP devices.

It includes these topics:

- Single Point Setup Overview
- Access Points
- Sessions
- Channel Management
- Wireless Neighborhood

Single Point Setup Overview

The Cisco WAP121 and WAP321 devices support Single Point Setup. Single Point Setup provides a centralized method to administer and control wireless services across multiple devices. You use Single Point Setup to create a single group, or cluster, of wireless devices. After the WAP devices are clustered, you can view, deploy, configure, and secure the wireless network as a single entity. After a wireless cluster is created, Single Point Setup also facilitates channel planning across your wireless services to reduce radio interference and maximize bandwidth on the wireless network.

When you first set up your WAP device, you can use the Setup Wizard to configure Single Point Setup or join an existing Single Point Setup. If you prefer not to use the Setup Wizard, you can use the web-based configuration utility.

Managing Single Point Setup Across WAP Devices

Single Point Setup creates a dynamic, configuration-aware cluster, or group, of WAP devices in the same subnet of a network. A cluster supports only a group of configured WAP121 devices or a group of configured WAP321 devices. A single cluster does not support a mix of WAP121 and WAP321 devices in the same group.

Single Point Setup allows the management of more than one cluster in the same subnet or network; however, they are managed as single independent entities. The table below shows Single Point Setup wireless service limits.

Group/Cluster Type	WAP Devices per Single Point Setup	Number of Active Clients per Single Point Setup	Maximum Number of Clients (Active and Idle)
WAP121	4	40	64
WAP321	8	160	256

A cluster can propagate configuration information, such as VAP settings, QoS queue parameters, and radio parameters. When you configure Single Point Setup on a device, settings from that device (whether they are manually set or set by default) are propagated to other devices as they join the cluster. To form a cluster, make sure the following prerequisites or conditions are met:

STEP 1 Plan your Single Point Setup cluster. Be sure the two or more WAP devices you want to cluster are the same model. For example, Cisco WAP121 devices can only cluster with other Cisco WAP121 devices.

It is strongly recommended to run the latest firmware version on all clustered WAP devices.

> **NOTE** Firmware upgrades **are not** propagated to all WAP devices in a cluster; you must upgrade each device independently.

STEP 2 Set up the WAP devices that will be clustered on the same IP subnet and verify that they are interconnected and accessible across the switched LAN network.

STEP 3 Enable Single Point Setup on all WAP devices. See **Access Points**.

STEP 4 Verify that the WAP devices all reference the same Single Point Setup name. See **Access Points**.

Single Point Setup Negotiation

When a WAP device is enabled and configured for Single Point Setup, it begins sending periodic advertisements every 10 seconds to announce its presence. If there are other WAP devices that match the criteria for the cluster, arbitration begins to determine which WAP device will distribute the master configuration to the rest of the members of the cluster.

The following rules apply to Single Point Setup cluster formation and arbitration:

- For existing Single Point Setup clusters, whenever the administrator updates the configuration of any member of the cluster, the configuration change is propagated to all members of the cluster, and the configured WAP device assumes control of the cluster.
- When two separate Single Point Setup clusters join into a single cluster, then the latest modified cluster wins arbitration of the configuration and overwrites and updates the configuration of all clustered WAP devices.
- If a WAP device in a cluster does not receive advertisements from a WAP device for more than 60 seconds (for example, if the device loses connectivity to other devices in the cluster), the device is removed from the cluster.
- If a WAP device in Single Point Setup mode loses connectivity, it is not immediately dropped from the cluster. If it regains connectivity and rejoins the cluster without having been dropped, and configuration changes were made to that device during the lost connectivity period, the changes are propagated to the other cluster members when connectivity resumes.
- If a WAP device in a cluster loses connectivity, is dropped, later rejoins the cluster, and configuration changes were made in the during the lost connectivity period, the changes are propagated to the device when it rejoins. If there are configuration changes in both the disconnected device and the cluster, then the device with the greatest number of changes and, secondarily, the most recent change, will be selected to propagate its configuration to the cluster. (That is, if WAP1 has more changes, but WAP2 has the most recent change, WAP1 is selected. If they have an equal number of changes, but WAP2 has the most recent change, then WAP2 is selected.)

Operation of a WAP Device Dropped From a Single Point Setup

When a WAP device that was previously a member of a cluster becomes disconnected from the cluster, the following guidelines apply:

- Loss of contact with the cluster prevents the WAP device from receiving the latest operational configuration settings. The disconnection results in a halt to proper seamless wireless service across the production network.
- The WAP device continues to function with the wireless parameters that it last received from the cluster.
- Wireless clients associated with the non-clustered WAP device continue to associate with the device with no interruption of the wireless connection. In other words, loss of contact with the cluster does not necessarily prevent wireless clients associated with that WAP device from continued access to network resources.
- If the loss of contact with the cluster is due to a physical or logical disconnect with the LAN infrastructure, network services out to the wireless clients may be impacted depending on the nature of the failure.

Propagation of Configuration Settings and Parameters in Single Point Setup

The tables summarize configurations that are shared and propagated among all clustered WAP devices.

Common Configuration Settings and Parameters that are Propagated in Single Point Setup

Captive Portal	Password Complexity
Client QoS	User Accounts
Email Alert	QoS
HTTP/HTTPs Service (Except SSL Certificate Configuration)	Radio Settings Including TSpec Settings (Some exceptions)
Log Settings	Rogue AP Detection

Common Configuration Settings and Parameters that are Propagated in Single Point Setup	
MAC Filtering	Scheduler
Management Access Control	SNMP General and SNMPv3
Networks	WPA-PSK Complexity
Time Settings	

Radio Configuration Settings and Parameters that are Propagated in Single Point Setup
Mode
Fragmentation Threshold
RTS Threshold
Rate Sets
Primary Channel
Protection
Fixed Multicast Rate
Broadcast or Multicast Rate Limiting
Channel Bandwidth
Short Guard Interval Supported

Radio Configuration Settings and Parameters that are Not Propagated in Single Point Setup
Channel
Beacon Interval
DTIM Period
Maximum Stations

Radio Configuration Settings and Parameters that are Not Propagated in Single Point Setup
Transmit Power

Other Configuration Settings and Parameters That Are Not Propagated in Single Point Setup	
Bandwidth Utilization	Port Settings
Bonjour	VLAN and IPv4
IPv6 Address	WDS Bridge
IPv6 Tunnel	WPS
Packet Capture	WorkGroup Bridge

Access Points

The Access Points page allows you to enable or disable Single Point Setup on a WAP device, view the cluster members, and configure the location and cluster name for a member. You can also click the IP address of a member to configure and view data on that device.

Configuring the WAP Device for Single Point Setup

To configure the location and name of an individual Single Point Setup cluster member:

STEP 1 Select **Single Point Setup > Access Points** in the navigation pane.

Single Point Setup is disabled by default on the WAP device. When disabled, the **Enable Single Point Setup** button is visible. If Single Point Setup is enabled, the **Disable Single Point Setup** button is visible. You can edit Single Point Setup options only when Single Point Setup is disabled.

Icons on the right side of the page indicate whether Single Point Setup is enabled and, if it is, the number of WAP devices that are currently joined in the cluster.

STEP 2 With Single Point Setup disabled, configure the following information for each individual member of a Single Point Setup cluster.

- **Location**—Enter a description of where the access point is physically located, for example, Reception. The location field is optional.
- **Cluster Name**—Enter the name of the cluster for the WAP device to join, for example Reception_Cluster.

  The cluster name is not sent to other WAP devices. You must configure the same name on each device that is a member. The cluster name must be unique for each Single Point Setup you configure on the network. The default is ciscosb-cluster.
- **Clustering IP Version**—Specify the IP version that the WAP devices in the cluster use to communicate with other members of the cluster. The default is IPv4.

  If you choose IPv6, Single Point Setup can use the link local address, autoconfigured IPv6 global address, and statically configured IPv6 global address. Ensure that when using IPv6, all the WAP devices in the cluster either use link-local addresses only or use global addresses only.

  Single Point Setup works only with devices using the same type of IP addressing. It does not work with a group of WAP devices where some have IPv4 addresses and some have IPv6 addresses.

STEP 3 Click **Enable Single Point Setup**.

The WAP device begins searching for other WAP devices in the subnet that are configured with the same cluster name and IP version. A potential cluster member sends advertisements every 10 seconds to announce its presence.

While searching for other cluster members, the status indicates that the configuration is being applied. Refresh the page to see the new configuration.

If one or more WAP devices are already configured with the same cluster settings, the WAP device joins the cluster and information on each member shows in a table.

STEP 4 Repeat these steps on additional WAP devices that you want to join the Single Point Setup.

Viewing Single Point Setup Information

When Single Point Setup is enabled, the WAP device automatically forms a cluster with other WAP devices with the same configuration. On the Access Points page, the WAP devices detected are listed in a table and the following information is shown:

- **Location**—Description of where the access point is physically located.
- **MAC Address**—Media Access Control (MAC) address of the access point. The address is the MAC address for the bridge (br0), and is the address by which the WAP device is known externally to other networks.
- **IP Address**—The IP address for the access point.

Note that the Single Point Setup status and the number of WAP devices are shown graphically on the right side of the page.

Adding a New Access Point to a Single Point Setup Cluster

To add a new access point that is currently in standalone mode into a Single Point Setup cluster:

STEP 1 Go to the web-based configuration utility on the standalone access point.

STEP 2 Select **Single Point Setup > Access Points** in the navigation pane.

STEP 3 Set the **Cluster name** to the same name that is configured for the cluster members.

STEP 4 (Optional) In the Location field, enter a description of where the access point is physically located, for example, Reception.

STEP 5 Click **Enable Single Point Setup**.

The access point automatically joins the Single Point Setup.

Removing an Access Point from a Single Point Setup Cluster

To remove an access point from the Single Point Setup cluster:

STEP 1 In the table showing the detected devices, click the IP address for the clustered WAP device you want to remove.

The web-based configuration utility for that WAP device shows.

STEP 2 Select **Single Point Setup > Access Points** in the navigation pane.

STEP 3 Click **Disable Single Point Setup**.

The **Single Point Setup** status field for that access point will now show **Disabled**.

Navigating to Configuration Information for a Specific WAP Device

All WAP devices in a Single Point Setup cluster reflect the same configuration (if the configurable items can be propagated). It does not matter which WAP device you connect to for administration—configuration changes on any WAP device in the cluster are propagated to the other members.

There may be situations, however, when you want to view or manage information on a particular WAP device. For example, you might want to check status information such as client associations or events for an access point. In this case, you can click the IP address in the table on the Access Points page to show the web-based configuration utility for the particular access point.

Navigating to a WAP Device Using its IP Address in a URL

You can also link to the web-based configuration utility of a specific WAP device by entering the IP address for that access point as a URL directly into a web browser address bar in the following form:

http://*IPAddressOfAccessPoint* (if using HTTP)

https://IPAddressofAccessPoint (if using HTTPS)

Sessions

The Sessions page shows information on WLAN clients that are associated with the WAP devices in the Single Point Setup cluster. Each WLAN client is identified by its MAC address, along with the device location where it is currently connected.

NOTE The Sessions page shows a maximum of 20 clients per radio on the clustered WAP devices. To see all WLAN clients associated with a particular WAP device, view the Status > Associated Clients page directly on that device.

To view a particular statistic for a WLAN client session, select an item from the Display list and click **Go**. You can view information about idle time, data rate, and signal strength.

A session in this context is the period of time in which a user on a client device (station) with a unique MAC address maintains a connection with the wireless network. The session begins when the WLAN client logs on to the network, and the session ends when the WLAN client either logs off intentionally or loses the connection for some other reason.

NOTE A session is not the same as an association, which describes a WLAN client connection to a particular access point. A WLAN client association can shift from one clustered access point to another within the same session.

To view sessions associated with the cluster, select **Single Point Setup > Sessions** in the navigation pane.

The following data shows for each WLAN client session with a Single Point Setup.

- **AP Location**—The location of the access point.

  The location is derived from the location specified on the Administration > System Settings page.

- **User MAC**—The MAC address of the wireless client.

  A MAC address is a hardware address that uniquely identifies each node of a network.

- **Idle**—The amount of time this WLAN client has remained inactive.

  A WLAN client is considered to be inactive when it is not receiving or transmitting data.

- **Rate**—The negotiated data rate. Actual transfer rates can vary depending on overhead.

  The data transmission rate is measured in megabits per second (Mbps). The value should fall within the range of the advertised rate set for the mode in use on the access point. For example, 6 to 54 Mbps for 802.11a.

- **Signal**—The strength of the radio frequency (RF) signal the WLAN client receives from the access point. The measure is known as Received Signal Strength Indication (RSSI), and is a value between 0 and 100.

- **Receive Total**—The number of total packets received by the WLAN client during the current session.

- **Transmit Total**—The number of total packets transmitted to the WLAN client during this session.

- **Error Rate**—The percentage of time frames are dropped during transmission on this access point.

To sort the information shown in the tables by a particular indicator, click the column label you want to sort by. For example, if you want to see the table rows ordered by signal strength, click the Signal column label.

Channel Management

The Channel Management page shows the current and planned channel assignments for WAP devices in a Single Point Setup cluster.

When channel management is enabled, the WAP device automatically assigns radio channels used by WAP devices in a Single Point Setup cluster. Automatic channel assignment reduces mutual interference (or interference with other WAP devices outside of its cluster) and maximizes Wi-Fi bandwidth to help maintain efficient communication over the wireless network.

The automatic channel assignment feature is disabled by default. The state of channel management (enabled or disabled) is propagated to the other devices in the Single Point Setup cluster.

At a specified interval, the channel manager (that is, the device that provided the configuration to the cluster) maps all clustered WAP devices to different channels and measures interference levels of the cluster members. If significant channel interference is detected, the channel manager automatically reassigns some or all of the devices to new channels per an efficiency algorithm (or automated channel plan). If the channel manager determines that a change is necessary, then the reassignment information is sent to all members of the cluster. A syslog message is generated as well indicating the sender device and the new and old channel assignments.

To configure and view the channel assignments for the Single Point Setup members:

STEP 1 Select the **Single Point Setup** > **Channel Management** in the navigation pane.

From the Channel Management page, you can view channel assignments for all WAP devices in the cluster and stop or start automatic channel management. You can also use the advanced settings to modify the interference reduction potential that triggers channel reassignment, change the schedule for automatic updates, and reconfigure the channel set used for assignments.

STEP 2 To start automatic channel assignment, click **Start**.

Channel management overrides the default cluster behavior, which is to synchronize radio channels of all WAP devices that are members of the cluster. When channel management is enabled, the radio channel is not synchronized across the cluster to other devices.

When automatic channel assignment is enabled, the channel manager periodically maps radio channels used by WAP devices in a Single Point Setup cluster and, if necessary, reassigns channels to reduce interference with cluster members or with devices outside the cluster. The channel policy for the radio is automatically set to static mode, and the **Auto** option is not available for the **Channel** field on the Wireless > Radio page.

See Viewing Channel Assignments and Setting Locks for information on the current and proposed channel assignments.

STEP 3 To stop automatic channel assignment, click **Stop**.

No channel usage maps or channel reassignments are made. Only manual updates affect the channel assignment.

Viewing Channel Assignments and Setting Locks

When channel management is enabled, the page shows the Current Channel Assignations table and the Proposed Channel Assignments table.

Current Channel Assignments Table

The Current Channel Assignments table shows a list of all WAP devices in the Single Point Setup cluster by IP address.

The table provides the following details on the current channel assignments.

- **Location**—The physical location of the device.
- **IP Address**—The IP address for the access point.
- **Wireless Radio**—The MAC address of the radio.
- **Band**—The band on which the access point is broadcasting.
- **Channel**—The radio channel on which this access point is currently broadcasting.
- **Locked**—Forces the access point to remain on the current channel.
- **Status**—Shows the status of the wireless radio in the device. (Some WAP devices may have more than one wireless radio; each radio is displayed on a separate line in the table.) The radio status is up (operational) or down (not operational).

When selected for an access point, automated channel management plans do not reassign the WAP devices to a different channel as a part of the optimization strategy. Instead, WAP devices with locked channels are factored in as requirements for the plan.

Click **Save** to update the locked setting. Locked devices show the same channel for the Current Channel Assignments table and the Proposed Channel Assignments table. Locked devices keep their current channels.

Proposed Channel Assignments Table

The Proposed Channel Assignments table shows the proposed channels that are to be assigned to each WAP device when the next update occurs. Locked channels are not reassigned—the optimization of channel distribution among devices takes into account that locked devices must remain on their current channels. WAP devices that are not locked may be assigned to different channels than they were previously using, depending on the results of the plan.

For each WAP device in the Single Point Setup, the Proposed Channel Assignments table shows the location, IP Address, and Wireless Radio, as in the Current Channel Assignations table. It also shows the Proposed Channel, which is the radio channel to which this WAP device would be reassigned if the channel plan is applied.

Configuring Advanced Settings

The Advanced settings area enables you to customize and schedule the channel plan for the Single Point Setup.

By default, channels are automatically reassigned once every hour, but only if interference can be reduced by 25 percent or more. Channels are reassigned even if the network is busy. The default settings are designed to satisfy most scenarios where you would need to implement channel management.

You can change the Advanced settings to configure the following settings:

- **Change channels if interference is reduced by at least**—The minimum percentage of interference reduction a proposed plan must achieve in order to be applied. The default is 75 percent. Use the drop-down menu to choose percentages ranging from 5 percent to 75 percent. Using this setting lets you set a threshold gain in efficiency for channel reassignment so that the network is not continually disrupted for minimal gains in efficiency.

  For example, if channel interference must be reduced by 75 percent and the proposed channel assignments will only reduce interference by 30 percent, then channels will not be reassigned. However, if you reset the minimal channel interference benefit to 25 percent and click **Save**, the proposed channel plan will be implemented and channels will be reassigned as needed.

- **Determine if there is better set of channels every**—The schedule for automated updates. A range of intervals is provided, from 30 minutes to six months

The default is one hour, meaning that channel usage is reassessed and the resulting channel plan is applied every hour.

If you change these settings, click **Save**. The changes are saved to the active configuration and the Startup Configuration.

Wireless Neighborhood

The Wireless Neighborhood page shows up to 20 devices within range of each wireless radio in the cluster. (For example, if a WAP device has two wireless radios, 40 devices would be displayed for that device.) The Wireless Neighborhood page also distinguishes between cluster members and nonmembers.

The Wireless Neighborhood view can help you:

- Detect and locate unexpected (or rogue) devices in a wireless domain so that you can take action to limit associated risks.
- Verify coverage expectations. By assessing which WAP devices are visible and at what signal strength from other devices, you can verify that the deployment meets your planning goals.
- Detect faults. Unexpected changes in the coverage pattern are evident at a glance in the color coded table.

To view neighboring devices, select **Single Point Setup** > **Wireless Neighborhood** in the navigation pane. To see all the devices detected on a given Single Point Setup, navigate to the web interface of a member and select **Wireless** > **Rogue AP Detection** in the navigation pane.

For each neighbor access point, the following information is shown:

- **Display Neighboring APs**—Select one of the following radio buttons to change the view:
  - **In cluster**—Only neighbor WAP devices that are members of the cluster.
  - **Not in cluster**—Only neighbor WAP devices that are not cluster members.
  - **Both**—Shows all neighbor WAP devices (cluster members and nonmembers).

- **Cluster**—The list at the top of the table shows IP addresses for all WAP devices that are clustered together. (This list is the same as the members list on the **Single Point Setup** > **Access Points** page.)

  If there is only one WAP device in the cluster, only a single IP address column shows, indicating that the WAP device is grouped with itself.

  You can click on an IP address to view more details on a particular WAP device.

- **Neighbors**—Devices that are neighbors of one or more of the clustered devices are listed in the left column by SSID (network name).

A device that is detected as neighbor can also be a cluster member itself. Neighbors who are also cluster members are always shown at the top of the list with a heavy bar above and include a location indicator.

The colored bars to the right of each WAP device in the Neighbors list shows the signal strength for each of the neighbor WAP devices, as detected by the cluster member whose IP address is shown at the top of the column.

The color of the bar indicates the signal strength:

- Dark Blue Bar—A dark blue bar and a high signal strength number (for example 50) indicates good signal strength detected from the neighbor, as seen by the device whose IP address is listed above that column.
- Lighter Blue Bar—A lighter blue bar and a lower signal strength number (for example 20 or lower) indicates medium or weak signal strength from the neighbor, as seen by the device whose IP address is listed above that column
- White Bar—A white bar and the number 0 indicates that a neighboring device that was detected by one of the cluster members cannot be detected by the device whose IP address is listed above that column.
- Light Gray Bar—A light gray bar and no signal strength number indicates that no signal has been detected from the neighbor, but the neighbor may have been detected by other members of the cluster.
- Dark Gray Bar—A dark gray bar and no signal strength number indicates the WAP device itself that corresponds to the IP address listed above it. A signal strength of zero is displayed because the device's own signal strength is not measured.

Viewing Details for a Cluster Member

To view details on a cluster member, click the IP address of a member at the top of the page.

The following details for the device appear below the Neighbors list.

- **SSID**—The Service Set Identifier for the neighboring access point.
- **MAC Address**—The MAC address of the neighboring access point.
- **Channel**—The channel on which the access point is currently broadcasting.
- **Rate**—The rate in megabits per second at which this access point is currently transmitting. The current rate is always one of the rates shown in Supported Rates.
- **Signal**—The strength of the radio signal detected from the access point, measured in decibels (dB).
- **Beacon Interval**—The beacon interval used by the access point.
- **Beacon Age**—The date and time of the last beacon received from this access point.

A

Deauthentication Message Reason Codes

When a client deauthenticates from the WAP device, a message is sent to the system log. The message includes a reason code that may be helpful in determining why a client was deauthenticated. You can view log messages when you click **Status and Statistics > Log Status**.

The following table describes the deauthentication reason codes.

Reason code	Meaning
0	Reserved
1	Unspecified reason
2	Previous authentication no longer valid
3	Deauthenticated because sending station (STA) is leaving or has left Independent Basic Service Set (IBSS) or ESS
4	Disassociated due to inactivity
5	Disassociated because WAP device is unable to handle all currently associated STAs
6	Class 2 frame received from nonauthenticated STA
7	Class 3 frame received from nonassociated STA
8	Disassociated because sending STA is leaving or has left Basic Service Set (BSS)
9	STA requesting (re)association is not authenticated with responding STA
10	Disassociated because the information in the Power Capability element is unacceptable

Reason code	Meaning
11	Disassociated because the information in the Supported Channels element is unacceptable
12	Disassociated due to BSS Transition Management
13	Invalid element, i.e., an element defined in this standard for which the content does not meet the specifications in Clause 8
14	Message integrity code (MIC) failure
15	4-Way Handshake timeout
16	Group Key Handshake timeout
17	Element in 4-Way Handshake different from (Re)Association Request/Probe Response/Beacon frame
18	Invalid group cipher
19	Invalid pairwise cipher
20	Invalid AKMP
21	Unsupported RSNE version
22	Invalid RSNE capabilities
23	IEEE 802.1X authentication failed
24	Cipher suite rejected because of the security policy

B

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