391748

391747

ADMINISTRATION GUIDE

Cisco WAP131 Wireless-N Dual Radio Access Point with PoE
Cisco WAP351 Wireless-N Dual Radio Access Point with 5 Ports Switch

OL-32504-01

Contents

1

Getting Started

This chapter provides an introduction to the web-based Configuration Utility of the Cisco WAP131 and WAP351 Wireless-N Dual Radio Access Points. It includes these topics:

- Getting Started with the Configuration
- Using the Access Point Setup Wizard
- Changing the Default Password
- Quick Start Configuration
- Window Navigation

Getting Started with the Configuration

This section describes system requirements and how to access the web-based Configuration Utility.

Supported Browsers

Before you begin to use the configuration utility, make sure that you have a computer with Internet Explorer 7.0 or later, Firefox 3.0 or later, Chrome 5.0 or later, or 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 then 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

Follow these steps to access the configuration utility from your computer to configure the WAP device:

STEP 1 Connect the WAP device to the same network (IP subnet) as your computer. The factory default IP address configuration of the WAP device is DHCP. Make sure that your DHCP server is running and can be reached.

STEP 2 Locate the IP address of the WAP device.

a. The WAP device can be accessed and managed by Cisco network tools and services including the Cisco FindIT Network Discovery Utility that enables you to automatically discover all supported Cisco devices in the same local network segment as your computer. You can get a snapshot view of each device or launch the product configuration utility to view and configure the settings. For more information, see http://www.cisco.com/go/findit.

b. The WAP device is Bonjour-enabled and automatically broadcasts its services and listens for services being advertised by other Bonjour-enabled devices. If you have a Bonjour-enabled browser, such as Microsoft Internet Explorer with a Bonjour plug-in, or the Apple Mac Safari browser, you can find the WAP device on your local network without knowing its IP address.

   You can download the complete Bonjour for Microsoft Internet Explorer browser from Apple's website by visiting: http://www.apple.com/bonjour/.

c. Locate the IP address assigned by your DHCP server by accessing your router or DHCP server. See your DHCP server instructions for more information.

STEP 3 Launch a web browser, such as Microsoft Internet Explorer.

STEP 4 In the address bar, enter the default DHCP address and press the **Enter** key.

STEP 5 Enter the default user name of **cisco** and password of **cisco** in the **Username** and **Password** fields.

STEP 6 Click **Log In**. The Access Point Setup Wizard appears.

Follow the Setup Wizard instructions to finish the WAP device installation. We strongly recommend that you use the Setup Wizard for the first installation. See **Using the Access Point Setup Wizard** for more information.

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 configuration.

NOTE If you click **Cancel** to bypass the wizard, the Change Password page appears. You can then change the default password for logging in (see **Changing the Default Password** for more information). For all other settings, the factory default configurations apply.

Configuring Cisco WAP131 Setup Wizard

Follow these steps to complete the wizard (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 click **Static IP Address** to configure the IP address manually. For a description of these fields, see **IPv4 Setting**.

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

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

STEP 5 Click **Next**. The Configure Device - Set Password window appears.

STEP 6 Enter a new password in the **New Password** field and enter it again in the **Confirm Password** field.

NOTE Uncheck **Password Complexity** if you want to disable the password security rules. However, we strongly recommend keeping the password security rules enabled. For more information about passwords, see **Password Complexity**.

STEP 7 Click **Next**. The Configure Radio 1 - Name Your Wireless Network window appears.

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

STEP 9 Click **Next**. The Configure Radio 1 - Secure Your Wireless Network window appears.

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

STEP 11 Click **Next**. The Configure Radio 1 - Assign The VLAN ID For Your Wireless Network window appears.

STEP 12 Enter a **VLAN ID** for traffic received on the wireless network.

We recommend 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 13 Click **Next**. Repeat the step 7 to step 12 to configure the settings for Radio 2 interface.

STEP 14 Click **Next**. The Summary - Confirm Your Settings window appears.

STEP 15 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 16 If they are correct, click **Submit**. Your WAP setup settings are saved and a confirmation window appears.

STEP 17 Click **Finish**.

The WAP device was configured successfully. You are required to log in again with the new password.

Configuring Cisco WAP351 Setup Wizard

Follow these steps to complete the wizard (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 click **Static IP Address** to configure the IP address manually. For a description of these fields, see **IPv4 Setting**.

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 the WAP device, click **Create a New Cluster** and enter a **New Cluster Name**. When you configure your devices with the same cluster name and enable the 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 the location 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 Choose 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 Configure Device - Set Password window appears.

STEP 8 Enter a **New Password** and enter it again in the **Confirm Password** field.

NOTE Uncheck **Password Complexity** if you want to disable the password security rules. However, we strongly recommend keeping the password security rules enabled. For more information about passwords, see **Password Complexity**.

STEP 9 Click **Next**. The Configure Radio 1 - 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 Configure Radio 1 - 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 **Configuring Security Settings**.

STEP 13 Click **Next**. The Configure Radio 1 - Assign The VLAN ID For Your Wireless Network window appears.

STEP 14 Choose the **VLAN ID** for traffic received on the wireless network.

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

STEP 15 Click **Next**. Repeat the step 9 to step 14 to configure the settings for Radio 2 interface.

STEP 16 Click **Next**. The Enable Captive Portal - Create Your Guest Network window appears.

STEP 17 Select whether or not to set up an authentication method for guests on your network, and click **Next**.

If you click **No**, skip to **Step 25**.

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

STEP 18 Specify a **Guest Network Name**.

STEP 19 Click **Next**. The Enable Captive Portal - Secure Your Guest Network window appears.

STEP 20 Choose a security encryption type for the guest network and enter a security key. For a description of these options, see **Configuring Security Settings**.

STEP 21 Click **Next**. The Enable Captive Portal - Assign the VLAN ID window appears.

STEP 22 Specify a VLAN ID for the guest network. The guest network VLAN ID should be different from the management VLAN ID.

STEP 23 Click **Next**. The Enable Captive Portal - Enable Redirect URL window appears.

STEP 24 Check **Enable Redirect URL** and enter a fully qualified domain name (FQDN) or IP address in the **Redirect URL** field (including http://). If specified, the guest network users are redirected to the specified URL after authenticating.

STEP 25 Click **Next**. The Summary - Confirm Your Settings window appears.

STEP 26 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 27 If they are correct, click **Submit**. Your setup settings are saved and a confirmation window appears.

STEP 28 Click **Finish**.

The WAP device was configured successfully. You are required to log in again with the new password.

Changing the Default Password

For security reasons, you are required to change the administrative password from its default settings at your first login. If you click **Cancel** to bypass the wizard, the Change Password page appears. You can then change the default password for logging in.

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

To change the default administrative password:

STEP 1 Enter the following fields to set a new password:

- **Old Password**—Enter the current password (default is **cisco**).
- **New Password**—Enter a new password.
- **Confirm Password**—Enter the new password again for confirmation.
- **Password Strength Meter**—Displays the strength of the new password.
- **Password Complexity**—The password complexity enabled by default requires the password to conform to the following complexity settings:
  - Is different from the user name.
  - Is different from the current password.
  - Has a minimum length of eight characters.
  - Contains characters from at least three character classes (uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard).

NOTE Check **Disable** next to the **Password Complexity** option if you want to disable the password complexity rules. However, we strongly recommend keeping the password complexity rules enabled.

STEP 2 Click **Save**.

The Getting Started page appears. You are now ready to configure the WAP device.

Quick Start Configuration

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

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
	Configure Port Settings	Port Settings
	Configure Single Point Setup (for WAP351 only)	Single Point Setup
Quick Access	Change Account Password	User Accounts
	Upgrade Device Firmware	Manage Firmware
	Backup/Restore Configuration	Manage Configuration File
Device Status	System Summary	System Summary
	Wireless Status	Network Interfaces

There are three hot links on the Getting Started page that take you to specific web pages for more information. You can:

- Click the **Support** link to direct you to the product support page.
- Click the **Forums** link to direct you to the Cisco Support Community page.
- Click the **Wireless Planning Tool** link to direct you to the AirMagnet Planner page.

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:

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 context-sensitive online help. The online help is designed to be viewed with browsers using UTF-8 encoding. If the online help shows errant characters, verify that the encoding settings on your browser are set to UTF-8.

Navigation Pane/Main Menu

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

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 of the WAP device. It contains these topics:

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**, or click **System Summary** under **Device Status** on the Getting Started page.

The following information is displayed:

- **PID VID**—The hardware model and version of the WAP device.
- **Serial Number**—The serial number of the WAP device.

- **Base MAC Address**—The MAC address of the WAP device.
- **Host Name**—A name assigned to the WAP device.
- **Power Source**—The system may be powered by a power adapter, or may be receiving power over Ethernet (PoE) from a Power Sourcing Equipment (PSE).
- **PSE Status** (For WAP351 Only)
  - **Overload**—Indicates that an attached Powered Device (PD) requires power from the WAP device that is exceeding the configured allocation any time during the connectivity.
  - **Down**—Indicates that there is no PD device connector or there is a malfunction.
  - **Up**—Indicates that PSE normally works on 802.3af mode.
- **PSE Power Consumption** (For WAP351 Only)—The power allocation for the connected PD device.
- **Firmware Version (Active Image)**—The firmware version number of the active image.
- **Firmware MD5 Checksum (Active Image)**—The checksum for the active image.
- **Firmware Version (Non-active)**—The firmware version number of the backup image.
- **Firmware MD5 Checksum (Non-active)**—The checksum for the backup image.
- **System Uptime**—The time that has elapsed since the last reboot.
- **System Time**—The current system time.

The TCP/UDP Service table shows basic information about protocols and services operating on the WAP device, including:

- **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 the packets are being transmitted and received.
  - **Established**—A connection session is established between the WAP device and a server or client, depending on each device's role with respect to this protocol.
  - **Time Wait**—The closing sequence has been initiated and the WAP device 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

The Network Interfaces page shows the configuration and status information about the wired and wireless interfaces.

To view network interface information, select **Status and Statistics** > **Network Interfaces**.

The following information is displayed:

- **LAN Status**—Displays information for LAN interface, including:
  - **MAC Address**—The MAC address of the WAP device.
  - **IP Address**—The IP address of the WAP device.
  - **Subnet Mask**—The subnet mask of the WAP device.

- **Default Gateway**—The default gateway of the WAP device.
- **Domain Name Server-1**—The IP address of the domain name server 1 used by the WAP device.
- **Domain Name Server-2**—The IP address of the domain name server 2 used by the WAP device.
- **IPv6 Address**—The IPv6 address of the WAP device.
- **IPv6 Autoconfigured Global Address**—The IPv6 auto-configured global address.
- **IPv6 Link Local Address**—The IPv6 link local address of the WAP device.
- **Default IPv6 Gateway**—The default IPv6 gateway of the WAP device.
- **IPv6-DNS-1**—The IPv6 address of the IPv6 DNS server 1 used by the WAP device.
- **IPv6-DNS-2**—The IPv6 address of the IPv6 DNS server 2 used by the WAP device.
- **Green Ethernet Mode** (For WAP131 Only)—The Green Ethernet mode is enabled or disabled on the WAP device.
- **VLAN ID** (For WAP131 Only)—The VLAN ID number of the WAP device.

These settings apply to the internal interface. Click the **Edit** link to change any of these settings. You will be redirected to the **IPv4 Setting** page.

- **Port Status** (For WAP351 Only)—Displays the status for all 5 interfaces (LAN1 to LAN5).
  - **Interface**—Number of the Ethernet interface.
  - **Port Status**—Status of the Ethernet interface.
  - **Port Speed**—Speed of the Ethernet interface.
  - **Duplex Mode**—Duplex mode of the Ethernet interface.

  Click the **Edit** link to change any of these settings. You will be redirected to the **Port Settings** page.
- **VLAN Status** (For WAP351 Only)—Displays information for all existed VLANs, including:
  - **VLAN ID**—Identifier of the VLAN.

- **Description**—Description of the VLAN.
- **LAN1-LAN5**—Ethernet interface status of the VLAN.

Click the **Edit** link to change any of these settings. You will be redirected to the **VLAN Configuration** page.

- **Radio Status**—Displays information for the wireless radio interfaces, including:
  - **Wireless Radio**—The wireless radio mode is enabled or disabled for the radio interface.
  - **MAC Address**—The MAC address associated with the radio interface.
  - **Mode**—The 802.11 mode (a/b/g/n) used by the radio interface.
  - **Channel**—The channel used by the radio interface.
  - **Operational bandwidth**—The operational bandwidth used by the radio interface.

  Click the **Edit** link to change any of these settings. You will be redirected to the **Radio** page.
- **Interface Status**—Displays status information for each Virtual Access Point (VAP) and on each Wireless Distribution System (WDS) interface, including:
  - **Interface**—The wireless interface of the WAP device.
  - **Name (SSID)**—The wireless interface name.
  - **Status**—The administrative status (up or down) of the VAP.
  - **MAC Address**— The MAC address of the radio interface.
  - **VLAN ID**—The VLAN ID of the radio interface.
  - **Profile**—The name of any associated scheduler profile.
  - **State**—The current state (active or inactive). The state indicates whether the VAP is exchanging data with a client.

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

Traffic Statistics

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

To view traffic statistics, select **Status and Statistics** > **Traffic Statistics**.

The following information is displayed:

- **Interface**—Name of the Ethernet interface, each VAP interface, and each WDS interface. The name for each VAP interface is followed by its SSID in parentheses.
- **Total Packets**—The total number of packets sent (in Transmit table) or received (in Received table) by the WAP device.
- **Total Bytes**—The total number of bytes sent (in Transmit table) or received (in Received table) by the WAP device.
- **Total Dropped Packets**—The total number of dropped packets sent (in Transmit table) or received (in Received table) by the WAP device.
- **Total Dropped Bytes**—The total number of dropped bytes sent (in Transmit table) or received (in Received table) by the WAP device.
- **Errors**—The total number of errors related to sending and receiving data on the 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. See **WorkGroup Bridge** for more information on configuring WorkGroup Bridges.

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

The Traffic Statistics table shows information for each network interface that is configured as a WorkGroup Bridge interface, including:

- **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.
- **Name (SSID)**—Wireless network name, also known as the SSID. This alphanumeric key uniquely identifies a wireless local area network.

The Transmit and Receive tables show information for the transmit and receive direction for each WorkGroup Bridge interface, including:

- **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

The Associated Clients page shows the client stations associated with a particular access point.

To view information for all associated clients, select **Status and Statistics** > **Associated Clients**.

The associated stations are shown along with the information about packet traffic transmitted and received for each station, including:

- **Total Number of Associated Clients**—The total number of clients currently associated with the WAP device.
- **Network Interface**—The VAP with which the client is associated.
- **Station**—The MAC address of the associated wireless client.
- **Status**—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 security mode of the WAP device is None or Static WEP, the authentication and association status of the 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 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**—The counters in the **From Station** column indicate the packets or bytes received by the wireless client. The counters in the **To Station** column 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 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 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 traffic stream downlink bandwidth, or for an access category requiring admission control to which the client STA has not been admitted.
- **Up Time (DD:HH:MM)**—The amount of time that the client has been associated with the WAP device.

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

Radio Statistics

The Radio Statistics page shows the packet-level and byte-level statistics for the wireless radio interface.

To view the radio statistics, select S**tatus and Statistics** > **Radio Statistics**.

The following information is displayed:

- **Packets Received**—Total number of packets received by the selected radio interface.
- **Packets Transmitted**—Total number of packets transmitted by the selected radio interface.
- **Bytes Received**—Total number of bytes received by the selected radio interface.
- **Bytes Transmitted**—Total number of bytes transmitted by the selected radio interface.
- **Packets Receive Dropped**—Number of packets received by the selected radio interface that were dropped.
- **Packets Transmit Dropped**—Number of packets transmitted by the selected radio interface that were dropped.
- **Bytes Receive Dropped**—Number of bytes received by the selected radio interface that were dropped.
- **Bytes Transmit Dropped**—Number of bytes transmitted by the selected radio interface that were dropped.
- **Fragments Received**—Number of fragmented frames received by the selected radio interface.
- **Fragments Transmitted**—Number of fragmented frames sent by the selected radio interface.
- **Multicast Frames Received**—Number of MSDU frames received with the multicast bit set in the destination MAC address.
- **Multicast Frames Transmitted**—Number of successfully transmitted MSDU frames where the multicast bit was set in the destination MAC address.
- **Duplicate Frame Count**—Number of times that a frame was received and the **Sequence Control** field indicates it was a duplicate.

- **Failed Transmit Count**—Number of times that an MSDU was not transmitted successfully due to transmit attempts exceeding either the short retry limit or the long retry limit.
- **FCS Error Count**—Number of FCS errors detected in a received MPDU frame.
- **Transmit Retry Count**—Number of times that an MSDU is successfully transmitted after one or more retries.
- **ACK Failure Count**—Number of ACK frames not received when expected.
- **RTS Failure Count**—Number of CTS frames not received in response to an RTS frame.
- **WEP Undecryptable Count**—Number of frames discarded because they cannot 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**—Number of CTS frames received in response to an RTS frame.
- **Multiple Retry Count**—Number of times that an MSDU is successfully transmitted after more than one retry.
- **Frames Transmitted Count**—Number 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 shows information about the email alerts sent based on the SYSLOG messages generated in the WAP device.

To view the email alert status, select **Status and Statistics** > **Email Alert Status**.

The following information is displayed:

- **Email Alert Status**—Shows if the Email Alert is enabled or disabled on the WAP device. 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.

View Log

The View Log page shows a list of system events that generated the log entries, such as login attempts and configuration changes. The log is cleared upon a reboot and can be cleared by an administrator. Up to 1000 events can be shown. Older entries are removed from the list as needed to make room for new events.

To view the logs, select **Status and Statistics** > **View Log**.

The following information is displayed:

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

You can filter the current log through **Severity** and **Key words**.

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.

TSPEC Client Associations

The TSPEC Client Associations page shows the real-time information about the TSPEC client data transmitted and received by the WAP device. The tables on the TSPEC Client Associations page show the voice and video packets transmitted and received since the association started, along with the 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) that 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 the TSPEC client association statistics, select **Status and Statistics** > **TSPEC Client Associations**.

The Status and Statistics table displays the following information:

- **Network Interface**—Radio interface used by the client.
- **SSID**—Service set identifier associated with this traffic stream client.
- **Station**—Station MAC address of the client.
- **TS Identifier**—TSPEC traffic session identifier. (range 0 to 7)
- **Access Category**—Traffic stream access category (voice or video).
- **Direction**—Traffic direction for this traffic stream. 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 traffic stream. 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**—MAC address of the Virtual Access Point (VAP).

The Statistics table displays the following information

- **Network Interface**—Radio interface used by the client.
- **Station**—Station MAC address of the client.

- **TS Identifier**—TSPEC traffic session identifier. (range 0 to 7)
- **Access Category**—Traffic stream access category (voice or video).
- **Direction**—The traffic direction for this traffic stream. 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**—Shows 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 shows the summary information about TSPEC sessions by radio, the summary information about TSPEC sessions by VAP, and the real-time transmit and receive statistics for the radio interface and the network interfaces.

All transmit and receive statistics shown on the page 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 the TSPEC status and statistics, select **Status and Statistics** > **TSPEC Status and Statistics**.

The following information for the WLAN (radio) and VAP interfaces is displayed:

- **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 traffic stream.
- **Medium Time Unallocated**—Time of unused bandwidth for this access category.

The following statistics appear separately for the transmit and receive paths on the wireless radio interface:

- **Wireless Radio**—Name of the radio interface.
- **Access Category**—The access category associated with this traffic stream (voice or video).
- **Total Packets**—Total number of traffic stream 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.

The following appear separately for the transmit and receive paths on the network interfaces (VAPs):

- **Interface**—Name of the VAP interface.
- **Total Voice Packets**—Total number of traffic stream voice packets sent (in Transmit table) or received (in Received table) by this WAP device for this VAP.

- **Total Voice Bytes**—Total number of traffic stream voice bytes sent (in Transmit table) or received (in Received table) by this WAP device for this VAP.
- **Total Video Packets**—Total number of traffic stream video packets sent (in Transmit table) or received (in Received table) by this WAP device for this VAP.
- **Total Video Bytes**—Total number of traffic stream 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 shows information on the voice and video traffic streams accepted and rejected by the WAP device.

To view the TSPEC AP statistics, select **Status and Statistics** > **TSPEC AP Statistics**.

The following information is displayed:

- **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.

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
- Manage Firmware
- Manage Configuration File
- Reboot
- Discovery—Bonjour
- Packet Capture
- Support Information
- Spanning Tree Settings

System Settings

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

To configure system settings:

STEP 1 Select **Administration** > **System Settings**.

STEP 2 Configure these parameters:

- **Host Name**—Enter the host name for the WAP device. By default, the name is the fully qualified domain name (FQDN) of the node. The default host name is **wap** concatenated with the last 6 hexidecimal digits of the MAC address of the WAP device. The host name label can contain only letters, digits, and hyphens. It cannot begin or end with a hyphen. No other symbols, punctuation characters, or blank spaces are permitted. The host name can be 1 to 63 characters long.
- **System Contact**—Enter the contact person for the WAP device. The system contact can be 0 to 255 characters long and can include spaces and special characters.
- **System Location**—Enter the physical location of the WAP device. The system location can be 0 to 255 characters long and can include spaces and special characters.

STEP 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**

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**.

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

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

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

STEP 3 Check the box for the new user and click **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** field.

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

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

STEP 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 click **Delete**. To save your deletion permanently, click **Save** when complete.

Changing a User Password

To change a user password:

STEP 1 Select **Administration** > **User Accounts**.

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** field.

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

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

STEP 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.

Automatically Acquiring the Time Settings through NTP

To automatically acquire the time settings from a NTP server:

STEP 1 Select **Administration** > **Time Settings**.

STEP 2 In the **System Clock Source** area, choose **Network Time Protocol (NTP)**.

STEP 3 Configure these parameters:

- **NTP Server(1 through 4)/IPv4/IPv6 Address/Name**—Specify the IPv4 address, IPv6 address, or host name of an NTP server. A default NTP server is listed.

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

- **Time Zone**—Select the time zone for your location.
- **Adjust Time for Daylight Savings**—If daylight savings time is applicable to your time zone, check this option and configure the following 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.

Manually Configuring the Time Settings

To manually configure the time settings:

STEP 1 Select **Administration** > **Time Settings**.

STEP 2 In the **System Clock Source** area, choose **Manually**.

STEP 3 Click **Cloning** next to the **Clone PC Time** field to clone the system time settings from your local PC.

STEP 4 You can also configure the following fields:

- **System Date**—Select the current month, day, and year date from the drop-down lists.
- **System Time**—Select the current hour and minutes in 24-hour clock format.
- **Time Zone**—Select the time zone for your location.
- **Adjust Time for Daylight Savings**—If daylight savings time is applicable to your time zone, check this option and configure the following 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 5 Click **Save**. The changes are saved to the Startup Configuration.

Log Settings

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

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**.

STEP 2 Configure these parameters:

- **Persistence**—Check **Enable** to save system logs to nonvolatile memory so that the logs are kept when the WAP device reboots. You can save up to 1000 log messages in the nonvolatile memory. When the limit of 1000 is

reached, the oldest log message is overwritten by the newest message. Clear this field to save system logs to volatile memory. Logs in volatile memory are deleted when the system reboots.

- **Severity**—Select the severity that an event must have for it to be written to the log in nonvolatile memory, the other will be written to volatile memory.
- **Depth**—Enter the maximum number of messages, up to 1000, that can be stored in volatile memory. When the number that you configure in this field is reached, the oldest log event is overwritten by the newest log event. Note that the maximum number of log messages that can be stored in nonvolatile memory (the persistent log) is 1000, which is not configurable.

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

Configuring Remote Log Server

The kernel log is a comprehensive list of system events and kernel messages such as error conditions.

You cannot view kernel log messages directly from the configuration utility. 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. The WAP device supports up to two remote log servers.

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

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

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

STEP 1 Select **Administration** > **Log Settings**.

STEP 2 In the **Remote Log Server Table**, configure these parameters :

- **Remote Log Server**—Enter the IPv4 or IPv6 address, or the host name of the remote log server.

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

- **Enable**—Check to enable this remote log server, and then define the log severity and UDP port.
- **Log Severity**—Check the severities that an event must have for it to be sent to remote log server.
- **UDP Port**—Enter the logical port number for the syslog process on the remote host. The range is from 1 to 65535. The default port is 514.

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

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

If you enable a remote log server, 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 configuration.

If you disabled a remote log server, clicking **Save** disables remote logging.

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

Email Alert

Use the Email Alert page to send messages to the configured email addresses when particular system events occur.

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

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.

Configuring Email Alert Settings

To configure the WAP device to send email alerts:

STEP 1 Select **Administration** > **Email Alert**.

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

- **Administrative Mode**—Enable or disable 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**—Enter the frequency at which scheduled messages are sent. The range is from 30 to 1440 minutes. The default is 30 minutes.
- **Scheduled Message Severity**—Specify the severity that an event must have for it to be sent to the configuration email address at the frequency specified by the **Log Duration**. The default severity is Emergency, Alert, Critical, Error and Warning.
- **Urgent Message Severity**—Specify the severity that an event must have for it to be sent to the configured email address immediately. The default is Emergency and Alert.

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

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

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

- **Data Encryption**—Choose the mode of security for the outbound email alert. The alert can be sent using the secure TLS protocol or the default Open protocol. Using the secure TLSv1 protocol can prevent eavesdropping and tampering during the communication across the public network.
- **Port**—Enter the SMTP port number to use for outbound emails. The range is a valid port number from 0 to 65535. The default port is 465. The port generally depends on the mode used by the email provider.
- **Username**—Enter the user name for the email account that will be used to send these emails. Typically (but not always) the user name is the full email address including the domain (such as Name@example.com). The specified account will be used as the email address of the sender. The user name can 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 In the **Message Configuration** area, configure the email addresses and subject line:

- **To Email Address 1/2/3**—Enter up to three addresses to receive 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 the web-based management connections. If HTTPS is used for secure management sessions, you can also use this page to manage the required SSL certificates.

Configuring HTTP and HTTPS Services

To configure the HTTP and HTTP services:

STEP 1 Select **Administration** > **HTTP/HTTPS Service**.

STEP 2 In the **Global Settings** area, configure these parameters:

- **Maximum Sessions**—Enter 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 configuration utility of the WAP device, 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**—Enter the maximum amount of time, in minutes, that an inactive user remains logged on to the 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 the HTTP and HTTPS services:

- **HTTP Server**—Enable or disable access through HTTP. By default, HTTP access is enabled. If you disable it, any current connections using that protocol are disconnected.
- **HTTP Port**—Enter 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**—Enable or disable access through secure HTTP (HTTPS). By default, HTTPS access is enabled. If you disable it, any current connections using that protocol are disconnected.
- **HTTPS Port**—Enter the logical port number to use for HTTPS connections, from 1025 to 65535. The default port number for HTTPS 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 the HTTPS services, the WAP device must have a valid SSL certificate. The WAP device can generate a certificate, or you can download it from your network or from a TFTP server.

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

In the **SSL Certificate File Status** area, you can view 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/HTTPS** or **TFTP** for the **Download Method** and then click **Download**.

- If you select HTTP/HTTPS, 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/HTTPS** or **TFTP** for the **Upload Method**.

- For HTTP/HTTPS, 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 configuration utility of the WAP device. If this feature is disabled, anyone can access the configuration utility from any network client by supplying the correct user name and password of the WAP device.

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. We recommend that you 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**.

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.

Manage Firmware

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

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

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

NOTE When you upgrade the firmware, the WAP device retains the existing configuration information.

Swapping the Firmware Image

To swap the firmware image running on the WAP device:

STEP 1 Select **Administration** > **Manage Firmware**.

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

STEP 2 Click **Swap Active Image**.

A dialog box appears confirming the firmware image switch and subsequent reboot.

STEP 3 Click **OK** to proceed.

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

TFTP Upgrade

To upgrade the firmware on the WAP device using TFTP:

STEP 1 Select TFTP as the transfer method.

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

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

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

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

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

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

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

HTTP/HTTPS Upgrade

To upgrade using HTTP/HTTPS:

STEP 1 Select **HTTP/HTTPS** as the 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 **Browse** and locate the firmware image file on your network.

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

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

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

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

Manage 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 WAP device 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.

Backup Configuration File

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

STEP 1 Select **Administration** > **Manage Configuration File**.

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 that 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/HTTPS backups, a window appears to enable you to browse to the desired location for saving the file.

Download 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** > **Manage Configuration File**.

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 to replace 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/HTTPS downloads, a window appears to enable you to browse to select the file to download.

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

Copy/Save Configuration

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

To copy a file to another file type:

STEP 1 Select **Administration** > **Manage Configuration File**.

STEP 2 In the **Source File Name** field, select one of the following source file types that you want to copy:

- **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 In the **Destination File Name** field, select the file type to be replaced with the file that you are copying.

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

Configuration Files Properties

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

To delete the Startup Configuration or Backup Configuration file:

STEP 1 Select **Administration** > **Manage Configuration File**.

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

STEP 3 Click **Clear Files**.

Reboot

Use the Reboot page to reboot the WAP device or reset the WAP device to its factory defaults.

To reboot or reset the WAP device:

STEP 1 Select **Administration** > **Reboot**.

STEP 2 To reboot the WAP device using Startup Configuration, click **Reboot**.

STEP 3 To reboot the WAP device using the factory default configuration file, click **Reboot To Factory Default**. Any customized settings are lost.

NOTE A window appears prompting you to confirm or cancel the reboot. The current management session may be terminated.

STEP 4 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 your environments.

The WAP device advertises these service types:

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

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

A system administrator can use an installed Internet 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**.

STEP 2 Enables or disables Bonjour on the WAP device.

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

Packet Capture

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

There are two methods of packet capture:

- **Local capture method**— Captured packets are stored in a file on the WAP device. The WAP device can transfer the file to a TFTP server. The file is formatted in pcap format and can be examined using 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 the radio interfaces. Packets captured on the radio interfaces include the 802.11 header.
- 802.3 packets received and transmitted on the Ethernet interface.
- 802.3 packets received and transmitted on the internal logical interfaces, such as VAPs and WDS interfaces.

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

Packet Capture Configuration

To configure packet capture settings:

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

STEP 2 In the **Packet Capture Configuration** area, 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 the 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 the 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 only capture the 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 that the MAC filter is active only when a capture is performed on an 802.11 interface.
- **Packet Capture Method**—Choose 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 3 Depending on the selected method, refer to the steps in the **Local Packet Capture** or **Remote Packet Capture** section to continue.

NOTE Changes to the packet capture configuration parameters take affect after the 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 Select **Administration** > **Packet Capture**.

STEP 2 Ensure that **Local File** is selected for the **Packet Capture Method**.

STEP 3 Configure these parameters:

- **Capture Interface** (For WAP131 Only)—Enter a capture interface type for packet capture:

- **Radio 1/Radio 2**—802.11 traffic on the radio interface.
- **Ethernet**—802.3 traffic on the Ethernet port.
- **Radio 1 - VAP0/Radio 2 - VAP0**—VAP0 traffic.
- **Radio 1 - VAP1** to **Radio 1 - VAP3** (if configured)—Traffic on the specified VAP.
- **Radio 2 - VAP1** to **Radio 2 - VAP3** (if configured)—Traffic on the specified VAP.
- **Radio 1 - WDS0 to Radio 1 - WDS3** (if configured)—Traffic on the specified WDS.
- **Radio 2 - WDS0 to Radio 2 - WDS3** (if configured)—Traffic on the specified WDS.
- **Brtrunk**—Linux bridge interface in the WAP device.

▪ **Capture Interface** (For WAP351 Only)—Enter a capture interface type for packet capture:

- **Radio 1/Radio 2**—802.11 traffic on the radio interface.
- **LAN1** to **LAN5**—802.3 traffic on the Ethernet port.
- **Radio 1 - VAP0/Radio 2 - VAP0**—VAP0 traffic.
- **Radio 1 - VAP1** to **Radio 1 - VAP7** (if configured)—Traffic on the specified VAP.
- **Radio 2 - VAP1** to **Radio 2 - VAP7** (if configured)—Traffic on the specified VAP.
- **Radio 1 - WDS0** to **Radio 1 - WDS3**(if configured)—Traffic on the specified WDS.
- **Radio 2 - WDS0** to **Radio 2 - WDS3**(if configured)—Traffic on the specified WDS.
- **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 kilobytes (KB). The range is from 64 to 4096. The default is 1024.

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

STEP 5 Click **Start Capture**.

In Packet File Capture mode, the WAP device stores the captured packets in the RAM file system. Upon activation, the packet capture proceeds until one of these events occurs:

- The capture time reaches the configured duration.
- The capture file reaches its maximum size.
- The administrator stops the capture.

Remote Packet Capture

The Remote Packet Capture feature enables you to specify a remote port as the destination 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 the 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 the remote capture mode is in use, the WAP device does not store any captured data locally in its file system.

If a firewall is installed between the Wireshark computer and the WAP device, the 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 Select **Administration** > **Packet Capture**.

STEP 2 Enable **Promiscuous Capture**.

STEP 3 For the **Packet Capture Method**, select **Remote**.

STEP 4 In the **Remote Capture Port** field, use the default port (2002), or if you are using a port other than the default, enter the desired port number used 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**. However, the selection of **Remote** as the **Packet Capture Method** is not saved.

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, click **Capture > Options**. A popup window appears.

STEP 3 In the **Interface** field, select **Remote**. A popup window appears.

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

STEP 5 In the **Port** field, enter the port number of the WAP device. For example, enter 2002 if you used the default, or enter the port number if you used a port other than the default.

STEP 6 Click **OK**.

STEP 7 Select the interface from which you need to capture the packets. At the Wireshark popup window, next to the IP address, there is a drop-down menu to select the interfaces. The interface can be one of the following:

Linux bridge interface in the wap device
`--rpcap://[192.168.1.220]:2002/brtrunk`
Wired LAN interface
`-- rpcap://[192.168.1.220]:2002/eth0`
VAP0 traffic on radio 1
`-- rpcap://[192.168.1.220]:2002/wlan0`
802.11 traffic
`-- rpcap://[192.168.1.220]:2002/radio1`
At WAP351, VAP1 ~ VAP7 traffic
`-- rpcap://[ 192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7`
At WAP131, 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 port range 58000-58004

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

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

tool. When capturing 802.11 traffic, a large portion of the captured frames tends to be beacons (typically sent every 100 ms by all access points). Although Wireshark supports a display filter for beacon frames, it does not support a capture filter to prevent the WAP device from forwarding the captured beacon packets to the Wireshark tool. To reduce the performance impact of capturing the 802.11 beacons, disable the capture beacons mode.

Packet Capture Status

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

- **Current Capture Status**—Whether the packet capture is running or stopped.
- **Packet Capture Time**—The elapsed capture time.
- **Packet Capture File Size**—The Local File capture file size; cannot record Remote capture file size.

Click **Refresh** to show the latest data from the WAP device, or click **Stop Capture** to stop a packet file capture.

Packet Capture File Download

You can download a capture file by TFTP to a configured TFTP server, or by HTTP/HTTPS to a computer. A capture is automatically stopped when the capture file download command is triggered.

Because the capture file is located in the RAM file system, it disappears if the WAP device is reset.

To download a packet capture file using TFTP:

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

STEP 2 Check **Use TFTP to download the capture file**.

STEP 3 Enter the **TFTP Server Filename** to download if it is different from the default. By default, the captured packets are stored in the folder file /tmp/apcapture.pcap on the WAP device.

STEP 4 Specify a **TFTP Server IPv4 Address** in the field provided.

STEP 5 Click **Download**.

To download a packet capture file using HTTP/HTTPS:

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

STEP 2 Uncheck **Use TFTP to download the captured file**.

STEP 3 Click **Download**. A confirmation window appears.

STEP 4 Click **OK**. A dialog box displays that enables you to choose a network location to save the file.

Support Information

Use the Support Information page to download a text file that contains detailed configuration information about the WAP device. This file includes the 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 the technical support personnel to assist them in troubleshooting problems.

To download the support information:

STEP 1 Select **Administration** > **Support Information**.

STEP 2 Click **Download** to generate the file based on the current system settings. After a short pause, a window appears to enable you to save the file to your computer.

Spanning Tree Settings

Use the Spanning Tree Settings page to configure the STP settings on the Cisco WAP351. It supports the configuration per port or on the whole device.

NOTE You can go to the **WDS Bridge** page to configure the STP settings for the Cisco WAP131.

To configure the STP settings on the Cisco WAP351:

STEP 1 Select **Administration** > **Spanning Tree Settings**.

STEP 2 Configure these parameters:

- **STP Status**—Enables or disables STP globally on the Cisco WAP351. By default, STP is enabled.
- **Flood BPDU if STP is disabled on port(s)**—Check to flood the BPDU packets received from the port(s) whose STP status is disabled, or uncheck to drop the BPDU packets received from the port(s) whose STP status is disabled.
- **Per Port STP Status Setting**—Check to enable STP on a port, or uncheck to disable STP on a port.

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

4

LAN

This chapter describes how to configure the port, VLAN, IPv4, and IPv6 settings of the WAP device. It includes these topics:

- Port Settings
- VLAN Configuration
- IPv4 Setting
- IPv6 Setting

Port Settings

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

Configuring Port Settings for Cisco WAP131

To configure the port settings:

STEP 1 Select **LAN** > **Port Settings**.

The **Operational Status** area shows the type of the port used for the LAN port and the link characteristics, as configured in the **Administrative Settings** area. If the settings change through configuration or autonegotiation, 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 **Auto Negotiation** is disabled, choose the **Port Speed** (10/100 Mbps) and the duplex mode (Half- or Full-duplex).

STEP 4 Enable or disable the **Green Ethernet Mode**.

- Green Ethernet Mode supports both auto-power-down mode and EEE (Energy Efficient Ethernet, IEEE 802.3az) mode. Green Ethernet Mode works only when the port has auto-negotiation enabled.
- The auto-power-down mode reduces the chip power when the signal from a link partner is not present. The WAP device automatically enters a low-power mode when the energy on the line is lost, and it resumes normal operation when the energy is detected.
- The EEE mode supports QUIET times during low link utilization, allowing both side of a link to disable the portions of each PHY's operating circuit and save power.

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

Configuring Port Settings for Cisco WAP351

To configure the port settings:

STEP 1 Select **LAN** > **Port Settings**.

The Port Settings Table includes the following status and configurations for all 5 Interfaces (LAN1 to LAN5):

- **Port Status**—Shows the current port link status.
- **Port Speed**—In review mode, it shows the current port speed. In edit mode, if Auto Negotiation is disabled, select a port speed such as 100 Mbps or 10 Mbps. 1000 Mbps speed is only supported through Auto-Negotiation enabled).
- **Duplex Mode**—In review mode, it shows the current port duplex mode. In edit mode, if Auto Negotiation is disabled, select either Half-Duplex or Full-Duplex.
- **Auto Negotiation**—When enabled, the port negotiates with its link partner to set the fastest link speed and duplex mode available. When disabled, you can manually configure the **Port Speed** and **Duplex Mode**.

- **Green Ethernet**—Green Ethernet Mode supports both auto-power-down mode and EEE (Energy Efficient Ethernet, IEEE 802.3az) mode. Green Ethernet Mode works only when the port has auto-negotiation enabled. Auto-power-down mode reduces chip power when the signal from a link partner is not present. 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. EEE mode supports QUIET times during low link utilization, allowing both side of a link to disable portions of each PHY's operating circuit and save power.
- **Jumbo Frames**—When enabled, the port supports packet length up to 9720 bytes. Otherwise, the port supports packet length up to 2000 bytes. The Jumbo Frame is supported only when link speed is in 1000 Mbps mode. Because the wireless interface does not support Jumbo Frames, it only works to forward packets between Ethernet (LAN1 to LAN5) ports. So it is better to disable it.
- **CoS** (port VLAN priority, 802.1p Class of Service)—Assigns the 802.1p class of service (CoS) when the port receives an untagged packet.

STEP 2 Check the interfaces that you want to edit, then click the **Edit** button to enter the edit mode. Then input your settings.

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

VLAN Configuration

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

Configuring VLAN Settings for Cisco WAP131

STEP 1 Select **LAN** > **VLAN Configuration**.

STEP 2 Configure these parameters:

- **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 WAP device 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 both the 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 that 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 Click **Save**. The changes are saved to the Startup Configuration.

Configuring VLAN Settings for Cisco WAP351

To configure the settings for a VLAN:

STEP 1 Select **LAN** > **VLAN Configuration**.

STEP 2 In the VLAN Setting Table, each VLAN record includes the following fields:

- **VLAN ID**—Indentifier of the VLAN. Each VLAN ID is ranged from 1 to 4094 and should be different with others VLAN ID.
- **Description**—Description of the related VLAN. The length should be fewer than 64 characters that are composed of A-Z, a-z, 0-9, _.
- **Management VLAN**—Management VLAN is the VLAN used to access the WAP device through Telnet or the web GUI. There must be one and only one VLAN as the management VLAN. If no interface (wire or wireless) belongs to the management VLAN, there will be no interface that a user can use to access the configuration utility.

- **LAN1 - LAN5**—Each port should have at most one untagged VLAN. The options are:
  - **Untagged**—The port is a member of the VLAN. A packet of the VLAN sent out from the port will be untagged. A untagged packet received by the port will be classified to the VLAN (tagged).
  - **Tagged**—The port is a member of the VLAN. A packet of the VLAN sent out from the port will be tagged with the VLAN header.
  - **Excluded**—The port does not belong to the VLAN.

NOTE The VLAN ID 1 cannot be deleted. If a port (wired or wireless) related to the VLAN has been deleted, the WAP device will set its VLAN ID to 1 automatically.

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

IPv4 Setting

Use the IPv4 Setting page to configure the static or dynamic IPv4 address assignment.

To configure the IPv4 address settings:

STEP 1 Select **LAN** > **IPv4 Setting**.

STEP 2 Configure these IPv4 settings:

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

  Choose one of these options:
  - **DHCP**—The WAP device acquires its IP address from a DHCP server on the LAN.
  - **Static IP**—Manually configure the IPv4 address. The IPv4 address should be in a form similar to xxx.xxx.xxx.xxx (192.0.2.10).

- **Static IP Address, Subnet Mask, and Default Gateway**—If you want to assign a static IP address, enter the IP information in these fields.
- **Domain Name Servers**—Select one of the following options:
  - **Dynamic**—The WAP device acquires the DNS server addresses from a DHCP server on the LAN.
  - **Manual**—Manually configure one or more DNS server addresses. Enter up to two IP addresses 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 condition happens, the WAP device may lose connectivity. We recommend that you change the WAP device settings when a loss of connectivity will least affect your wireless clients.

IPv6 Setting

Use the IPv6 Setting page to configure the WAP device to use IPv6 address and IPv6 tunnel.

To configure IPv6 address settings:

STEP 1 Select **LAN** > **IPv6 Setting**.

STEP 2 Configure these parameters:

- **IPv6 Connection Type**—Choose how the WAP device obtains an IPv6 address:
  - **DHCPv6**—The IPv6 address is assigned by a DHCPv6 server.
  - **Static IPv6**—Manually configure the IPv6 address. The IPv6 address should be in a form similar to xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).
- **IPv6 Administrative Mode**—Enables or disables IPv6 management access.
- **IPv6 Auto Configuration Administrative Mode**—Enables or disables 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**—Select one of the following options:
  - **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 Domain Name Servers**—Select one of the following options:
  - **Dynamic**—The DNS name servers are learned dynamically through DHCPv6.
  - **Manual**—Manually specify up to two IPv6 DNS name servers in the fields provided.

STEP 3 Configure an IPv6 tunnel using ISATAP.

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

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

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

- **ISATAP Status**—Enables or disables the administrative mode of ISATAP on the WAP device.
- **ISATAP Capable Host**—The IP address or DNS name of the ISATAP router. The default value is isatap.
- **ISATAP Query Interval**—Specifies how often the WAP device should send queries to the DNS server to attempt to resolve the ISATAP host name into an IP address. The WAP device sends DNS queries only when the IP address of an ISATAP router is unknown. The valid range is 120 to 3600 seconds. The default value is 120 seconds.
- **ISATAP Solicitation Interval**—Specifies how often the WAP device should send the router solicitation messages to the ISATAP routers that they learn about through the DNS query messages. The WAP device sends the router solicitation messages only when there is no active ISATAP router. The valid range is 120 to 3600 seconds. The default value is 120 seconds.

  NOTE When the tunnel is established, the **ISATAP IPv6 Link Local Address** and **ISATAP IPv6 Global Address** fields show on the page. These are the virtual IPv6 interface addresses to the IPv4 network.

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 condition happens, the WAP device may lose connectivity. We recommend that you change the WAP device settings when a loss of connectivity will least affect your wireless clients.

5

Wireless

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

- Radio
- Rogue AP Detection
- Networks
- Scheduler
- Scheduler Association
- Bandwidth Utilization
- MAC Filtering
- WDS Bridge
- WorkGroup Bridge
- Quality of Service

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 the wireless radio settings:

STEP 1 Select **Wireless** > **Radio**.

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

STEP 3 In the **Radio Setting Per Interface** area, select the radio interface to which the configuration parameters will be applied.

STEP 4 In the **Basic Settings** area, configure these parameters for the selected radio interface:

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

- **Radio**—Turns on or off the radio interface. By default, the radio is off.
- **MAC Address**—Shows the Media Access Control (MAC) address for the interface. The MAC address is assigned by the manufacturer and cannot be changed.
- **Mode**—Choose the IEEE 802.11 standard and frequency that the radio uses. The available modes are:
  - **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 MHz for 2.4 GHz and 20/40 MHz for 5 GHz.
- **Primary Channel** (802.11n modes with 20/40 MHz bandwidth only)—A 40 MHz channel can be considered to consist of two 20-MHz channels that are contiguous in the frequency domain. These two 20-MHz channels are often

referred to as the primary and secondary channels. The primary channel is used for 802.11n clients that support only a 20-MHz channel bandwidth and for legacy clients.

Choose one of these options:

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

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

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

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

STEP 5 In the **Advanced Settings** area, configure these parameters:

- **Short Guard Interval Supported**—This field is available only if the selected radio mode includes 802.11n. The guard interval is the dead time, in nanoseconds, between OFDM symbols. The guard interval prevents Inter-Symbol and Inter-Carrier Interference (ISI, ICI). The 802.11n mode allows for a reduction in this guard interval from the **a** and **g** definition of 800 nanoseconds to 400 nanoseconds. Reducing the guard interval can yield a 10 percent improvement in data throughput. The client with which the WAP device is communicating must also support the short guard interval.

  Choose one of these options:

  - **Yes**—The WAP device transmits data using a 400-nanosecond guard interval when communicating with clients that also support the short guard interval. This is the default selection.
  - **No**—The WAP device transmits data using an 800-nanosecond guard interval.

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

  You can disable the protection (Off); however, the legacy clients or the WAP devices within the range can be affected by 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 the 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 frames at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second). Enter an integer from 20 to 2000 milliseconds. The default is 100 milliseconds.

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

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

  The DTIM period 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 it to 1, the clients check for buffered data on the WAP device at every beacon. If you set it to 10, the clients check on every 10th beacon.

- **Fragmentation Threshold**—The frame size threshold 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 that 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, the fragmentation is not used. Setting the threshold to the largest value (2,346 bytes, which is the default) effectively disables the fragmentation.

The fragmentation involves more overhead both because of the extra work of dividing up and reassembling of frames that it requires, and because it increases message traffic on the network. However, the 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, the fragmentation is off. We recommend not using fragmentation unless you suspect the radio interference. The additional headers applied to each fragment increase the overhead on the network and can greatly reduce the throughput.

- **RTS Threshold**—The Request to Send (RTS) Threshold value. The valid integer range must be from 0 to 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 the traffic flow through the WAP device, especially one with a lot of clients. If you specify a low threshold value, the RTS packets are sent more frequently, which consumes more bandwidth and reduces the throughput of the packet. However, sending more RTS packets can help the network recover from interference or collisions that might occur on a busy network, or on a network experiencing electromagnetic interference.

- **Maximum Associated Clients**—The maximum number of stations allowed to access the WAP device at any one time. You can enter an integer between 0 and 200. The default is 200 stations.

- **Transmit Power**—A percentage value for the transmit power level for the 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 the WAP devices closer together and reduce the value of the transmit power. This setting helps reduce overlap and interference among the access points. A lower transmit power setting can also keep your network more secure because the weaker wireless signals are less likely to propagate outside of the physical location of your network.

Some channel ranges and country code combinations have relatively low maximum transmit power. When attempting to set the transmit power to the lower ranges (for example, 25 percent or 12 percent), 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 the wireless multicast video streaming occurs, provided the wireless clients are capable of handling the configured rate.

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

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

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

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

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

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

  - **Rate Limit**—The rate limit for multicast and broadcast traffic. 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, the TSPEC mode is off. The options are:
  - **On**—The WAP device handles TSPEC requests according to the TSPEC settings that you configure on the Radio page. Use this setting if the WAP device handles traffic from the 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 the 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 the voice priority traffic without requiring an admitted TSPEC. The WAP device ignores voice TSPEC requests from client stations.
- **TSPEC Voice ACM Limit**—The upper limit on the amount of traffic that the WAP device attempts to transmit on the wireless medium using a voice AC to gain access. The default limit is 20 percent of 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 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 condition happens, the WAP device may lose connectivity. We recommend that you change the WAP device settings when a loss of connectivity will least affect your wireless clients.

Rogue AP Detection

The Cisco WAP351 supports the Rogue AP detection feature. A Rogue AP is an access point that has been installed on a secure network without explicit authorization from a system administrator. Rogue APs 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.

NOTE The Rogue AP Detection feature is available only on the Cisco WAP351. The Cisco WAP131 does not support Rogue AP Detection.

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

Viewing the Rogue AP List

Rogue AP detection will not function until the wireless radio has been enabled. You should first enable the radio interface before you enable the Rogue AP detection for the radio interface.

To enable the radio to collect information about rogue APs:

STEP 1 Select **Wireless** > **Rogue AP Detection**.

STEP 2 Check **Enable** next to the **AP Detection for Radio 1** and **AP Detection for Radio 2** fields.

STEP 3 Click **Save**.

The Detected Rogue AP List table shows information for all detected rogue APs, and the Trusted AP List shows information for all trusted APs.

- **MAC Address**—The MAC address of the rogue AP.
- **Beacon Interval**—The beacon interval used by the rogue AP. Beacon frames are transmitted by an AP at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second). The Beacon Interval is set on the Radio page.
- **Type**—The type of the device. The options are:
  - **AP**—Indicates that the rogue device is an AP that supports the IEEE 802.11 Wireless Networking Framework in infrastructure mode.
  - **Ad hoc**—Indicates that the rogue station is running in Ad hoc mode. The stations set to the Ad hoc mode communicate with each other directly, without the use of a traditional AP. The Ad hoc mode is an IEEE 802.11 Wireless Networking Framework also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS).
- **SSID**—The Service Set Identifier (SSID) for the WAP device. 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. The options are:
  - **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. You can use the **Networks** page to configure the security settings on the WAP device.

- **WPA**—Shows whether the WPA security is on or off for the rogue AP.
- **Band**—The IEEE 802.11 mode being used on the rogue AP, such as IEEE 802.11a, IEEE 802.11b, IEEE 802.11g.

  The number shown indicates the mode:

  - 2.4 indicates IEEE 802.11b, 802.11g, or 802.11n mode (or a combination of the modes).
  - 5 indicates IEEE 802.11a or 802.11n mode (or both modes).
- **Channel**—The channel on which the rogue AP is currently broadcasting. The channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. You can use the **Radio** page to set the channel.
- **Rate**—The rate in megabits per second at which the rogue AP is currently transmitting. The current rate is always one of the rates shown in the Supported Rates field.
- **Signal**—The strength of the radio signal emitting from the rogue AP. If you hover the mouse pointer over the bars, a number representing the strength in decibels (dB) appears.
- **Beacons**—The total number of beacons received from the rogue AP since it was first discovered.
- **Last Beacon**—The date and time of the last beacon received from the rogue AP.
- **Rates**—Supported and basic (advertised) 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.

STEP 4 If the AP is in the Detected Rogue AP List, click **Trust** to move the AP to the Trusted AP List. If the AP is in the Trusted AP List, click **Untrust** to move the AP to the Detected Rogue AP List.

STEP 5 Click **Refresh** to refresh the screen and show the most current information.

Saving the Trusted AP List

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

STEP 1 Select **Wireless** > **Rogue AP Detection**.

STEP 2 In the Detected Rogue AP List, click **Trust** for the APs that are known to you. The trusted APs move to the Trusted AP List.

STEP 3 In the **Download/Backup Trusted AP List** area, click **Backup (AP to PC)**.

STEP 4 Click **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 may be acquired from another AP or created from a text file. If the MAC address of an AP appears in the Trusted AP List, it is not detected as a rogue.

To import an AP list from a file:

STEP 1 Select **Wireless** > **Rogue AP Detection**.

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

STEP 3 In the **Source File Name** field, click **Browse** to choose the file to import.

The 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 4 In the **File Management Destination** field, choose whether to replace the existing Trusted AP List or add the entries in the imported file to the Trusted AP List. The options are:

- **Replace**—Imports the list and replaces the contents of the Known AP List.
- **Merge**—Imports the list and adds the APs in the imported file to the APs currently shown in the Known AP List.

STEP 5 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 Cisco WAP131 and up to eight VAPs are supported on the Cisco WAP351.

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 It 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 Cisco WAP131 supports five active VLANs (four for WLAN plus one management VLAN). The Cisco WAP351 supports 17 active VLANs (16 for WLAN plus one management VLAN).

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

Configuring VAPs

To configure VAPs:

STEP 1 Select **Wireless** > **Networks**.

STEP 2 In the **Radio** field, click the radio interface to which the VAP configuration parameters are applied.

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

STEP 4 Check **Enable** for the VAP that you want to configure.

STEP 5 Configure these parameters:

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

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

  When a wireless client connects to the WAP device by using this VAP, the WAP device tags all traffic from the wireless client with the VLAN ID that 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.

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

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

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

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

  Specify whether to allow the WAP device to broadcast the SSID in its beacon frames. The Broadcast SSID parameter is enabled by default. When the VAP does not broadcast its SSID, the network name is not shown in the list of available networks on a client station. Instead, you must 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**—Choose the type of authentication required for access to the VAP. The options are:

  - None
  - Static WEP
  - Dynamic WEP
  - WPA Personal
  - WPA Enterprise

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

We recommend using WPA Personal or WPA Enterprise as the authentication type as it provides stronger security protection. Use Static WEP or Dynamic WEP only for legacy wireless computers or devices that do not support WPA Personal and WPA Enterprise. If you need to set security as Static WEP or Dynamic WEP, configure the 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 Filter**—Specifies whether the stations that can access this VAP are restricted to a configured global list of MAC addresses. You can choose one of these types of MAC filtering:
  - **Disabled**—Does not use MAC filtering.
  - **Local**—Uses the MAC authentication list that you configure on the **MAC Filtering** page.
  - **RADIUS**—Uses the MAC authentication list on an external RADIUS server.
- **Channel Isolation**—Enables and disables the station isolation.

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

  When enabled, the WAP device blocks communication between the wireless clients on the same VAP. The WAP device still allows data traffic between its wireless clients and the wired devices on the network, across a WDS link, and with other wireless clients associated with a different VAP, but not among the wireless clients.

STEP 6 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 condition happens, the WAP device may lose connectivity. We recommend that you change the WAP device settings when a loss of connectivity will least affect your wireless clients.

NOTE To delete a VAP, check 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 plus 24-bit initialization vector (IV)) or 128-bit (104-bit secret key plus 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**—Enter 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**— Choose either 64 bits or 128 bits as the length of the key.
- **Key Type**—Choose either ASCII or Hex as the key type.
- **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 the key type that 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 the key type.
- **802.1X Authentication**—The authentication algorithm defines the method used to determine whether a client station is allowed to associate with the WAP device when static WEP is the security mode.

  Specify the authentication algorithm that 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 plain text, 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, the 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, the 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.
- The 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 that 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 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 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.

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

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

- **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.

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 the wireless clients that support the original WPA.

These parameters configure WPA Personal:

- **WPA Versions**—Choose the types of client stations that you want to support:
  - **WPA-TKIP**—The network has some client stations that only support the original WPA and TKIP security protocol. Note that choosing only WPA-TKIP for access point is not allowed as per the latest WiFi Alliance requirement.
  - **WPA2-AES**—All client stations on the network support WPA2 and AES-CCMP cipher/security protocol. This WPA version provides the best security per IEEE 802.11i standard. As per the latest WiFi Alliance requirement, the AP has to support this mode all the time.

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

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

- **Key**—The shared secret key for WPA Personal security. Enter a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include uppercase and lowercase alphabetic letters, the numeric digits, and special symbols such as @ and #.
- **Show Key as Clear Text**—When enabled, the text you type is visible. When disabled, the text is not masked as you enter it.
- **Key Strength Meter**—The WAP device checks the key against complexity criteria such as how many different types of characters (uppercase and lowercase alphabetic letters, numbers, and special characters) are used and how long 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 the users.

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

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

These parameters configure WPA Enterprise:

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

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

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

  Client stations configured to use WPA with RADIUS must have one of these addresses and keys:
  - A valid TKIP RADIUS IP address and RADIUS Key
  - A valid CCMP (AES) IP address and RADIUS Key
- **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.

  Check this option to use the global RADIUS server settings, or uncheck this option to use a separate RADIUS server for the VAP and enter the RADIUS server IP address and key in the appropriate fields.
- **Server IP Address Type**—The IP version that the RADIUS server uses. You can toggle between the address types to configure the IPv4 and IPv6 global RADIUS address settings, but the WAP device contacts only the RADIUS server or servers for the address type that you select in this field.

- **Server IP Address 1** or **Server IPv6 Address 1**—The address for the primary RADIUS server for this VAP. 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 that 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 that 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 the 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 the scheduler status and add a scheduler profile:

STEP 1 Select **Wireless** > **Scheduler**.

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

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 that the radio or VAP can be operational. The rules are periodic in nature and are repeated every week. A valid rule must contain all of the 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 Choose 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, choose the recurring schedule for the rule. You can configure the rule to occur daily, each weekday, each weekend day (Saturday and Sunday), or any single day of the week.

STEP 5 Set the start and end times:

- **Start Time**—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**.

STEP 2 In the **Radio** area, select the radio interface to which the configuration parameters will be applied.

STEP 3 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 4 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 enabled by default.

To change bandwidth utilization settings:

STEP 1 Select **Wireless** > **Bandwidth Utilization** in the navigation pane.

STEP 2 Click **Enable** to enable Bandwidth Utilization, or uncheck **Enable** to disable this feature.

STEP 3 In the **Maximum Utilization Threshold** field, 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 condition happens, the WAP device may lose connectivity. We recommend that you change the 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 block or allow only listed client stations to authenticate with the WAP device. 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**.

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

- **Allow only stations in 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 condition happens, the WAP device may lose connectivity. We recommend that you change the 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
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 WAP devices. With WDS, the WAP devices communicate with one another without wires. This capability is critical in providing a seamless experience for roaming the 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 the 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 the 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 may be too far apart to be within cell range. When acting as a repeater, the WAP device does not have a wired connection to the LAN and repeats signals by using the wireless connection. No special configuration is required for the WAP device to function as a repeater, and there are no repeater mode settings. The wireless clients can still connect to an WAP device that is operating as a repeater.

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

- WDS only works with the Cisco WAP131 and Cisco WAP351 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)

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.

Configuring STP for Cisco WAP131

STEP 1 Select **Wireless** > **WDS Bridge**.

STEP 2 In the **Spanning Tree Mode** field, check **Enable** to enable STP mode on the Cisco WAP131.

When enabled, STP helps prevent switching loops. STP is recommended if you configure WDS links.

STEP 3 Click **Save**.

Configuring Untagged VLAN for Cisco WAP351

To configure the untagged VLAN for the Cisco WAP351:

STEP 1 Select **Wireless** > **WDS Bridge**.

STEP 2 Configure these parameters:

- **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 WAP device uses VLAN 1 as the default untagged VLAN. This setting 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**—Choose a VLAN ID from the VLAN ID list. 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.

STEP 3 Click **Save**.

Configuring WDS Bridge

To configure a WDS bridge:

STEP 1 Select **Wireless** > **WDS Bridge**.

STEP 2 Check **Enable** for **WDS Interface**.

STEP 3 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. 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 that 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 the security issues on the WDS link, you may decide not to set any type of encryption. Alternatively, if you have security concerns, you can choose 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** for more information about encryption options.

STEP 4 Repeat these steps for up to three additional WDS interfaces.

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

STEP 6 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 condition happens, the WAP device may lose connectivity. We recommend that you change the 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, choose either **ASCII** or **Hex** as the WEP key type.
- **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 that you have created. It is important that the same WDS ID is also entered at the other end of the WDS link. If this WDS ID is not the same for both WAP devices on the WDS link, they will not be able to communicate and exchange data.

  The WDS ID can be any alphanumeric combination.
- **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.

We recommend that you use the WorkGroup Bridge mode only when the WDS bridge feature cannot be operational with a peer WAP device. WDS is a better solution and is preferred over the WorkGroup Bridge solution. Use WDS if you are bridging the Cisco WAP131 and Cisco WAP351 devices. If you are not, then consider the 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 the downstream STAs. The BSS managed by the other WAP device (that is, the one to which the WAP device associates as an STA) is referred to as the infrastructure client interface, and the other WAP device is referred as the upstream AP.

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

The 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**.

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

STEP 3 In the **Radio Setting Per Interface** field, select the radio interface to which the configuration parameters will be applied.

STEP 4 Configure these parameters for the Infrastructure Client Interface (upstream):

- **SSID**—The SSID of the BSS. 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. The options are:

- None
- Static WEP
- WPA Personal
- WPA Enterprise

- **VLAN ID**—The VLAN associated with the BSS. 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 **Refresh** at the top of the page to view the latest connection status.

STEP 5 Configure the following additional fields for the Access Point Interface:

- **Status**—Check **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**—Check if you want the downstream SSID to be broadcast. SSID Broadcast is enabled by default.
- **Security**—The type of security to use for authenticating. The options are:
  - None
  - Static WEP
  - WPA Personal
- **MAC Filtering**—Choose 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 choose 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 6 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 the transmission queues for optimized throughput and better performance when handling differentiated wireless traffic, such as VoIP, other types of audio, video, streaming media, and traditional IP data.

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

The WAP Enhanced Distributed Channel Access (EDCA) parameters affect traffic flowing from the WAP device to the client station. The 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 the station EDCA should not need to be changed. Changing these values affects the QoS provided.

To configure the WAP device and Station EDCA parameters:

STEP 1 Select **Wireless** > **Quality of Service**.

STEP 2 Choose the radio interface (Radio1 or Radio2).

STEP 3 Choose one of these options from the **EDCA Template** list:

- **WFA Defaults**—Populates the WAP device and the Station EDCA parameters with WiFi Alliance default values, which are best for general, mixed traffic.

- **Optimized for Voice**—Populates the WAP device and the Station EDCA parameters with values that are best for voice traffic.
- **Custom**—Enables you to choose custom EDCA parameters.

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

- **Data 0 (Voice)**—High priority queue, 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 4 Configure the following EDCA and Station EDCA parameters:

NOTE These parameters are configurable only if you choose 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**—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 5 Configure the following additional settings:

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

STEP 6 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 condition happens, the WAP device may lose connectivity. We recommend that you change the WAP device settings when a loss of connectivity will least affect your wireless clients.

6

System Security

This chapter describes how to configure the security settings on the WAP device. It contains these topics:

- **RADIUS Server**
- **802.1X/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 the clients. The MAC address filtering feature, where the client access is restricted to a list, may also be configured to use a RADIUS server to control the access. The Captive Portal feature also uses RADIUS to authenticate the clients.

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

NOTE In addition to using the global RADIUS servers, you can also configure each VAP to use a specific set of RADIUS servers. See the **Networks** page for more information.

To configure global RADIUS servers:

STEP 1 Select **Security** > **RADIUS Server**.

STEP 2 Configure these parameters:

- **Server IP Address Type**—Select the IP version that the RADIUS server uses. You can toggle between the address types to configure IPv4 and IPv6 global RADIUS address settings, but the WAP device contacts only the RADIUS server or servers with the address type that you select in this field.
- **Server IP Address 1** or **Server IPv6 Address 1**—Enter the address for the primary global RADIUS server. When the first wireless client tries to authenticate with the WAP device, the WAP device sends an authentication request to the primary server. If the primary server responds to the authentication request, the WAP device continues to use this RADIUS server as the primary server, and authentication requests are sent to the address specified.
- **Server IP Address (2** through **4)** or **Server IPv6 Address** (**2** through **4)**—Enter the addresses for up to three backup IPv4 or IPv6 RADIUS servers. If authentication fails with the primary server, each configured backup server is tried in sequence.
- **Key 1**—Enter the shared secret key that the WAP device uses to authenticate to the primary RADIUS server. You can use from 1 to 64 standard alphanumeric and special characters. The key is case sensitive and must match the key configured on the RADIUS server. The text that you enter appears as asterisks.
- **Key** (**2** through **4**)—Enter 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.
- **Authentication Port**—Enter the port that the WAP device uses to connect to the primary RADIUS server.
- **Authentication Port (2** through **4)**—Enter the port associated with the configured backup RADIUS servers. The server at **Server IP (IPv6) Address 2** uses **Authentication Port 2**, the server at **Server IP (IPv6) Address 3** uses **Authentication Port 3**, and so on.

- **Enable RADIUS Accounting**—Enables tracking and measuring of the resources that 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/802.1X Supplicant

This section provides a description about the 802.1X feature and describes how to configure it.

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

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

Configure 802.1X Supplicant for Cisco WAP131

To configure the 802.1X supplicant settings:

STEP 1 Click **System Security** > **802.1X Supplicant**.

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.

STEP 2 In the **Supplicant Configuration** area, you can configure the 802.1X operational status and basic settings:

- **Administrative Mode**—Enables or disables the 802.1X supplicant functionality.

- **EAP Method**—Choose the algorithm to be used for encrypting authentication user names and passwords. The options are:
  - **MD5**—A hash function defined in RFC 3748 that provides basic security.
  - **PEAP**—Protected Extensible Authentication Protocol, which provides a higher level of security than MD5 by encapsulating it within a TLS tunnel.
  - **TLS**—Transport Layer Security, as defined in RFC 5216, an open standard that provides a high level of security.
- **Username**—The WAP device uses this user name when responding to requests from an 802.1X authenticator. The user name can be 1 to 64 characters long. ASCII-printable characters are allowed, which includes 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 In the **Certificate File Upload** area, you can upload a certificate file to the WAP device:

a. Choose either **HTTP** or **TFTP** as the **Transfer Method**.

b. If you selected HTTP, click **Browse** to select the file. See **HTTP/HTTPS Service** for more information on configuring the HTTP server settings.

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

d. Click **Upload**. A confirmation window appears, followed by a progress bar to indicate the status of the upload.

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 condition happens, the WAP device may lose connectivity. We recommend that you change the WAP device settings when a loss of connectivity will least affect your wireless clients.

Configure 802.1X for Cisco WAP351

To configure the 802.1X settings:

STEP 1 Click **System Security** > **802.1X**.

There are five ports coordinating with five LAN interfaces that you can set for 802.1X authentication in the Cisco WAP351.

STEP 2 Check a port and click **Edit**.

STEP 3 Select to enable or disable the supplicant or authenticator for the port.

- **Supplicant**—Enables the 802.1X supplicant functionality.
- **Authenticator**—Enables the 802.1X authenticator functionality.

STEP 4 If you enable the supplicant, click **Show Details** to configure these 802.1X supplicant parameters:

- **EAP Method**—Choose the algorithm to be used for encrypting authentication user names and passwords. The options are:
  - **MD5**—A hash function defined in RFC 3748 that provides basic security.
  - **PEAP**—Protected Extensible Authentication Protocol, which provides a higher level of security than MD5 by encapsulating it within a TLS tunnel.
  - **TLS**—Transport Layer Security (TLS), as defined in RFC 5216, an open standard that provides a high level of security.
- **Username**—The WAP device uses this user name when responding to the requests from an 802.1X authenticator. The user name 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 the 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.

  NOTE The user name and password that are encrypted using the MD5 algorithm can be configured to allow the WAP device to authenticate using 802.1X.
- **Certificate File Status**—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.

▪ **Certificate File Upload**—Enables you to upload a certificate file to the WAP device. You can:

- Choose either HTTP or TFTP as the **Transfer Method**.
- If you selected HTTP, click **Browse** to select the file. See **HTTP/HTTPS Service** for more information on configuring the HTTP server settings. 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.
- Click **Upload**. A confirmation window appears, followed by a progress bar to indicate the status of the upload.

STEP 5 If you enable the authenticator, click **Show Details** to configure these parameters:

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

Check to use the global RADIUS server settings, or uncheck to use a separate RADIUS server for a port and enter the **Server IP Address** or **Server IPv6 Address**, **Key**, and **Authentication Port** 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 Ethernet port.

  When the first PC plugs in and 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.
- **Authentication Port**—The port that the WAP device uses to connect to the primary RADIUS server.
- **Authentication Port 2** to **4**—The port associated with the configured backup RADIUS servers. The server at **Server IP (IPv6) Address 2** uses **Authentication Port 2**, the server at **Server IP (IPv6) Address 3** uses **Authentication Port 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.
- **Periodic Reauthentication**—Enables EAP reauthentication.
- **Reauthentication Period**—Enter the EAP reauthentication period in seconds. The default is 3600. The valid range is from 300 to 4294967295 seconds.

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 condition happens, the WAP device may lose connectivity. We recommend that you change the WAP device settings when a loss of connectivity will least affect your wireless clients.

Password Complexity

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

To configure the password complexity requirements:

STEP 1 Select **Security** > **Password Complexity**.

STEP 2 Check **Enable** next to the **Password Complexity** field.

STEP 3 Configure these parameters:

- **Password Minimum Character Class**—Enter the minimum number of character classes that must be represented in the password string. The four possible character classes are uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard.
- **Password Different From Current**—Check to request that 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**—Check to expire the passwords after a configured time period.
- **Password Aging Time**—Enter the number of days before a newly created password expires, from 1 to 365. The default is 180 days.

STEP 4 Click **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 the complexity requirements for the key used in the authentication process. More complex keys provide increased security.

To configure the WPA-PSK complexity:

STEP 1 Select **Security** > **WPA-PSK Complexity**.

STEP 2 Check **Enable** next to the **WPA-PSK Complexity** field to enable the WAP device to check the WPA-PSK keys against the criteria that you configure. If you disable this feature, none of these settings are used. WPA-PSK Complexity is disabled by default.

STEP 3 Configure these parameters:

- **WPA-PSK Minimum Character Class**—Choose the minimum number of character classes that must be represented in the key string. The four possible character classes are uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard. Three is the default.
- **WPA-PSK Different From Current**—When enabled, users must configure a different key after their current key expires. When disabled, 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.

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

7

Quality of Service

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

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

Global Settings

Use the Global Settings page to enable or disable the QoS functionality on the WAP device, and configure the trust mode and other QoS settings if you are using a Cisco WAP351 device.

Configuring QoS Settings for Cisco WAP131

To configure the QoS mode on your WAP device:

STEP 1 Select **Quality of Service** > **Global Settings**.

STEP 2 In the **QoS Mode** field, enable or disable the QoS functionality globally on the WAP device.

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

Configuring QoS Settings for Cisco WAP351

If you are using a Cisco WAP351 device and the QoS mode is enabled, you can configure the trust mode and other settings for Ethernet switch:

STEP 1 Select **Quality of Service** > **Global Settings**.

STEP 2 Enable the **QoS Mode** on the device.

STEP 3 Choose the trust mode of Ethernet switch from the **Trust Mode** list. The options are:

- **CoS/802.1p**—The priority of a packet received from an Ethernet port is based on the 802.1p value in this packet. If the incoming packet is not tagged, we will consider it as 0. You can configure the priority mapping settings in the **CoS/802.1p to Output Queue Table**.
- **DSCP**—The priority of a packet received from an Ethernet port is based on the IP ToS/DSCP value in this packet. If the incoming packet is not of IPv4/IPv6 type, we will consider it as 0. You can configure the priority mapping settings in the **DSCP to Output Queue Table**.
- **Port**—This is the port-based mode. The priority of a packet received from an Ethernet port is based on CoS attached to this port. You can configure the CoS value of each port on the Port Settings page (see **Port Settings** for more information). Then you can configure the priority mapping settings in the **CoS/802.1p to Output Queue Table**.

STEP 4 If the priority of a packet is based on CoS/802.1p, the packet will be scheduled into a corresponding queue per the configuration in the **CoS/802.1p to Output Queue Table**. Queue scheduling method can be set in the **Scheduling Settings** area.

STEP 5 If the priority of a packet is based on DSCP, the packet will be scheduled into a corresponding queue per the configuration in the **DSCP to Output Queue Table**. There are 4 queues supported. Queue scheduling method can be set in the **Scheduling Settings** area.

STEP 6 In the **Scheduling Settings** area, you can set the scheduling method of queues. When it is in strict priority (SP), the priority is Queue3 > Queue2 > Queue1 > Queue0. When it is weighted round robin (WRR) mode, the queues are scheduled in a round-robin method according to the service weight of each queue. WRR mode is only allowed as [Q0, Q1], [Q0, Q1, Q2] and [Q0, Q1, Q2, Q3]. The range of WRR weight is 1 to 49.

STEP 7 Click **Save**. The changes are saved to the Startup Configuration.

Class Map

The 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 the classes of traffic, and use the **Policy Map** page to define the policies and associate the class maps to them.

Configuring an IPv4 Class Map

To add and configure an IPv4 class map:

STEP 1 Select **Quality of Service** > **Class Map**.

STEP 2 In the **Class Map Name** field, enter the name for the new class map. The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

STEP 3 Choose **IPv4** as the type of class map from the **Class Map Type** list. The IPv4 class map applies only to IPv4 traffic on the WAP device.

STEP 4 In the **Match Criteria Configuration** area, configure these parameters to match the packets to a class:

- **Class Map Name**—Choose the IPv4 class map from the list.
- **Match Every Packet**—The match condition is true to all parameters in a Layer 3 packet. When enabled, all Layer 3 packets will match the condition.
- **Protocol**—Uses a Layer 3 or Layer 4 protocol match condition based on the value of the IP Protocol field in IPv4 packets or the Next Header field in IPv6 packets. Choose the protocol to match by keyword or enter a protocol ID:
  - **Select From List**—Matches the selected protocol: IP, ICMP, IGMP, TCP, UDP.
  - **Match to Value**—Matches a protocol that is not listed by name. Enter the protocol ID. The protocol ID is a standard value assigned by IANA. The range is a number from 0 to 255.
- **Source IP**—Requires a packet's source IPv4 address to match the IPv4 address defined in the appropriate fields.
  - **Source IP Address**—Enter the IPv4 address to apply this criteria.
  - **Source IP Mask**—Enter the source IPv4 address mask. The mask for DiffServ is a network-style bit mask in IP dotted decimal format indicating which part(s) of the destination IP address to use for matching against packet content.

    A DiffServ mask of 255.255.255.255 indicates that all bits are important, and 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 Port**—Includes a source port in the match condition for the rule. The source port is identified in the datagram header.
  - **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

- **Mask**—The port mask. The mask determines which bits are used and which bits are ignored. Only the hexadecimal digit (0-0xFFFF) is allowed. 1 means the bit matters and 0 means that we should ignore this bit.

- **Destination IP**—Requires a packet's destination IPv4 address to match the IPv4 address defined in the appropriate fields.
  - **Destination IP Address**—Enter the IPv4 address to apply this criteria.
  - **Destination IP Mask**—Enter the destination IP address mask.
- **Destination Port**—Includes a destination port in the match condition for the rule. The destination port is identified in the datagram header.
  - **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
  - **Mask**—The port mask. The mask determines which bits are used and which bits are ignored. Only the hexadecimal digit (0-0xFFFF) is allowed. 1 means the bit matters and 0 means that we should ignore this bit.
- **Service Type**—Specifies the type of service to use in matching the packets to the class criteria.
  - **IP DSCP Select From List**—Choose a DSCP value to use as a match criterion.
  - **IP DSCP Match to Value**—Enter a custom DSCP value from 0 to 63.
  - **IP Precedence**—Matches the packet's IP precedence value to the IP precedence value defined in this field. The IP precedence range is from 0 to 7.

- **IP ToS Bits**—Uses the packet's type of service (ToS) bits in the IP header as the match criteria. The IP ToS bit value ranges between (00 to FF). The high-order three bits represent the IP precedence value. The high-order six bits represent the IP DSCP value.
- **IP ToS Mask**—Enter an IP ToS Mask value to identify the bit positions in the IP ToS Bits value that are used for comparison against the IP ToS field in a packet.

  The IP ToS Mask value is a two-digit hexadecimal number from 00 to FF, 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.

STEP 5 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.

Configuring an IPv6 Class Map

To add and configure an IPv6 class map:

STEP 1 Select **Quality of Service** > **Class Map**.

STEP 2 In the **Class Map Name** field, enter the name for the new class map. The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

STEP 3 Choose **IPv6** as the type of class map from the **Class Map Type** list. The IPv6 class map applies only to IPv6 traffic on the WAP device.

STEP 4 In the **Match Criteria Configuration** area, configure these parameters to match the packets to a class:

- **Class Map Name**—Choose the IPv6 class map from the list.
- **Match Every Packet**—The match condition is true to all parameters in a Layer 3 packet. When enabled, all Layer 3 packets will match the condition.

- **Protocol**—Uses a Layer 3 or Layer 4 protocol match condition based on the value of the IP Protocol field in IPv4 packets or the Next Header field in IPv6 packets. Choose the protocol to match by keyword or enter a protocol ID:
  - **Select From List**—Matches the selected protocol: IPv6, ICMPv6, TCP, UDP.
  - **Match to Value**—Matches a protocol that is not listed by name. Enter the protocol ID. The protocol ID is a standard value assigned by IANA. The range is a number from 0 to 255.
- **Source IPv6**—Requires a packet's source IPv6 address to match the IPv6 address defined in the appropriate fields.
  - **Source IPv6 Address**—Enter the IPv6 address to apply this criteria.
  - **Source IPv6 Prefix Length**—Enter the prefix length of the source IPv6 address.
- **Source Port**—Includes a source port in the match condition for the rule. The source port is identified in the datagram header.
  - **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
  - **Mask**—The port mask. The mask determines which bits are used and which bits are ignored. Only the hexadecimal digit (0 to 0xFFFF) is allowed. 1 means the bit matters and 0 means that we should ignore this bit.
- **Destination IPv6**—Requires a packet's destination IPv6 address to match the IPv6 address defined in the appropriate fields.
  - **Destination IPv6 Address**—Enter the IPv6 address to apply this criteria.
  - **Destination IPv6 Prefix Length**—Enter the prefix length of the destination IPv6 address.

- **Destination Port**—Includes a destination port in the match condition for the rule. The destination port is identified in the datagram header.
  - **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
  - **Mask**—The port mask. The mask determines which bits are used and which bits are ignored. Only the hexadecimal digit (0 to 0xFFFF) is allowed. 1 means the bit matters and 0 means that we should ignore this bit.
- **IPv6 Flow Label**—Enter a 20-bit number that is unique to an IPv6 packet. It is used by end stations to signify QoS handling in routers (range 0 to 1048575).
- **IP DSCP**—Uses the DSCP value as a match criterion.
  - **Select from List**—Choose the DSCP type from the list.
  - **Match to Value**—Enter a custom DSCP value from 0 to 63.

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

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

Configuring a MAC Class Map

To add and configure a MAC class map:

STEP 1 Select **Quality of Service** > **Class Map**.

STEP 2 In the **Class Map Name** field, enter the name for the new class map. The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

STEP 3 Choose **MAC** as the type of class map from the **Class Map Type** list. The MAC class map applies to Layer 2 criteria.

STEP 4 In the **Match Criteria Configuration** area, configure these parameters to match the packets to a class:

- **Class Map Name**—Choose the MAC class map from the list.
- **Match Every Packet**—When enabled, all Layer 2 packets will match the condition.
- **EtherType**—Compares the match criteria against the value in the header of an Ethernet frame. Choose an EtherType keyword or enter an EtherType value to specify the match criteria:
  - **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**—Specifies the class of service 802.1p user priority value to be matched for the packets. The valid range is from 0 to 7.
- **Source MAC**—Includes a source MAC address in the match condition for the rule.
  - **Source MAC Address**—Enter the source MAC address to compare against an Ethernet frame.
  - **Source MAC Mask**—Enter the source MAC address mask specifying which bits in the destination MAC address to compare against an Ethernet frame.

    For each bit position in the MAC mask, a 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**—Includes a destination MAC address in the match condition for the rule.
  - **Destination MAC Address**—Enter the destination MAC address to compare against an Ethernet frame.

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

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

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

NOTE To delete a class map, choose 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 the 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 32 class maps in all created policy maps.

To add and configure a policy map:

STEP 1 Select **Quality of Service** > **Policy Map**.

STEP 2 In the **Policy Map Name** field, enter the name for the policy map. The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

STEP 3 Click **Add Policy Map**.

STEP 4 In the **Policy Class Definition** area, configure these parameters for the policy map:

- **Policy Map Name**—Choose the policy map to configure.

- **Class Map Name**—Choose the class map to apply this policy.

- **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 enable this feature, 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.

  NOTE The CoS remark only takes effect in the CoS/802.1p trust mode for the Ethernet ports of the Cisco WAP351.

- **Mark IP DSCP**—Marks all packets for the associated traffic stream with the IP DSCP value that you select from the list.
  - **Select From List**—A list of DSCP types.
- **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 5 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**.

QoS Association

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

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

To configure QoS association parameters:

STEP 1 Select **Quality of Service** > **QoS Association**.

STEP 2 In the **Interfaces** field, choose the radio or Ethernet interface on which you want to configure the QoS parameters.

STEP 3 From the **DiffServ Policy** list, choose a DiffServ policy applied to traffic sent to the WAP device for the selected interface.

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

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

NOTE Policy containing IPv6 class maps is not supported at the Ethernet ports of the Cisco WAP351.

QoS Status

The QoS Status page shows the details of policy map and class map, including which class map a policy map contains and which interfaces this policy map bound to.

The IPv4 QoS, IPv6 QoS, and MAC QoS tables show information for the class maps defined on the Class Map page, including:

- **Member Class**—The class map name.
- **Match All**—Shows if this map matches all packets.
- **Rule Field**—Shows the detailed definition of this class map. See **Class Map** for more information.

The Policy Map table shows information for the policy maps defined on the Policy Map page, including:

- **Policy Map Name**—Policy map name.
- **Interface Bound**—Shows which interface this policy map has been associated to.
- **Class Map Name**—Lists the class maps that this policy map contains.
- **Policy**—Shows the policy details of this class map. See **Policy Map** for more information.

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

8

ACL

This chapter describes how to configure the ACL feature on the WAP device. It contains these topics:

- ACL Rule
- ACL Association
- ACL Status

ACL Rule

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 32 IPv4, IPv6, and MAC ACL rules.

IPv4 and IPv6 ACLs

IP ACLs classify traffic for Layers 3 and 4.

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

NOTE There is an implicit deny at the end of every rule created. To avoid deny all, we strongly recommend that you 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 the WAP device port, the WAP device inspects the frame and checks the ACL rules against the content of the frame. If any of the rules match the content, a permit or deny action is taken on the frame.

Workflow to Configure ACLs

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

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

STEP 1 Select **ACL** > **ACL Rule**.

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 **ACL Association** page to apply the ACL to one or more interfaces.

Configure IPv4 ACLs

To configure an IPv4 ACL:

STEP 1 Select **ACL** > **ACL Rule**.

STEP 2 In the **ACL Name** field, enter the name to identify the ACL. The name can contain from 1 to 31 alphanumeric and special characters. Spaces are not allowed.

STEP 3 Choose IPv4 as the type of ACL from the **ACL Type** list. IPv4 ACLs control access to network resources based on Layer 3 and Layer 4 criteria.

STEP 4 Click **Add ACL**.

STEP 5 In the **ACL Rule Configuration** area, configure these ACL rule parameters:

- **ACL Name - ACL Type**—Choose the ACL to configure with the new rule.
- **Rule**—Choose **New Rule** to configure a new rule for the selected ACL. 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**—Choose whether the ACL rule permits or denies an action.

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

  When you choose **Deny**, the rule blocks all traffic that meets the rule criteria from entering the WAP device. Traffic that does not meet the criteria is forwarded unless this rule is the final rule. Because there is an implicit deny all rule at the end of every ACL, traffic that is not explicitly permitted is dropped.
- **Match Every Packet**—If enabled, the rule, which either has a permit or deny action, matches the frame or packet regardless of its contents. If you enable this feature, you cannot configure any additional match criteria. This option is selected by default for a new rule. You must disable the option to configure other match fields.
- **Protocol**—Uses a Layer 3 or Layer 4 protocol match condition based on the value of the IP Protocol field in IPv4 packets or the Next Header field in IPv6 packets. You can choose one of these options or choose **Any**:
  - **Select From List**—Choose 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**—Requires the packet's source IP address to match the address defined in the appropriate fields.
  - **Source IP Address**—Enter the IP address to apply this criteria.
  - **Wild Card Mask**—Enter 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.
  - **Select From List**—Choose the keyword associated with the source port to match: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these keywords translates into its equivalent port number.
  - **Match to Port**—Enter the IANA port number to match to the source port identified in the datagram header. The port range is 0 to 65535 and includes three different types of ports:

    0 to 1023—Well Known Ports

    1024 to 49151—Registered Ports

    49152 to 65535—Dynamic and/or Private Ports
  - **Mask**—Enter the port mask. The mask determines which bits are used and which bits are ignored. Only the hexadecimal digit (0 – 0xFFFF) is allowed. 0 means the bit matters and 1 means that we should ignore this bit.
- **Destination IP**—Requires a packet's destination IP address to match the address defined in the appropriate fields.
  - **Destination IP Address**—Enter an IP address to apply this criteria.
  - **Wild Card Mask**—Enter 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.

- **Select From List**—Choose the keyword associated with the destination port to match: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these keywords translates into its equivalent port number.
- **Match to Port**—Enter the IANA port number to match to the destination port identified in the datagram header. The port range is from 0 to 65535 and includes three different types of ports:

  0 to 1023—Well-Known Ports

  1024 to 49151—Registered Ports

  49152 to 65535—Dynamic and/or Private Ports
- **Mask**—Enter the port mask. The mask determines which bits are used and which bits are ignored. Only the hexadecimal digit (0 – 0xFFFF) is allowed. 0 means the bit matters and 1 means that we should ignore this bit.

▪ **Service Type**—Matches the packets based on specific service type.

- **IP DSCP Select From List**—Matches the packets based on their DSCP Assured Forwarding (AS), Class of Service (CS), or Expedited Forwarding (EF) values.
- **IP DSCP Match to Value**—Matches the packets based on a custom DSCP value. If selected, enter an value from 0 to 63 in this field.
- **IP Precedence**—Matches the 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 ToS 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.

STEP 6 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**.

Configure IPv6 ACLs

To configure an IPv6 ACL:

STEP 1 Select **ACL** > **ACL Rule**.

STEP 2 In the **ACL Name** field, enter the name to identify the ACL.

STEP 3 Choose IPv6 as the type of ACL from the **ACL Type** list. IPv6 ACLs control access to network resources based on Layer 3 and Layer 4 criteria.

STEP 4 Click **Add ACL**.

STEP 5 In the **ACL Rule Configuration** area, configure these ACL rule parameters:

- **ACL Name - ACL Type**—Choose the ACL to configure with the new rule.
- **Rule**—Choose **New Rule** to configure a new rule for the selected ACL. 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**—Choose whether the ACL rule permits or denies an action.

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

  When you choose **Deny**, the rule blocks all traffic that meets the rule criteria from entering the WAP device. Traffic that does not meet the criteria is forwarded unless this rule is the final rule. Because there is an implicit deny all rule at the end of every ACL, traffic that is not explicitly permitted is dropped.

- **Match Every Packet**—If enabled, the rule, which either has a permit or deny action, matches the frame or packet regardless of its contents. If you enable this feature, you cannot configure any additional match criteria. This option is selected by default for a new rule. You must disable the option to configure other match fields.
- **Protocol**—Choose the protocol to match by keyword or protocol ID.
- **Source IPv6**—Requires a packet's source IPv6 address to match the IPv6 address defined in the appropriate fields.
  - **Source IPv6 Address**—Enter the IPv6 address to apply this criteria.
  - **Source IPv6 Prefix Length**—Enter the prefix length of the source IPv6 address.
- **Source Port**—Includes a source port in the match condition for the rule. The source port is identified in the datagram header.
  - **Select From List**—If selected, choose the port name from the list.
  - **Match to Port**—Enter the IANA port number to match to the source port identified in the datagram header. The port range is 0 to 65535 and includes three different types of ports:

    0 to 1023—Well Known Ports

    1024 to 49151—Registered Ports

    49152 to 65535—Dynamic and/or Private Ports
  - **Mask**—Enter the port mask. The mask determines which bits are used and which bits are ignored. Only the hexadecimal digit (0 – 0xFFFF) is allowed. 0 means the bit matters and 1 means that we should ignore this bit.
- **Destination IPv6**—Requires a packet's destination IPv6 address to match the IPv6 address defined in the appropriate fields.
  - **Destination IPv6 Address**—Enter an IPv6 address to apply this criteria.
  - **Destination IPv6 Prefix Length**—Enter the prefix length of the destination IPv6 address.
- **Destination Port**—Includes a destination port in the match condition for the rule. The destination port is identified in the datagram header.
  - **Select From List**—If selected, choose the port name from the list.

- **Match to Port**—Enter the IANA port number to match to the source port identified in the datagram header. The port range is 0 to 65535 and includes three different types of ports:

  0 to 1023—Well Known Ports

  1024 to 49151—Registered Ports

  49152 to 65535—Dynamic and/or Private Ports

- **Mask**—Enter the port mask. The mask determines which bits are used and which bits are ignored. Only the hexadecimal digit (0 – 0xFFFF) is allowed. 0 means the bit matters and 1 means that we should ignore this bit.

- **IPv6 Flow Label**—Specifies 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).

- **IPv6 DSCP**—Matches the packets based on their IP DSCP value. If selected, choose one of these options as the match criteria:

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

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

STEP 6 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, check **Delete ACL**, and click **Save**.

Configure MAC ACLs

To configure a MAC ACL:

STEP 1 Select **ACL** > **ACL Rule**.

STEP 2 In the **ACL Name** field, enter the name to identify the ACL.

STEP 3 Choose **MAC** as the type of ACL from the **ACL Type** list. MAC ACLs control access based on Layer 2 criteria.

STEP 4 Click **Add ACL**.

STEP 5 In the **ACL Rule Configuration** area, configure these ACL rule parameters:

- **ACL Name - ACL Type**—Choose the ACL to configure with the new rule.
- **Rule**—Choose **New Rule** to configure a new rule for the selected ACL. 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**—Choose whether the ACL rule permits or denies an action.

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

  When you choose **Deny**, the rule blocks all traffic that meets the rule criteria from entering the WAP device. Traffic that does not meet the criteria is forwarded unless this rule is the final rule. Because there is an implicit deny all rule at the end of every ACL, traffic that is not explicitly permitted is dropped.
- **Match Every Packet**—If enabled, the rule, which either has a permit or deny action, matches the frame or packet regardless of its contents. If you enable this feature, you cannot configure any additional match criteria. This option is selected by default for a new rule. You must disable the option to configure other match fields.
- **EtherType**—Choose to compare the match criteria against the value in the header of an Ethernet frame. You can select an EtherType keyword or enter an EtherType value to specify the match criteria.
  - **Select from List**—Choose 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**—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**—Requires the packet's source MAC address to match the address defined in the appropriate fields.
  - **Source MAC Address**—Enter the source MAC address to compare against an Ethernet frame.
  - **Source MAC Mask**—Enter the source MAC address mask specifying which bits in the source MAC to compare against an Ethernet frame.

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

- **Destination MAC**—Requires the packet's destination MAC address to match the address defined in the appropriate fields.
  - **Destination MAC Address**—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.
- **VLAN ID**—Enter the specific VLAN ID to compare against an Ethernet frame. This field is located in the first/only 802.1Q VLAN tag.

STEP 6 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, check **Delete ACL**, and click **Save**.

ACL Association

The ACL Association page provides the ACL list bound to the wireless and Ethernet interfaces. In addition, it also provides control of the amount of bandwidth that 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 interfaces.

To associate an ACL to an interface:

STEP 1 Select **ACL** > **ACL Association**.

STEP 2 In the **Interface** field, click the radio or Ethernet interface on which you want to configure the ACL parameters.

STEP 3 Configure these parameters for the selected interface:

- **Bandwidth Limit Down**—Enter 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**—Enter 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**—Choose the type of ACL that is applied to traffic entering the WAP device, which can be one of these options:
  - **IPv4**—Examines the IPv4 packets that match the ACL rules.
  - **IPv6**—Examines the IPv6 packets that match the ACL rules.
  - **MAC**—Examines the Layer 2 frames that match the ACL rules.
  - **None**—Does not examine the traffic entering the WAP device.
- **ACL Name**—Choose the name of the ACL applied to traffic entering the WAP device.

  When a packet or frame is received by the WAP device, the ACL rules are checked for a match. The packet or frame is processed if it is permitted and discarded if it is denied

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

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

NOTE IPv6 type is not supported at the Ethernet ports of the Cisco WAP351.

ACL Status

The ACL Status page shows the details for different types of ACL rules.

To view the ACL status, select **ACL** > **ACL Status**.

The following information is displayed:

- **ACL Name**—The name of the ACL.
- **Interface Bound**—The interface to which the ACL has been associated.
- **Rule No.**—The number of the rule that the ACL contains.

- **Action**—The action to be taken by the ACL.
- **Match All**—Shows whether or not the ACL rule matches all packets.
- **Rule Field**—Shows the detailed settings for the ACL. See **ACL Rule** for more information.

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

9

SNMP

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

- General
- Views
- Groups
- Users
- Targets

General

Use the General page to enable SNMP and configure basic protocol settings.

To configure general SNMP settings:

STEP 1 Select **SNMP** > **General**.

STEP 2 Enable or disable SNMP on the WAP device. SNMP is disabled by default.

STEP 3 If you enable SNMP, specify a **UDP Port** for SNMP traffic.

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

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

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

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

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

  To specify a subnet, enter one or more subnetwork address ranges in the form address/mask_length where 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 host name, 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).

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

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

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

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

  Also see the note about host names 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 the 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**.

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

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

To add and configure an SNMP group:

STEP 1 Select **SNMP** > **Groups**.

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 these parameters:

- **Group Name**—Enter the 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:
  - **noAuthNoPriv**—No authentication and no data encryption (no security).
  - **authNoPriv**—Authentication, but no data encryption. With this security level, users send SNMP messages that use an SHA key or password for authentication, but not a DES key or password for encryption.
  - **authPriv**—Authentication and data encryption. With this security level, users send an SHA key or password for authentication and a DES key or password for encryption. For groups that require authentication, encryption, or both, you must define the SHA and DES keys or passwords on the SNMP Users page.
- **Write Views**—Choose the write access to MIBs for the group, which can be one of these options:
  - **view-all**—The group can create, alter, and delete MIBs.
  - **view-none**—The group cannot create, alter, or delete MIBs.
- **Read Views**—Choose the read access to MIBs for the group, which can be one of these options:
  - **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, check the group in the list and click **Delete**.

Users

Use the SNMP Users page to define users, associate a security level to each user, and configure the 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 SHA 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**.

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 these parameters:

- **User Name**—Enter the name that identifies the SNMPv3 user. User names can contain up to 32 alphanumeric characters.
- **Group**—Enter the group that the user is mapped to. The default groups are RW and RO. You can define additional groups on the SNMP Groups page.
- **Authentication Type**—Choose the type of authentication to use on the SNMPv3 requests from the user, which can be one of these options:
  - **SHA**—Requires SHA authentication on SNMP requests from the user.
  - **None**—SNMPv3 requests from this user require no authentication.
- **Authentication Pass Phrase**—If you specify SHA as the authentication type, enter the pass phrase to enable the SNMP agent to authenticate the requests sent by the user. The pass phrase must be between 8 and 32 characters in length.
- **Encryption Type**—Choose the type of privacy to use on SNMP requests from the user, which can be one of these options:
  - **DES**—Uses 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, enter the 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 complete before configuring SNMPv3 targets.

NOTE The WAP device supports a maximum of eight targets.

To add SNMP targets:

STEP 1 Select **SNMP** > **Targets**.

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 these parameters:

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

10

Captive Portal

This chapter describes the Captive Portal (CP) feature, which allows you to block the wireless clients from accessing the network until the user verification has been established. You can configure the CP verification to allow access for both guest and authenticated users.

NOTE The Captive Portal feature is available only on the Cisco WAP351. The Cisco WAP131 does not support Captive Portal.

Authenticated users must be validated against a database of authorized CP groups or users before the 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. The Cisco WAP351 devices operate concurrently with some VAPs configured for CP authentication and other VAPs configured for normal wireless authentication methods, such as WPA or WPA Enterprise.

This chapter includes these topics:

- **Global Configuration**
- **Local Groups/Users**
- **Instance Configuration**
- **Instance Association**
- **Web Portal Customization**
- **Authenticated Clients**

Global Configuration

Use the Global CP Configuration page to control the administrative state of the Captive Portal feature and configure global settings that affect all CP instances configured on the WAP device.

To configure CP global settings:

STEP 1 Select **Captive Portal** > **Global Configuration**.

STEP 2 Configure these parameters:

- **Captive Portal Mode**—Enables or disables the Captive Portal operation on the WAP device.
- **Authentication Timeout**—To access the network through a portal, the client must first enter the authentication information on an authentication web page. This field specifies the number of seconds that the WAP device keeps an authentication session open with the associated wireless client. If the client fails to enter the 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 a port number between 1025 and 65535, or 443. The HTTP and HTTPS ports cannot be the same.

STEP 3 The **Captive Portal Configuration Counters** area shows the 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. The 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 4 Click **Save**. The changes are saved to the Startup Configuration.

Local Groups/Users

Use the Local Groups/Users page to manage local groups and users.

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 a local user group:

STEP 1 Select **Captive Portal** > **Local Groups/Users**.

STEP 2 In the **Local Groups Settings** area, configure these parameters:

- **Captive Portal Groups**—Choose **Create** to create a new group.
- **Group Name**—Enter the name for the new group.

STEP 3 Click **Add Group**. The changes are saved to the Startup Configuration.

To delete a local user groups:

STEP 1 Select **Captive Portal** > **Local Groups/Users**.

STEP 2 In the **Local Groups Settings** area, choose the group that you want to delete.

STEP 3 Check the **Delete Group** option.

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

Local Users

You can configure a CP 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 configure up to 128 authorized users in the local database.

To add and configure a local user:

STEP 1 Select **Captive Portal** > **Local Groups/Users**.

STEP 2 In the **Local Users Settings** area, configure these parameters:

- **Captive Portal Users**—Choose **Create** to create a new user.
- **User Name**—Enter the name for the new user.

STEP 3 Click **Add User**.

STEP 4 The **Local Users Settings** area reappears with additional options. Configure these 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 that you type is visible. When disabled, the text is not masked as you enter it.
- **Away Timeout**—Enter the period of time that a user remains in the CP authenticated client list after the client disassociates from the WAP device. If the time specified in this field expires before the client attempts to 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 CP instance, unless the user value is set to 0. When it is set to 0, the timeout value configured for the CP instance is used.
- **Group Name**—Choose the assigned user group. Each CP instance is configured to support a particular group of users.

- **Maximum Bandwidth Upstream**—Enter the maximum upload speed, in megabits per second, that a client can transmit traffic when using the Captive Portal. This setting limits the bandwidth used to send data into the network. The range is from 0 to 300 Mbps. The default is 0.
- **Maximum Bandwidth Downstream**—Enter the maximum download speed, in megabits per second, that a client can receive traffic when using the Captive Portal. This setting limits the bandwidth used to receive data from the network. The range is from 0 to 300 Mbps. The default is 0.

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

To delete a local user:

STEP 1 Select **Captive Portal** > **Local Groups/Users**.

STEP 2 In the **Local Users Settings** area, choose the user that you want to delete.

STEP 3 Check the **Delete User** option.

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

Instance Configuration

You can create up to two CP 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 the **Networks** page to add a VAP.
- Do you need to add a new group or a new user? If yes, go to the **Local Groups/Users** page to add a group or add a user.

To create a CP instance and configure its settings:

STEP 1 Select **Captive Portal** > **Instance Configuration**.

STEP 2 Choose **Create** from the **Captive Port Instances** list.

STEP 3 Enter the name from 1 to 32 alphanumeric characters for the CP instance in the **Instance Name** field.

STEP 4 Click **Save**.

STEP 5 The **Captive Portal Instance Parameters** area reappears with additional options. Configure these parameters:

- **Instance ID**—Shows the instance ID. This field is not configurable.
- **Administrative Mode**—Enables and disables the CP instance.
- **Protocol**—Choose either HTTP or HTTPS as the protocol for the CP instance to use during the verification process.
  - **HTTP**—Does not use encryption during verification.
  - **HTTPS**—Uses the Secure Sockets Layer (SSL), which requires a certificate to provide encryption. The certificate is presented to the user at connection time.
- **Verification**—Choose the authentication method for CP to use to verify the clients. The options are:
  - **Guest**—The users do not need to be authenticated by a database.
  - **Local**—The WAP device uses a local database to authenticate the users.
  - **RADIUS**—The WAP device uses a database on a remote RADIUS server to authenticate the users.
- **Redirect**—When enabled, Captive Portal should redirect the newly authenticated client to the configured URL. If this option is disabled, the user sees the locale-specific welcome page after a successful verification.
- **Redirect URL**—If the Redirect mode is enabled, enter the URL (including http://) to which the newly authenticated client is redirected. The range is from 0 to 256 characters.
- **Away Timeout**—Enter the amount of time that a user remains in the CP authenticated client list after the client disassociates from the WAP device. If the time specified in this field expires before the client attempts to 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.

An away timeout value is also configured for each user (see the **Local Groups/Users** page). The away timeout value set on the Local Groups/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**—Enter 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**—Enter the maximum upload speed, in megabits per second, that a client can transmit traffic when using the Captive Portal. This setting limits the bandwidth 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**—Enter the maximum download speed, in megabits per second, that a client can receive traffic when using the Captive Portal. This setting limits the bandwidth 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 set to 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 set to RADIUS, check **Enable** to use the default global RADIUS server list to authenticate the 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**—Check **Enable** to track and measure the resources that a particular user has consumed, such as the system time and the amount of data transmitted and received.

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

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

- **Server IP Address** (**2** through **4**) or **Server IPv6 Address** (**2** through **4**)—Enter up to three IPv4 or IPv6 backup RADIUS server addresses. If the authentication fails with the primary server, each configured backup server is tried in sequence.
- **Key-1**—Enter the shared secret key that the WAP device uses to authenticate to the primary RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive and must match the key configured on the RADIUS server. The text that you enter is shown as asterisks.
- **Key-2** to **-4**—Enter the RADIUS key associated with the configured backup RADIUS servers. The server at Server IP Address-1 uses Key-1, Server IP Address-2 uses Key-2, and so on.
- **Locale Count**—Shows 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**—Check to delete the current instance.

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

Instance Association

After you create an instance, 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**.

STEP 2 Choose the radio that you want to configure.

STEP 3 Choose the instance name for each VAP to which you want to associate an instance.

STEP 4 Click **Save**. Your change are saved to the Startup Configuration.

Web Portal Customization

After 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 CP instance, the user sees an authentication page.

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.

Configuring CP Authentication Page

To create and customize a CP authentication page:

STEP 1 Select **Captive Portal** > **Web Portal Customization**.

STEP 2 Choose **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 In the **Captive Portal Web Locale Parameters** area, configure these parameters:

- **Web Locale Name**—Enter a web locale name to assign to the page. The name can be from 1 to 32 alphanumeric characters.
- **Captive Portal Instances**—Choose the CP instance with which this locale is associated. 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 4 Click **Save**. The changes are saved to the Startup Configuration.

STEP 5 The **Captive Portal Web Locale Parameters** area reappears the additional options for modifying the locale. The **Locale ID** and **Instance Name** fields cannot be edited. The editable fields are populated with default values. Configure these parameters:

- **Background Image Name**—Choose the image to show as the page background. You can click **Upload/Delete Custom Image** to upload the images for CP instances. See **Uploading and Deleting Images** for more information.
- **Logo Image Name**—Choose 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 upload a custom logo image to the WAP device, you can choose it from the list.
- **Foreground color**—Enter the HTML code for the foreground color in 6-digit hexadecimal format. The range is from 1 to 32 characters. The default is #999999.
- **Background color**—Enter the HTML code for the background color in 6-digit hexadecimal format. The range is from 1 to 32 characters. The default is #BFBFBF.
- **Separator**—Enter the HTML code for the color of the thick horizontal line that separates the page header from the page body, in 6-digit hexadecimal format. The range is from 1 to 32 characters. The default is #BFBFBF.
- **Locale Label**—Enter the descriptive label for the locale, from 1 to 32 characters. The default is English.
- **Locale**—Enter the abbreviation for the locale, from 1 to 32 characters. The default is en.
- **Account Image**—Choose 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 and 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.
- **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.
- **Work In Progress Text**—The text that shows during the authentication. The range is from 1 to 128 characters.
- **Denied Text**—The text that shows when a user fails the authentication. The range is from 1 to 128 characters.
- **Welcome Title**—The text that shows when the client has authenticated to the VAP. The range is from 1 to 128 characters.
- **Welcome Content**—The text that shows when the client has connected to the network. The range is from 1 to 256 characters.
- **Delete Locale**—Deletes the current locale.

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

STEP 7 Click **Preview** to view the updated page.

NOTE Clicking **Preview** will show the text and the 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 the access to a VAP that is associated with a CP 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
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 Click **Browse** to choose the image.

STEP 3 Click **Upload**.

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

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

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

STEP 7 Click **Save**.

STEP 8 To delete an image, on the Web Portal Custom Image page, choose it from the **Delete Web Customization Image** list and click **Delete**. You cannot delete the default images.

Authenticated Clients

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

To view the list of authenticated clients or the list of clients who failed the authentication, select **Captive Portal** > **Authenticated Clients**.

The following information is displayed:

- **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 that the user used to establish the connection (HTTP or HTTPS).
- **Verification**—The method used to authenticate the user on the Captive Portal, which can be one of these values:
  - **Guest**—The user does not need to be authenticated by a database.
  - **Local**—The WAP device uses a local database to authenticate the users.
  - **RADIUS**—The WAP device uses a database on a remote RADIUS server to authenticate the users.
- **VAP ID**—The VAP that the user is associated with.
- **Radio ID**—The radio ID.
- **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.
- **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.

11

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

NOTE The Single Point Setup feature is available only on the Cisco WAP351. The Cisco WAP131 does not support the Single Point Setup feature.

Single Point Setup Overview

Single Point Setup provides a centralized method to administer and control the wireless services across multiple devices. You can use Single Point Setup to create a single group or cluster of the WAP 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 the channel planning across your wireless services to reduce the radio interference and maximize the 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 Access Points

Single Point Setup creates a dynamic, configuration-aware cluster or group of the WAP devices in the same subnet of a network. A cluster supports only a group of the configured Cisco WAP351 devices.

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 following table shows the wireless service limits of Single Point Setup:

Group/ Cluster Type	WAP Devices per Single Point Setup	Number of Active Clients per Single Point Setup	Maximum Number of Clients (Active and Idle)
Cisco WAP351	8	160	256

A cluster can propagate the configuration information, such as the VAP settings, the QoS queue parameters, and the radio parameters. When you configure Single Point Setup on a device, the 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 that the following prerequisites or conditions are met:

STEP 1 Plan your Single Point Setup cluster. Be sure that two or more WAP devices that you want to cluster are the same model. For example, the Cisco WAP351 devices can only cluster with other Cisco WAP351 devices.

We strongly recommend that you 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** for more information.

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

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, the 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 the 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 the advertisements from a WAP device for more than 60 seconds (for example, if the device loses connectivity to other devices in the cluster), the WAP 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 the configuration changes were made to that device during the lost connectivity period, the changes are propagated to the other cluster members when the connectivity resumes.
- If a WAP device in a cluster loses connectivity, is dropped, later rejoins the cluster, and the configuration changes were made 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 WAP 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 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:

- The 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.
- The 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, the loss of contact with the cluster does not necessarily prevent the 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 disconnection with the LAN infrastructure, the network services out to the wireless clients may be impacted depending on the nature of the failure.

Configuration Parameters Propagated and Not Propagated to Single Point Setup Access Points

The following tables summarize the 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
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	
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	Packet Capture

WorkGroup Bridge

Access Points

Use the Access Points page to enable or disable Single Point Setup on the 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**.

Single Point Setup is disabled on the WAP device by default. When it is 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 the Single Point Setup settings 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 the WAP devices that are currently joined in the cluster.

STEP 2 With Single Point Setup disabled, configure these parameters for each individual member of a Single Point Setup cluster:

- **Location**—Enter a description of where the WAP device 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 that you configure on the network. The default is ciscosb-cluster.
- **Clustering IP Version**—Choose 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. When using IPv6, ensure that all WAP devices in the cluster either use link-local addresses only or use global addresses only.

Single Point Setup works only with the WAP devices using the same type of IP addressing. It does not work with a group of the 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 the 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 the 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. The Access Points page lists the detected WAP devices in a table and the following information is displayed:

- **Location**—Description of where the WAP device is physically located.
- **MAC Address**—MAC address of the WAP device. 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 WAP device.

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

Adding a WAP Device to a Single Point Setup

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

STEP 1 Go to the configuration utility of the standalone WAP device.

STEP 2 Select **Single Point Setup** > **Access Points**.

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 WAP device is physically located.

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

The WAP device automatically joins the Single Point Setup.

Removing a WAP Device from a Single Point Setup

To remove a WAP device from the Single Point Setup cluster:

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

The configuration utility for that WAP device appears.

STEP 2 Select **Single Point Setup** > **Access Points**.

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

The **Single Point Setup** status field for that WAP device will now show **Disabled**.

Navigating to Configuration Information for a Specific 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 may want to check the status information such as the client associations or the events for a WAP device. In this case, you can click the IP address in the table on the Access Points page to show the configuration utility for the particular WAP device.

Navigating to a Device Using its IP Address in a URL

You can also link to the configuration utility of a specific WAP device by entering the IP address for that WAP device 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

Use the Sessions page to show information on the 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 This 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, choose an item from the **Display** list and click **Go**. You can view information about the idle time, the data rate, and the 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 WAP device. A WLAN client association can shift from one clustered WAP device to another within the same session.

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

The following information is displayed for each WLAN client session with a Single Point Setup:

- **AP Location**—The location of the WAP device. The location is derived from the location specified on the Administration > System Settings page.
- **User MAC**—The MAC address of the WAP device. A MAC address is a hardware address that uniquely identifies each node of a network.
- **Idle**—The amount of time that 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 WAP device. For example, 6 to 54 Mbps for 802.11a.
- **Signal**—The strength of the radio frequency (RF) signal the WLAN client receives from the WAP device. 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 the WAP device.

To sort the information shown in the tables by a particular indicator, click the column label that 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

Use the Channel Management page to show the current and planned channel assignments for the WAP devices in a Single Point Setup cluster.

When the channel management is enabled, the WAP device automatically assigns the radio channels used by the WAP devices in a Single Point Setup cluster. The automatic channel assignment reduces mutual interference (or interference with other WAP devices outside of its cluster) and maximizes the 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 the interference levels of the cluster members. If a 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.

Configuring and Viewing the Channel Assignments

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

STEP 1 Select **Single Point Setup** > **Channel Management**.

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

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

When the automatic channel assignment is enabled, the channel manager periodically maps the radio channels used by the WAP devices in a Single Point Setup cluster and, if necessary, reassigns the channels to reduce the interference with the cluster members or with the devices outside the cluster. The channel policy for the radio is automatically set to the 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 more 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 the 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 WAP device.
- **IP Address**—The IP address for the WAP device.
- **Wireless Radio**—The MAC address of the radio.
- **Band**—The band on which the WAP device is broadcasting.
- **Channel**—The radio channel on which the WAP device is currently broadcasting.
- **Locked**—Forces the WAP device to remain on the current channel.

- **Status**—Shows the status of the wireless radio in the WAP 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 a WAP device, the automated channel management plans do not reassign the WAP device to a different channel as a part of the optimization strategy. Instead, the WAP devices with locked channels are factored in as requirements for the plan.

Click **Save** to update the locked setting. The locked devices show the same channel for the Current Channel Assignments table and the Proposed Channel Assignments table. The 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. The locked channels are not reassigned—the optimization of channel distribution among the devices takes into account that the locked devices must remain on their current channels. The WAP devices that are not locked may be assigned to different channels than what 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** 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 the interference can be reduced by 25 percent or more. The channels are reassigned even if the network is busy. The default settings are designed to satisfy most scenarios where you would need to implement the channel management.

You can change the advanced settings by configure the following settings:

- **Change channels if interference is reduced by at least**—The minimum percentage of interference reduction that a proposed plan must achieve in order to be applied. The default is 75 percent. Choose the 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 the channel interference must be reduced by 75 percent and the proposed channel assignments will only reduce the interference by 30 percent, then the 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 the 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 the 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

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

The Wireless Neighborhood page can help you:

- Detect and locate unexpected (or rogue) devices in a wireless domain so that you can take action to limit the associated risks.
- Verify the 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.

Viewing Neighboring Devices

To view the neighboring devices, select **Single Point Setup** > **Wireless Neighborhood**.

To see all devices detected on a given Single Point Setup, navigate to the web-based interface of a member and select **Wireless** > **Rogue AP Detection**.

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

- **Display Neighboring APs**—Choose one of the following radio buttons to change the view:
  - **In cluster**—Only display the neighbor WAP devices that are members of the cluster.
  - **Not in cluster**—Only display the neighbor WAP devices that are not cluster members.
  - **Both**—Displays all neighbor WAP devices, including 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 Single Point Setup 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 the 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 the access point.

A

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the Cisco WAP131 and WAP351 Wireless-N Dual Radio Access Points.

Cisco Support Community	www.cisco.com/go/smallbizsupport
Cisco 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 Firmware Downloads	www.cisco.com/go/smallbizfirmware Select a link to download firmware for Cisco products. No login is required.
Cisco Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Cisco WAP131 and WAP351 Administration Guide	www.cisco.com/go/100_wap_resources www.cisco.com/go/300_wap_resources
Cisco Power Adapters	www.cisco.com/go/wap_accessories
Cisco Partner Central (Partner Login Required)	www.cisco.com/web/partners/sell/smb