REVIEW DRAFT Version 2—CISCO CONFIDENTIALL

ADMINISTRATION GUIDE

Cisco Small Business

WAP121 Wireless-N Access Point with Power over Ethernet

WAP321 Wireless-N Selectable-Band Access Point with POE

2

Getting Started

This chapter provides an introduction to the web-based access point (AP) configuration utility, and includes the following topics:

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

Starting the Web-based AP Configuration Utility

This section describes how to navigate the AP configuration utility.

Browsers have the following restrictions:

- If you are using Internet Explorer 6, you cannot directly use an IPv6 address to access the AP. You can, however, use the DNS (Domain Name System) server to create a domain name that contains the IPv6 address, and then use that domain name in the address bar in place of the IPv6 address.
- To use Internet Explorer 8, open a browser window and configure the following settings:

  Click **Tools > Internet Options** and then select the **Security** tab. Select **Local Intranet** and click **Sites**. Click **Advanced** and then click **Add**. Add the intranet address of the AP (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 IPv6 link local address to access the AP from your browser.

Launching the Utility

To open the web-based AP configuration utility:

STEP 1 Open a Web browser.

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

Logging In

To log in to the web-based AP configuration utility:

STEP 1 Enter the user name and password. The factory default user name is **cisco** and the default password is **cisco**.

STEP 2 If this is the first time that you logged on with the default user name (**cisco**) and the default password (**cisco**) or your password has expired, the Change Admin Password page opens. Enter the new password and confirm it, click **Apply**, and then click **Close**. The new password is saved.

Then, enter the user name **cisco** and the new password on the Login page.

STEP 3 Click **Login**.

When the login attempt is successful, the Access Point Startup Wizard page opens.

If you entered an incorrect user name or password, an error message is displayed and the Login page remains displayed on the screen.

See **Using the Access Point Setup Wizard, page 9** for instructions on using the wizard.

Logging Out

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

To logout, click **Logout** in the top right corner of any page.

Using the Access Point Setup Wizard

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

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

STEP 1 Click **Next**. The Wizard displays the first of several Configuration windows, the Access Point Setup Wizard—IP Address window.

STEP 2 Configure the system to receive its IP information from a DHCP server, or specify this information manually. For a description of these fields, see **LAN, page 31**.

STEP 3 Click **Next**. The Access Point Setup Wizard—Time Settings window displays.

STEP 4 Select your time zone, and then configure the system time manually or set the AP to get its time from an NTP server. For a description of these options, see **Time Settings, page 33**.

STEP 5 Click **Next**. The Wizard displays the first of four security windows, the Access Point Setup Wizard—Device Password window.

STEP 6 Enter a **New Password** and enter it again in the **Confirm Password** text box. For more information about passwords, see **User Accounts, page 87**.

STEP 7 Click **Next**. The Wizard displays the second of four security windows, the Access Point Setup Wizard—Network Name window.

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

STEP 9 Click **Next**. The Wizard displays the third of four security windows, the Access Point Setup Wizard—Wireless Security window.

STEP 10 Choose a security type. For a description of these options, see **System Security, page 110**.

STEP 11 Click **Next**. The Wizard displays the Access Point Setup Wizard—Summary window.

STEP 12 Review the settings you configured. If they are correct, click **Submit**. Or, click **Back** to reconfigure one or more settings. If you click **Cancel**, all settings are returned to the previous values.

If you click **Next**, the Wizard displays the Access Point Setup Wizard—Finish window.

STEP 13 Click **Finish**. The Getting Started window displays.

Getting Started

To simplify device configuration through quick navigation, the Getting Started page provides links for performing common tasks.

Links on the Getting Started Page

Category	Link Name (on the Page)	Linked Page
Initial Setup	Run Setup Wizard	Access Point Startup Wizard
	Configure Radio Settings	Radio
	Configure Wireless Network Settings	Networks
	Configure LAN Settings	LAN
	Run WPS	WPS Setup
Device Status	System Summary	System Summary
	Wireless Client Associations	Network Interfaces
Quick Access	Change Account Password	User Accounts
	Upgrade Device Firmware	Upgrade Firmware
	Backup/Restore Configuration	Download/Backup Configuration File
Other Resources	Support	Cisco AP support site
	Forums	Cisco Support Community site

Window Navigation

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

Application Header

Application Header

The Application Header is displayed on every page. It provides the following buttons:

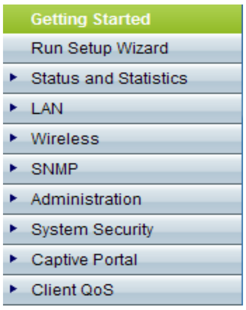
Buttons

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

Navigation Window

Navigation Window

A navigation window is located on the left side of each page. Click a top-level category to display links to related pages. Links that are preceded by an arrow are subcategories that expand to display the related page links.



Management Buttons

Management Buttons

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

Management Buttons

Button Name	Description
Add	Click to display the related Add page and add an entry to a table. Enter the information and click **Save** to save it to the Running Configuration and to the Startup Configuration.
Cancel	Click to reset changes made on the page.
Clear All	Click to clear all entries in the log table.
Delete	Select the entry in the table or list to be deleted and click **Delete**.
Details	Click to display details associated with the entry selected on the main page.
Edit	Select an entry and click **Edit** to open it for editing. The Edit page opens, or the relevant fields become editable.
Refresh	Click o redisplay the current page with the latest data.
Save	Click to save the settings to save any configuration changes to the Running Configuration in RAM and to the Startup Configuration in nonvolatile memory.
Update	Click to save any configuration changes on part of a page to the Running Configuration in RAM and to the Startup Configuration in nonvolatile memory.

3

Viewing Statistics

This chapter describes how to display WAP121/WAP321 statistics.

It contains the following topics.

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

System Summary

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

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

The System Summary page displays the following information:

- **PID VID**—The AP hardware model and version.
- **Serial Number**—Serial number of the WAP121/WAP321.
- **Base MAC Address**—The AP MAC address.
- **Firmware Version**—Firmware version number of the active image.
- **Firmware MD5 Checksum**—The checksum for the active image.
- **Host Name**—A name assigned to the device.
- **System Uptime**—Time that has elapsed since the last reboot.
- **System Time**—Current system time.

The NET_STAT table displays basic information about protocols and services operating on the AP.

- **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 switch. A value of All indicates that any IP address on the device can use this service.
- **Local Port**—The logical port number for the service.
- **Remote IP Address**—The IP address of a remote host, if any, that is using this service. A value of All indicates that the service is available to all remote hosts that access the system.
- **Remote Port**—The logical port number of any remote device communicating with this service.

- **Connection State**—The state of the service. For UDP, only connections in the Active state display in the table. In the Active state, a connection is established between the switch and a client or server. The TCP states are:
  - **Listen**—The service is listening for connection requests.
  - **Active**—A connection session is established and packets are being transmitted and received.
  - **Established**—A connection session is established between the switch 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 AP is waiting for a system-defined timeout period (typically 60 seconds) before closing the connection.

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

Network Interfaces

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

The Network Interfaces page displays the following information:

- **LAN Status**—These settings apply to the internal interface. These include the MAC Address; VLAN ID; IPv4 Address, subnet mask, and default gateway; and the IPv6 address and default gateway. The two configured DNS server IP addresses are also listed. For the WAP321 whether Green Ethernet mode is enabled also displays.

  To change any of these settings, click the Edit link. After you click Edit, you are redirected to the LAN page. See **LAN, page 31** for descriptions of these fields.

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

  To change the wireless settings, click the Edit link. After you click Edit, you are redirected to the Radio page. See **Radio, page 36** for descriptions of these fields.

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

Traffic Statistics

Use the Traffic Statistics page to view basic information about the AP and a real-time display of transmit and receive statistics for the Ethernet interface and the VAPs on both radio interfaces. All transmit and receive statistics reflect the totals since the AP was last started. If you reboot the AP, these figures indicate transmit and receive totals since the reboot.

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

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

The following summary traffic statics display:

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

- **Errors**—The total number of errors related to sending and receiving data on this AP.

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

WorkGroup Bridge Transmit/Receive

The WorkGroup Bridge Transmit/Receive page displays packet and byte counts for traffic between stations on a workgroup bridge. For information on configuring workgroup bridges, see **Work Group Bridge, page 62**.

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

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

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

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

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

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

Associated Clients

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

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

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

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

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

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

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

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

TSPEC Client Associations

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

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

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

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

The following information is provided on the TSPEC Client Associations page.

Status:

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

  The value may differ depending on other priority traffic sessions.
- **Medium Time**—Time (in 32 microsecond per second units) that the TS traffic occupies the transmission medium.
- **Excess Usage Events**—Number of times the client has exceeded the medium time established for its TSPEC. Minor, infrequent violations are ignored.
- **VAP MAC Address**—Virtual Access Point MAC address.

Statistics:

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

- **Direction**—The traffic direction for this TS. Direction can be one of the following:
  - uplink
  - downlink
  - 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. The following also display:
  - **Packets**—Number of packets in excess of an admitted TSPEC.
  - **Bytes**—Number of packets for which no TSPEC has been established when admission is required by the AP.
- **To Station**—The number of packets and bytes transmitted from the AP to the wireless client and the number of packets and bytes that were dropped upon transmission. The following also display:
  - **Packets**—Number of packets in excess of an admitted TSPEC.
  - **Bytes**—Number of packets for which no TSPEC has been established when admission is required by the AP.

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

Rogue AP Detection

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

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

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

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

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

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

Neighbor AP detection can be enabled and disabled. To enable the radio to collect information about neighbor APs, click **Enable**. next to **AP Detection for Radio 1**.

The following information about detected and trusted rogue access points displays.

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

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

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

- **MAC Address**—The MAC address of the neighboring AP.

- **Beacon Interval**—The Beacon interval used by this AP.

  Beacon frames are transmitted by an AP at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second).

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

- **Type**—The type of device:

  - AP indicates the neighboring device is an AP that supports the IEEE 802.11 Wireless Networking Framework in Infrastructure Mode.

  - Ad hoc indicates a neighboring station running in Ad hoc Mode. Stations set to ad hoc mode communicate with each other directly, without the use of a traditional AP. Ad-hoc mode is an IEEE 802.11 Wireless Networking Framework also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS).

- **SSID**—The Service Set Identifier (SSID) for the AP.

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.

NOTE You can set the SSID on the Wireless > Wireless Network Setup (VAPs) page.

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

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

  The number shown indicates the mode according to the following map:
  - 2.4 indicates IEEE 802.11b, 802.11g, or 802.11n mode (or a combination of the modes).
  - 5 indicates IEEE 802.11a or 802.11n mode (or both modes).
- **Channel**—The channel on which the AP is currently broadcasting.

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

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

  The current rate will always be one of the rates shown in Supported Rates.
- **Signal**—The strength of the radio signal emitting from this AP. If you hover the mouse pointer over the bars, a number representing the strength in decibels (dB) displays.
- **Beacons**—The total number of beacons received from this AP since it was first discovered.

- **Last Beacon**—The date and time of the last beacon received from this AP.
- **Rates**—Supported and basic (advertised) rate sets for the neighboring AP. Rates are shown in megabits per second (Mbps).

  All Supported Rates are listed, with Basic Rates shown in bold. Rate sets are configured on the Wireless > Radio page.

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

Use the Import AP List from a file feature to import a list of known APs from a saved list. The list might be acquired from another AP or created from a text file. If the MAC address of an AP appears in the Trusted AP List, it will not be detected as a rogue.

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

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

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

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

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

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

STEP 3 Click **Import**.

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

TSPEC Status and Statistics

The TSPEC Status and Statistics page provides the following:

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

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

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

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

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

  NOTE This is a configuration status (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 (in 32 microsecond per second units) allocated for this Access Category over the transmission medium to carry data. This value should be less than or equal to the maximum bandwidth allowed over the medium for this TS.
- **Medium Time Unallocated**—Time (in 32 microsecond per second units) of unused bandwidth for this Access Category.

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

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

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

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

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

TSPEC AP Statistics

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

The TSPEC AP Statistics page displays the following information:

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

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

RADIO Statistics

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

The following information displays:

- **Packets Received**—Total packets received by the AP.
- **Bytes Received**—Total bytes received by the AP.
- **Packets Transmitted**—Total packets transmitted by the AP.
- **Bytes Transmitted**—Total bytes transmitted by the AP.
- **Packets Receive Dropped**—Number of packets received by the AP that were dropped.
- **Bytes Receive Dropped**—Number of bytes received by the AP that were dropped.
- **Packets Transmit Dropped**—Number of packets transmitted by the AP that were dropped.
- **Bytes Transmit Dropped**—Number of bytes transmitted by the AP that were dropped.
- **Fragments Received**—Number of fragmented frames received by the AP.
- **Fragments Transmitted**—Number of fragmented frames sent by the AP.
- **Multicast Frames Received**—Count of MSDU frames received with the multicast bit set in the destination MAC address.
- **Multicast Frames Transmitted**—Count of successfully transmitted MSDU frames where the multicast bit is set in the destination MAC address.
- **Duplicate Frame Count**—Number of times a frame is received and the Sequence Control field indicates is a duplicate.
- **Failed Transmit Count**—Number of times an MSDU is not transmitted successfully due to transmit attempts exceeding either the short retry limit or the long retry limit.
- **Transmit Retry Count**—Number of times an MSDU is successfully transmitted after one or more retries.

- **Multiple Retry Count**—Number of times an MSDU is successfully transmitted after more than one retry.
- **RTS Success Count**—Count of CTS frames received in response to an RTS frame.
- **RTS Failure Count**—Count of CTS frames not received in response to an RTS frame.
- **ACK Failure Count**—Count of ACK frames not received when expected.
- **FCS Error Count**—Count of FCS errors detected in a received MPDU frame.
- **Frames Transmitted Count**—Count of each successfully transmitted MSDU.
- **WEP Undecryptable Count**—Count of encrypted frames received and the key configuration of the transmitter indicates that the frame should not have been encrypted or that frame was discarded due to the receiving station not implementing the privacy option.

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

Email Alert Status

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

This page displays the following fields:

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

Log

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

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

This page displays the following fields for each log entry:

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

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

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

4

LAN Settings

This chapter describes how to configure the AP's port, network, and clock settings.

It includes the following topics:

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

Port Settings

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

To view and configure LAN settings:

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

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

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

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

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

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

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

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

LAN

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

To configure LAN settings:

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

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

STEP 2 Configure the following Global Settings:

- **Management VLAN ID—**The VLAN associated with the IP address you use to access the AP. The default management VLAN ID is 1.

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

  The VLAN VLAN ID range is 1 to 4094.

- **Port VLAN ID**—This VLAN ID is used as the default VLAN for any traffic received on the LAN port that arrives without a VLAN tag. The AP supports one untagged VLAN on the LAN interface.

  VLAN 1 is the both default untagged VLAN and the default management VLAN. If you want to segregate management traffic from the untagged VLAN traffic, set this value to a different value than the management VLAN ID.

  The valid VLAN ID range is 1 to 4094.

- **Admit Only VLAN Tagged Frames**—Select to enable the forwarding of traffic that is received with no VLAN tag. Clear the checkbox if you want untagged traffic to be forwarded on the VLAN identified by the Port VLAN ID value.

STEP 3 Configure the following IPv4 settings:

- **Connection Type**—By default, the DHCP client on the WAP121/WAP321 automatically broadcasts requests for network information. If you want to use a static IP address, you must disable the DHCP client and manually configure the IP address and other network information.

  Select one of the following values from the list:

  - **DHCP**—The AP will acquire its IP address from a DHCP server on the LAN.
  - **Static IP**—You will manually assign an IP address to the AP.

- **Static IP Address, Subnet Mask, and Default Gateway—**If you elected to assign a static IP address, enter the IP information:

- **Domain Name Servers**—Select an option from the list:

  - **Dynamic**—The AP will acquire DNS server addresses from a DHCP server on the LAN.
  - **Manual**—You will manually configure one or more DNS server addresses. Enter up to two IP addresses in the text boxes provided.

STEP 4 Configure the following IPv6 settings:

- **IPv6 Connection Type**—How the switch obtains an IPv6 address:

  - **DHCPv6**—The IPv6 address will be assigned by a DHCPv6 server.
  - **Static IPv6**—You will manually configure the IPv6 address.

- **IPv6 Administration Mode**—Enables IPv6 management access.

- **IPv6 Auto Configuration Administration Mode**—Select to enable IPv6 automatic address configuration on the AP.

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

- **Static IPv6 Address**—The static IPv6 address. The AP 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 0–128.
- **IPv6 Autoconfigured Global Addresses**—If the AP has been assigned one or more IPv6 addresses automatically, the addresses are listed.
- **IPv6 Link Local Address**—The IPv6 address used by the local physical link. The link local address is not configurable and is assigned by using the IPv6 Neighbor Discovery process.
- **Default IPv6 Gateway**—The statically configured default IPv6 gateway.

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

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

Time Settings

A system clock is used to provide a network-synchronized time-stamping service for switch software events such as message logs. You can configure the system clock manually or configure the switch 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 AP is configured to obtain its time from a predefined list of NTP servers.

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

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

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

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

STEP 2 Configure the following parameters:

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

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

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

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

To manually configure the time settings:

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

STEP 2 Configure the following parameters:

- **System Date**—Select the current month, day, and year date from the drop-down lists.
- **System Time**—Select the current hour and minutes in 24-hour clock format, such as 22:00:00 for 10 p.m.
- **Time Zone—**Select the time zone for your location.

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

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

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

Wireless Settings

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

It includes the following topics:

- **Radio**
- **Networks**
- **Scheduler**
- **Scheduler Association**
- **Bandwidth Utilization**
- **MAC Filtering**
- **WDS Bridge**
- **Work Group Bridge**
- **QoS**
- **WPS Setup**
- **WPS Process**

Radio

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

To configure radio settings:

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

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

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

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

  NOTE The modes available depend on the country code setting.

  Select one of the following modes:

  - 802.11a—Only 802.11a clients can connect to the AP.
  - 802.11b/g—802.11b and 802.11g clients can connect to the AP.
  - 802.11a/n—802.11a clients and 802.11n clients operating in the 5-GHz frequency can connect to the AP.
  - 802.11b/g/n (default)—802.11b, 802.11g, and 802.11n clients operating in the 2.4-GHz frequency can connect to the AP.
  - 5 GHz 802.11n—Only 802.11n clients operating in the 2.4-GHz frequency can connect to the AP.
  - 2.4 GHz 802.11n—Only 802.11n clients operating in the 5-GHz frequency can connect to the AP.
- **Channel Bandwidth** (802.11n modes only)—The 802.11n specification allows a 40 MHz-wide channel in addition to the legacy 20 MHz channel available with other modes. The 40 MHz channel enables higher data rates but leaves fewer channels available for use by other 2.4 GHz and 5 GHz devices.

  Set the field to 20 MHz to restrict the use of the channel bandwidth to a 20 MHz channel.
- **Primary Channel** (802.11n modes with 40 MHz bandwidth only)—A 40 MHz channel can be considered to consist of two 20 MHz channels that are contiguous in the frequency domain. These two 20 MHz channels are often

referred to as the Primary and Secondary channels. The Primary Channel is used for 802.11n clients that support only a 20 MHz channel bandwidth and for legacy clients.

Select one of the following options:

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

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

  The range of available channels is determined by the mode of the radio interface and the country code setting. If you select **Auto** for the channel setting, the AP scans available channels and selects a channel where no traffic is detected.

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

NOTE The modes available depend on the country code setting. □

Country code is assigned in the flash when mass produced in factory. User won't be □ able to select country in web GUI. Different country code will have different channel □ range. For example, US sku will meet FCC regulation. Its channel will be 1~11 at □ 2.4G; Band 1 and Band 4 at 5G. EU sku will meet CE regulation. Its channel will be □ 1~13 at 2.4G; Band 1 only at 5G.

STEP 4 In the Advanced Settings area, configure the following settings:□
Short Guard Interval Supported —This field is available only if the selected□ radio mode includes 802.11n.□

□

The guard interval is the dead time, in nanoseconds, between OFDM□ symbols. The guard interval prevents Inter-Symbol and Inter-Carrier□ Interference (ISI, ICI). The 802.11n mode allows for a reduction in this guard□ interval from the a and g definition of 800 nanoseconds to 400 nanoseconds.□ Reducing the guard interval can yield a 10% improvement in data throughput.□

□

The client with which the AP is communicating must also support the short□ guard interval.□

□

Select one of the following options:□

□

Yes—The AP transmits data using a 400 ns guard Interval when□ communicating with clients that also support the short guard interval.□

□

No—The AP transmits data using an 800 ns guard interval.

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

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

  NOTE This setting does not affect the ability of the client to associate with the AP.

- **Beacon Interval**—The interval between the transmission of beacon frames. The AP transmits these at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second).

  Enter a value from 20 to 2000 milliseconds.

- **DTIM Period**—The Delivery Traffic Information Map (DTIM period, from 1 to 255 beacons.

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

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

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

- **Fragmentation Threshold**—The frame size threshold in bytes, from 256 to 2,346.

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

  If the packet being transmitted is equal to or less than the threshold, fragmentation is not used.

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

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

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

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

- **RTS Threshold**—The Request to Send (RTS) Threshold value, from 0 to 2347.

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

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

- **Maximum Associated Clients**—The maximum number of stations allowed to access this AP at any one time.

  You can enter a value between 0 and 200.

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

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

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

- **Fixed Multicast Rate**—The multicast traffic transmission rate the AP supports.
- **Legacy Rate Sets**—The transmission rate sets the AP supports and the basic rate sets the AP advertises:

  Rates are expressed in megabits per second.

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

  Basic Rate Sets indicate rates that the AP will advertise to the network for the purposes of setting up communication with other APs and client stations on the network. It is generally more efficient to have an AP broadcast a subset of its supported rate sets.
- **MCS (Data Rate) Settings**—The Modulation and Coding Scheme (MCS) index values that the AP advertises. MCS can enhance throughput for 802.11n wireless clients.

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

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

  The MCS settings can be configured only if the radio mode includes 802.11n support.
- **Broadcast/Multicast Rate Limiting**—Multicast and broadcast rate limiting can improve overall network performance by limiting the number of packets transmitted across the network.

  By default the Multicast/Broadcast Rate Limiting option is disabled. Until you enable Multicast/Broadcast Rate Limiting, the following fields will be disabled.
- **Rate Limit**—The rate limit for multicast and broadcast traffic. The limit should be greater than 1, but less than 50 packets per second. Any traffic that falls below this rate limit will always conform and be transmitted to the appropriate destination.

  The default and maximum rate limit setting is 50 packets per second.

- **Rate Limit Burst**—Setting a rate limit burst determines how much traffic bursts can be before all traffic exceeds the rate limit. This burst limit allows intermittent bursts of traffic on a network above the set rate limit.

  The default and maximum rate limit burst setting is 75 packets per second.

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

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

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

- **TSPEC Voice ACM Mode** —Regulates mandatory admission control (ACM) for the voice access category. The options are:

  - **On** — A station is required to send a TSPEC request for bandwidth to the AP before sending or receiving a voice traffic stream. The AP responds with the result of the request, which includes the allotted medium time if the TSPEC was admitted.

  - **Off** — A station can send and receive voice priority traffic without requiring an admitted TSPEC; the AP ignores voice TSPEC requests from client stations.

- **TSPEC Voice ACM Limit** —The upper limit on the amount of traffic the AP attempts to transmit on the wireless medium using a voice AC to gain access.

- **TSPEC Video ACM Mode** —Regulates mandatory admission control for the video access category. The options are:

  - **On** — A station is required to send a TSPEC request for bandwidth to the AP before sending or receiving a video traffic stream. The AP 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 AP ignores video TSPEC requests from client stations.

- **TSPEC Video ACM Limit** —The upper limit on the amount of traffic the AP attempts to transmit on the wireless medium using a video AC to gain access.

- **TSPEC AP Inactivity Timeout** —The amount of time for an AP to detect an downlink TS as idle before deleting it.
- **TSPEC Station Inactivity Timeout** —The amount of time for an AP to detect an uplink TS as idle before deleting it.
- **TSPEC Legacy WMM Queue Map Mode** —Enables or disables the intermixing of legacy traffic on queues operating as ACM.

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

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

Networks

Virtual Access Points (VAPs) segment the wireless LAN into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. VAPs simulate multiple APs in one physical AP. Up to 4 VAPs are supported on the WAP121 and up to 8 VAPs are supported on the WAP321.

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

Each VAP is identified by a user-configured Service Set Identifier (SSID). Multiple VAPs can have the same SSID. Whether the AP broadcasts an SSID is enabled or disabled independently on each VAP. By default, SSIDs are not broadcast. When SSID broadcasts are disabled the VAP suppresses responses to probes from clients.

SSID Naming Conventions

The default SSID for VAP0 is ‘ciscosb’. For all other VAPs, the default SSID is “Virtual Access Point x” where ‘x’ is the VAP number in the range of 1–4 for the WAP121 and 1–8 for the WAP321. The SSIDs for all VAPs can be configured to other values.

The SSID can be any alphanumeric, case-sensitive entry from 2 to 32 characters. The printable characters plus the space (ASCII 0x20) are allowed, but the following 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, the following three characters cannot be the first character:

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

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

NOTE This means that spaces are allowed within the SSID, but not as the first or last character, and the period "." (ASCII 0x2E) is also allowed.

VLAN IDs

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

By default, the VID assigned to the management interface for the AP 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 that VAP can administer the AP. If needed, an access control list (ACL) can be created to disable administration from WLAN clients.

Configuring VAPs

To configure VAPs:

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

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

—Or—

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

NOTE: VAP0 is not editable.

STEP 3 Configure the parameters:

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

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

  You configure the untagged and management VLAN IDs on the Ethernet Settings page. For more information, see **LAN, page 31**.

- **SSID**—A name for the wireless network. The SSID is an alphanumeric string of up to 32 characters. You can use the same SSID for multiple VAPs, or you can choose a unique SSID for each VAP.

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

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

  Specify whether to allow the AP to broadcast the Service Set Identifier (SSID) in its beacon frames. The Broadcast SSID parameter is enabled by default. When the VAP does not broadcast its SSID, the network name is not displayed in the list of available networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it is able to connect.

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

- **Security**—The type of authentication required for access to the VAP:

  - None

- Static WEP
- Dynamic WEP
- WPA Personal
- WPA Enterprise

If you select a security mode other than None, additional fields appear. These fields are explained in **Configuring Security Settings, page 47**.

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

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

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

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

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

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

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

Configuring Security Settings

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

None (Plain-text)

If you select None as your security mode, no further options are configurable on the AP. This mode means that any data transferred to and from the AP 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 APs on the network are configured with a static 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

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

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

The following parameters display for Static WEP configuration:

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

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

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

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

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

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

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

- **Shared Key** authentication requires the client station to have the correct WEP key in order to associate with the AP. When the authentication algorithm is set to Shared Key, a station with an incorrect WEP key will not be able to associate with the AP.

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

Static WEP Rules

If you use Static WEP, the following rules apply:

- All client stations must have the Wireless LAN (WLAN) security set to WEP, and all clients must have one of the WEP keys specified on the AP in order to de-code AP-to-station data transmissions.

- The AP must have all keys used by clients for station-to-AP transmit so that it can de-code the station transmissions.

- The same key must occupy the same slot on all nodes (AP and clients). For example if the AP defines abc123 key as WEP key 3, then the client stations must define that same string as WEP key 3.

- Client stations can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)

- On some wireless client software, you can configure multiple WEP keys and define a client station “transfer key index”, and then set the stations to encrypt the data they transmit using different keys. This ensures that neighboring APs cannot decode each other’s transmissions.

- You cannot mix 64-bit and 128-bit WEP keys between the access point and its client stations.

Dynamic WEP

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

EAP messages 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 AP requires a RADIUS server that supports EAP, such as the Microsoft Internet Authentication Server. To work with 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 AP uses.

The following parameters display for Dynamic WEP configuration:

- **Use Global RADIUS Server Settings**—By default, each VAP uses the global RADIUS settings that you define for the AP (see **RADIUS Server, page 110**. However, you can configure each VAP to use a different set of RADIUS servers.

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

  To use a separate RADIUS server for the VAP, clear the check box and enter the RADIUS server IP address and key in the following 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 AP contacts only the RADIUS server or servers for the address type you select in this field.

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

  When the first wireless client tries to authenticate with the AP, the AP sends an authentication request to the primary server. If the primary server responds to the authentication request, the AP continues to use this RADIUS server as the primary server, and authentication requests are sent to the address you specify.

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

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

- **Key**—The shared secret key that the AP uses to authenticate to the primary RADIUS server.

  You can use up to 63 standard alphanumeric and special characters. The key is case sensitive and must match the key configured on the RADIUS server. The text you enter will be displayed as "*" characters.

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

- **Enable RADIUS Accounting**—Enables tracking and measuring the resources a particular user has consumed, such as system time, amount of data transmitted and received, and so on.

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

- **Active Server**—Enables administratively selecting the active RADIUS server, rather than having the AP attempt to contact each configured server in sequence and choose the first server that is up.

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

  The default is 300. The valid range is 0–86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

- **Session Key Refresh Rate**—The interval at which the AP refreshes session (unicast) keys for each client associated to the VAP.

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

WPA Personal

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

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

The following parameters display for WPA Personal configuration:

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

  If the network has a mix of clients, some of which support WPA2 and others which support only the original WPA, select both of the check boxes. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.

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

  You can select either or both. Both TKIP and AES clients can associate with the AP. WPA clients must have one of the following to be able to associate with the AP:

  - A valid TKIP key
  - A valid AES-CCMP key

  Clients not configured to use a WPA Personal will not be able to associate with the AP.

- **Key**—The shared secret key for WPA Personal security. Enter a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.

- **Key Strength Meter**—The AP checks the key against complexity criteria such as how many different types of characters (uppercase, lowercase, numbers, and special characters) are used and how long the string is. If the WPA-PSK complexity check feature is enabled, the key will not be accepted unless it meets the minimum criteria. See **WPA-PSK Complexity, page 114** for information on configuring the complexity check.

- **Broadcast Key Refresh Rate**—The interval at which the broadcast (group) key is refreshed for clients associated to this VAP (the default is 300). The valid range is 0–86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

WPA Enterprise

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

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

The following parameters display for WPA Enterprise configuration:

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

  Click **Enable** pre-authentication if you want WPA2 wireless clients to send pre-authentication packet. The pre-authentication information will be relayed from the AP the client is currently using to the target AP. Enabling this feature can help speed up authentication for roaming clients who connect to multiple APs.

  This option does not apply if you selected WPA for WPA Versions because the original WPA does not support this feature.
- **Cipher Suites**—The cipher suite you want to use:
  - TKIP

  - CCMP (AES)
  - TKIP and CCMP (AES)

  By default both TKIP and CCMP are selected. When both TKIP and CCMP are selected, client stations configured to use WPA with RADIUS must have one of the following:

  - 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 AP (see **RADIUS Server, page 110**. However, you can configure each VAP to use a different set of RADIUS servers.

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

  To use a separate RADIUS server for the VAP, clear the check box and enter the RADIUS server IP address and key in the following 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 AP contacts only the RADIUS server or servers for the address type you select in this field.

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

  If the IPv4 RADIUS IP Address Type option is selected in the previous field, enter the IP address of the RADIUS server that all VAPs use by default, for example 192.168.10.23. If the IPv6 RADIUS IP Address Type option is selected, enter the IPv6 address of the primary global RADIUS server, for example 2001:0db8:1234::abcd.

- **Server IP Address** or **Server IPv6 Address 1–3**—Up to three IPv4 and/or IPv6 addresses to use as the backup RADIUS servers for this VAP.The field label is RADIUS IP Address when the IPv4 RADIUS IP Address Type option is selected and RADIUS IPv6 Address when the IPv6 RADIUS IP Address Type option is selected.

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

- **Key**—The RADIUS key is the shared secret key for the global RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive, and you must configure the same key on the AP and on your RADIUS server. The text you enter will be displayed as "*" characters to prevent others from seeing the RADIUS key as you type.
- **Key 1–3**—The RADIUS key associated with the configured backup RADIUS servers. The server at RADIUS IP Address-1 uses RADIUS Key-1, RADIUS IP Address-2 uses RADIUS Key-2, and so on.
- **Enable RADIUS Accounting**—Tracks and measures the resources a particular user has consumed such as system time, amount of data transmitted and received, and so on.

  If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers.
- **Active Server**—Enables administratively selecting the active RADIUS server, rather than having the AP attempt to contact each configured server in sequence and choose the first server that is up.

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

  The default is 300. The valid range is 0–86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.
- **Session Key Refresh Rate**—The interval at which the AP refreshes session (unicast) keys for each client associated to the VAP.

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

Scheduler

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

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

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

Adding Scheduler Profiles

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

To view Scheduler status and add a Scheduler profile:

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

STEP 2 Ensure that the **Administrative Mode** is enabled. By default it is disabled.

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

- **Status**—The operational status of the Scheduler. The range is Up or Down. The default is Down.
- **Reason**—The reason for the scheduler operational status. Possible values are:
  - IsActive—The scheduler is administratively enabled.
  - ConfigDown—Operational status is down because global configuration is disabled.
  - TimeNotSet—Time is set on the AP neither manually nor through NTP.

STEP 3 To add a profile, enter a profile name in the **Scheduler Profile** text box and click **Add**.

The profile name can be up to 32 alphanumeric characters.

Configuring Scheduler Rules

You can configure up to 16 rules for a profile. Each rule specifies the start time, end time and day (or days) of the week the radio or VAP can be operational. The rules are periodic in nature and are repeated every week. A valid rule must contain all of the parameters (days of the week, hour, and minute) for the start time and the end time. Rules cannot conflict; for example, you can configure one rule to start on each weekday and another to start on each weekend day, but you cannot configure one rule to begin daily and another rule to begin on weekends.

To configure a rule for a profile:

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

STEP 2 Click **Add Rule**.

The new rule displays in the rule table.

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

STEP 4 From the **Day of the Week** menu, select the recurring schedule for the rule. You can configure the rule to occur daily, each weekday, each weekend day (Saturday and Sunday), or any single day of the week.

STEP 5 Set the start and end times:

- **Start Time**—The time when the radio or VAP will be operationally enabled. The time is in HH:MM 24-hour format. The range is <00-24>:<00-59>. The default is 00:00.

- **End Time**—The time when the radio or VAP will be operationally disabled. The time is in HH:MM 24-hour format. The range is <00-24>:<00-59>. The default is 00:00.

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

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

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

Scheduler Association

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

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

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

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

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

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

Bandwidth Utilization

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

To enable bandwidth utilization:

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

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

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

The default is 0, which means that all new associations will be allowed regardless of the utilization rate.

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

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

MAC Filtering

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

Configuring a MAC Filter List Locally on the AP

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

The AP supports one local MAC filter list only; that is, the same list applies to all VAPs that are enabled to use the local list. The filter can be configured to grant access only to the MAC addresses on the list, or to deny access only to addresses on the list.

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

To configure MAC filtering:

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

STEP 2 Select how the AP uses the filter list:

- **Allow only stations in the list**. Any station that is not in the Stations List is denied access to the network through the AP.
- **Block all stations in list**. Only the stations that appear in the list are denied access to the network through the AP. All other stations are permitted access.

  NOTE: The filter setting also applies to the MAC filtering list stored on the RADIUS server, if one exists.

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

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

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

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

NOTE: Changing some settings might cause the AP to stop and restart system processes. If this happens, wireless clients will temporarily lose connectivity. We recommend that you change AP settings when WLAN traffic is low.

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 the following table.

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

WDS Bridge

The Wireless Distribution System (WDS) allows you to connect multiple APs. With WDS, APs communicate with one another without wires in a standardized way. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required. You can configure the AP 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 AP accepts client associations and communicates with wireless clients and other repeaters. The AP forwards all traffic meant for the other network over the tunnel that is established between the APs. 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 AP acts as the common link between multiple APs. In this mode, the central AP accepts client associations and communicates with the clients and other repeaters. All other APs associate only with the central AP that forwards the packets to the appropriate wireless bridge for routing purposes.

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

Before you configure WDS on the AP, note the following guidelines:

- When using WDS, be sure to configure WDS settings on both APs participating in the WDS link.
- You can have only one WDS link between any pair of APs. That is, a remote MAC address may appear only once on the WDS page for a particular AP.
- Both APs participating in a WDS link must be on the same Radio channel and using the same IEEE 802.11 mode. (See **Radio, page 36** for information on configuring the radio mode and channel.)
- When 802.11h is operational, setting up two WDS links can be difficult. See **Using the 802.11h Wireless Mode, page 60**.
- If you use WPA encryption on the WDS link VAP0 must use WPA Personal or WPA Enterprise as the security mode.

To configure a WDS bridge:

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

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

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

STEP 4 Configure the remaining parameters:

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

  If you are unconcerned about security issues on the WDS link, you may decide not to set any type of encryption. Alternatively, if you have security concerns you can choose between Static WEP and WPA Personal. In WPA Personal mode, the AP uses WPA2-PSK with CCMP (AES) encryption over the WDS link.

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

  See **Configuring Security Settings, page 47** for more information about WEP and WPA Personal security settings.

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

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

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

Work Group Bridge

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

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

It is recommended that Work Group Bridge mode be used only when the WDS bridge feature cannot be operational with a peer AP. WDS is a better solution and is preferred over the Work Group Bridge solution. The Work Group Bridge feature should be used only when WDS links cannot be established due to hardware mismatches within an extended service set (ESS). When the Work Group Bridge feature is enabled, the VAP configurations are not applied; only the Work Group Bridge configuration is applied.

NOTE The WDS feature does not work when the Work Group Bridge mode is enabled on the AP.

In Work Group Bridge mode, the BSS managed by the AP while operating in AP mode is referred to as the downstream BSS, and associated STAs as downstream STAs. The BSS managed by the other AP (i.e., the one to which the AP associates as an STA) is referred to as the upstream BSS, and the other AP is referred as the upstream AP.

The devices connected to the wired interface of the AP, as well as the downstream stations associated to the AP's downstream BSS can access the network connected by the upstream BSS. To allow the bridging of packets, the VLAN configuration for the downstream BSS and wired interface should match that of the upstream BSS.

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

NOTE Work Group Bridge mode currently supports only IPv4 traffic.

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

To configure Work Group Bridge mode:

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

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

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

- **SSID**—The SSID if the BSS
- **Broadcast SSID** (downstream only)—Select **On** if you want the downstream SSID to be broadcast. SSID Broadcast is off by default.
  - **None**

- **Static WEP**
- **WPA Personal**

See **Configuring Security Settings, page 47** for information about WEP and WPA Personal security settings.

Configure the upstream BSS with the same SSID and security as advertised by upstream AP. The upstream BSS will be associated to the upstream AP with the configured credentials. The AP may obtains its IP address from a DHCP server on the upstream link. Alternatively, you can assign a static IP address.

In the downstream direction, clients associate to the downstream BSS.

- **Security**—The type of security to use for authenticating as a client station on the upstream AP and for authenticating downstream client stations to the AP.
- **MAC Filtering**—Select one of the following:
  - **Disabled**—The set of clients in the APs BSS that can access the upstream network is not restricted to the clients specified in a MAC address list.
  - **Local**—The set of clients in the APs BSS that can access the upstream network is restricted to the clients specified in a locally defined MAC address list.
  - **RADIUS**—The set of clients in the APs BSS that can access the upstream network is restricted to the clients specified in a MAC address list on a RADIUS server.

  If you select Local or RADIUS, see **MAC Filtering, page 59** for instructions on creating the MAC filter list.
- **VLAN ID**—The VLAN associated with the BSS.

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

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

QoS

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

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

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

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

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

To configure AP and Station EDCA parameters:

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

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

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

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

- Data 0 (Voice)—High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
- Data 1 (Video)—High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
- Data 2 (Best Effort)—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.

- Data 3 (Background)—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

To configure QoS on the AP:

STEP 3 Configure the following parameters:

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

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

  This value is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.

  The first random number generated will be a number between 0 and the number specified here.

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

  Valid values for are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. This value must be lower than the value for the Maximum Contention Window.
- **Maximum Contention Window**—The upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.

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

  Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. This value must be higher than the value for the Minimum Contention Window.
- **Maximum Burst** (AP only)—An AP EDCA parameter that applies only to traffic flowing from the AP to the client station.

  This value specifies (in milliseconds) the maximum burst length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance.

Valid values are 0.0 through 999.

- **Wi-Fi MultiMedia (WMM)**—Select **Enabled** to enable Wi-Fi MultiMedia (WMM) extensions. This is enabled by default. With WMM enabled, QoS prioritization and coordination of wireless medium access is on. With WMM enabled, QoS settings on the AP control downstream traffic flowing from the AP 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 AP. With WMM disabled, you can still set some parameters on the downstream traffic flowing from the AP 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 AP. The Transmission Opportunity (TXOP) is an interval of time, in milliseconds, when a WME client station has the right to initiate transmissions onto the wireless medium (WM) towards the Unified Access Point. The TXOP Limit maximum value is 65535.

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

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

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

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

WPS Setup

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

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

WPS Overview

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

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

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

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

Usage Scenarios

Typical scenarios for using WPS include the following:

- A user wishes to enroll a client station on a WPS-enabled WLAN. (The enrolling client device may detect the network, and prompt the user to enroll, although this is not necessary.) The user triggers the enrollment by pushing a button on the device. The AP's administrator then pushes a button on the AP. During a brief exchange of WPS protocol messages, the AP supplies the new client with a new security configuration via the Extensible Authentication Protocol (EAP). The two devices disassociate, and then reassociate and authenticate with the new settings.
- A user wishes to enroll a client station on a WPS-enabled WLAN by supplying the AP administrator with the PIN of the client device. The administrator enters this PIN on the UI of the AP and triggers the device enrollment. The new enrollee and the AP exchange WPS messages, including a new security configuration, disassociate, reassociate, and authenticate.
- An AP administrator purchases a new AP that has been certified by the Wi-Fi Alliance to be compliant with WPS version 2.0, and wishes to add the AP to an existing (wired or wireless) network. The administrator turns on the AP, and then accesses a network host that supports the WPS registration protocol. The administrator enters the AP device’s pin on the UI of this

"external registrar," and triggers the WPS registration process at this UI. (On a wired LAN, the WPS protocol messages are transported via the Universal Plug and Play, or UPnP, protocol.) The host registers the AP as a new network device and configures the AP with new security settings.

- An AP administrator has just added a new AP to an existing (wireless or wired) network via WPS, and wishes to grant network access to a new client device. The device is enrolled through either the "PIN" or "push button control (PBC)" methods described above, but this time the device enrolls with the external registrar, with the AP acting solely as a proxy.
- A wireless device that does not support WPS must join the WPS-enabled WLAN. The administrator, who cannot use WPS in this case, instead manually configures the device with the SSID, public shared key, and cryptography modes of the WPS-enabled AP. The device joins the network.

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

WPS Roles

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

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

The WAP121 can act as an AP and supports an internal registrar. It does not function as a enrollee.

Enabling and disabling WPS on a VAP

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

- The AP is configured to broadcast the VAP SSID.
- MAC address filtering is disabled on the VAP.
- WEP encryption is disabled on the VAP.

- The VAP is configured to use either WPA-Personal security or none. If WPA2-PSK encryption mode is enabled, then an valid pre-shared key (PSK) must be configured and CCMP (AES) encryption must be enabled.
- The VAP is operationally enabled.

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

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

External and Internal Registration

It is not necessary for the WAP121 itself to handle the registration of clients on the network. The AP can either use its internal registrar, or act as a proxy for an external registrar. The external registrar may be accessed either via the wired or wireless LAN. An external registrar may also configure the SSID, encryption mode, and public shared key of a WPS-enabled BSS. This capability is very useful for "out-of-box" deployments; that is, when an administrator simply attaches a new AP to a LAN for the first time.

If the AP is using an internal registrar, it enrolls new clients using the configuration of the VAP associated with the WPS service, whether this configuration was configured directly on the AP or acquired by an external registrar through WPS.

Client Enrollment

Push-button Control

The AP enrolls 802.11 clients via WPS by one of two methods: the push-button control (PBC) method, or the personal identification number (PIN) method.

Using the PBC method, when the user of a prospective client pushes a button on the enrolling device, the administrator of the AP with an enabled internal registrar pushes a similar (hardware or software) button. This sequence begins enrollment process, and the client device joins the network. Although the WAP121 does not support an actual hardware button, it allows the administrator to initiate the enrollment for a particular VAP using a “software button” in the web-based AP configuration utility.

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