PIN Control

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

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

Optional Use of Internal Registrar

Although the AP supports an internal registrar for WPS, its use is optional. After an external registrar has configured the AP, the AP acts as a proxy for that external registrar, regardless of whether the AP's internal registrar is enabled (it is enabled by default).

Lockdown Capability

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

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

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

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

VAP Configuration Changes

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

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

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

External Registration

The AP supports the registration with WPS external registrars (ER) on the wired and wireless LAN. On the WLAN, external registrars advertise their capabilities within WPS-specific information elements (IEs) of their beacon frames; on the wired LAN, external registrars announce their presence via UPnP.

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

1. Initiating the registration process on the AP by entering the ER's PIN on the AP.
2. Registering the AP by entering the AP's PIN on the user interface of the ER.

NOTE The registration process can also configure the AP as specified in **VAP Configuration Changes, page 72** if the AP has declared within the WPS-specific IEs of its beacon frames or UPnP messages that it requires such configuration.

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

Exclusive Operation of WPS Transactions

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

Backward Compatibility with WPS Version 1.0

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

Configuring WPS Settings

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

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

To configure the AP as a WPS-capable device:

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

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

STEP 2 Configure the global parameters:

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

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

STEP 3 Configure the WPS instance parameters:

- **WPS Instance ID**—An identifier for the instance. As there is only one instance, the only option is wps1.
- **WPS Mode**—Enables or disables the instance.
- **WPS VAP**—The VAP associated with this WPS instance.
- **WPS Built-in Registrar**—Select to enable the built-in registrar function. When disabled, another device on the network can act as the registrar and the AP can serve as a proxy for forwarding client registration requests and the registrar's responses.
- **WPS Configuration State**—Whether the VAP will be configured from the external registrar as a part of WPS process. It can be set to one of the following values:
  - **Unconfigured**—VAP settings will be configured using WPS, after which the state will be change to Configured.
  - **Configured**—VAP settings will not be configured by the external registrar and will retain the existing configuration.

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

The operational status of the instance and the reason for that status also display. See **Enabling and disabling WPS on a VAP, page 69** for information about conditions that may cause the instance to be disabled.

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

WPS Process

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

Enrolling a Client Using the PIN Method

To enroll a client station using the PIN method:

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

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

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

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

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

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

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

Enrolling a Client Using the Push Button Method

To enroll a client station using the push method:

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

STEP 2 Push the hardware button on the client station.

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

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

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

Viewing Instance Summary Information

The following information displays for WPS instance:

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

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

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

6

SNMPv3

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

It contains the following topics:

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

SNMP Overview

Simple Network Management Protocol (SNMP) defines a standard for recording, storing, and sharing information about network devices. SNMP facilitates network management, troubleshooting, and maintenance.

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

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

General SNMP Settings

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

To configure general SNMP settings:

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

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

STEP 3 Configure the parameters:

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

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

  The community name can be in any alphanumeric format.

- **UDP Port**—By default an SNMP agent only listens to requests from logical port 161. However, you can configure this so the agent listens to requests on another port. The valid range is 1-65535.

- **SNMP Set**—When enabled, machines on the network can execute configuration changes via an SNMP agent to the System MIB on the AP.

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

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

  The community name can be in any alphanumeric format.

- **Management Station**—Determines which stations can access the AP via SNMP: Select one of the following:

  - **All**—The set of stations that can access the AP via SNMP is not restricted.

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

- **NMS Hostname, IPv4 Address/Name**—The IPv4 DNS hostname or subnet of the machines that can execute get and set requests to the managed devices. The valid range is 1–256 characters.

  As with community names, this provides a level of security on SNMP settings. The SNMP agent will only accept requests from the hostname or subnet specified here.

  To specify a subnet, enter one or more subnetwork address ranges in the form *address/mask_length* where *address* is an IP address and *mask_length* is the number of mask bits. Both formats *address/mask* and *address/mask_length* are supported. Individual hosts can be provided for this, i.e. I.P Address or Hostname. For example, if you enter a range of 192.168.1.0/24 this specifies a subnetwork with address 192.168.1.0 and a subnet mask of 255.255.255.0.

  The address range is used to specify the subnet of the designated NMS. Only machines with IP addresses in this range are permitted to execute get and set requests on the managed device. Given the example above, the machines with addresses from 192.168.1.1 through 192.168.1.254 can execute SNMP commands on the device. (The address identified by suffix .0 in a subnetwork range is always reserved for the subnet address, and the address identified by .255 in the range is always reserved for the broadcast address).

  As another example, if you enter a range of 10.10.1.128/25 machines with IP addresses from 10.10.1.129 through 10.10.1.254 can execute SNMP requests on managed devices. In this example, 10.10.1.128 is the network address and 10.10.1.255 is the broadcast address. 126 addresses would be designated.

- **NMS IPv6 Address/Name**—The IPv6 DNS hostname or subnet of the machines that can execute get and set requests to the managed devices.

- **Trap Community Name**—A global community string associated with SNMP traps. Traps sent from the device will provide this string as a community name.

  The community name can be in any alphanumeric format. Special characters are not permitted. The valid range is 1–256 characters

- **Trap Destination Table**—A list of up to three IP addresses or hostnames to receive SNMP traps. The valid range is 1-256 characters. Select the checkbox and choose a **Host Type** (IPv4 or IPv6) before adding the **IP Address/Hostname**.

An example of a DNS hostname is: `snmptraps.foo.com`. Since SNMP traps are sent randomly from the SNMP agent, it makes sense to specify where exactly the traps should be sent. You can add up to a maximum of three DNS hostnames. Ensure you select the **Enabled** check box and select the appropriate Host Type.

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

NOTE 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.

SNMP Views

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

The AP supports a maximum of 16 views.

The following notes summarize some critical guidelines regarding SNMPv3 view configuration. Please read all the notes before proceeding.

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

NOTE By default, view-all and view-none SNMPv3 views are created on the AP. These views cannot be deleted, but the OID, Mask, and Type fields can be modified.

To configure an SNMP view:

STEP 1 Click **SNMPv3** > **Views** in the navigation window.

STEP 2 Configure the parameters:

- **View Name**—A name that identifies the MIB view. View names can contain up to 32 alphanumeric characters.
- **Type**—Whether to include or exclude the view subtree or family of subtrees from the MIB view.

- **OID**—An OID string for the subtree to include or exclude from the view.

  For example, the system subtree is specified by the OID string .1.3.6.1.2.1.1.

- **Mask**—An OID mask. The mask is 47 characters in length. The format of the OID mask is xx.xx.xx (.)... or xx:xx:xx.... (:) and is 16 octets in length. Each octet is two hexadecimal characters separated by either . (period) or : (colon). Only hex characters are accepted in this field.

  For example, OID mask FA.80 is 11111010.10000000.

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

STEP 3 Click **Add**, and then click **Save**. The view is added to the SNMPv3 Views list and your changes are saved to the Running Configuration and to the Startup Configuration.

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

SNMP Groups

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

- .noAuthNoPriv.
- .authNoPriv.
- .authPriv.

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

By default, the AP has three groups:

- **RO**—A read-only group with no authentication and no data encryption. No security is provided by this group. By default, users of this group have read access to the default all MIB view, which can be modified by the user.
- **RWAuth**—A read/write group using authentication, but no data encryption. Users in this group send SNMP messages that use an MD5 key/password

for authentication, but not a DES key/password for encryption. By default, users of this group will have read and write access to the default all MIB view, which can be modified by the user.

- **RWPriv**—A read/write group using authentication and data encryption. Users in this group use an MD5 key/password for authentication and a DES key/password for encryption. Both the MD5 and DES key/passwords must be defined. By default, users of this group have read and write access to the default all MIB view, which can be modified by the user.

NOTE The default groups RO, RWAuth, and RWPriv cannot be deleted.

NOTE The AP supports a maximum of eight groups.

To add an SNMP group:

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

STEP 2 Configure the parameters:

- **Name**—A name that identifies the group. The default group names are RWPriv, RWAuth, and RO.

  Group names can contain up to 32 alphanumeric characters.

- **Security Level**—The security level for the group, which can be one of the following:

  - noAuthentication-noPrivacy—No authentication and no data encryption (no security).

  - Authentication-noPrivacy—Authentication, but no data encryption. With this security level, users send SNMP messages that use an MD5 key/password for authentication, but not a DES key/password for encryption.

- **Authentication-Privacy**—Authentication and data encryption. With this security level, users send an MD5 key/password for authentication and a DES key/password for encryption.

  For groups that require authentication, encryption, or both, you must define the MD5 and DES key/passwords on the SNMP Users page.

- **Write Views**—The write access to management objects (MIBs) for the group, which can be one of the following:

  - **write-all**—The group can create, alter, and delete MIBs.

  - **write-none**—The group cannot create, alter, or delete MIBS.

- **Read Views**—The read access to management objects (MIBs) for the group:
  - **view-all**—The group is allowed to view and read all MIBs.
  - **view-none**—The group cannot view or read MIBs.

STEP 3 Click **Add**, and then click **Save**. The group is added to the SNMPv3 Groups list and your changes are saved to the Running Configuration and to the Startup Configuration.

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

SNMP Users

You can use the SNMP Users page to define users, associate a security level to each user, and configure per-user security keys.

Each user is mapped to an SNMPv3 group, either from the predefined or user-defined groups, and, optionally, is configured for authentication and encryption. For authentication, only the MD5 type is supported. For encryption, only the DES type is supported. There are no default SNMPv3 users on the AP.

To add SNMP users:

STEP 1 Click **SNMPv3** > **Users** in the navigation window.

STEP 2 Configure the parameters:

- **Name**—A name that identifies the SNMPv3 user.

  User names can contain up to 32 alphanumeric characters.
- **Group**—The group that the user is mapped to. The default groups are RWAuth, RWPriv, and RO. You can define additional groups on the SNMP Groups page.
- **Authentication Type**—The type of authentication to use on SNMP requests from the user, which can be one of the following:
  - **MD5**—Require MD5 authentication on SNMPv3 requests from the user.
  - **None**—SNMPv3 requests from this user require no authentication.

- **Authentication Key**—(If you specify MD5 as the authentication type) A password to enable the SNMP agent to authenticate requests sent by the user.

  The password must be between 8 and 32 characters in length.

- **Encryption Type**—The type of privacy to use on SNMP requests from the user, which can be one of the following:
  - **DES**—Use DES encryption on SNMPv3 requests from the user.
  - **None**—SNMPv3 requests from this user require no privacy.
- **Encryption Key**—(If you specify DES as the privacy type) A key to use to encrypt the SNMP requests.

  The key must be between 8 and 32 characters in length.

STEP 3 Click **Add**, and then click **Save**. The user is added to the SNMPv3 Users list and your changes are saved to the Running Configuration and to the Startup Configuration.

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

SNMP Targets

SNMPv3 targets send trap messages to the SNMP manager. Inform messages are not supported. Each target is defined with a target IP address, UDP port, and SNMPv3 user name.

NOTE SNMPv3 user configuration (see **SNMP Users, page 106**) should be completed before configuring SNMPv3 targets.

NOTE The AP supports a maximum of eight targets.

To add SNMP targets:

STEP 1 Click **SNMPv3** > **Targets** in the navigation window.

STEP 2 Configure the parameters:

- **IPv4/IPv6 Address**—Enter the IP address of the remote SNMP manager to receive the target.

- **Port**—Enter the UDP port to use for sending SNMP targets.
- **Users**—Enter the name of the SNMP user to associate with the target. To configure SNMP users, see “Configuring SNMPv3 Users” on page 125.
- **SNMPv3 Targets**—This field shows the SNMPv3 Targets on the AP. To remove a target, select it and click Remove.

STEP 3 Click **Add**, and then click **Save**. The user is added to the SNMPv3 Targets list and your changes are saved to the Running Configuration and to the Startup Configuration.

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

7

Administration

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

It contains the following topics.

- System Settings
- User Accounts
- Firmware Upgrade
- Packet Capture
- Log Settings
- Email Alert
- Discovery—Bonjour
- HTTP/HTTPS Service
- Telnet/SSH Service
- Management Access Control
- Download/Backup Configuration File
- Configuration Files Properties
- Copying and Saving the Configuration
- Rebooting

System Settings

The System Settings page enables you to configure information that identifies the switch within the network.

To configure system settings:

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

STEP 2 Enter the parameters:

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

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

User Accounts

One management user is configured on the switch by default:

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

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

Adding a User

To add a new user:

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

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

Firmware Upgrade

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

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

NOTE When you upgrade the firmware, the access point retains the existing configuration information.

TFTP Upgrade

To upgrade the firmware on an access point using TFTP:

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

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

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

STEP 3 Enter a name (1 to 256 characters) for the image file in the **Source File Name** field, including the path to the directory that contains the image to upload.

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

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

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

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

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

HTTP Upgrade

To upgrade using HTTP:

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

STEP 2 If you know the name and path to the new file, enter it in the **Source File Name** field. Otherwise, click the **Browse** button and locate the firmware image file on your network.

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

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

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

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

Packet Capture

The wireless packet capture feature enables capturing and storing packets received and transmitted by the AP. The captured packets can then be analyzed by a network protocol analyzer, for troubleshooting or performance optimization. Packet capture can operate in either of two modes:

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

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

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

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

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

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

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

As you enter a password, the number and color of vertical bars changes to indicate the password strength, as follows:

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

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

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

Changing a User Password

To change a user password:

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

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

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

As you enter a password, the number and color of vertical bars changes to indicate the password strength, as follows:

- Capture file mode— Captured packets are stored in a file on the AP. The AP can transfer the file to a TFTP server. The file is formatted in pcap format and can be examined using tools such as Wireshark and OmniPeek.
- Remote capture mode—Captured packets are redirected in real time to an external PC running the Wireshark tool.

The AP can capture the following types of packets:

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

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

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

Packet Capture Configuration

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

To configure packet capture settings:

STEP 1 Configure the following parameters:

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

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

As soon as the capture is completed, the radio reverts to non-promiscuous mode operation.

- **Radio Client Filter**—Enables or disables the WLAN client filter to capture only frames that are transmitted to, or received from, a WLAN client with a specified MAC address.
- **Client Filter MAC Address**—The MAC address for WLAN client filtering.

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

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

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

Local Packet Capture

To initiate a local packet capture:

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

STEP 2 Configure the following parameters:

- **Capture Interface**—The AP capture interface names eligible for packet capture are:
  - radio1—802.11 traffic.
  - eth0—802.3 traffic on the Ethernet port.
  - wlan0—VAP0 traffic on radio 1.
  - wlan0vap1 to wlan0vap15—VAP1 through VAP15 traffic (if configured).

- brtrunk—Linux bridge interface in the AP.

- **Capture Duration**—The time duration in seconds for the capture (range 10 to 3600).
- **Max Capture File Size**—The maximum allowed size for the capture file in KB (range 64 to 4096).

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

STEP 4 Click **Start Capture**.

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

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

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

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

Click **Refresh** to display the latest data from the AP.

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

Remote Packet Capture

The Remote Packet Capture feature enables you to specify a remote port as the destination for packet captures. This feature works in conjunction with the Wireshark network analyzer tool for Windows. A packet capture server runs on the AP and sends the captured packets via a TCP connection to the Wireshark tool.

A Windows PC running the Wireshark tool allows you to display, log, and analyze captured traffic.

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

Your can trace up to five interfaces on the AP at the same time. However, you must start a separate Wireshark session for each interface. You can configure the IP port number used for connecting Wireshark to the AP. The default port number is 2002. The system uses five consecutive port numbers, starting with the configured port for the packet capture sessions.

If a firewall is installed between the Wireshark PC and the AP, these ports must be allowed to pass through the firewall. The firewall must also be configured to allow the Wireshark PC to initiate TCP connection to the AP.

To configure Wireshark to use the AP as the source for captured packets, you must specify the remote interface in the "Capture Options" menu. For example to capture packets on an AP with IP address 192.168.1.10 on radio 1 using the default IP port, specify the following interface:

rpcap://192.168.1.10/radio1

To capture packets on the Ethernet interface of the AP and VAP0 on radio 1 using IP port 58000, start two Wireshark sessions and specify the following interfaces:

rpcap://192.168.1.10:58000/eth0

rpcap://192.168.1.10:58000/wlan0

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

- Data frames in the trace
- Traffic on specific BSSIDs
- Traffic between two clients

Some examples of useful display filters are:

- Exclude beacons and ACK/RTS/CTS frames:

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

- Data frames only:

  wlan.fc.type == 2

- Traffic on a specific BSSID:

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

- All traffic to and from a specific client:

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

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

not portrange 58000-58004.

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

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

In order to minimize performance impact on the AP while traffic capture is in progress, you should install capture filters to limit which traffic is sent to the Wireshark tool. When capturing 802.11 traffic, large portion of the captured frames tend to be beacons (typically sent every 100 ms by all APs). Although Wireshark supports a display filter for beacon frames, it does not support a capture filter to prevent the AP from forwarding captured beacon packets to the Wireshark tool. In order to reduce the performance impact of capturing the 802.11 beacons, you can disable the capture beacons mode.

The remote packet capture facility is a standard feature of the Wireshark tool for Windows.

NOTE Remote packet capture is not standard on the Linux version of Wireshark; the Linux version does not work with the AP.

Wireshark is an open source tool and is available for free; it can be downloaded from http://www.wireshark.org.

To start a remote packet capture:

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

STEP 2 Specify the **Remote Capture Port** to use as the destination for packet captures. (range 1 to 65530).

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

STEP 4 Click **Start Capture**.

A confirmation window displays to remind you to make sure the monitoring application is ready.

STEP 5 Click **OK**.

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

Packet Capture File Download

You can download a capture file by TFTP to a configured TFTP server, or by HTTP(S) to a PC. A capture is automatically stopped when the capture file download command is triggered.

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

To download a packet capture file using TFTP:

STEP 1 Select **Use TFTP to download the capture file**.

STEP 2 Enter the **TFTP Server Filename** to download, if different from the default. By default, the captured packets are stored in the folder file /tmp/apcapture.pcap on the AP.

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

STEP 4 Click **Download**.

To download a packet capture file using HTTP:

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

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

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

Log Settings

You can use the Log Settings page to enable log messages to be saved in permanent memory and to specify a remote host that provides syslog relay services.

Configuring the Persistent Log

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

CAUTION Enabling persistent logging can wear out the flash (non-volatile) memory and degrade network performance. You should only enable persistent logging to debug a problem. Make sure you disable persistent logging after you finish debugging the problem.

To configure persistent log settings:

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

parameters and initiate a packet capture.

STEP 2 Configure the parameters:

- **Persistence**—Click **Enable** to save system logs to nonvolatile memory so that the logs are not erased when the AP reboots. Clear this field to save system logs to volatile memory. Logs in volatile memory are deleted when the system reboots.
- **Severity**—The minimum severity that an event must have for it to be written to the log in nonvolatile memory. For example, if you specify 2, critical, then critical, alert and emergency events are logged to nonvolatile memory. Error messages with a severity level of 3–7 are written to volatile memory. The severity levels are as follows:

- 0—emergency
- 1—alert
- 2—critical
- 3—error
- 4—warning
- 5—notice
- 6—info
- 7—debug

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

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

Remote Log Server

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

You cannot view kernel log messages directly from the Web interface. You must first set up a remote server running a syslog process and acting as a syslog log relay host on your network. Then, you can configure the AP to send syslog messages to the remote server.

Remote log server collection for AP syslog messages provides the following features:

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

To use Kernel Log relaying, you must configure a remote server to receive the syslog messages. The procedure to configure a remote log host depends on the type of system you use as the remote host.

To specify a host on your network that serves as a syslog relay host:

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

STEP 2 Configure the parameters:

- **Relay Log**—Enables the AP to send log messages to a remote host. When disabled, all log messages are kept on the local system.
- **Server IPv4 Address/Name**—The IP address or DNS name of the remote log server.
- **UDP Port**—The logical port number for the syslog process on the relay host. The default port is 514.

  Using the default port is recommended. However; If you choose to reconfigure the log port, make sure that the port number you assign to syslog is not being used by another process.

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

If you enabled the Log Relay Host, clicking **Save** will activate remote logging. The AP will send its kernel messages real-time for display to the remote log server monitor, a specified kernel log file, or other storage, depending on how you configured the Log Relay Host.

If you disabled the Log Relay Host, clicking **Save** will disable remote logging.

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.

Email Alert

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

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

To configure the AP to send email alerts:

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

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

- **Admin Mode**—Enables the email alert feature globally.
- **From Address**—Email alert From Address configuration. The address is a 255 character string with only printable characters. The default is null.
- **Log Duration**—The email alert log duration in minutes. The range is 30-1440 minutes. The default is 30 minutes.
- **Scheduled Message Severity**—Log messages of this severity level or higher are grouped and sent periodically to the configuration email address. Select from the following values: None, Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug. If set to None, then no scheduled severity messages are sent.
- **Urgent Message Severity**—Log messages of this severity level or higher are are sent to the configured email address immediately. Possible values are: None, Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug. If set to None, then no urgent severity messages are sent. The default is Alert.

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

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

STEP 4 Configure the email addresses and subject line.

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

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

The following is a sample format of the email alert sent from the AP:

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

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

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

Discovery—Bonjour

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

The AP advertises the following service types:

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

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

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

Bonjour works in both IPv4 and IPv6 networks.

To enable the AP to be discovered through Bonjour:

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

STEP 2 Select **Enable**.

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

HTTP/HTTPS Service

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

Configuring HTTP and HTTPS Services

To configure the HTTP and HTTP services:

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

STEP 2 Configure the following Global Parameters:

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

  When a user logs on to the AP web interface, a session is created. This session is maintained until the user logs off or the session inactivity timer expires. The range is 1–10 sessions. The default is 5. If the maximum number of sessions is reached, the next user who attempts to log on to the AP web interface receives an error message about the session limit.

- **Session Timeout**—The maximum amount of time, in minutes, an inactive user remains logged on to the AP web interface. When the configured timeout is reached, the user is automatically logged off the AP. The range is 1–1440 minutes (1440 minutes = 1 day). The default is 5 minutes.

STEP 3 Configure HTTP and HTTPS services:

- **HTTPS Server**—Enables access via secure HTTP. By default, HTTPS access is enabled. If you disable it, any current connections using that protocol are disconnected.

- **HTTPS Port**—The logical port number to use for HTTP connections, from 1025 to 65535. The default port number for HTTP connections is the well-known IANA port number 443.
- **HTTP Server**—Enables access via HTTP. By default, HTTP access is enabled. If you disable it, any current connections using that protocol are disconnected.
- **HTTP Port**—The logical port number to use for HTTP connections, from 1025 to 65535. The default port number for HTTP connections is the well-known IANA port number 80.
- **Redirect HTTP to HTTPS**—Redirects management HTTP access attempts on the HTTP port to the HTTPS port. This field is available only when HTTP access is disabled.

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

Managing SSL Certificates

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

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

In the Certificate File Status area, you can view whether a certificate currently exists on the AP, and, if one does, the following information about it:

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

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

- If you select HTTP, you will be prompted to confirm the download and then to browse to the location to save the file on your network.
- If you select TFTP, additional fields display to enable you to enter the File Name to assign to the downloaded file, and the TFTP server address where the file will be downloaded.

You can also upload a certificate file from your PC to the AP. In the Upload SSL Certificate (From PC to Device), select **HTTP** or **TFTP** for the **Upload Method**

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

A confirmation displays to indicate that the upload was successful.

Telnet/SSH Service

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

To enable Telnet or SSH:

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

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

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

Management Access Control

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

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

To create an access list:

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

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

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

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

Download/Backup Configuration File

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

The AP maintains the following configuration files:

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

NOTE In addition to downloading and uploading these files to another system, you can copy them to different file types on the AP. See **Copying and Saving the Configuration, page 108**.

Backing Up a Configuration File

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

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

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

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

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

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

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

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

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

Downloading a Configuration File

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

To download a configuration file to the AP:

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

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

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

STEP 4 For a TFTP download only, enter the **Source File Name**, including path, where the file exists on the server, then enter the **TFTP Server IPv4 Address**.

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

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

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

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

Configuration Files Properties

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

To delete the Startup Configuration or Backup Configuration file:

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

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

STEP 3 Click **Clear Files**.

Copying and Saving the Configuration

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

To copy a file to another file type:

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

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

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

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

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

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

Rebooting

You can use the Reboot page reboot the AP, as follows:

STEP 1 Click **Administration** > **Reboot** in the navigation window.

STEP 2 Select one of the following options:

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

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

STEP 3 Click **OK** to reboot.

8

System Security

This chapter describes how to configure security settings on the AP.

It contains the following topics.

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

RADIUS Server

Several of the AP features require communication with a RADIUS authentication server. For example, when you configure virtual access points (VAPs) on the AP, you can configure security methods that control wireless client access (see **Radio, page 36**). The Dynamic WEP and WPA Enterprise security methods use an external RADIUS server to authenticate clients. The MAC address filtering feature, whereby client access is restricted to a list, may also be configured to use a RADIUS server to control access. The Captive Portal feature also uses RADIUS to authenticate clients.

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

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

To configure global RADIUS servers:

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

STEP 2 Enter the parameters:

- **Server IP Address Type**—The IP version that the RADIUS server uses.

  You can toggle between the address types to configure IPv4 and IPv6 global RADIUS address settings, but the AP contacts only the RADIUS server or servers of the address type you select in this field.

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

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

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

- **Key-1**—The shared secret key that the 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-(2** through **4)**—The RADIUS key associated with the configured backup RADIUS servers. The server at RADIUS IP Address-2 uses RADIUS Key-2, RADIUS IP Address-3 uses RADIUS Key-3, and so on.

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

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

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

802.1X Supplicant

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

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

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

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

To configure the AP's 802.1X supplicant functionality:

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

STEP 2 Enter the parameters:

- **802.1X Supplicant**—Enables the 802.1X supplicant functionality.
- **EAP Method**—The algorithm to be used for encrypting authentication user names and passwords.
  - **MD5**—A hash function defined in RFC 3748 that provides basic security.
  - **PEAP**—Protected Extensible Authentication Protocol, which provides a higher level of security than MD5 by encapsulating it within a TLS tunnel.
  - **TLS**—Transport Layer Security, as defined in RFC 5216, an open standard that provides a high level of security.
- **Username**— The user name for the AP to use when responding to requests from an 802.1X authenticator. The user name can be 1 to 64 characters long. ASCII-printable characters are allowed, which includes upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.

- **Password**—The MD5 password for the AP to use when responding to requests from an 802.1X authenticator. The password can be 1 to 64 characters in length. ASCII-printable characters are allowed, which includes upper and lower case letters, numbers, and special symbols such as @ and #.

STEP 3 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.

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

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

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

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

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

NOTE: To configure the HTTP and HTTPS server settings, see **HTTP/HTTPS Service, page 129**.

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

STEP 3 Click **Upload**.

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

Password Complexity

You can configure minimum complexity requirements for passwords used to access the AP management interfaces. More complex passwords increase security.

To configure password complexity requirements:

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

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

STEP 3 Configure the parameters:

- **Password Minimum Character Class**—The minimum number of character classes that must be represented in the password string. The four possible character classes are: uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard.
- **Password Different From Current**—Select to have users enter a different password when their current passwords expire. If not selected, users can reenter the previous password when their current password expires.
- **Maximum Password Length**—The maximum password length in number of characters, from 64 to 80.
- **Minimum Password Length**—The minimum password length in number of characters, from 0 to 64.
- **Password Aging Support**—Select to have passwords expire after a configured time period.
- **Password Aging Time**—The number of days before a newly created password expires, from 1 to 365.

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

WPA-PSK Complexity

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

To configure WPA-PSK complexity:

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

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

STEP 3 Configure the parameters:

- **WPA-PSK Minimum Character Class**—The minimum number of character classes that must be represented in the key string. The four possible character classes are: uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard.
- **WPA-PSK Different From Current**—Select one of the following:
  - **Yes**—Users must configure a different key when their current key expire.
  - **No**— Users can reenter the previous key when their current key expires.
- **Maximum WPA-PSK Length**—The maximum key length in number of characters, from 64 to 80.
- **Minimum WPA-PSK Length**—The minimum key length in number of characters, from 8 to 64. Select the checkbox to make the field editable and to activate this requirement.

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

9

Captive Portal

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

NOTE The Captive Portal feature is available only on the WAP321 AP.

Authenticated users must be validated against a database of authorized Captive Portal users before access is granted. The database can be stored locally on the AP or on a RADIUS server.

You can create up to two CP instances, which can then be assigned to VAPs in the system. The instances can be configured with different parameters that affect the user experience when attempting to access a particular VAP. For example, users may be redirected to a particular web page after authenticating to VAP0, but to another web page after authenticating to VAP1, based on the differing CP instances associated with each VAP.

This chapter includes the following topics:

- **Configuring Global Captive Portal Settings**
- **Configuring Instances**
- **Configuring VAPs**
- **Uploading Binary Files**
- **Customizing the Captive Portal Web Pages**
- **Web Customization Preview**
- **Local Groups**
- **Local Users**
- **Local User/Group Associations**
- **Authenticated Clients**

- **Failed Authentication Clients**

Configuring Global Captive Portal Settings

You can use the CP Global Configuration page to control the administrative state of the CP feature and configure global settings that affect all captive portal instances configured on the AP.

To configure CP Global settings:

STEP 1 Click **Captive Portal** > **Global Configuration** in the navigation window.

Step body

STEP 2 Configure the parameters:

- **Captive Portal Mode**—Enables CP operation on the AP.
- **Authentication Timeout**—To access the network through a portal, the client must first enter authentication information on an authentication Web page. This field specifies the number of seconds the AP will keep an authentication session open with the client. When the timeout expires, the AP disconnects any active TCP or SSL connection with the client.
- **Additional HTTP Port**—HTTP traffic uses port 80, but you can configure an additional port for HTTP traffic. Enter a port number between 0-65535.
- **Additional HTTPS Port**—HTTP traffic over SSL (HTTPS) uses port 443, but you can configure an additional port for HTTPS traffic. Enter a port number between 0-65535.

The following fields display nonconfigurable CP information:

- **Instance Count**—The number of CP instances currently configured on the AP. Up to two instances can be configured.
- **Group Count**—The number of CP groups currently configured on the AP. Up to three groups can be configured.
- **User Count**—The number of CP users currently configured on the AP. Up to 128 users can be configured.

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

Configuring Instances

You can create up to two captive portal instances, which is a defined set of CP parameters. Instances can be associated with one or more VAPs. Different instances can be configured to respond differently to users as they attempt to access the associated VAP.

To create a CP instance and configure its settings:

STEP 1 Click **Captive Portal** > **Instance Configuration** in the navigation window.

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

The Captive Portal Instance Parameters fields display.

STEP 3 Enter and **Instance Name** (1–32 characters) and **Instance ID** (either 1 or 2) and click **Save**.

STEP 4 Select the instance name from the **Captive Port Instances** list.

The Captive Portal Instance Parameters fields redisplay, with additional options.

STEP 5 Configure the parameters:

- **Administrative Mode**—Enables and disables the CP instance.
- **Protocol**—Specifies HTTP or HTTPs as the protocol for the CP instance to use during the verification process.
  - **HTTP**—Does not use encryption during verification.
  - **HTTPS**—Uses the Secure Sockets Layer (SSL), which requires a certificate to provide encryption.

    The certificate is presented to the user at connection time.
- **Verification**—The mode for the CP to use to verify clients:
  - **Guest**—The user does not need to be authenticated by a database.
  - **Local**—The AP uses a local database to authenticated users.
  - **RADIUS**—The AP uses a database on a remote RADIUS server to authenticate users.
- **Redirect**—Specifies that the CP should redirect the newly authenticated client to the configured URL. If this option is clear, the user sees the locale-specific welcome page after a successful verification.

- **Redirect URL**—The URL to which the newly authenticated client is redirected if the URL Redirect Mode is enabled.
- **Idle Time**—The number of seconds a user can remain idle before automatically being logged out. If the value is set to 0, the timeout is not enforced. The default value is 0.
- **Session Timeout**—The number of seconds to wait before terminating a session. A user is logged out once the session timeout is reached. If the value is set to 0, the timeout is not enforced. The default value is 0.
- **User Up Rate**—The maximum speed, in megabytes per second, that a client can transmit traffic when using the captive portal. This setting limits the bandwidth at which the client can send data into the network.
- **User Down Rate**—The maximum speed, in megabytes per second, that a client can receive traffic when using the captive portal. This setting limits the bandwidth at which the client can receive data from the network.
- **User Group Name**—If the Verification Mode is Local or RADIUS, assigns an existing User Group to the captive portal. All users who belong to the group are permitted to access the network through this portal.
- **RADIUS IP Network**—Whether the the AP RADIUS client will use the configured IPv4 or IPv6 RADIUS server addresses.
- **Global RADIUS**—If the Verification Mode is RADIUS, select to specify that the default RADIUS server list is used to authenticating clients. (See **RADIUS Server, page 110** for information about configuring the global RADIUS servers.) If you want the CP feature to use a different set of RADIUS servers, clear this setting and configure the servers in the fields on this page.
- **RADIUS Accounting**—Enables tracking and measuring the resources a particular user has consumed, such as system time and amount of data transmitted and received.

  If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers, and for globally or locally configured servers.
- **RADIUS IP**—The IPv4 or IPv6 address for the primary RADIUS server for this VAP.

  When the first wireless client tries to authenticate with a VAP, 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.

- **Radius Backup IP 1–3**—Up to three IPv4or IPv6 backup RADIUS server addresses.

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

- **RADIUS Current**—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.

- **RADIUS 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.

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

- **Locale Count**—The number of locales associated with the instance. You assign locales to instances on the Web Customization page.

- **Delete Instance**—Deletes the current instance.

STEP 6 Click **Save**. You changes are saved to the Running Configuration.

Configuring VAPs

You can use the VAP configuration page to associate a CP instance to a VAP. The associated CP instance settings will apply to users who attempt to authenticate on the VAP.

To associate an instance to a VAP:

STEP 1 Click **Captive Portal** > **VAP Configuration** in the navigation window.

STEP 2 From the **VAP ID** list, select the VAP to which you want to associate a CP instance.

STEP 3 From the **Instance Name** list select the CP instance you want to associate with the VAP.

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

Uploading Binary Files

When users initiate access to a VAP that is associated to a captive portal instance, an authentication page displays. You can customize this page with your own logo and other graphics. You can use the Upload Binary Files page to upload these graphics to the AP.

To upload binary graphic files to the AP:

STEP 1 Create or identify custom graphics to replace the default graphics, as shown in the following table.:

Image Type	Use	Default Width x Height
Logo	Displays at top left of page to provide branding information.	168 × 78 pixels
Account	Displays above the login field to depict an authenticated login.	295 × 55 pixels
Background	Displays in the page background.	10 × 800

Images will be resized to fit the specified dimensions. For best results, the logo and account images should be similar in proportion to the default images.

All images must be 5 kilobytes or smaller and must be in GIF or JPG format.

STEP 2 Click **Captive Portal** > **Upload Binary Files** in the navigation window.

STEP 3 Click **Browse** next to **Upload Web Customization Image** to select the file from your PC or network.

STEP 4 Click **Upload**.

STEP 5 Go to the Web Customization page to apply an uploaded graphic to a CP web page.

NOTE: To delete an image, select it from the **Delete Web Customization Image** list and click **Delete**.

Customizing the Captive Portal Web Pages

When users initiate access to a VAP that is associated to a captive portal instance, an authentication page displays. You can use the Web Customization page to create unique pages for different locales on your network, and to customize the textual and graphic elements of the pages.

To create and customize a CP authentication page:

STEP 1 Click **Captive Portal** > **Web Customization** in the navigation window.

STEP 2 Select **Create** from the **Captive Portal Web Locale** list.

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

STEP 3 Enter a **Web Locale Name** to assign to the page.

STEP 4 Specify a **Locale ID**, from 1–3.

STEP 5 From the **Captive Portal Instances** list, select the CP instance that this locale is associated with.

You can associate multiple locales with an instance. When a user attempts to access a particular VAP that is associated with a CP instance, the locales that are associated with that instance display as links on the authentication page. The user can select a link to switch to that locale.

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

STEP 7 From the **Captive Portal Web Locale** list, select the locale you created.

The page displays additional fields for modifying the locale. The **Locale ID**, **Instance ID**, and **Instance Name** fields display and cannot be edited. The editable fields are populated with default values.

STEP 8 Configure the parameters:

- **Background Image Name**—The image to display as the page background. If you uploaded a custom background image to the AP, you can select it from the list.

- **Logo Image Name**—The image file to display on the top left corner of the page. This image is used for branding purposes, such as the company logo. If you uploaded a custom logo image to the AP, you can select it from the list.
- **Foreground color**—The HTML code for the foreground color in 6-digit hexadecimal format.
- **Background color**—The HTML code for the background color in 6-digit hexadecimal format.
- **Separator**—The HTML code for the color of the thick horizontal line that separates the page header from the page body, in 6-digit hexadecimal format.
- **Locale Label**—A descriptive label for the locale, from 1–32 characters. The default is English.
- **Locale**—An abbreviation for the locale, from 1–32 characters. The default is en.
- **Account Image**—The image file to display above the login field to depict an authenticated login.
- **Account Label**—The text that instructs the user to enter a user name.
- **User Label**—The label for the user name text box.
- **Password Label**—The label for the user password text box.
- **Button Label**—The label on the button users click to submit their user name/password for authentication.
- **Fonts**—The name of the font to use for all text on the CP page. You can enter multiple font names, each separated by a comma. If the first font is not available on the client system, the next font will be used, and so on. For font names that have spaces, surround the entire name in quotes.
- **Browser Title**—The text to display in the browser title bar.
- **Browser Content**—The text that displays in the page header, to the right of the logo.
- **Content**—The instructive text that displays in the page body below the user name and password text boxes.
- **Acceptance Use Policy**—The text that appears in the Acceptance Use Policy box.

- **Accept Label**—The text that instructs users to select the check box to acknowledge reading and accepting the Acceptance Use Policy.
- **No Accept Text**—Error: The text that displays in a pop-up window when a user submits login credentials without selecting the Acceptance Use Policy check box.
- **Work In Progress Text**—The text that displays during authentication.
- **Denied Text**—The text that displays when a user fails authentication.
- **Resource Text**—The text that displays when the authenticator is unavailable.
- **Timeout Text**—The text that displays when the authenticator has not replied in the configured time frame.
- **Welcome Title**—The text that displays when the client has authenticated to the VAP.
- **Welcome Content**—The text that displays when the client has connected to the network.
- **Delete Locale**—Deletes the current locale.

STEP 9 Click **Save**. Your changes are saved to the Running Configuration and the Startup Configuration.

You can use the Web Customization Preview page view the updated page.

Web Customization Preview

Use the Web Customization Preview page to view a locale page that you have modified.

To preview a customized page:

STEP 1 Click **Captive Portal** > **Web Customization Preview** in the navigation window.

STEP 2 Select the locale you want to preview from the **Captive Portal Web Locale** list.

The page for the locale displays in the Captive Portal Web Locale Parameters Preview area.

Local Groups

Each local user is assigned to a user group. Each group is assigned to a CP instance. The group facilitates managing the assignment of users to CP instances.

The user group named default is built-in and cannot be deleted. You can create up to two additional user groups.

To add local user groups:

STEP 1 Click **Captive Portal** > **Local Groups** in the navigation window.

STEP 2 In the **Captive Portal Groups** list, click **Create**.

The page displays additional fields for configuring a new group.

STEP 3 Enter a **Group Name** and **Group ID** and click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

NOTE: To delete a group, select it in the **Captive Portal Groups** list, select the **Delete Group** check box, and click **Save**.

Local Users

You can configure a captive portal instance to accommodate either guest users and authorized users.

Guest users do not have assigned user names and passwords. The CP instance to which guest users are assigned might be associated with a VAP that provides a more restricted access to the network.

Authorized users provide a valid user name and password that must first be validated against a local database or RADIUS server. Authorized users are typically assigned to a CP instance that is associated with a different VAP than guest users.

You can use the Local Users page to configure up to 128 authorized users in the local database.

To add and configure a local user:

STEP 1 Click **Captive Portal** > **Local Users** in the navigation window.

STEP 2 Select **Create** in the **Captive Portal Users** list.

The page displays additional fields for creating a new user.

STEP 3 Enter a **User Name** and **User ID**, then click **Save**.

STEP 4 From the **Captive Port Users** list, select the name of the user you created.

The page displays additional fields for configuring the user.

STEP 5 Enter the parameters:

- **User Password**—Enter the user's password, from 8 to 64 alphanumeric and special characters. A user enter must enter the password to log into the network through the Captive Portal.
- **Idle Time**—The period of time after which the user is logged out if there is no activity.
- **Group Name**—The group the user is assigned to. Each CP instance is configured to support a particular group of users.
- **Maximum Bandwidth Up**—The maximum speed, in megabytes per second, that a client can transmit traffic when using the captive portal. This setting limits the bandwidth at which the client can send data into the network.
- **Maximum Bandwidth Down**—The maximum speed, in megabytes per second, that a client can receive traffic when using the captive portal. This setting limits the bandwidth at which the client can receive data from the network.
- **Delete User**—Deletes the current user.

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

Local User/Group Associations

When you define CP users, you assign them to groups. The groups are assigned to a CP instance, enabling all members access to that CP instance. In addition to making a user a member of a group, you can also associate the user with another group (without assigning them as member). The association enables a user access to an additional CP instance.

To associate a user to a group (of which the user is not already a member):

STEP 1 Click **Captive Portal** > **Local User/Group Associations** in the navigation window.

STEP 2 In the **Captive Portal User/Group** list, click **Create**.

The page displays additional fields for associating a user to a group.

STEP 3 Enter a **User/Group Name.**

STEP 4 Enter the **Group ID** and **User ID** to associate and click **Save**. The changes are saved to the Running Configuration and to the Startup Configuration.

NOTE: To delete a group, select it in the **Captive Portal User/Groups** list, select the **Delete Group** check box, and click **Save**.

Authenticated Clients

The Authenticated Clients page provides information about clients that have authenticated on any Captive Portal instance.

To view the list of authenticated clients, click **Captive Portal** > **Authenticated Clients** in the navigation window.

The following fields display:

- **MAC Address**—The MAC address of the client.
- **IP Address**—The IP address of the client.
- **User Name**—The clients Captive Portal user name.
- **Protocol**—The protocol the user used to establish the connection (HTTP or HTTPS).

- **Verification**—The method used to authenticate the user on the Captive Portal, which can be one of the following values:
  - **Guest**—The user does not need to be authenticated by a database.
  - **Local**—The AP uses a local database to authenticated users.
  - **RADIUS**—The AP uses a database on a remote RADIUS server to authenticate users.
- **VAP ID**—The VAP that the user is associated with.
- **Radio ID**—The ID of the radio. Because the AP has a single radio, this field always displays Radio1.
- **Captive Portal ID**—The ID of the Captive Portal instance to which the user is associated.
- **Session Time**—The time that has elapsed since the user authenticated on Captive Portal.
- **Idle Time**—The time that has elapsed since the last user activity.
- **Initial URL Request**—The URL that the user initially attempted to access.
- **Received Packets**—The number of IP packets received by the AP from the user station.
- **Transmitted Packets**—The number of IP packets transmitted from the AP to the user station.
- **Received Bytes**—The number of bytes received by the AP from the user station.
- **Transmitted Bytes**—The number of bytes transmitted from the AP to the user station.

You can click **Refresh** to show the latest data from the switch.

Failed Authentication Clients

The Failed Authenticated Clients page lists information about clients that attempted to authenticate on a Captive Portal and failed.

To view a list of clients who failed authentication, click **Captive Portal** > **Failed Authentication Clients** in the navigation window.

The following fields display:

- **MAC Address**—The MAC address of the client.
- **IP Address**—The IP address of the client.
- **User Name**—The clients Captive Portal user name.
- **Verification**—The method the client attempted to use to authenticate on the Captive Portal, which can be one of the following values:
  - **Guest**—The user does not need to be authenticated by a database.
  - **Local**—The AP uses a local database to authenticated users.
  - **RADIUS**—The AP uses a database on a remote RADIUS server to authenticate users.
- **VAP ID**—The VAP that the user is associated with.
- **Radio ID**—The ID of the radio. Because the AP has a single radio, this field always displays Radio1.
- **Captive Portal ID**—The ID of the Captive Portal instance to which the user is associated.
- **Failure Time**—The time that the authentication failure occurred.

You can click **Refresh** to show the latest data from the switch.

10

Client Quality of Service

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

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

ACLs

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

The AP supports up to 50 IPv4, IPv6, and MAC ACLs.

IPv4 and IPv6 ACLs

IP ACLs classify traffic for Layers 3 and 4.

Each ACL is a set of up to 10 rules applied to traffic sent from a wireless client or to be received by a wireless client. Each rule specifies whether the contents of a given field should be used to permit or deny access to the network. Rules can be based on various criteria and may apply to one ore more fields within a packet, such as the source or destination IP address, the source or destination L4 port, or the protocol carried in the packet.

MAC ACLs

MAC ACLs are Layer 2 ACLs. You can configure the rules to inspect fields of a frame such as the source or destination MAC address, the VLAN ID, or the Class of Service 802.1p priority. When a frame enters or exits the AP port (depending on whether the ACL is applied in the up or down direction), the AP inspects the frame and checks the ACL rules against the content of the frame. If any of the rules match the content, a permit or deny action is taken on the frame.

Configuring ACLs

Configure ACLs and rules on the ACL Configuration page (steps 1–5), and then apply the rules to a specified VAP.

Use the following general steps to configure ACLs:

STEP 1 Specify a name for the ACL.

STEP 2 Select the type of ACL to add.

STEP 3 Add the ACL

STEP 4 Add new rules to the ACL.

STEP 5 Configure the match criteria for the rules.

STEP 6 Use the Client QoS Association page to apply the ACL to one or more VAPs.

To add an ACL and configure its rules:

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

STEP 2 Enter the following parameters to create a new ACL:

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

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

STEP 3 Click **Add ACL**.

The page displays additional fields for configuring the ACL.

STEP 4 Configure the rule parameters:

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

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

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

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

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

For IPv4 ACLs, configure the following parameters:

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

  If you select the checkbox, select one of the following:

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

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

  The wild card masks determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all of the bits are important. This field is required when Source IP Address is checked.

  A wild card mask is, in essence, the inverse of a subnet mask. For example, To match the criteria to a single host address, use a wildcard mask of 0.0.0.0. To match the criteria to a 24-bit subnet (for example 192.168.10.0/24), use a wild card mask of 0.0.0.255.
- **Source Port**—Includes a source port in the match condition for the rule. The source port is identified in the datagram header.

  If you select this checkbox, choose the port name or enter the port number.
  - **Select From List**—The keyword associated with the source port to match: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.

    Each of these keywords translates into its equivalent port number.
  - **Match to Port**—The IANA port number to match to the source port identified in the datagram header. The port range is 0–65535 and includes three different types of ports:

    0–1023: Well Known Ports

    1024–49151: Registered Ports

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

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

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

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

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

  - **Select From List**—Select the keyword associated with the destination port to match: ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.

    Each of these keywords translates into its equivalent port number.

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

    0–1023: Well Known Ports

    1024–49151: Registered Ports

    49152–65535: Dynamic and/or Private Ports

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

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

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

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

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

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

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

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

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

  The TOS Mask value is a two-digit hexadecimal number from 00 to ff, representing an inverted (i.e. wildcard) mask. The zero-valued bits in the TOS Mask denote the bit positions in the TOS Bits value that are used for comparison against the IP TOS field of a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a TOS Bits value of a0 and a TOS Mask of 00. This is an optional configuration.

For IPv6 ACLs, configure the following parameters:

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

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

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

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

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

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

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

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

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

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

- **IPv6 Flow Label**—Flow label is 20-bit number that is unique to an IPv6 packet. It is used by end stations to signify quality-of-service handling in routers (range 0 to 1048575).
- **IP DSCP**—Matches packets based on their IP DSCP value.

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

  - **Select From List**—DSCP Assured Forwarding (AS), Class of Service (CS) or Expedited Forwarding (EF) values.
  - **Match to Value**—A custom DSCP value, from 0–63.

For a MAC ACL, configure the following parameters:

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

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

  - **Select from List**—Select one of the following protocol types: appletalk, arp, ipv4, ipv6, ipx, netbios, pppoe
  - **Match to Value**—Enter a custom protocol identifier to which packets are matched. The value is a four-digit hexadecimal number in the range of 0600–FFFF.
- **Class of Service**—Select this field and enter an 802.1p user priority to compare against an Ethernet frame.

  The valid range is 0–7. This field is located in the first/only 802.1Q VLAN tag.
- **Source MAC Address**—Select this field and enter the source MAC address to compare against an Ethernet frame.
- **Source MAC Mask**—Select this field and enter the source MAC address mask specifying which bits in the source MAC to compare against an Ethernet frame.

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

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

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

- **VLAN ID**—Select this field and enter the VLAN IDs to compare against an Ethernet frame.

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

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

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

Class Map

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

Standard IP-based networks are designed to provide best effort data delivery service. Best effort service implies that the network delivers the data in a timely fashion, although there is no guarantee that it will. During times of congestion, packets may be delayed, sent sporadically, or dropped. For typical Internet applications, such as e-mail and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. However, on applications with strict timing requirements, such as voice or multimedia, any degradation of service has undesirable effects.

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

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

Adding a Class Map

To add a class map:

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

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

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

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

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

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

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

Defining a Class Map

To configure a class map:

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

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

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

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

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

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

  - **Select From List**—Match the selected protocol: IP, ICMP, IPv6, ICMPv6, IGMP, TCP, UDP.
  - **Match to Value**—Match a protocol that is not listed by name. Enter the protocol ID. The protocol ID is a standard value assigned by the IANA. The range is a number from 0–255.

- **Source IP Address** or **Source IPv6 Address**—Requires a packet's source IP address to match the address listed here. Select the checkbox and enter an IP address in the text box.
- **Source IP Mask** (IPv4 only)—The source IP address mask.

  The mask for DiffServ is a network-style bit mask in IP dotted decimal format indicating which part(s) of the destination IP Address to use for matching against packet content.

  A DiffServ mask of 255.255.255.255 indicates that all bits are important, and a mask of 0.0.0.0 indicates that no bits are important. The opposite is true with an ACL wild card mask. For example, to match the criteria to a single host address, use a mask of 255.255.255.255. To match the criteria to a 24-bit subnet (for example 192.168.10.0/24), use a mask of 255.255.255.0.
- **Source IPv6 Prefix Length** (IPv6 only)—The prefix length of the source IPv6 address.
- **Destination IP Address** or **Destination IPv6 Address**—Requires a packet's destination IP address to match the address listed here. Enter an IP address in the appropriate field to apply this criteria.
- **Destination IP Mask** (IPv4 only)—The destination IP address mask.

  The mask for DiffServ is a network-style bit mask in IP dotted decimal format indicating which part(s) of the destination IP Address to use for matching against packet content.

  A DiffServ mask of 255.255.255.255 indicates that all bits are important, and a mask of 0.0.0.0 indicates that no bits are important. The opposite is true with an ACL wild card mask. For example, to match the criteria to a single host address, use a mask of 255.255.255.255. To match the criteria to a 24-bit subnet (for example 192.168.10.0/24), use a mask of 255.255.255.0.
- **Destination IPv6 Prefix Length** (IPv6 only)—The prefix length of the destination IPv6 address.
- **IPv6 Flow Label** (IPv6 only)—A 20-bit number that is unique to an IPv6 packet. It is used by end stations to signify quality-of-service handling in routers (range 0 to 1048575).

- **IP DSCP**—See description under Service Types below.
- **Source Port**—Includes a source port in the match condition for the rule. The source port is identified in the datagram header.

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

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

    Each of these keywords translates into its equivalent port number.

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

    0–1023–Well Known Ports

    1024–49151: Registered Ports

    49152–65535: Dynamic and/or Private Ports

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

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

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

    Each of these keywords translates into its equivalent port number.

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

    0–1023: Well Known Ports

    1024–49151: Registered Ports

    49152–65535: Dynamic and/or Private Ports

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

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