Cisco Wireless LAN Controller Configuration Guide, Release 7.4

First Published: January 08, 2013

Last Modified: March 26, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-28744-01

CONTENTS

Preface

This preface describes the audience, organization, and conventions of this document. It also provides information on how to obtain other documentation. This chapter includes the following sections:

Audience

This publication is for experienced network administrators who configure and maintain Cisco wireless LAN controllers and Cisco lightweight access points.

Conventions

This document uses the following conventions:

Table 1: Conventions

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Convention	Indication
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means the following information will help you solve a problem.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Related Documentation

These documents provide complete information about Cisco Wireless:

- Cisco Wireless LAN Controller configuration guides:
  http://www.cisco.com/en/US/products/ps10315/products_installation_and_configuration_guides_list.html
- Cisco Wireless LAN Controller command references:
  http://www.cisco.com/en/US/products/ps10315/prod_command_reference_list.html
- *Cisco Wireless LAN Controller System Message Guide*:
- http://www.cisco.com/en/US/products/ps10315/products_system_message_guides_list.html
- *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points*:
- http://www.cisco.com/en/US/products/ps10315/prod_release_notes_list.html
- *Cisco Wireless Mesh Access Points, Design and Deployment Guide*:
- http://www.cisco.com/en/US/products/ps11451/products_implementation_design_guides_list.html
- Cisco Prime Infrastructure documentation:
  http://www.cisco.com/en/US/products/ps12239/products_documentation_roadmaps_list.html

- Cisco Mobility Services Engine documentation:

  http://www.cisco.com/en/US/products/ps9806/tsd_products_support_series_home.html

Click this link to access user documentation pertaining to Cisco Wireless solution:

http://www.cisco.com/cisco/web/psa/default.html?mode=prod

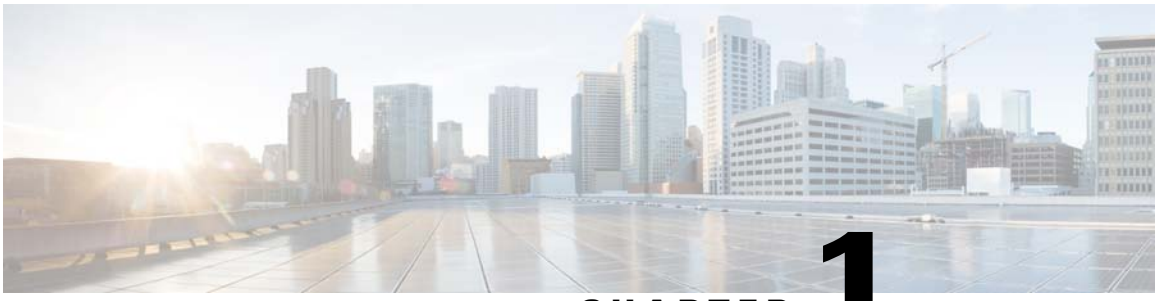
Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*, at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

PART I

System Management



CHAPTER 1

Overview

Cisco Wireless Overview

Cisco Wireless is designed to provide 802.11 wireless networking solutions for enterprises and service providers. Cisco Wireless simplifies deploying and managing large-scale wireless LANs and enables a unique best-in-class security infrastructure. The operating system manages all data client, communications, and system administration functions, performs radio resource management (RRM) functions, manages system-wide mobility policies using the operating system security solution, and coordinates all security functions using the operating system security framework.

Cisco Wireless solution consists of Cisco wireless LAN controllers and their associated lightweight access points controlled by the operating system, all concurrently managed by any or all of the operating system user interfaces:

- An HTTP and/or HTTPS full-featured Web User Interface hosted by Cisco wireless LAN controllers can be used to configure and monitor individual controllers.
- A full-featured command-line interface (CLI) can be used to configure and monitor individual Cisco wireless LAN controllers.

- The Cisco Prime Infrastructure, which you use to configure and monitor one or more Cisco wireless LAN controllers and associated access points. The Prime Infrastructure has tools to facilitate large-system monitoring and control. For more information about Cisco Prime Infrastructure, see http://www.cisco.com/en/US/products/ps12239/tsd_products_support_series_home.html.
- An industry-standard SNMP V1, V2c, and V3 interface can be used with any SNMP-compliant third-party network management system.

The Cisco Wireless solution supports client data services, client monitoring and control, and all rogue access point detection, monitoring, and containment functions. It uses lightweight access points, Cisco wireless LAN controllers, and the optional Cisco Prime Infrastructure to provide wireless services to enterprises and service providers.

Note Unless otherwise noted in this publication, all of the Cisco wireless LAN controllers are referred to as controllers, and all of the Cisco lightweight access points are referred to as access points.

Single-Controller Deployments

A standalone controller can support lightweight access points across multiple floors and buildings simultaneously and support the following features:

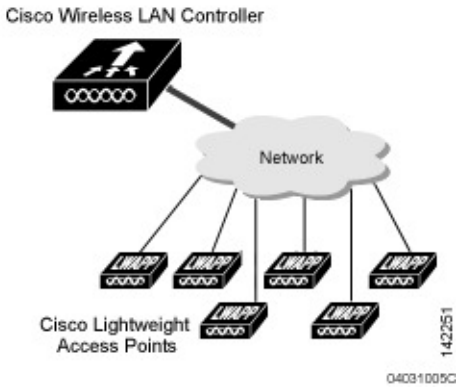
- Autodetecting and autoconfiguring lightweight access points as they are added to the network.
- Full control of lightweight access points.
- Lightweight access points connect to controllers through the network. The network equipment may or may not provide Power over Ethernet (PoE) to the access points.

Some controllers use redundant Gigabit Ethernet connections to bypass single network failures.

Note Some controllers can connect through multiple physical ports to multiple subnets in the network. This feature can be helpful when you want to confine multiple VLANs to separate subnets.

This figure shows a typical single-controller deployment.

Figure 1: Single-Controller Deployment



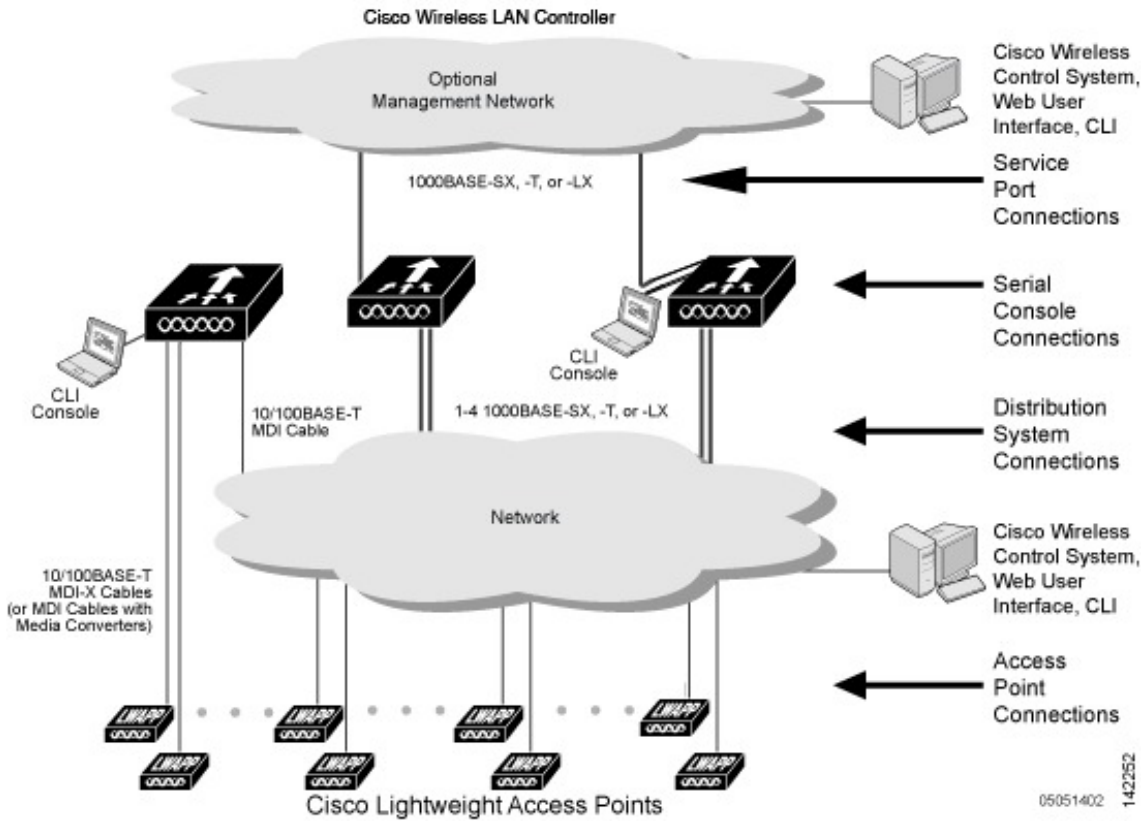
Multiple-Controller Deployments

Each controller can support lightweight access points across multiple floors and buildings simultaneously. However, full functionality of the Cisco wireless LAN solution occurs when it includes multiple controllers. A multiple-controller system has the following additional features:

- Autodetecting and autoconfiguring RF parameters as the controllers are added to the network.
- Same-subnet (Layer 2) roaming and inter-subnet (Layer 3) roaming.
- Automatic access point failover to any redundant controller with a reduced access point load.

The following figure shows a typical multiple-controller deployment. The figure also shows an optional dedicated management network and the three physical connection types between the network and the controllers.

Figure 2: Typical Multiple-Controller Deployment



Operating System Software

The operating system software controls controllers and lightweight access points. It includes full operating system security and radio resource management (RRM) features.

Operating System Security

Operating system security bundles Layer 1, Layer 2, and Layer 3 security components into a simple, Cisco WLAN solution-wide policy manager that creates independent security policies for each of up to 16 wireless LANs.

The 802.11 Static WEP weaknesses can be overcome using the following robust industry-standard security solutions:

- 802.1X dynamic keys with extensible authentication protocol (EAP).
- Wi-Fi protected access (WPA) dynamic keys. The Cisco WLAN solution WPA implementation includes:
  - Temporal key integrity protocol (TKIP) and message integrity code checksum dynamic keys
  - WEP keys, with or without a preshared key passphrase

- RSN with or without a preshared key
- Optional MAC filtering

The WEP problem can be further solved using the following industry-standard Layer 3 security solutions:

- Passthrough VPNs
- Local and RADIUS MAC address filtering
- Local and RADIUS user/password authentication
- Manual and automated disabling to block access to network services. In manual disabling, you block access using client MAC addresses. In automated disabling, which is always active, the operating system software automatically blocks access to network services for a user-defined period of time when a client fails to authenticate for a fixed number of consecutive attempts. This feature can be used to deter brute-force login attacks.

These and other security features use industry-standard authorization and authentication methods to ensure the highest possible security for your business-critical wireless LAN traffic.

Layer 2 and Layer 3 Operation

Lightweight Access Point Protocol (LWAPP) communications between the controller and lightweight access points can be conducted at Layer 2 or Layer 3. Control and Provisioning of Wireless Access Points protocol (CAPWAP) communications between the controller and lightweight access points are conducted at Layer 3. Layer 2 mode does not support CAPWAP.

Note The IPv4 network layer protocol is supported for transport through a CAPWAP or LWAPP controller system. IPv6 (for clients only) and AppleTalk are also supported but only on Cisco 5500 Series Controllers and the Cisco WiSM2. Other Layer 3 protocols (such as IPX, DECnet Phase IV, OSI CLNP, and so on) and Layer 2 (bridged) protocols (such as LAT and NetBeui) are not supported.

Operational Requirements

The requirement for Layer 3 LWAPP communications is that the controller and lightweight access points can be connected through Layer 2 devices on the same subnet or connected through Layer 3 devices across subnets. Another requirement is that the IP addresses of access points should be either statically assigned or dynamically assigned through an external DHCP server.

The requirement for Layer 3 CAPWAP communications is that the controller and lightweight access points can be connected through Layer 2 devices on the same subnet or connected through Layer 3 devices across subnets.

Configuration Requirements

When you are operating the Cisco wireless LAN solution in Layer 2 mode, you must configure a management interface to control your Layer 2 communications.

When you are operating the Cisco wireless LAN solution in Layer 3 mode, you must configure an AP-manager interface to control lightweight access points and a management interface as configured for Layer 2 mode.

Cisco Wireless LAN Controllers

When you are adding lightweight access points to a multiple-controller deployment network, it is convenient to have all lightweight access points associate with one master controller on the same subnet. That way, the you do not have to log into multiple controllers to find out which controller newly-added lightweight access points associated with.

One controller in each subnet can be assigned as the master controller while adding lightweight access points. As long as a master controller is active on the same subnet, all new access points without a primary, secondary, and tertiary controller assigned automatically attempt to associate with the master controller. This process is described in Cisco Wireless LAN Controller Failover Protection, on page 12.

You can monitor the master controller using the Cisco Prime Infrastructure Web User Interface and watch as access points associate with the master controller. You can then verify the access point configuration and assign a primary, secondary, and tertiary controller to the access point, and reboot the access point so it reassociates with its primary, secondary, or tertiary controller.

Note Lightweight access points without a primary, secondary, and tertiary controller assigned always search for a master controller first upon reboot. After adding lightweight access points through the master controller, you should assign primary, secondary, and tertiary controllers to each access point. We recommend that you disable the master setting on all controllers after initial configuration.

Client Location

When you use Cisco Prime Infrastructure in your Cisco wireless LAN solution, controllers periodically determine the client, rogue access point, rogue access point client, radio frequency ID (RFID) tag location and store the locations in the Cisco Prime Infrastructure database.

Controller Platforms

Controllers are enterprise-class high-performance wireless switching platforms that support 802.11a/n and 802.11b/g/n protocols. They operate under control of the operating system, which includes the radio resource management (RRM), creating a Cisco UWN solution that can automatically adjust to real-time changes in the 802.11 RF environment. Controllers are built around high-performance network and security hardware, resulting in highly reliable 802.11 enterprise networks with unparalleled security.

The following controllers are supported:

Cisco 2500 Series Controllers

The Cisco 2500 Series Wireless Controller works in conjunction with Cisco lightweight access points and the Cisco Prime Infrastructure to provide system-wide wireless LAN functions. The Cisco 2500 Series controller provides real-time communication between a wireless access points and other devices to deliver centralized security policies, guest access, wireless intrusion prevention system (wIPS), context-aware

(location), RF management, quality of services for mobility services such as voice and video, and OEAP support for the teleworker solution.

For more information about Cisco 2500 series controllers, see http://www.cisco.com/en/US/products/ps11630/index.html.

Cisco 5500 Series Controller

The Cisco 5500 Series Wireless LAN Controller is currently available in one model: 5508. The Cisco 5500 Series Wireless Controller is a highly scalable and flexible platform that enables systemwide services for mission-critical wireless networking in medium-sized to large enterprises and campus environments.

The Cisco 5500 Series Controller can be equipped with one or two power supplies. When the controller is equipped with two power supplies, the power supplies are redundant, and either power supply can continue to power the controller if the other power supply fails.

For more information about the Cisco 5500 Series Controller, see http://www.cisco.com/en/US/products/ps10315/tsd_products_support_series_home.html.

Cisco Flex 7500 Series Controllers

The Cisco Flex 7500 Series Controller enables you to deploy full featured, scalable, and secure FlexConnect network services across geographic locations. Cisco Flex 7500 Series Controller virtualizes the complex security, management, configuration and troubleshooting operations within the data center and then transparently extends those services to each store. Deployments using Cisco Flex 7500 Series Controller are easier for IT to set up, manage and scale.

The Cisco Flex 7500 Series Controller is designed to meet the scaling requirements to deploy the FlexConnect solution in branch networks. Cisco Wireless supports two major deployment models: FlexConnect and monitor mode. FlexConnect is designed to support wireless branch networks by allowing the data to be switched locally while the access points are being controlled and managed by a centralized controller. It aims at delivering a cost effective FlexConnect solution on a large scale.

Restrictions

For a FlexConnect only deployment, the following restrictions apply:

- Multicast-unicast is the only available default mode.
- Global multicast and IGMP snooping are not supported.
- IPv6 and Generic Attribute Registration Protocol (GARP) are supported but not multicast data.

For more information about the Cisco Flex 7500 series controllers, see http://www.cisco.com/en/US/products/ps11635/tsd_products_support_series_home.html.

Cisco 8500 Series Controllers

Cisco 8500 Series Controllers were introduced in the 7.3 release with support for local mode, FlexConnect, and mesh modes. The Cisco 8500 Series Controller is a highly scalable and flexible platform that enables mission-critical wireless networking in large-scale service provider and large-campus deployments.

Note The DC powered 8510 controller is not available with any of the country-specific power cords. Therefore, we recommend that you use a 12 gauge wire and connect to the DC power supply.

Restrictions

- Local mode only deployment—Multicast-multicast is the default mode.
- Local and FlexConnect mode deployment:
  - If you require IPv6 on FlexConnect mode APs, disable global multicast and change to multicast-unicast mode. IPv6 and Generic Attribute Registration Protocol (GARP) works, but multicast data and video streaming are not supported across the controller.
  - If you do not require IPv6 and GARP on FlexConnect APs, change the mode to multicast-multicast and enable global multicast and IGMP/MLD snooping. IPv6, GARP, multicast data, and VideoStream are supported on FlexConnect APs.

For more information about the Cisco 8500 series controllers, see http://www.cisco.com/en/US/products/ps12722/tsd_products_support_series_home.html.

Cisco Virtual Wireless LAN Controllers

The virtual wireless LAN controller is software that can run on hardware that is compliant with an industry standard virtualization infrastructure. Virtual Wireless LAN controllers provide flexibility for users to select the hardware based on their requirement.

Note When you take a snapshot of the virtual wireless LAN controller, the VMware suspends activities for about 15 seconds. During this time, the APs are disconnected from the virtual wireless LAN controller.

For more information about the Cisco Virtual Wireless LAN controllers, see http://www.cisco.com/en/US/products/ps12723/tsd_products_support_series_home.html.

Cisco Wireless Services Module 2

The Cisco Wireless Services Module 2 (WiSM2) provides medium-sized to large single-site WLAN deployments with exceptional performance, security, and scalability to support mission-critical wireless business communications. It helps to lower hardware costs and offers flexible configuration options that can reduce the total cost of operations and ownership for wireless networks.

For more information about Cisco WiSM2, see http://www.cisco.com/en/US/products/ps11634/index.html.

Cisco Wireless Controller on Cisco Services-Ready Engine (SRE)

The Cisco wireless controller application on the Cisco Services-Ready Engine (SRE) enables systemwide wireless functions in small to medium-sized enterprises and branch offices. Delivering 802.11n performance and scalability, the Cisco wireless controller on the SRE is an entry-level controller that provides low total cost of ownership and investment protection by integrating seamlessly with the existing network. The Cisco

SRE modules are router blades for the Cisco Integrated Services Routers Generation 2 (ISR G2), which allows you to provision the Cisco Wireless Controller applications on the module remotely at any time. This can help your organization to quickly deploy wireless on-demand, reduce operating costs, and consolidate the branch office infrastructure.

This controller provides real-time communication between Cisco Aironet access points, the Cisco Prime Infrastructure, and the Cisco Mobility Services Engine (MSE) to deliver centralized security policies, wireless intrusion prevention system (wIPS) capabilities, award-winning RF management, context-aware capabilities for location tracking, and quality of service (QoS) for voice and video.

For more information about Cisco wireless controller application on the Cisco Services-Ready Engine (SRE), see http://www.cisco.com/en/US/products/ps11716/index.html.

Cisco UWN Solution WLANs

The Cisco UWN solution can control up to 512 WLANs for lightweight access points. Each WLAN has a separate WLAN ID (1 through 512), a separate profile name, and a WLAN SSID and can be assigned with unique security policies. The lightweight access points broadcast all active Cisco UWN solution WLAN SSIDs and enforce the policies defined for each WLAN.

Note We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that controllers operate with optimum performance and ease of management.

If management over wireless is enabled across the Cisco UWN solution, you can manage the system across the enabled WLAN using CLI and Telnet, HTTP/HTTPS, and SNMP.

File Transfers

You can upload and download operating system code, configuration, and certificate files to and from the controller using the GUI, CLI, or Cisco Prime Infrastructure.

Power over Ethernet

Lightweight access points can receive power through their Ethernet cables from 802.3af-compatible Power over Ethernet (PoE) devices, which can reduce the cost of discrete power supplies, additional wiring, conduits, outlets, and installation time. PoE frees you from having to mount lightweight access points or other powered equipment near AC outlets, which provides greater flexibility in positioning the access points for maximum coverage.

When you are using PoE, you run a single CAT-5 cable from each lightweight access point to PoE-equipped network elements, such as a PoE power hub or a Cisco WLAN solution single-line PoE injector. When the PoE equipment determines that the lightweight access point is PoE-enabled, it sends 48 VDC over the unused pairs in the Ethernet cable to power the access point.

The PoE cable length is limited by the 100BASE-T or 10BASE-T specification to 100 m or 200 m, respectively.

Cisco Wireless LAN Controller Memory

The controller contains two kinds of memory: volatile RAM, which holds the current, active controller configuration, and NVRAM (nonvolatile RAM), which holds the reboot configuration. When you are configuring the operating system in the controller, you are modifying volatile RAM; you must save the configuration from the volatile RAM to the NVRAM to ensure that the controller reboots in the current configuration.

Knowing which memory you are modifying is important when you are doing the following tasks:

- Using the configuration wizard
- Clearing the controller configuration
- Saving configurations
- Resetting the controller
- Logging out of the CLI

Cisco Wireless LAN Controller Failover Protection

During installation, we recommend that you connect all lightweight access points to a dedicated controller, and configure each lightweight access point for final operation. This step configures each lightweight access point for a primary, secondary, and tertiary controller and allows it to store the configured mobility group information.

During the failover recovery, the following tasks are performed:

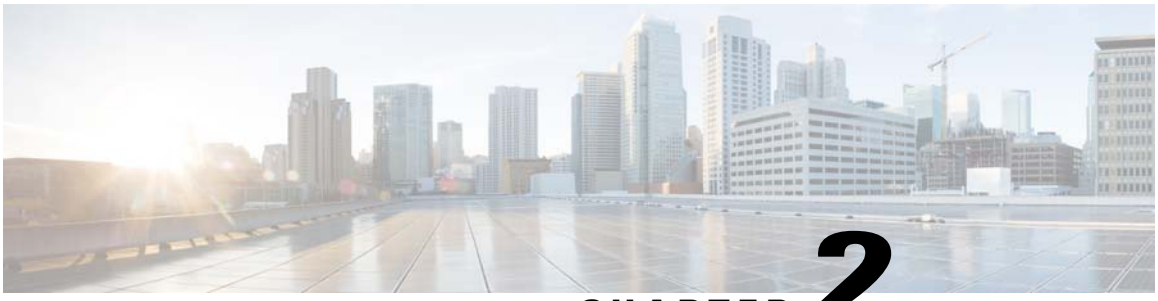
- The configured access point attempts to contact the primary, secondary, and tertiary controllers, and then attempts to contact the IP addresses of the other controllers in the mobility group.
- DNS is resolved with the controller IP address.
- DHCP servers get the controller IP addresses (vendor-specific option 43 in DHCP offer).

In multiple-controller deployments, if one controller fails, the access points perform the following tasks:

- If the lightweight access point has a primary, secondary, and tertiary controller assigned, it attempts to associate with that controller.
- If the access point has no primary, secondary, or tertiary controllers assigned or if its primary, secondary, or tertiary controllers are unavailable, it attempts to associate with a master controller.
- If the access point finds no master controller, it attempts to contact stored mobility group members by the IP address.
- If the mobility group members are available, and if the lightweight access point has no primary, secondary, and tertiary controllers assigned and there is no master controller active, it attempts to associate with the least-loaded controller to respond to its discovery messages.

When controllers are deployed, if one controller fails, active access point client sessions are momentarily dropped while the dropped access point associates with another controller, allowing the client device to immediately reassociate and reauthenticate.

To know more about high availability, see http://www.cisco.com/en/US/products/ps6366/products_tech_note09186a00809a3f5d.shtml



CHAPTER 2

Getting Started

Configuring the Controller Using the Configuration Wizard

The configuration wizard enables you to configure basic settings on the controller. You can run the wizard after you receive the controller from the factory or after the controller has been reset to factory defaults. The configuration wizard is available in both GUI and CLI formats.

Connecting the Console Port of the Controller

Before you can configure the controller for basic operations, you need to connect it to a PC that uses a VT-100 terminal emulation program (such as HyperTerminal, ProComm, Minicom, or Tip).

Note On Cisco 5500 Series Controllers, you can use either the RJ-45 console port or the USB console port. If you use the USB console port, plug the 5-pin mini Type B connector into the controller's USB console port and the other end of the cable into the PC's USB Type A port. The first time that you connect a Windows PC to the USB console port, you are prompted to install the USB console driver. Follow the installation prompts to install the driver. The USB console driver maps to a COM port on your PC; you then need to map the terminal emulator application to the COM port.

Step 1 Connect one end of a null-modem serial cable to the controller's console port and the other end to your PC's serial port.

Step 2 Start the PC's VT-100 terminal emulation program.

Step 3 Configure the terminal emulation program for these parameters:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- No hardware flow control

Step 4 Plug the AC power cord into the controller and a grounded 100 to 240 VAC, 50/60-Hz electrical outlet.Turn on the power supply. The bootup script displays operating system software initialization (code download and power-on self test verification) and basic configuration.
If the controller passes the power-on self test, the bootup script runs the configuration wizard, which prompts you for basic configuration input.

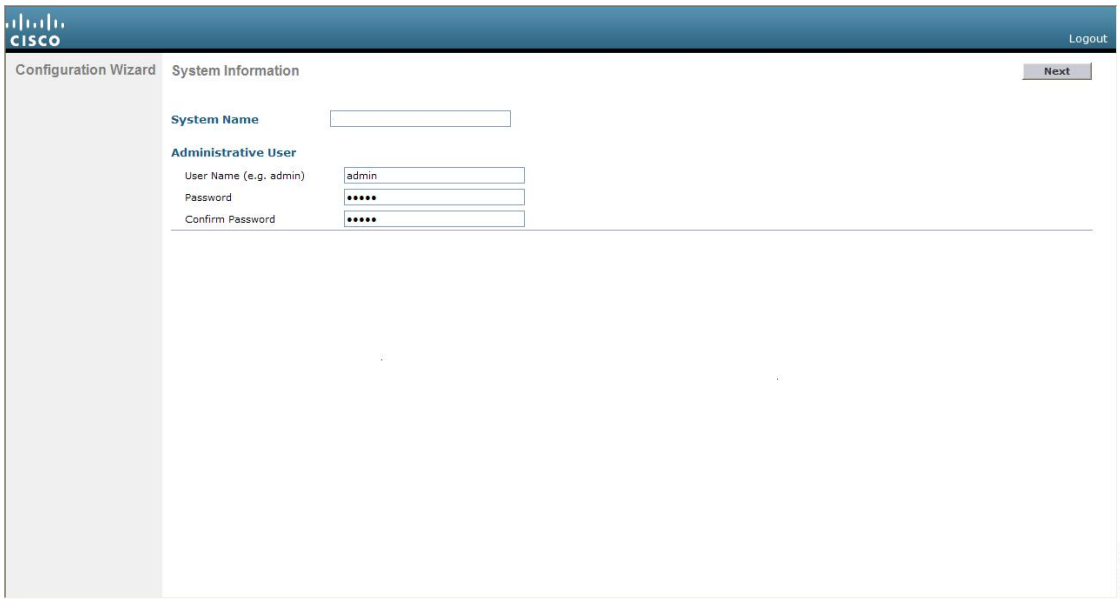
Configuring the Controller (GUI)

Step 1 Connect your PC to the service port and configure it to use the same subnet as the controller.

Step 2 Start Internet Explorer 6.0 SP1 (or later) or Firefox 2.0.0.11 (or later) on your PC and browse to http://192.168.1.1. The configuration wizard appears.

Note You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled. The default IP address to connect to the service port interface is 192.168.1.1.

Figure 3: Configuration Wizard — System Information Screen



Step 3 In the System Name text box, enter the name that you want to assign to this controller. You can enter up to 31 ASCII characters.

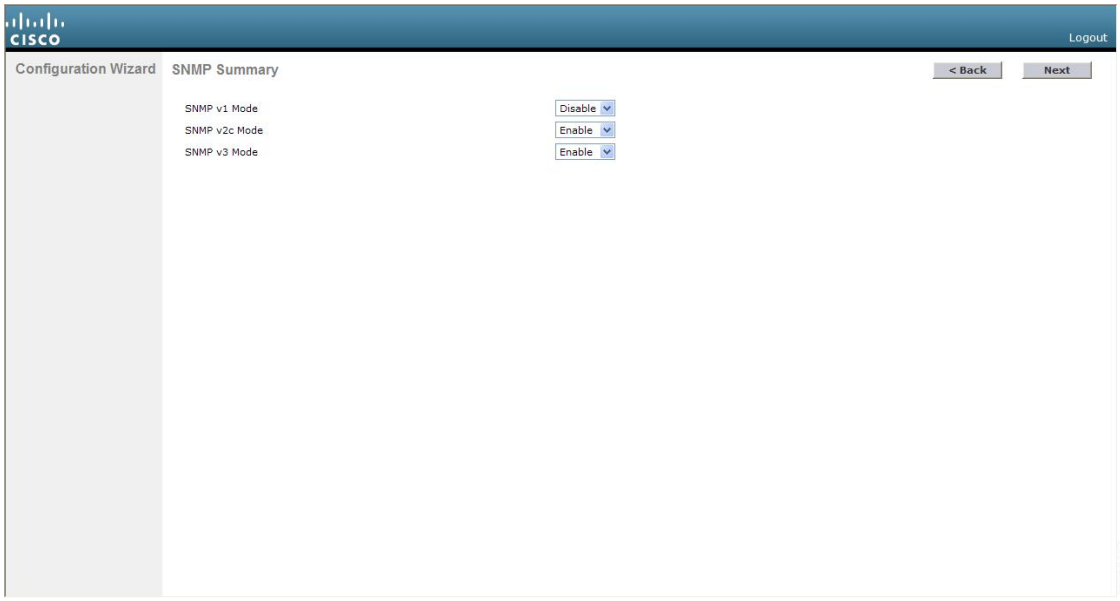
Step 4 In the User Name text box, enter the administrative username to be assigned to this controller. You can enter up to 24 ASCII characters. The default username is *admin*.

Step 5 In the Password and Confirm Password text boxes, enter the administrative password to be assigned to this controller. You can enter up to 24 ASCII characters. The default password is *admin*.
Starting in release 7.0.116.0, the following password policy has been implemented:

- The password must contain characters from at least three of the following classes:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters
- No character in the password must be repeated more than three times consecutively.
- The new password must not be the same as the associated username and not be the username reversed.
- The password must not be cisco, ocsic, or any variant obtained by changing the capitalization of letters of the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s.

Step 6 Click **Next**. The SNMP Summary screen appears.

Figure 4: Configuration Wizard — SNMP Summary Screen



Step 7 If you want to enable Simple Network Management Protocol (SNMP) v1 mode for this controller, choose **Enable** from the SNMP v1 Mode drop-down list. Otherwise, leave this parameter set to **Disable**.

Note SNMP manages nodes (servers, workstations, routers, switches, and so on) on an IP network. Currently, there are three versions of SNMP: SNMPv1, SNMPv2c, and SNMPv3.

Step 8 If you want to enable SNMPv2c mode for this controller, leave this parameter set to **Enable**. Otherwise, choose **Disable** from the SNVP v2c Mode drop-down list.

Step 9 If you want to enable SNMPv3 mode for this controller, leave this parameter set to **Enable**. Otherwise, choose **Disable** from the SNVP v3 Mode drop-down list.

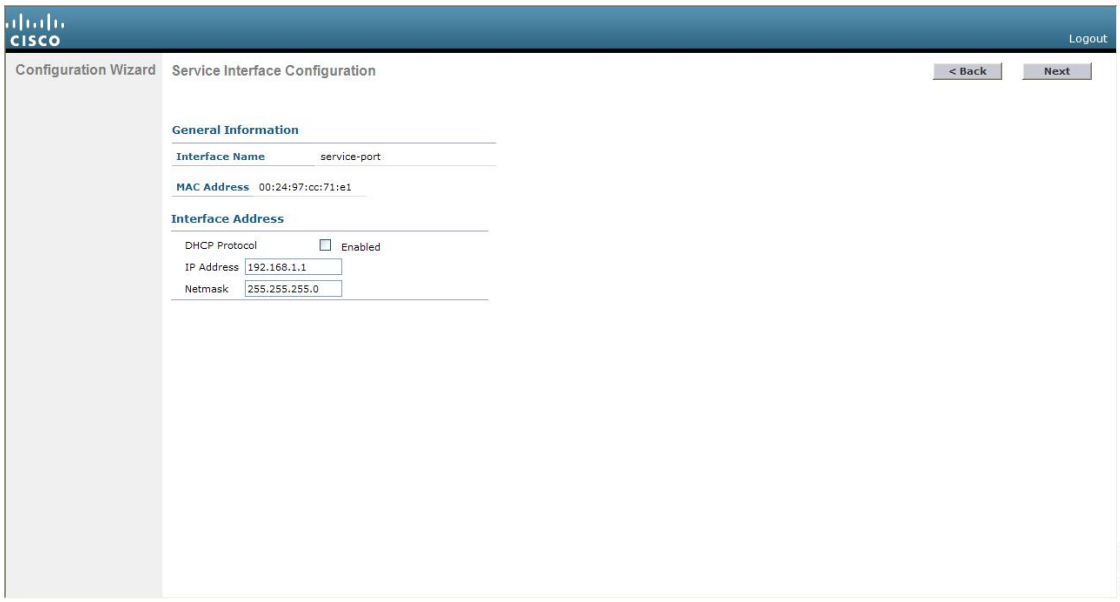
Step 10 Click **Next**.

Step 11 When the following message appears, click **OK**:

```
Default values are present for v1/v2c community strings.
Please make sure to create new v1/v2c community strings once the system comes up.
Please make sure to create new v3 users once the system comes up.
```

The Service Interface Configuration screen appears.

Figure 5: Configuration Wizard — Service Interface Configuration Screen



Step 12 If you want the controller's service-port interface to obtain an IP address from a DHCP server, select the **DHCP Protocol Enabled** check box. If you do not want to use the service port or if you want to assign a static IP address to the service port, leave the check box unselected.

Note The service-port interface controls communications through the service port. Its IP address must be on a different subnet from the management interface. This configuration enables you to manage the controller directly or through a dedicated management network to ensure service access during network downtime.

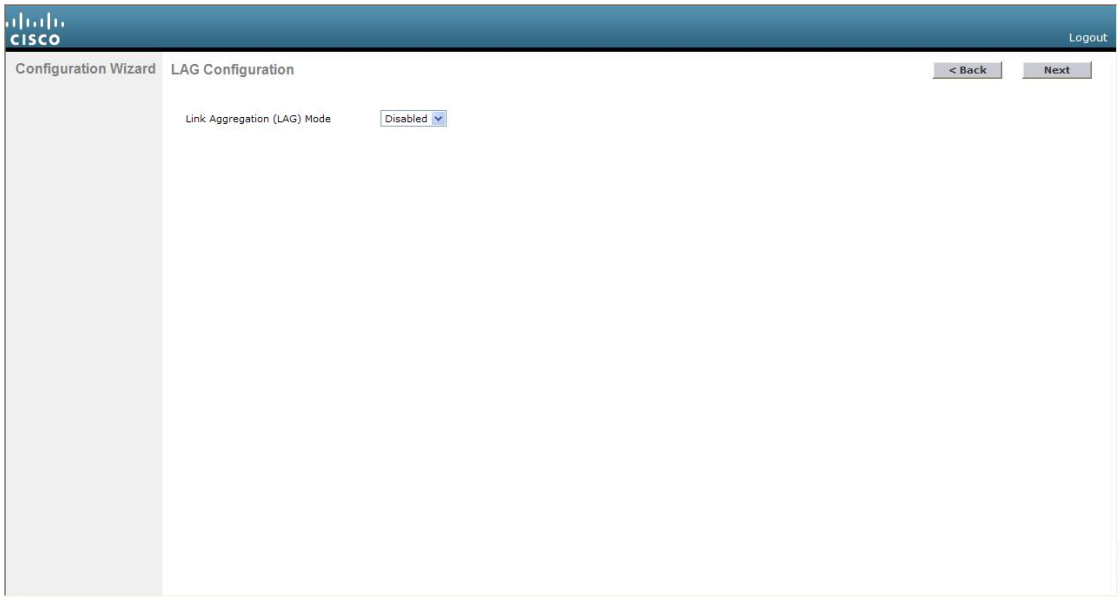
Step 13 Perform one of the following:

- If you enabled DHCP, clear out any entries in the IP Address and Netmask text boxes, leaving them blank.
- If you disabled DHCP, enter the static IP address and netmask for the service port in the IP Address and Netmask text boxes.

Step 14 Click **Next**.

The LAG Configuration screen appears.

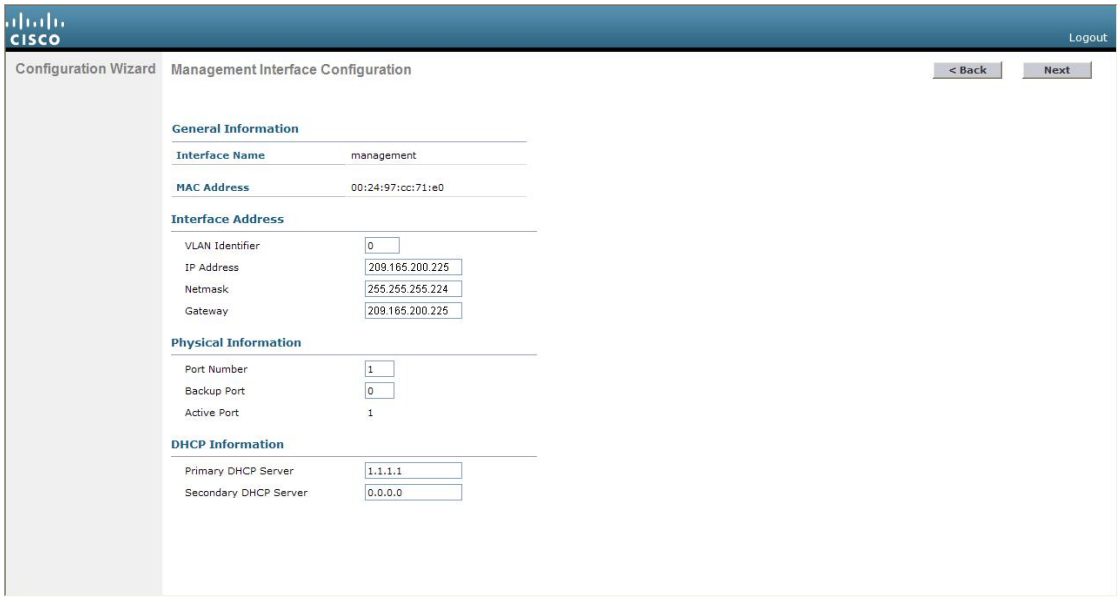
Figure 6: Configuration Wizard — LAG Configuration Screen



Step 15 To enable link aggregation (LAG), choose **Enabled** from the Link Aggregation (LAG) Mode drop-down list. To disable LAG, leave this text box set to **Disabled**.

Step 16 Click **Next**
The Management Interface Configuration screen appears.

Figure 7: Configuration Wizard — Management Interface Configuration Screen



Note The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers.

Step 17 In the VLAN Identifier text box, enter the VLAN identifier of the management interface (either a valid VLAN identifier or **0** for an untagged VLAN). The VLAN identifier should be set to match the switch interface configuration.

Step 18 In the IP Address text box, enter the IP address of the management interface.

Step 19 In the Netmask text box, enter the IP address of the management interface netmask.

Step 20 In the Gateway text box, enter the IP address of the default gateway.

Step 21 In the Port Number text box, enter the number of the port assigned to the management interface. Each interface is mapped to at least one primary port.

Step 22 In the Backup Port text box, enter the number of the backup port assigned to the management interface. If the primary port for the management interface fails, the interface automatically moves to the backup port.

Step 23 In the Primary DHCP Server text box, enter the IP address of the default DHCP server that will supply IP addresses to clients, the controller's management interface, and optionally, the service port interface.

Step 24 In the Secondary DHCP Server text box, enter the IP address of an optional secondary DHCP server that will supply IP addresses to clients, the controller's management interface, and optionally, the service port interface.

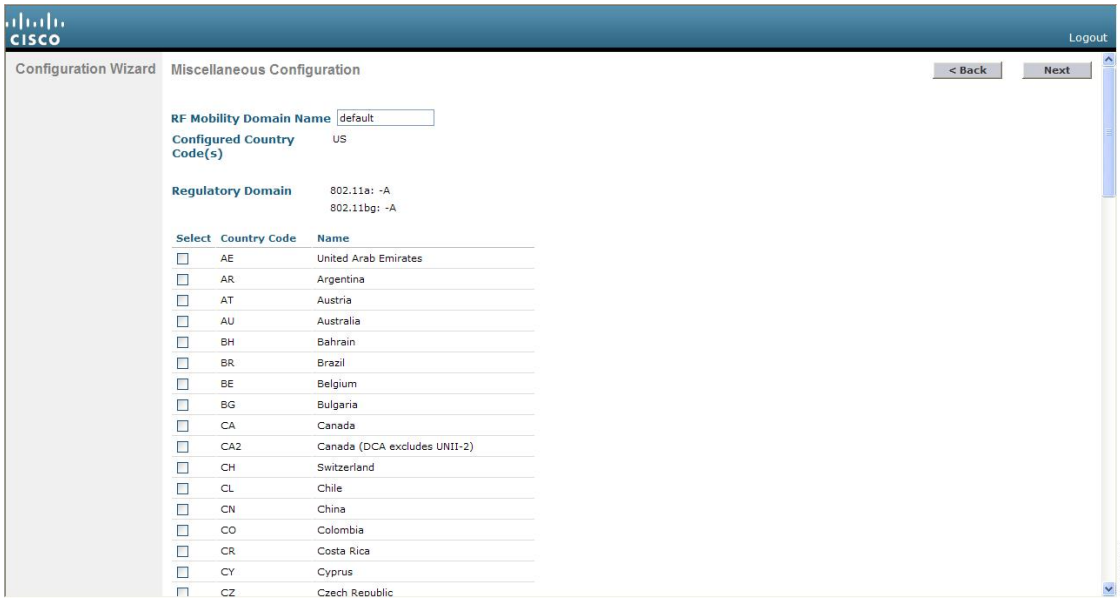
Step 25 Click **Next**. The AP-Manager Interface Configuration screen appears.

Note This screen does not appear for Cisco 5500 Series Controllers because you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

Step 26 In the IP Address text box, enter the IP address of the AP-manager interface.

Step 27 Click **Next**. The Miscellaneous Configuration screen appears.

Figure 8: Configuration Wizard — Miscellaneous Configuration Screen



Step 28 In the RF Mobility Domain Name text box, enter the name of the mobility group/RF group to which you want the controller to belong.

Note Although the name that you enter here is assigned to both the mobility group and the RF group, these groups are not identical. Both groups define clusters of controllers, but they have different purposes. All of the controllers in an RF group are usually also in the same mobility group and vice versa. However, a mobility group facilitates scalable, system-wide mobility and controller redundancy while an RF group facilitates scalable, system-wide dynamic RF management.

Step 29 The Configured Country Code(s) text box shows the code for the country in which the controller will be used. If you want to change the country of operation, select the check box for the desired country.

Note You can choose more than one country code if you want to manage access points in multiple countries from a single controller. After the configuration wizard runs, you must assign each access point joined to the controller to a specific country.

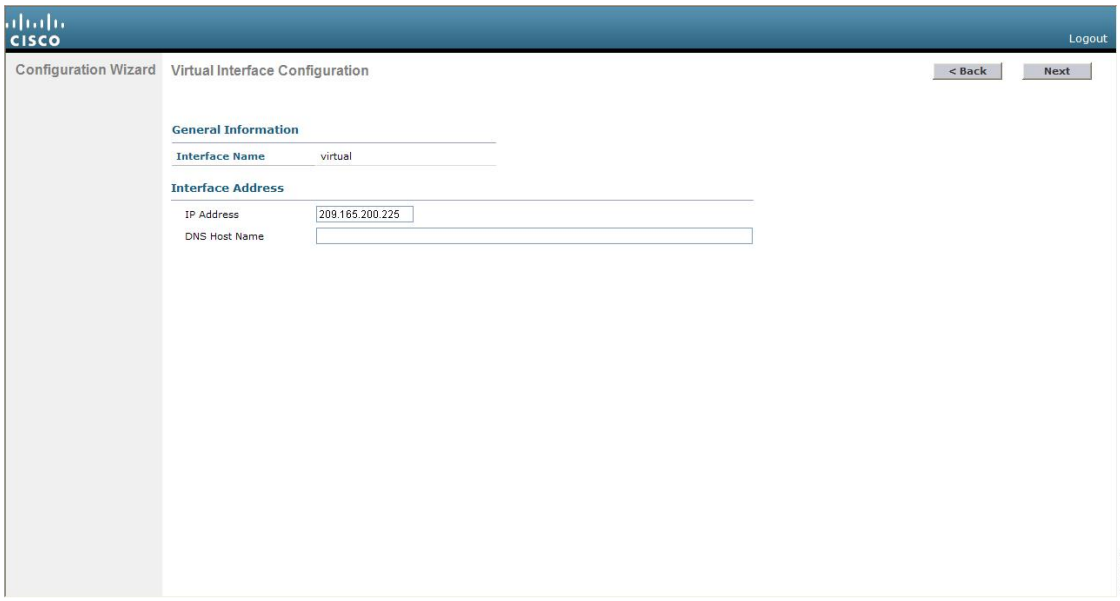
Step 30 Click **Next**.

Step 31 When the following message appears, click **OK**:

```
Warning! To maintain regulatory compliance functionality, the country code
setting may only be modified by a network administrator or qualified IT professional.
Ensure that proper country codes are selected before proceeding.?
```

The Virtual Interface Configuration screen appears.

Figure 9: Configuration Wizard — Virtual Interface Configuration Screen



Step 32 In the IP Address text box, enter the IP address of the controller's virtual interface. You should enter a fictitious, unassigned IP address.

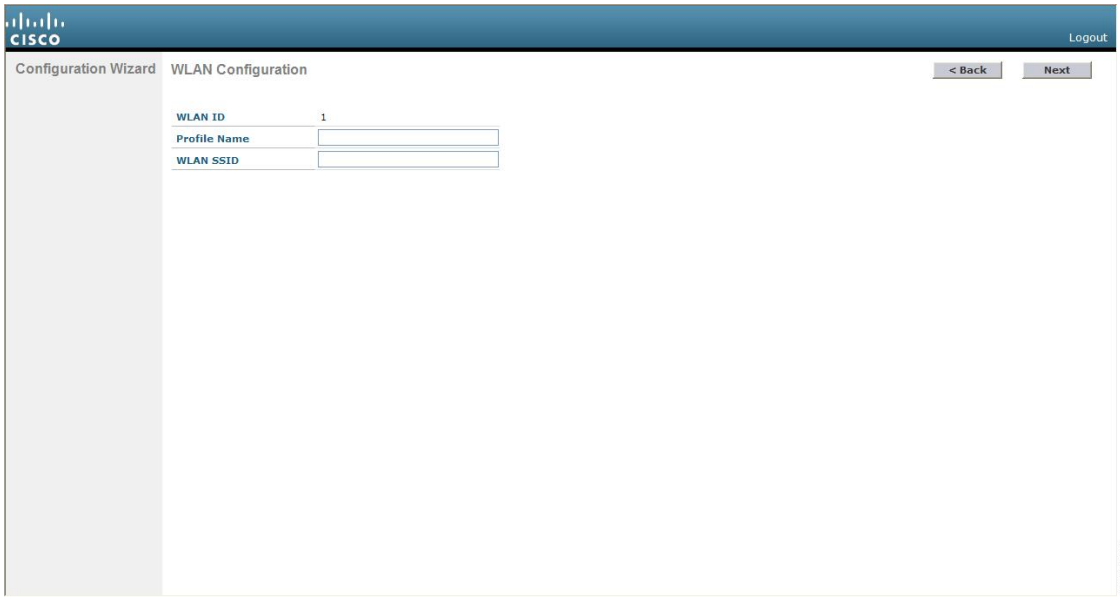
Note The virtual interface is used to support mobility management, DHCP relay, and embedded Layer 3 security such as guest web authentication and VPN termination. All controllers within a mobility group must be configured with the same virtual interface IP address.

Step 33 In the DNS Host Name text box, enter the name of the Domain Name System (DNS) gateway used to verify the source of certificates when Layer 3 web authorization is enabled.

Note To ensure connectivity and web authentication, the DNS server should always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then the same DNS hostname must be configured on the DNS servers used by the client.

Step 34 Click **Next**. The WLAN Configuration screen appears.

Figure 10: Configuration Wizard — WLAN Configuration Screen



Step 35 In the Profile Name text box, enter up to 32 alphanumeric characters for the profile name to be assigned to this WLAN.

Step 36 In the WLAN SSID text box, enter up to 32 alphanumeric characters for the network name, or service set identifier (SSID). The SSID enables basic functionality of the controller and allows access points that have joined the controller to enable their radios.

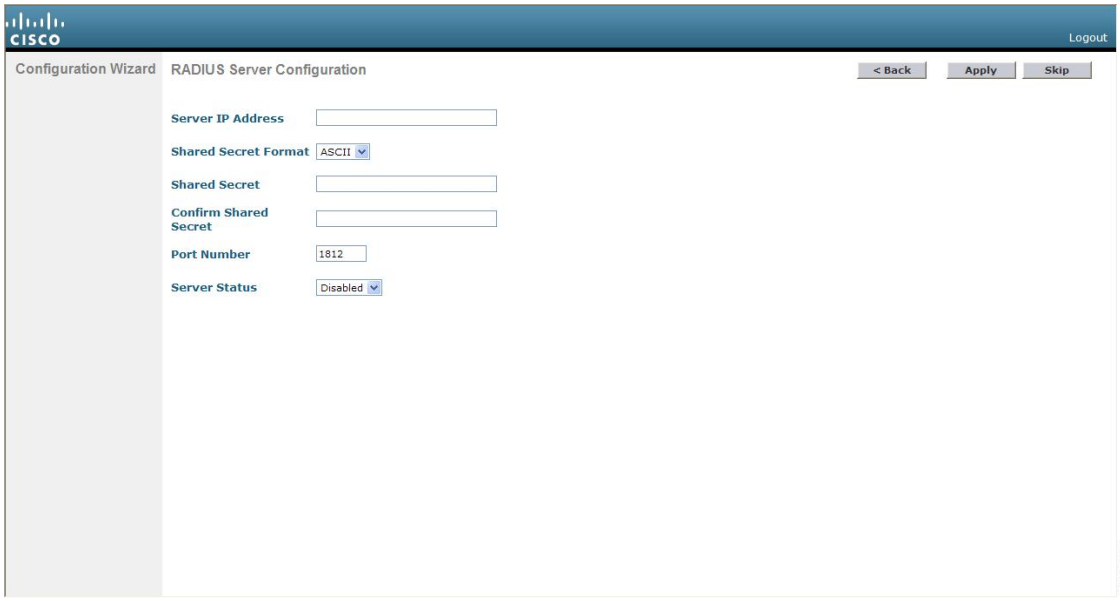
Step 37 Click **Next**.

Step 38 When the following message appears, click **OK**:

```
Default Security applied to WLAN is: [WPA2(AES)][Auth(802.1x)]. You can change
this after the wizard is complete and the system is rebooted.?
```

The RADIUS Server Configuration screen is displayed.

Figure 11: Configuration Wizard — RADIUS Server Configuration Screen



Step 39 In the Server IP Address text box, enter the IP address of the RADIUS server.

Step 40 From the Shared Secret Format drop-down list, choose **ASCII** or **Hex** to specify the format of the shared secret.

Note Due to security reasons, the RADIUS shared secret key reverts to ASCII mode even if you have selected HEX as the shared secret format from the Shared Secret Format drop-down list.

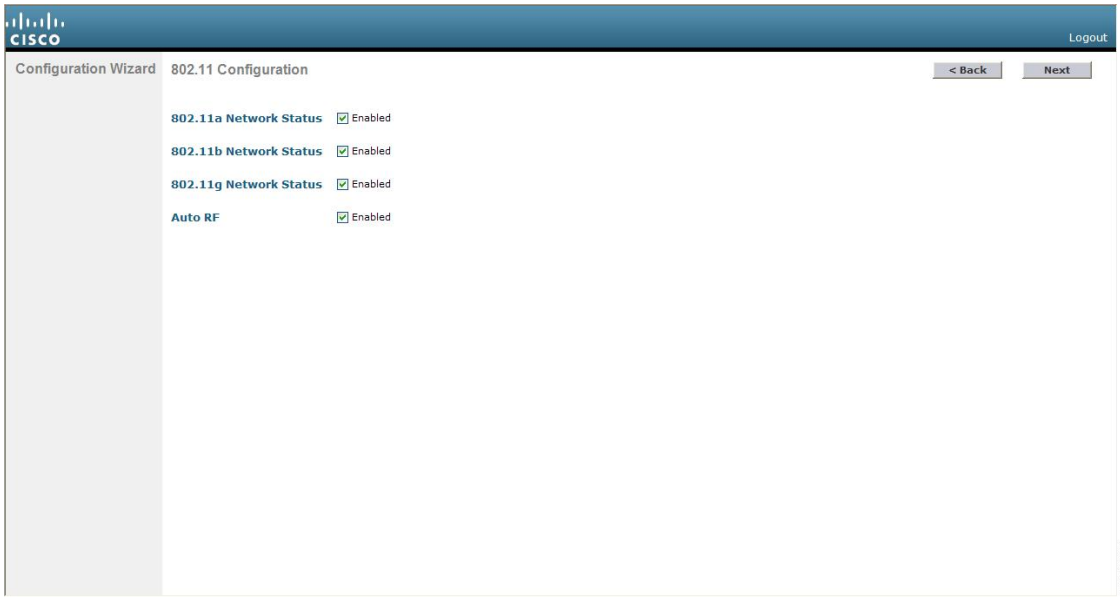
Step 41 In the Shared Secret and Confirm Shared Secret text boxes, enter the secret key used by the RADIUS server.

Step 42 In the Port Number text box, enter the communication port of the RADIUS server. The default value is 1812.

Step 43 To enable the RADIUS server, choose **Enabled** from the Server Status drop-down list. To disable the RADIUS server, leave this text box set to **Disabled**.

Step 44 Click **Apply**. The 802.11 Configuration screen appears.

Figure 12: Configuration Wizard — 802.11 Configuration Screen



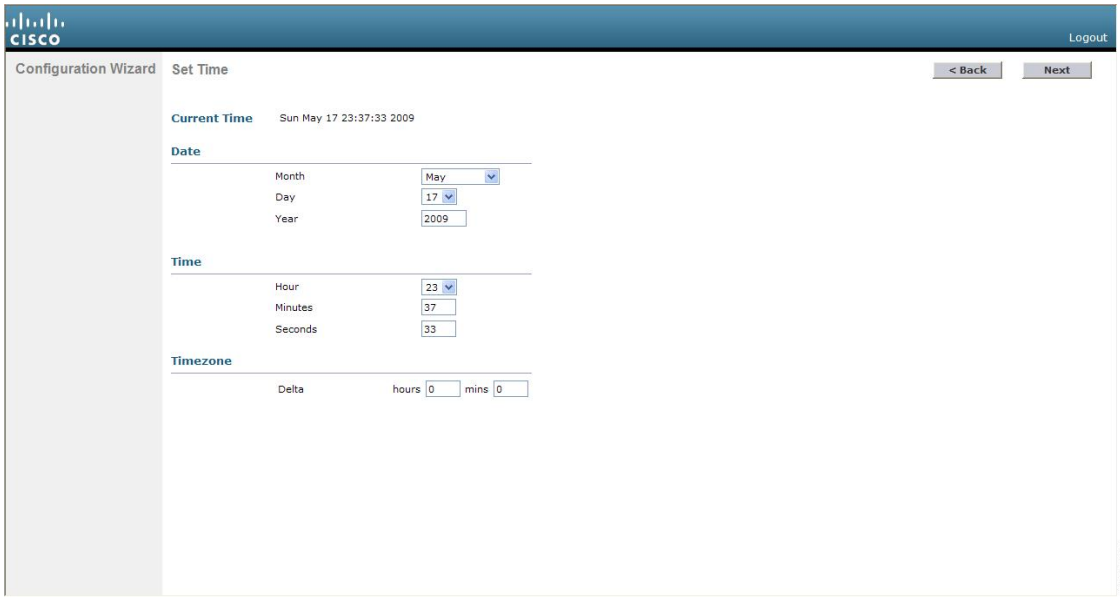
Step 45 To enable the 802.11a, 802.11b, and 802.11g lightweight access point networks, leave the **802.11a Network Status**, **802.11b Network Status**, and **802.11g Network Status** check boxes selected. To disable support for any of these networks, unselect the check boxes.

Step 46 To enable the controller's radio resource management (RRM) auto-RF feature, leave the **Auto RF** check box selected. To disable support for the auto-RF feature, unselect this check box.

Note The auto-RF feature enables the controller to automatically form an RF group with other controllers. The group dynamically elects a leader to optimize RRM parameter settings, such as channel and transmit power assignment, for the group.

Step 47 Click **Next**. The Set Time screen appears.

Figure 13: Configuration Wizard — Set Time Screen



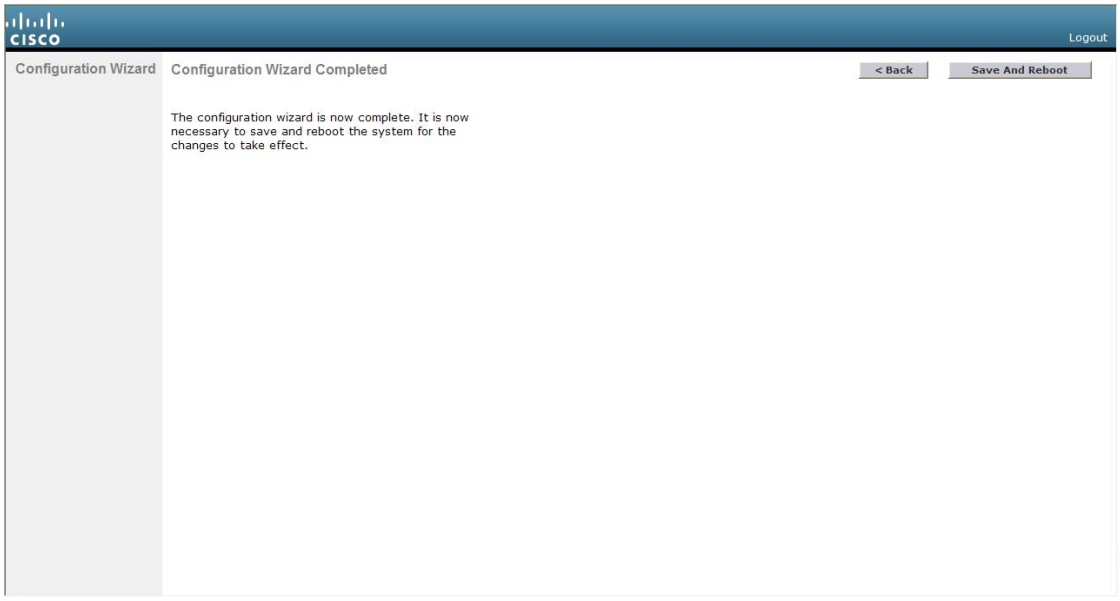
Step 48 To manually configure the system time on your controller, enter the current date in Month/DD/YYYY format and the current time in HH:MM:SS format.

Step 49 To manually set the time zone so that Daylight Saving Time (DST) is not set automatically, enter the local hour difference from Greenwich Mean Time (GMT) in the Delta Hours text box and the local minute difference from GMT in the Delta Mins text box.

Note When manually setting the time zone, enter the time difference of the local current time zone with respect to GMT (+/–). For example, Pacific time in the United States is 8 hours behind GMT. Therefore, it is entered as –8.

Step 50 Click **Next**. The Configuration Wizard Completed screen appears.

Figure 14: Configuration Wizard — Configuration Wizard Completed Screen



Step 51 Click **Save and Reboot** to save your configuration and reboot the controller.

Step 52 When the following message appears, click **OK**:

```
Configuration will be saved and the controller will be
rebooted. Click ok to confirm.?
```

The controller saves your configuration, reboots, and prompts you to log on.

Configuring the Controller—Using the CLI Configuration Wizard

Before You Begin

- The available options appear in brackets after each configuration parameter. The default value appears in all uppercase letters.
- If you enter an incorrect response, the controller provides you with an appropriate error message, such as "Invalid Response," and returns you to the wizard prompt.
- Press the **hyphen** key if you ever need to return to the previous command line.

Step 1 When prompted to terminate the AutoInstall process, enter **yes**. If you do not enter **yes**, the AutoInstall process begins after 30 seconds.

Note The AutoInstall feature downloads a configuration file from a TFTP server and then loads the configuration onto the controller automatically.

Step 2 Enter the system name, which is the name that you want to assign to the controller. You can enter up to 31 ASCII characters.

Step 3 Enter the administrative username and password to be assigned to this controller. You can enter up to 24 ASCII characters for each.
Starting in release 7.0.116.0, the following password policy has been implemented:

- The password must contain characters from at least three of the following classes:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters
- No character in the password must be repeated more than three times consecutively.
- The new password must not be the same as the associated username and not be the username reversed.
- The password must not be cisco, ocsic, or any variant obtained by changing the capitalization of letters of the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s.

Step 4 If you want the controller's service-port interface to obtain an IP address from a DHCP server, enter **DHCP**. If you do not want to use the service port or if you want to assign a static IP address to the service port, enter none.

Note The service-port interface controls communications through the service port. Its IP address must be on a different subnet from the management interface. This configuration enables you to manage the controller directly or through a dedicated management network to ensure service access during network downtime.

Step 5 If you entered none in *Step 4*, enter the IP address and netmask for the service-port interface on the next two lines.

Step 6 Enable or disable link aggregation (LAG) by choosing yes or NO.

Step 7 Enter the IP address of the management interface.

Note The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers.

Step 8 Enter the IP address of the management interface netmask.

Step 9 Enter the IP address of the default router.

Step 10 Enter the VLAN identifier of the management interface (either a valid VLAN identifier or 0 for an untagged VLAN). The VLAN identifier should be set to match the switch interface configuration.

Step 11 Enter the IP address of the default DHCP server that will supply IP addresses to clients, the management interface of the controller, and optionally, the service port interface. Enter the IP address of the AP-manager interface.

Note This prompt does not appear for Cisco 5500 Series Controllers because you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

Step 12 Enter the IP address of the controller's virtual interface. You should enter a fictitious unassigned IP address.

Note The virtual interface is used to support mobility management, DHCP relay, and embedded Layer 3 security such as guest web authentication and VPN termination. All controllers within a mobility group must be configured with the same virtual interface IP address.

Step 13 If desired, enter the name of the mobility group/RF group to which you want the controller to belong.

Note Although the name that you enter here is assigned to both the mobility group and the RF group, these groups are not identical. Both groups define clusters of controllers, but they have different purposes. All of the controllers in an RF group are usually also in the same mobility group and vice versa. However, a mobility group facilitates scalable, system-wide mobility and controller redundancy while an RF group facilitates scalable, system-wide dynamic RF management.

Step 14 Enter the network name or service set identifier (SSID). The SSID enables basic functionality of the controller and allows access points that have joined the controller to enable their radios.

Step 15 Enter YES to allow clients to assign their own IP address or no to require clients to request an IP address from a DHCP server.

Step 16 To configure a RADIUS server now, enter YES and then enter the IP address, communication port, and secret key of the RADIUS server. Otherwise, enter no. If you enter no, the following message appears: "Warning! The default WLAN security policy requires a RADIUS server. Please see the documentation for more details."

Step 17 Enter the code for the country in which the controller will be used.

Note Enter help to view the list of available country codes.

Note You can enter more than one country code if you want to manage access points in multiple countries from a single controller. To do so, separate the country codes with a comma (for example, US,CA,MX). After the configuration wizard runs, you need to assign each access point joined to the controller to a specific country.

Step 18 Enable or disable the 802.11b, 802.11a, and 802.11g lightweight access point networks by entering **YES** or **no**.

Step 19 Enable or disable the controller's radio resource management (RRM) auto-RF feature by entering **YES** or **no**.

Note The auto-RF feature enables the controller to automatically form an RF group with other controllers. The group dynamically elects a leader to optimize RRM parameter settings, such as channel and transmit power assignment, for the group.

Step 20 If you want the controller to receive its time setting from an external Network Time Protocol (NTP) server when it powers up, enter **YES** to configure an NTP server. Otherwise, enter **no**.

Note The controller network module installed in a Cisco Integrated Services Router does not have a battery and cannot save a time setting. Therefore, it must receive a time setting from an external NTP server when it powers up.

Step 21 If you entered **no** in *Step 20* and want to manually configure the system time on your controller now, enter **YES**. If you do not want to configure the system time now, enter **no**.

Step 22 If you entered **YES** in *Step 21*, enter the current date in the MM/DD/YY format and the current time in the HH:MM:SS format.

Step 23 When prompted to verify that the configuration is correct, enter **yes** or **NO**.

The controller saves your configuration, reboots, and prompts you to log on.

Using the Controller Web GUI

A web browser, or graphical user interface (GUI), is built into each controller.

It allows up to five users to simultaneously browse into the controller HTTP or HTTPS (HTTP + SSL) management pages to configure parameters and monitor the operational status for the controller and its associated access points.

Note We recommend that you enable the HTTPS interface and disable the HTTP interface to ensure more robust security for your Cisco UWN solution.

Guidelines and Limitations

Follow these guidelines when using the controller GUI:

- The GUI must be used on a PC running Windows 7, Windows XP SP1 (or later releases), or Windows 2000 SP4 (or later releases).
- The controller GUI is compatible with Microsoft Internet Explorer version 6.0 SP1 (or later versions) or Mozilla Firefox 2.0.0.11 (or later versions).

  Note Opera and Netscape are not supported.

- You can use either the service port interface or the management interface to access the GUI. We recommend that you use the service-port interface.
- You can use both HTTP and HTTPS when using the service port interface. HTTPS is enabled by default and HTTP can also be enabled. The default IP address to connect to the service port interface is 192.168.1.1.
- Click **Help** at the top of any page in the GUI to display online help. You might need to disable your browser's pop-up blocker to view the online help.

Logging On to the Web GUI

Step 1 Enter the controller IP address in your browser's address bar. For a secure connection, enter https://**ip-address**. For a less secure connection, enter http://**ip-address**.

Step 2 When prompted, enter a valid username and password, and click **OK**.
The **Summary** page is displayed.

Note The administrative username and password that you created in the configuration wizard are case sensitive. The default username is admin, and the default password is admin.

Logging out of the GUI

Step 1 Click **Logout** in the top right corner of the page.

Step 2 Click **Close** to complete the log out process and prevent unauthorized users from accessing the controllercontroller GUI.

Step 3 When prompted to confirm your decision, click **Yes**.

Enabling Web and Secure Web Modes

This section provides instructions to enable the distribution system port as a web port (using HTTP) or as a secure web port (using HTTPS). You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Sockets Layer (SSL) protocol. When you enable HTTPS, the controller generates its own local web administration SSL certificate and automatically applies it to the GUI. You also have the option of downloading an externally generated certificate.

You can configure web and secure web mode using the controller GUI or CLI.

Enabling Web and Secure Web Modes (GUI)

Step 1 Choose **Management** > **HTTP-HTTPS**.
The **HTTP-HTTPS Configuration** page is displayed.

Step 2 To enable web mode, which allows users to access the controller GUI using "http://*ip-address*," choose **Enabled** from the **HTTP Access** drop-down list. Otherwise, choose **Disabled**. The default value is Disabled. Web mode is not a secure connection.

Step 3 To enable secure web mode, which allows users to access the controller GUI using "https://*ip-address*," choose **Enabled** from the **HTTPS Access** drop-down list. Otherwise, choose **Disabled**. The default value is Enabled. Secure web mode is a secure connection.

Step 4 In the **Web Session Timeout** text box, enter the amount of time, in minutes, before the web session times out due to inactivity. You can enter a value between 10 and 160 minutes (inclusive). The default value is 30 minutes.

Step 5 Click **Apply**.

Step 6 If you enabled secure web mode in Step 3, the controller generates a local web administration SSL certificate and automatically applies it to the GUI. The details of the current certificate appear in the middle of the **HTTP-HTTPS Configuration** page.

Note If desired, you can delete the current certificate by clicking **Delete Certificate** and have the controller generate a new certificate by clicking **Regenerate Certificate**.

Step 7 Click **Save Configuration**.

Enabling Web and Secure Web Modes (CLI)

Step 1 Enable or disable web mode by entering this command:
config network webmode {**enable** | **disable**}

This command allows users to access the controller GUI using "http://*ip-address*." The default value is disabled. Web mode is not a secure connection.

Step 2 Enable or disable secure web mode by entering this command:
config network secureweb {**enable** | **disable**}

This command allows users to access the controller GUI using "https://*ip-address*." The default value is enabled. Secure web mode is a secure connection.

Step 3 Enable or disable secure web mode with increased security by entering this command:
config network secureweb cipher-option high {**enable** | **disable**}

This command allows users to access the controller GUI using "https://*ip-address*" but only from browsers that support 128-bit (or larger) ciphers. The default value is disabled.

Step 4 Enable or disable SSLv2 for web administration by entering this command:
config network secureweb cipher-option sslv2 {**enable** | **disable**}

If you disable SSLv2, users cannot connect using a browser configured with SSLv2 only. They must use a browser that is configured to use a more secure protocol such as SSLv3 or later. The default value is disabled.

Step 5 Enable or disable preference for RC4-SHA (Rivest Cipher 4-Secure Hash Algorithm) cipher suites (over CBC cipher suites) for web authentication and web administration by entering this command:
config network secureweb cipher-option rc4-preference {**enable** | **disable**}

Step 6 Verify that the controller has generated a certificate by entering this command:
show certificate summary

Information similar to the following appears:

```
Web Administration Certificate..................... Locally Generated
Web Authentication Certificate..................... Locally Generated
Certificate compatibility mode:.................... off
```

Step 7 (Optional) Generate a new certificate by entering this command:
config certificate generate webadmin

After a few seconds, the controller verifies that the certificate has been generated.

Step 8 Save the SSL certificate, key, and secure web password to nonvolatile RAM (NVRAM) so that your changes are retained across reboots by entering this command:
save config

Step 9 Reboot the controller by entering this command:
reset system

Loading an Externally Generated SSL Certificate

This section describes how to load an externally generated SSL certificate.

Information About Externally Generated SSL Certificates

You can use a TFTP server to download an externally generated SSL certificate to the controller. Follow these guidelines for using TFTP:

- If you load the certificate through the service port, the TFTP server must be on the same subnet as the controller because the service port is not routable, or you must create static routes on the controller. Also, if you load the certificate through the distribution system network port, the TFTP server can be on any subnet.
- A third-party TFTP server cannot run on the same PC as the Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP server and the third-party TFTP server require the same communication port.

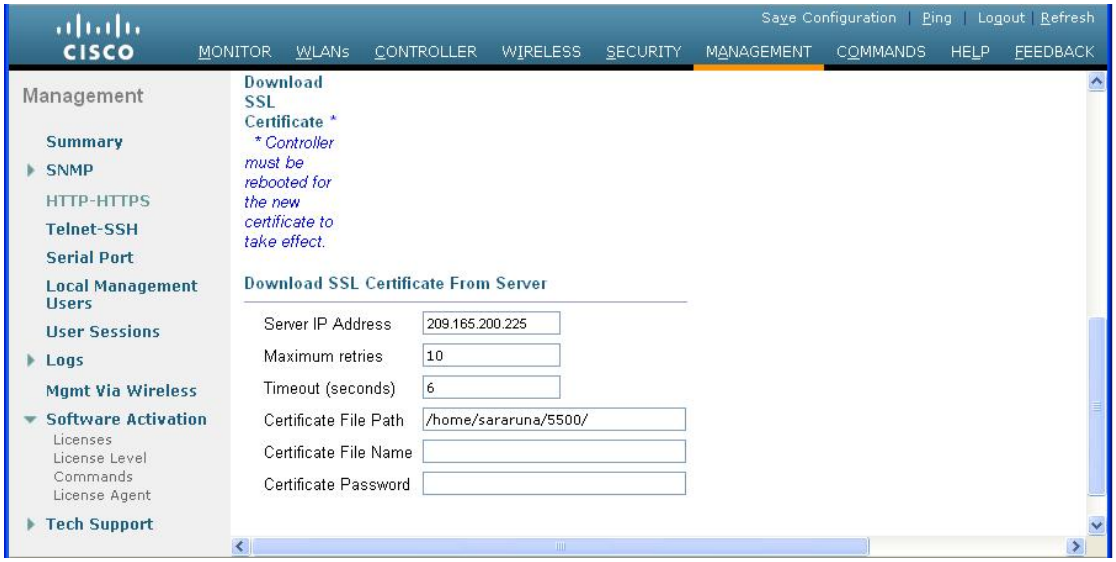
Note Chained certificates are supported for web authentication only and not for the management certificate.

Note Every HTTPS certificate contains an embedded RSA key. The length of the key can vary from 512 bits, which is relatively insecure, to thousands of bits, which is very secure. When you obtain a new certificate from a Certificate Authority, make sure that the RSA key embedded in the certificate is at least 768 bits long.

Loading an SSL Certificate (GUI)

Step 1 On the HTTP Configuration page, select the **Download SSL Certificate** check box.

Figure 15: HTTP Configuration Page



Step 2 In the **Server IP Address** text box, enter the IP address of the TFTP server.

Step 3 In the **Maximum Retries** text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 4 In the **Timeout** text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 5 In the **Certificate File Path** text box, enter the directory path of the certificate.

Step 6 In the **Certificate File Name** text box, enter the name of the certificate (webadmincert_name.pem).

Step 7 (Optional) In the **Certificate Password** text box, enter a password to encrypt the certificate.

Step 8 Click **Apply**.

Step 9 Click **Save Configuration**.

Step 10 Choose **Commands** > **Reboot** > **Reboot** > **Save and Reboot** to reboot the controller for your changes to take effect,

Loading an SSL Certificate (CLI)

Step 1 Use a password to encrypt the HTTPS certificate in a .PEM-encoded file. The PEM-encoded file is called a web administration certificate file (`webadmincert_name.pem`).

Step 2 Move the `webadmincert_name.pem` file to the default directory on your TFTP server.

Step 3 To view the current download settings, enter this command and answer **n** to the prompt:
transfer download start

Information similar to the following appears:

```
Mode..................................... TFTP
Data Type................................ Admin Cert
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ <directory path>
TFTP Filename.............................
Are you sure you want to start? (y/n) n
Transfer Canceled
```

Step 4 Use these commands to change the download settings:
transfer download mode *tftp*

transfer download datatype *webauthcert*

transfer download serverip *TFTP_server IP_address*

transfer download path *absolute_TFTP_server_path_to_the_update_file*

transfer download filename *webadmincert_name.pem*

Step 5 To set the password for the .PEM file so that the operating system can decrypt the web administration SSL key and certificate, enter this command:
transfer download certpassword *private_key_password*

Step 6 To confirm the current download settings and start the certificate and key download, enter this command and answer **y** to the prompt:
transfer download start

Information similar to the following appears:

```
Mode..................................... TFTP
Data Type................................ Site Cert
TFTP Server IP........................... xxx.xxx.xxx.xxx
TFTP Path................................ directory path
TFTP Filename............................ webadmincert_name
Are you sure you want to start? (y/n) y
TFTP Webadmin cert transfer starting.
Certificate installed.
Please restart the switch (reset system) to use the new certificate.
```

Step 7 To save the SSL certificate, key, and secure web password to NVRAM so that your changes are retained across reboots, enter this command:

save config

Step 8 To reboot the controller, enter this command:
reset system

Using the Controller CLI

A Cisco UWN solution command-line interface (CLI) is built into each controller. The CLI enables you to use a VT-100 terminal emulation program to locally or remotely configure, monitor, and control individual controllers and its associated lightweight access points. The CLI is a simple text-based, tree-structured interface that allows up to five users with Telnet-capable terminal emulation programs to access the controller.

Note See the Cisco Wireless LAN Controller Command Reference for information on specific commands.

Note If you want to input any strings from the XML configuration into CLI commands, you must enclose the strings in quotation marks.

Logging on to the Controller CLI

You can access the controller CLI using one of the following two methods:

- A direct serial connection to the controller console port
- A remote console session over Ethernet through the preconfigured service port or the distribution system ports

Before you log on to the CLI, configure your connectivity and environment variables based on the type of connection you use.

Guidelines and Limitations

On Cisco 5500 Series Controllers, you can use either the RJ-45 console port or the USB console port. If you use the USB console port, plug the 5-pin mini Type B connector into the controller's USB console port and the other end of the cable into the PC's USB Type A port. The first time that you connect a Windows PC to the USB console port, you are prompted to install the USB console driver. Follow the installation prompts to install the driver. The USB console driver maps to a COM port on your PC; you then need to map the terminal emulator application to the COM port.

See the Configuring Telnet and Secure Shell Sessions section for information on enabling Telnet sessions.

Using a Local Serial Connection

Before You Begin

You need these items to connect to the serial port:

- A PC that is running a VT-100 terminal emulation program (such as HyperTerminal, ProComm, Minicom, or Tip)
- A null-modem serial cable

To log on to the controller CLI through the serial port, follow these steps:

Step 1 Connect one end of a null-modem serial cable to the controller's console port and the other end to your PC's serial port.

Step 2 Start the PC's VT-100 terminal emulation program. Configure the terminal emulation program for these parameters:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity
- No hardware flow control

Note Minimum serial timeout on Controller is 15 seconds instead of 1 minute.

Note The controller serial port is set for a 9600 baud rate and a short timeout. If you would like to change either of these values, enter config serial baudrate baudrate and config serial timeout timeout to make your changes. If you enter config serial timeout 0, serial sessions never time out.

Step 3 When prompted, enter a valid username and password to log into the controller. The administrative username and password that you created in the configuration wizard are case sensitive.

Note The default username is admin, and the default password is admin.

The CLI displays the root level system prompt:

```
#(system prompt)>
```

Note The system prompt can be any alphanumeric string up to 31 characters. You can change it by entering the **config prompt** command.

Using a Remote Ethernet Connection

Before You Begin

You need these items to connect to a controller remotely:

- A PC with access to the controller over the Ethernet network

- The IP address of the controller
- A VT-100 terminal emulation program or a DOS shell for the Telnet session

Note By default, controllers block Telnet sessions. You must use a local connection to the serial port to enable Telnet sessions.

Step 1 Verify that your VT-100 terminal emulation program or DOS shell interface is configured with these parameters:

- Ethernet address
- Port 23

Step 2 Use the controller IP address to Telnet to the CLI.

Step 3 When prompted, enter a valid username and password to log into the controller. The administrative username and password that you created in the configuration wizard are case sensitive.

Note The default username is admin, and the default password is admin.

The CLI displays the root level system prompt.

Note The system prompt can be any alphanumeric string up to 31 characters. You can change it by entering the **config prompt** command.

Logging Out of the CLI

When you finish using the CLI, navigate to the root level and enter logout. The system prompts you to save any changes you made to the volatile RAM.

Note The CLI automatically logs you out without saving any changes after 5 minutes of inactivity. You can set the automatic logout from 0 (never log out) to 160 minutes using the **config serial timeout** command.

Navigating the CLI

The CLI is organized into five levels:

- Root Level
- Level 2
- Level 3
- Level 4
- Level 5

When you log into the CLI, you are at the root level. From the root level, you can enter any full command without first navigating to the correct command level.

The following table lists commands you use to navigate the CLI and to perform common tasks.

Table 2: Commands for CLI Navigation and Common Tasks

Command	Action
help	At the root level, view system wide navigation commands
?	View commands available at the current level
command ?	View parameters for a specific command
exit	Move down one level
Ctrl-Z	Return from any level to the root level
save config	At the root level, save configuration changes from active working RAM to nonvolatile RAM (NVRAM) so they are retained after reboot
reset system	At the root level, reset the controller without logging out

Using the AutoInstall Feature for Controllers Without a Configuration

This section describes how to use the AutoInstall feature for controllers without a configuration.

Information About the AutoInstall Feature

When you boot up a controller that does not have a configuration, the AutoInstall feature can download a configuration file from a TFTP server and then load the configuration onto the controller automatically.

If you create a configuration file on a controller that is already on the network (or through a Prime Infrastructure filter), place that configuration file on a TFTP server, and configure a DHCP server so that a new controller can get an IP address and TFTP server information, the AutoInstall feature can obtain the configuration file for the new controller automatically.

When the controller boots, the AutoInstall process starts. The controller does not take any action until AutoInstall is notified that the configuration wizard has started. If the wizard has not started, the controller has a valid configuration.

If AutoInstall is notified that the configuration wizard has started (which means that the controller does not have a configuration), AutoInstall waits for an additional 30 seconds. This time period gives you an opportunity to respond to the first prompt from the configuration wizard:

```
Would you like to terminate autoinstall? [yes]:
```

When the 30-second abort timeout expires, AutoInstall starts the DHCP client. You can abort the AutoInstall task even after this 30-second timeout if you enter **Yes** at the prompt. However, AutoInstall cannot be aborted if the TFTP task has locked the flash and is in the process of downloading and installing a valid configuration file.

Guidelines and Limitations

AutoInstall uses the following interfaces:

- Cisco 5500 Series Controllers
  - eth0—Service port (untagged)
  - dtl0—Gigabit port 1 through the NPU (untagged)

Obtaining an IP Address Through DHCP and Downloading a Configuration File from a TFTP Server

AutoInstall attempts to obtain an IP address from the DHCP server until the DHCP process is successful or until you abort the AutoInstall process. The first interface to successfully obtain an IP address from the DHCP server registers with the AutoInstall task. The registration of this interface causes AutoInstall to begin the process of obtaining TFTP server information and downloading the configuration file.

Following the acquisition of the DHCP IP address for an interface, AutoInstall begins a short sequence of events to determine the host name of the controller and the IP address of the TFTP server. Each phase of this sequence gives preference to explicitly configured information over default or implied information and to explicit host names over explicit IP addresses.

The process is as follows:

- If at least one Domain Name System (DNS) server IP address is learned through DHCP, AutoInstall creates a /etc/resolv.conf file. This file includes the domain name and the list of DNS servers that have been received. The Domain Name Server option provides the list of DNS servers, and the Domain Name option provides the domain name.
- If the domain servers are not on the same subnet as the controller, static route entries are installed for each domain server. These static routes point to the gateway that is learned through the DHCP Router option.
- The host name of the controller is determined in this order by one of the following:
  - If the DHCP Host Name option was received, this information (truncated at the first period [.]) is used as the host name for the controller.
  - A reverse DNS lookup is performed on the controller IP address. If DNS returns a hostname, this name (truncated at the first period [.]) is used as the hostname for the controller.
- The IP address of the TFTP server is determined in this order by one of the following:
  - If AutoInstall received the DHCP TFTP Server Name option, AutoInstall performs a DNS lookup on this server name. If the DNS lookup is successful, the returned IP address is used as the IP address of the TFTP server.

- If the DHCP Server Host Name (sname) text box is valid, AutoInstall performs a DNS lookup on this name. If the DNS lookup is successful, the IP address that is returned is used as the IP address of the TFTP server.
- If AutoInstall received the DHCP TFTP Server Address option, this address is used as the IP address of the TFTP server.
- AutoInstall performs a DNS lookup on the default TFTP server name (cisco-wlc-tftp). If the DNS lookup is successful, the IP address that is received is used as the IP address of the TFTP server.
- If the DHCP server IP address (siaddr) text box is nonzero, this address is used as the IP address of the TFTP server.
- The limited broadcast address (255.255.255.255) is used as the IP address of the TFTP server.

- If the TFTP server is not on the same subnet as the controller, a static route (/32) is installed for the IP address of the TFTP server. This static route points to the gateway that is learned through the DHCP Router option.

Selecting a Configuration File

After the hostname and TFTP server have been determined, AutoInstall attempts to download a configuration file. AutoInstall performs three full download iterations on each interface that obtains a DHCP IP address. If the interface cannot download a configuration file successfully after three attempts, the interface does not attempt further.

The first configuration file that is downloaded and installed successfully triggers a reboot of the controller. After the reboot, the controller runs the newly downloaded configuration.

AutoInstall searches for configuration files in the order in which the names are listed:

- The filename that is provided by the DHCP Boot File Name option
- The filename that is provided by the DHCP File text box
- *host name*-confg
- *host name*.cfg
- *base MAC address*-confg (for example, 0011.2233.4455-confg)
- *serial number*-confg
- ciscowlc-confg
- ciscowlc.cfg

AutoInstall runs through this list until it finds a configuration file. It stops running if it does not find a configuration file after it cycles through this list three times on each registered interface.

Note The downloaded configuration file can be a complete configuration, or it can be a minimal configuration that provides enough information for the controller to be managed by the Cisco Prime Infrastructure. Full configuration can then be deployed directly from the Prime Infrastructure.

Note AutoInstall does not expect the switch connected to the controller to be configured for either channels. AutoInstall works with a service port in LAG configuration.

Note Cisco Prime Infrastructure provides AutoInstall capabilities for controllers. A Cisco Prime Infrastructure administrator can create a filter that includes the host name, the MAC address, or the serial number of the controller and associate a group of templates (a configuration group) to this filter rule. The Prime Infrastructure pushes the initial configuration to the controller when the controller boots up initially. After the controller is discovered, the Prime Infrastructure pushes the templates that are defined in the configuration group. For more information about the AutoInstall feature and Cisco Prime Infrastructure, see the Cisco Prime Infrastructure documentation.

Example: AutoInstall Operation

The following is an example of an AutoInstall process from start to finish:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
Would you like to terminate autoinstall? [yes]:
AUTO-INSTALL: starting now...
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Filename ==> 'abcd-confg'
AUTO-INSTALL: interface 'service-port' - setting DHCP TFTP Server IP ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'service-port' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'service-port' - setting DHCP yiaddr ==> 172.19.29.253
AUTO-INSTALL: interface 'service-port' - setting DHCP Netmask ==> 255.255.255.0
AUTO-INSTALL: interface 'service-port' - setting DHCP Gateway ==> 172.19.29.1
AUTO-INSTALL: interface 'service-port' registered
AUTO-INSTALL: interation 1 -- interface 'service-port'
AUTO-INSTALL: DNS reverse lookup 172.19.29.253 ===> 'wlc-1'
AUTO-INSTALL: hostname 'wlc-1'
AUTO-INSTALL: TFTP server 1.100.108.2 (from DHCP Option 150)
AUTO-INSTALL: attempting download of 'abcd-confg'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: interface 'management' - setting DHCP file ==> 'bootfile1'
AUTO-INSTALL: interface 'management' - setting DHCP TFTP Filename ==> 'bootfile2-confg'
AUTO-INSTALL: interface 'management' - setting DHCP siaddr ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[0] ==> 1.100.108.2
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[1] ==> 1.100.108.3
AUTO-INSTALL: interface 'management' - setting DHCP Domain Server[2] ==> 1.100.108.4
AUTO-INSTALL: interface 'management' - setting DHCP Domain Name ==> 'engtest.com'
AUTO-INSTALL: interface 'management' - setting DHCP yiaddr ==> 1.100.108.238
AUTO-INSTALL: interface 'management' - setting DHCP Netmask ==> 255.255.254.0
AUTO-INSTALL: interface 'management' - setting DHCP Gateway ==> 1.100.108.1
AUTO-INSTALL: interface 'management' registered
AUTO-INSTALL: TFTP status - 'Config file transfer failed - Error from server: File not
found' (3)
AUTO-INSTALL: attempting download of 'wlc-1-confg'
AUTO-INSTALL: TFTP status - 'TFTP Config transfer starting.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... updating configuration.' (2)
AUTO-INSTALL: TFTP status - 'TFTP receive complete... storing in flash.' (2)
AUTO-INSTALL: TFTP status - 'System being reset.' (2)
Resetting system
```

Managing the Controller System Date and Time

This section describes how to manage the date and time of a controller system.

Information About Controller System Date and Time

You can configure the controller system date and time at the time of configuring the controller using the configuration wizard. If you did not configure the system date and time through the configuration wizard or if you want to change your configuration, you can follow the instructions in this section to configure the controller to obtain the date and time from a Network Time Protocol (NTP) server or to configure the date and time manually. Greenwich Mean Time (GMT) is used as the standard for setting the time zone on the controller.

You can also configure an authentication mechanism between various NTP servers.

Guidelines and Limitations

- If you are configuring wIPS, you must set the controller time zone to UTC.
- Cisco Aironet lightweight access points might not connect to the controller if the date and time are not set properly. Set the current date and time on the controller before allowing the access points to connect to it.
- You can configure an authentication channel between the controller and the NTP server.

Configuring an NTP Server to Obtain the Date and Time

Each NTP server IP address is added to the controller database. Each controller searches for an NTP server and obtains the current time upon reboot and at each user-defined polling interval (daily to weekly).

Use these commands to configure an NTP server to obtain the date and time:

- To specify the NTP server for the controller, enter this command:

  config time ntp server *index ip_address*

- To specify the polling interval (in seconds), enter this command:

  config time ntp *interval*

Configuring NTP Authentication (GUI)

Step 1 Choose **Controller > NTP > Servers** to open the NTP Servers page.
Step 2 Click **New** to add an NTP server.
Step 3 Choose a server priority from the Server Index (Priority) drop-down list.
Step 4 Enter the NTP server IP address in the Server IP Address text box.
Step 5 Enable NTP server authentication by selecting the **NTP Server Authentication** check box.
Step 6 Click **Apply**.
Step 7 Choose **Controller > NTP > Keys**.
Step 8 Click **New** to create a key.
Step 9 Enter the key index in the Key Index text box.
Step 10 Choose the key format from the Key Format drop-down list.
Step 11 Enter the key in the Key text box.
Step 12 Click **Apply**.

Configuring NTP Authentication (CLI)

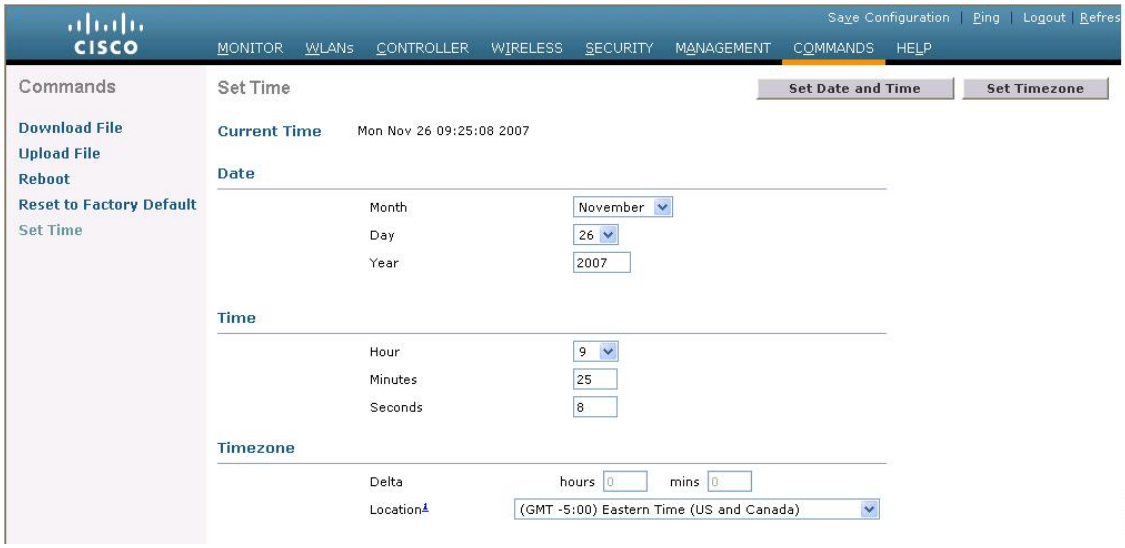
Note By default, MD5 is used.

- **config time ntp auth enable** *server-index key-index*
- **config time ntp auth disable** *server-index*
- **config time ntp key-auth add key-index md5** *key-format key*
- Delete an authentication key by entering this command:
  config time ntp key-auth delete *key-index*
- View the list of NTP key Indices by entering this command:
  show ntp-keys

Configuring the Date and Time (GUI)

Step 1 Choose **Commands > Set Time** to open the Set Time page.

Figure 16: Set Time Page



The current date and time appear at the top of the page.

Step 2 In the Timezone area, choose your local time zone from the Location drop-down list.

Note When you choose a time zone that uses Daylight Saving Time (DST), the controller automatically sets its system clock to reflect the time change when DST occurs. In the United States, DST starts on the second Sunday in March and ends on the first Sunday in November.

Note You cannot set the time zone delta on the controller GUI. However, if you do so on the controller CLI, the change is reflected in the Delta Hours and Mins text boxes on the controller GUI.

Step 3 Click **Set Timezone** to apply your changes.

Step 4 In the Date area, choose the current local month and day from the Month and Day drop-down lists, and enter the year in the Year text box.

Step 5 In the Time area, choose the current local hour from the Hour drop-down list, and enter the minutes and seconds in the Minutes and Seconds text boxes.

Note If you change the time zone location after setting the date and time, the values in the Time area are updated to reflect the time in the new time zone location. For example, if the controller is currently configured for noon Eastern time and you change the time zone to Pacific time, the time automatically changes to 9:00 a.m.

Step 6 Click **Set Date and Time** to apply your changes.

Step 7 Click **Save Configuration** to save your changes.

Configuring the Date and Time (CLI)

Step 1 Configure the current local date and time in GMT on the controller by entering this command:
config time manual *mm/dd/yy hh:mm:ss*

Note When setting the time, the current local time is entered in terms of GMT and as a value between 00:00 and 24:00. For example, if it is 8:00 a.m. Pacific time in the United States, you would enter 16:00 because the Pacific time zone is 8 hours behind GMT.

Step 2 Perform one of the following to set the time zone for the controller:

- Set the time zone location in order to have Daylight Saving Time (DST) set automatically when it occurs by entering this command:

  config time timezone location *location_index*

  where *location_index* is a number representing one of the following time zone locations:

  1 (GMT-12:00) International Date Line West

  2 (GMT-11:00) Samoa

  3 (GMT-10:00) Hawaii

  4 (GMT-9:00) Alaska

  5 (GMT-8:00) Pacific Time (US and Canada)

  6 (GMT-7:00) Mountain Time (US and Canada)

  7 (GMT-6:00) Central Time (US and Canada)

  8 (GMT-5:00) Eastern Time (US and Canada)

  9 (GMT-4:00) Atlantic Time (Canada)

  10 (GMT-3:00) Buenos Aires (Argentina)

  11 (GMT-2:00) Mid-Atlantic

  12 (GMT-1:00) Azores

  13 (GMT) London, Lisbon, Dublin, Edinburgh (default value)

  14 (GMT +1:00) Amsterdam, Berlin, Rome, Vienna

  15 (GMT +2:00) Jerusalem

  16 (GMT +3:00) Baghdad

  17 (GMT +4:00) Muscat, Abu Dhabi

  18 (GMT +4:30) Kabul

  19 (GMT +5:00) Karachi, Islamabad, Tashkent

  20 (GMT +5:30) Colombo, Kolkata, Mumbai, New Delhi

  21 (GMT +5:45) Katmandu

  22 (GMT +6:00) Almaty, Novosibirsk

23 (GMT +6:30) Rangoon

24 (GMT +7:00) Saigon, Hanoi, Bangkok, Jakarta

25 (GMT +8:00) Hong Kong, Beijing, Chongqing

26 (GMT +9:00) Tokyo, Osaka, Sapporo

27 (GMT +9:30) Darwin

28 (GMT+10:00) Sydney, Melbourne, Canberra

29 (GMT+11:00) Magadan, Solomon Is., New Caledonia

30 (GMT+12:00) Kamchatka, Marshall Is., Fiji

31 (GMT+12:00) Auckland (New Zealand)

Note If you enter this command, the controller automatically sets its system clock to reflect DST when it occurs. In the United States, DST starts on the second Sunday in March and ends on the first Sunday in November.

- Manually set the time zone so that DST is not set automatically by entering this command:

  config time timezone *delta_hours delta_mins*

  where *delta_hours* is the local hour difference from GMT, and *delta_mins* is the local minute difference from GMT.

  When manually setting the time zone, enter the time difference of the local current time zone with respect to GMT (+/–). For example, Pacific time in the United States is 8 hours behind GMT. Therefore, it is entered as –8.

  Note You can manually set the time zone and prevent DST from being set only on the controller CLI.

Step 3 Save your changes by entering this command:
save config

Step 4 Verify that the controller shows the current local time with respect to the local time zone by entering this command:
show time

Information similar to the following appears:

```
Time..................................... Thu Apr  7 13:56:37 2011
Timezone delta........................... 0:0
Timezone location....................... (GMT +5:30) Colombo, New Delhi, Chennai, Kolkata

NTP Servers
    NTP Polling Interval.........................     3600

     Index     NTP Key Index     NTP Server       NTP Msg Auth Status
    -------  ------------------------------------------------------------
       1              1           209.165.200.225      AUTH SUCCESS
```

Note If you configured the time zone location, the Timezone Delta value is set to "0:0." If you manually configured the time zone using the time zone delta, the Timezone Location is blank.

Configuring Telnet and Secure Shell Sessions

This section describes how to configure Telnet and Secure Shell (SSH) sessions.

Information About Telnet and SSH

Telnet is a network protocol used to provide access to the controller's CLI. Secure Shell (SSH) is a more secure version of Telnet that uses data encryption and a secure channel for data transfer. You can use the controller GUI or CLI to configure Telnet and SSH sessions.

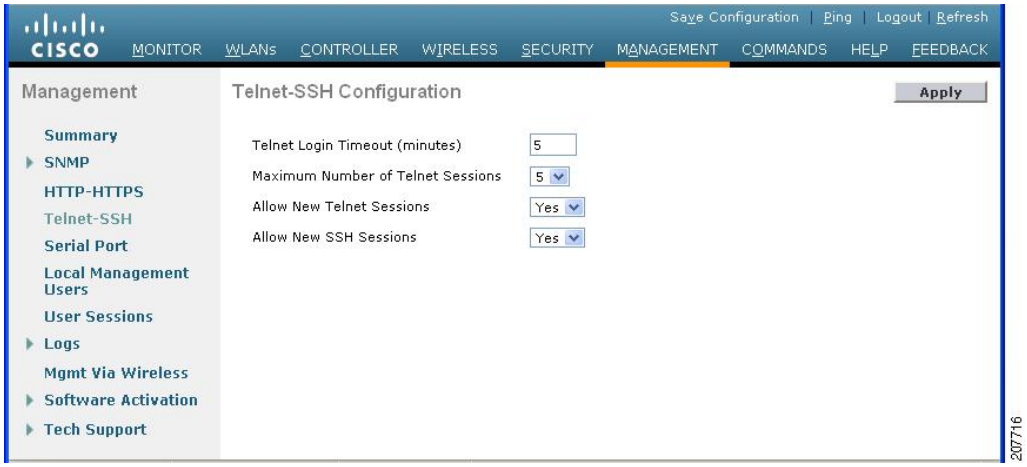
Restrictions for Telnet and SSH

- Only the FIPS approved algorithm aes128-cbc is supported when using SSH to control WLANs.
- The controller does not support raw Telnet mode.

Configuring Telnet and SSH Sessions (GUI)

Step 1 Choose **Management** > **Telnet-SSH** to open the Telnet-SSH Configuration page.

Figure 17: Telnet-SSH Configuration Page



Step 2 In the **Telnet Login Timeout** text box, enter the number of minutes that a Telnet session is allowed to remain inactive before being terminated. The valid range is 0 to 160 minutes (inclusive), and the default value is 5 minutes. A value of 0 indicates no timeout.

Step 3 From the **Maximum Number of Sessions** drop-down list, choose the number of simultaneous Telnet or SSH sessions allowed. The valid range is 0 to 5 sessions (inclusive), and the default value is 5 sessions. A value of zero indicates that Telnet/SSH sessions are disallowed.

Step 4 From the **Allow New Telnet Sessions** drop-down list, choose **Yes** or **No** to allow or disallow new Telnet sessions on the controller. The default value is No.

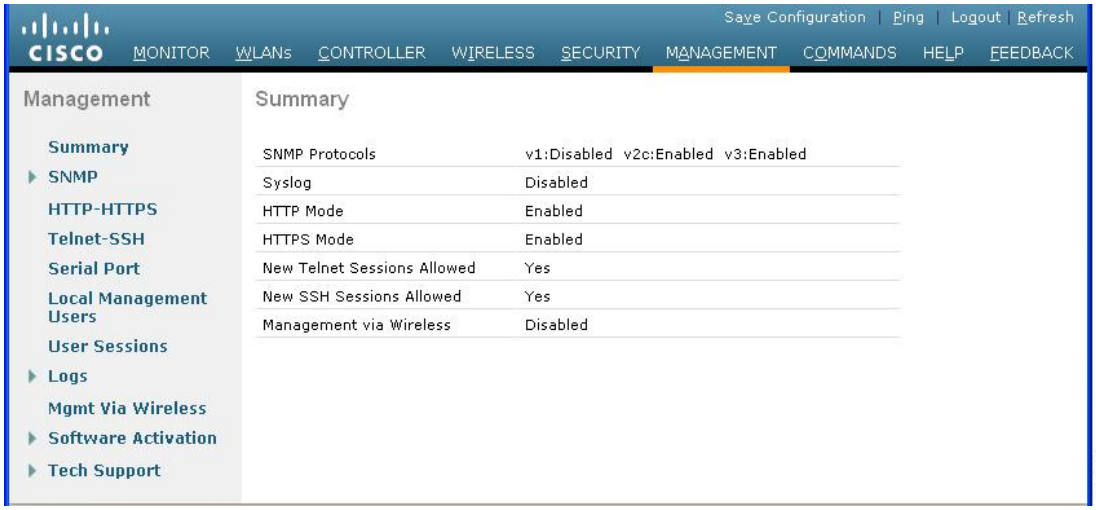
Step 5 From the \ drop-down list, choose **Yes** or **No** to allow or disallow new SSH sessions on the controller. The default value is Yes.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Step 8 To see a summary of the Telnet configuration settings, choose **Management** > **Summary**. The Summary page appears.

Figure 18: Summary Page



This page shows whether additional Telnet and SSH sessions are permitted.

Configuring Telnet and SSH Sessions (CLI)

Step 1 Allow or disallow new Telnet sessions on the controller by entering this command:
config network telnet {**enable** | **disable**}

The default value is disabled.

Step 2 Allow or disallow new SSH sessions on the controller by entering this command:
config network ssh {**enable** | **disable**}

The default value is enabled.

Step 3 Specify the number of minutes that a Telnet session is allowed to remain inactive before being terminated by entering this command:
config sessions timeout *timeout*

where *timeout* is a value between 0 and 160 minutes (inclusive). The default value is 5 minutes. A value of 0 indicates no timeout.

Step 4 Specify the number of simultaneous Telnet or SSH sessions allowed by entering this command:
config sessions maxsessions *session_num*

where *session_num* is a value between 0 and 5 (inclusive). The default value is 5 sessions. A value of zero indicates that Telnet/SSH sessions are disallowed.

Step 5 Save your changes by entering this command:
save config

Step 6 See the Telnet and SSH configuration settings by entering this command:
show network summary

Information similar to the following appears:

```
RF-Network Name............................. TestNetwork1
Web Mode.................................... Enable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
Secure Shell (ssh).......................... Enable
Telnet..................................... Disable
...
```

Step 7 See the Telnet session configuration settings by entering this command:
show sessions

Information similar to the following appears:

```
CLI Login Timeout (minutes)............. 5
Maximum Number of CLI Sessions....... 5
```

Step 8 See all active Telnet sessions by entering this command:
show loginsession

Information similar to the following appears:

```
ID    User Name     Connection From   Idle Time    Session Time
-- ---------------  ---------------  ------------  ------------
00    admin        EIA-232       00:00:00      00:19:04
```

Step 9 You can close all active Telnet sessions or a specific Telnet session by entering this command:
config loginsession close {**all** | **session_id**}

Troubleshooting Access Points Using Telnet or SSH_old

The controller supports the use of the Telnet and Secure Shell (SSH) protocols to troubleshoot lightweight access points. Using these protocols makes debugging easier, especially when the access point is unable to connect to the controller.

- To avoid potential conflicts and security threats to the network, the following commands are unavailable while a Telnet or SSH session is enabled: **config terminal, telnet, ssh, rsh, ping, traceroute, clear, clock, crypto, delete, fsck, lwapp, mkdir, radius, release, reload, rename, renew, rmdir, save, set, test, upgrade**.
- Commands available during a Telnet or SSH session include **debug, disable, enable, help, led, login, logout, more, no debug, show, systat, undebug** and **where**.

Note For instructions on configuring Telnet or SSH SSH sessions on the controller, see the Configuring Telnet and Secure Shell Sessions section.

Troubleshooting Access Points Using Telnet or SSH (GUI)

Step 1 Choose **Wireless > Access Points > All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to enable Telnet or SSH.

Step 3 Choose the **Advanced** tab to open the **All APs > Details for (Advanced)** page.

Step 4 Select the **Telnet** check box to enable Telnet connectivity on this access point. The default value is unchecked.

Step 5 Select the **SSH** check box to enable SSH connectivity on this access point. The default value is unchecked.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Troubleshooting Access Points Using Telnet or SSH (CLI)

Step 1 Enable Telnet or SSH connectivity on an access point by entering this command:
config ap {**telnet** | **ssh**} **enable** *Cisco_AP*

The default value is disabled.

Note Disable Telnet or SSH connectivity on an access point by entering this command: **config ap** {**telnet** | **ssh**} **disable** *Cisco_AP*

Step 2 Save your changes by entering this command:
save config

Step 3 See whether Telnet or SSH is enabled on an access point by entering this command:
show ap config general *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 5
Cisco AP Name.................................... AP33
Country code..................................... Multiple Countries:US,AE,AR,AT,AU,BH
Reg. Domain allowed by Country................... 802.11bg:-ABCENR 802.11a:-ABCEN
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 2
MAC Address...................................... 00:19:2f:11:16:7a
IP Address Configuration......................... Static IP assigned
IP Address....................................... 10.22.8.133
IP NetMask....................................... 255.255.248.0
Gateway IP Addr.................................. 10.22.8.1
Domain.......................................
Name Server.....................................
Telnet State..................................... Enabled
Ssh State........................................ Enabled
...
```

Managing the Controller Wirelessly

You can monitor and configure controllers using a wireless client. This feature is supported for all management tasks except uploads from and downloads to the controller.

Before you can open the GUI or the CLI from a wireless client device, you must configure the controller to allow the connection.

Enabling Wireless Connections (GUI)

Step 1 Log onto the GUI.

Step 2 Choose **Management** > **Mgmt Via Wireless** page.

Step 3 Enable the Controller Management to be accessible from wireless clients.

Step 4 Click **Apply**.

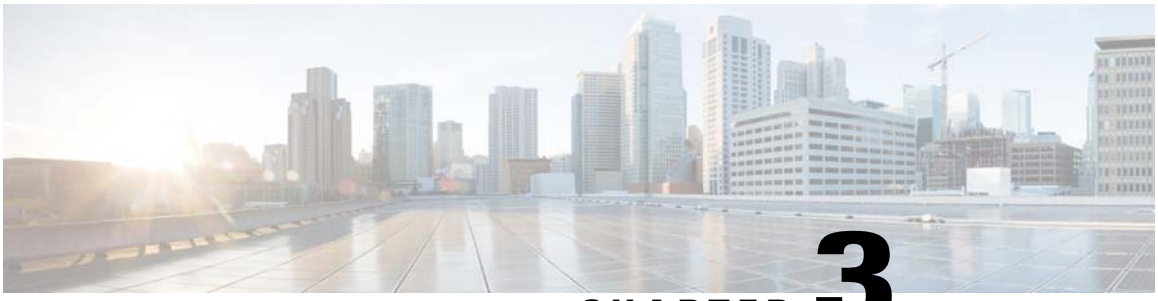
Enabling Wireless Connections (CLI)

Step 1 Log onto the CLI.

Step 2 Enter the **config network mgmt-via-wireless enable** command.

Step 3 Use a wireless client to associate to a lightweight access point connected to the controller.

Step 4 On the wireless client, open a Telnet session to the controller, or browse to the controller GUI.



CHAPTER 3

Managing Licenses

Installing and Configuring Licenses

Information About Installing and Configuring Licenses

You can order Cisco 5500 Series Controllers with support for 12, 25, 50, 100, 250 or 500 access points as the controller's base capacity. You can add additional access point capacity through capacity adder licenses available at 25, 50, 100 and 250 access point capacities. You can add the capacity adder licenses to any base license in any combination to arrive at the maximum capacity of 500 access points. The base and adder licenses are supported through both rehosting and RMAs.

The base license supports the standard base software set, and the premium software set is included as part of the base feature set, which includes this functionality:

- Datagram Transport Layer Security (DTLS) data encryption for added security across remote WAN and LAN links.
- The availability of data DTLS is as follows:
  - Cisco 5500 Series Controller—The Cisco 5500 Series Controller is available with two licensing options: One with data DTLS capabilities and another image without data DTLS.
  - 2500, WiSM2—These platforms by default do not contain DTLS. To turn on data DTLS, you must install a license. These platforms will have a single image with data DTLS turned off. To use data DTLS, you must have a license.
- Support for OfficeExtend access points, which are used for secure mobile teleworking.

All features included in a Wireless LAN Controller WPLUS license are now included in the base license. There are no changes to Cisco Prime Infrastructure BASE and PLUS licensing. These WPlus license features are included in the base license:

- OfficeExtend AP
- Enterprise Mesh
- CAPWAP Data Encryption

For information about upgrade and capacity adder licenses, see the product data sheet of your controller model.

Restrictions for Using Licenses

The following are the restrictions you must keep in mind when using licenses for the controllers:

- The licensing change can affect features on your wireless LAN when you upgrade or downgrade software releases, so you should be aware of these guidelines:
  - If you have a WPlus license and you upgrade from 6.0.x.x to 7.x.x.x, your license file contains both Basic and WPlus license features. There is no disruption in feature availability and operation.
  - If you have a WPlus license and you downgrade from 7.x.x.x to 6.0.196.0 or 6.0.188.0 or 6.0.182.0, your license file contains only base license, and you will lose all WPlus features.
  - If you have a base license and you downgrade from 6.0.196.0 to 6.0.188.0 or 6.0.182.0, when you downgrade, you lose all WPlus features.
- In the controller software 7.0.116.0 and later releases, the AP association trap is ciscoLwappApAssociated. In prior releases, the trap was bsnAPAssociated.
- The ap-count licenses and their corresponding image-based licenses are installed together. The controller keeps track of the licensed access point count and does not allow more than the number of access points to associate to it.
- The Cisco 5500 Series Controller is shipped with both permanent and evaluation base and base-ap-count licenses. If desired, you can activate the evaluation licenses, which are designed for temporary use and set to expire after 60 days.
- No licensing steps are required after you receive your Cisco 5500 Series Controller because the licenses you ordered are installed at the factory. In addition, licenses and product authorization keys (PAKs) are preregistered to serial numbers. However, as your wireless network evolves, you might want to add support for additional access points or upgrade from the standard software set to the base software set. To do so, you must obtain and install an upgrade license.

Obtaining an Upgrade or Capacity Adder License

This section describes how to get an upgrade or capacity adder license.

Information About Obtaining an Upgrade or Capacity Adder License

A certificate with a product authorization key (PAK) is required before you can obtain an upgrade license.

You can use the capacity adder licenses to increase the number of access points supported by the controller up to a maximum of 500 access points. The capacity adder licenses are available in access point capacities of 10, 25, 50, 100 and 250 access points. You can add these licenses to any of the base capacity licenses of 12, 25, 50, 100 and 250 access points.

For example, if your controller was initially ordered with support for 100 access points (base license AIR-CT5508-100-K9), you could increase the capacity to 500 access points by purchasing a 250 access point, 100 access point, and a 50 access point additive capacity license (LIC-CT5508-250A, LIC-CT5508-100A, and LIC-CT5508-50A).

You can find more information on ordering capacity adder licenses at this URL: http://www.cisco.com/en/US/products/ps10315/products_data_sheets_list.html

Note If you skip any tiers when upgrading (for example, if you do not install the -25U and -50U licenses along with the -100U), the license registration for the upgraded capacity fails.

For a single controller, you can order different upgrade licenses in one transaction (for example, -25U, -50U, -100U, and -250U), for which you receive one PAK with one license. Then you have only one license (instead of four) to install on your controller.

If you have multiple controllers and want to upgrade all of them, you can order multiple quantities of each upgrade license in one transaction (for example, you can order 10 each of the -25U, -50U, -100U, and -250 upgrade licenses), for which you receive one PAK with one license. You can continue to register the PAK for multiple controllers until it is exhausted.

For more information about the base license SKUs and capacity adder licenses, see the respective controller's data sheet.

Obtaining and Registering a PAK Certificate

Step 1 Order the PAK certificate for an upgrade license through your Cisco channel partner or your Cisco sales representative, or order it online at this URL:
http://www.cisco.com/go/ordering

Step 2 If you are ordering online, begin by choosing the primary upgrade SKU **L-LIC-CT5508-UPG or LIC CT5508-UPG**. Then, choose any number of the following options to upgrade one or more controllers under one PAK. After you receive the certificate, use one of the following methods to register the PAK:

- **Cisco License Manager (CLM)—**This method automates the process of obtaining licenses and deploying them on Cisco devices. For deployments with more than five controllers, we recommend using CLM to register PAKs and install licenses. You can also use CLM to rehost or RMA a license.

  Note You cannot use CLM to change the licensed feature set or activate an ap-count evaluation license. To perform these operations, you must follow the instructions in the Activating an AP-Count Evaluation License section. Because you can use CLM to perform all other license operations, you can disregard the remaining licensing information in this chapter except these two sections and the Configuring the License Agent section if you want your controller to use HTTP to communicate with CLM.

  Note You can download the CLM software and access user documentation at this URL: http://www.cisco.com/go/clm

- **Licensing portal—**This alternative method enables you to manually obtain and install licenses on your controller. If you want to use the licensing portal to register the PAK, follow the instructions in *Step 3*.

Step 3 Use the licensing portal to register the PAK as follows:

a) Go to http://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet

b) On the main Product License Registration page, enter the PAK mailed with the certificate in the Product Authorization Key (PAK) text box and click **Submit**.
c) On the Validate Features page, enter the number of licenses that you want to register in the Qty text box and click **Update**.
d) To determine the controller's product ID and serial number, choose **Controller** > **Inventory** on the controller GUI or enter the **show license udi** command on the controller CLI.
Information similar to the following appears on the controller CLI:

```
Device#         PID                SN                  UDI
-------  ------------------- ---------------  ------------------------
*0          AIR-CT5508-K9      CW1308L030     AIR-CT5508-K9:FCW1308L030
```

e) On the Designate Licensee page, enter the product ID and serial number of the controller on which you plan to install the license, read and accept the conditions of the end-user license agreement (EULA), complete the rest of the text boxes on this page, and click **Submit**.
f) On the Finish and Submit page, verify that all information is correct and click **Submit**.
g) When a message appears indicating that the registration is complete, click **Download License**. The license is e-mailed within 1 hour to the address that you specified.
h) When the e-mail arrives, follow the instructions provided.
i) Copy the license file to your TFTP server.

Installing a License

Installing a License (GUI)

Step 1 Choose **Management** > **Software Activation** > **Commands** to open the License Commands page.

Step 2 From the Action drop-down list, choose **Install License**. The Install License from a File section appears.

Step 3 In the File Name to Install text box, enter the path to the license (*.lic) on the TFTP server.

Step 4 Click **Install License**. A message appears to show whether the license was installed successfully. If the installation fails, the message provides the reason for the failure, such as the license is an existing license, the path was not found, the license does not belong to this device, you do not have correct permissions for the license, and so on.

Step 5 If the end-user license agreement (EULA) acceptance dialog box appears, read the agreement and click **Accept** to accept the terms of the agreement.

Note Typically, you are prompted to accept the EULA for evaluation, extension, and rehost licenses. The EULA is also required for permanent licenses, but it is accepted during license generation.

Step 6 Save a backup copy of all installed licenses as follows:

a) From the Action drop-down list, choose **Save License**.
b) In the File Name to Save text box, enter the path on the TFTP server where you want the licenses to be saved.

Note You cannot save evaluation licenses.

c) Click **Save Licenses**.

Step 7 Reboot the controller.

Installing a License (CLI)

Step 1 Install a license on the controller by entering this command:
license install *url*

where *url* is tftp://*server_ip*/*path*/*filename*.

Note To remove a license from the controller, enter the **license clear** *license_name* command. For example, you might want to delete an expired evaluation license or any unused license. You cannot delete unexpired evaluation licenses, the permanent base image license, or licenses that are in use by the controller.

Step 2 If you are prompted to accept the end-user license agreement (EULA), read and accept the terms of the agreement.

Note Typically, you are prompted to accept the EULA for evaluation, extension, and rehost licenses. The EULA is also required for permanent licenses, but it is accepted during license generation.

Step 3 Add comments to a license or delete comments from a license by entering this command:
license comment {**add** | **delete**} *license_name comment_string*

Step 4 Save a backup copy of all installed licenses by entering this command:
license save *url*

where *url* is tftp://*server_ip*/*path*/*filename*.

Step 5 Reboot the controller by entering this command:
reset system.

Viewing Licenses

Viewing Licenses (GUI)

Step 1 Choose **Management** > **Software Activation** > **Licenses** to open the Licenses page.
This page lists all of the licenses installed on the controller. For each license, it shows the license type, expiration, count (the maximum number of access points allowed for this license), priority (low, medium, or high), and status (in use, not in use, inactive, or EULA not accepted).

Note Controller platforms do not support the status of “grace period” or “extension” as a license type. The license status will always show “evaluation” even if a grace period or an extension evaluation license is installed.

Note If you ever want to remove a license from the controller, hover your cursor over the blue drop-down arrow for the license and click **Remove**. For example, you might want to delete an expired evaluation license or any unused license. You cannot delete unexpired evaluation licenses, the permanent base image license, or licenses that are in use by the controller.

Step 2 Click the link for the desired license to view more details for a particular license. The License Detail page appears. This page shows the following additional information for the license:

- The license type (permanent, evaluation, or extension)
- The license version
- The status of the license (in use, not in use, inactive, or EULA not accepted)
- The length of time before the license expires

  Note Permanent licenses never expire.

- Whether the license is a built-in license
- The maximum number of access points allowed for this license
- The number of access points currently using this license

Step 3 If you want to enter a comment for this license, type it in the Comment text box and click **Apply**.

Step 4 Click **Save Configuration** to save your changes.

Viewing Licenses (CLI)

Before You Begin

- See the license level, license type, and number of access points licensed on the controller by entering this command:

  show sysinfo

  Information similar to the following appears:

```
Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 7.0
RTOS Version..................................... 7.0
Bootloader Version............................... 5.2
Emergency Image Version.......................... N/A
Build Type....................................... DATA + WPS
System Name...................................... Cisco 69
System Location.................................. na
System Contact................................... abc@cisco.com
System ObjectID.................................. 1.3.6.1.4.1.14179.1.1.4.3
IP Address....................................... 10.10.10.10
System Up Time................................... 3 days 1 hrs 12 mins 42 secs
System Timezone Location.........................
CurrentBoot License Level.........................base
CurrentBoot License Type..........................Permanent
NextBoot License Level............................base
NextBoot License Type............................Permanent
Operating Environment............................ Commercial (0 to 40 C)
```

```
Internal Temp Alarm Limits..... 0 to 65 C
Internal Temperature..... +40 C
State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
Number of WLANs..... 4
Number of Active Clients..... 0
Burned-in MAC Address..... 00:1A:6D:DD:1E:40
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Absent
Power Supply 2..... Present, OK
Maximum number of APs supported..... 12
```

Note The Operating Environment and Internal Temp Alarm Limits data are not displayed for Cisco Flex 7500 Series Controllers.

- See a brief summary of all active licenses installed on the controller by entering this command:

  show license summary

  Information similar to the following appears:

```
Index 1 Feature: wplus
        Period left: 0 minute 0 second
Index 2 Feature: wplus-ap-count
  Period left: 0 minute 0 second
Index3   Feature: base
  Period left: Life time
  License Type: Permanent
  License State: Active, In Use
  License Count: Non-Counted
  License Priority: Medium
Index 4 Feature: base-ap-count
  Period left: 6 weeks, 4 days
  License Type: Evaluation
  License State: Active, In Use
  License Count: 250/250/0
  License Priority: High
```

- See all of the licenses installed on the controller by entering this command:

  show license all

  Information similar to the following appears:

```
License Store: Primary License Storage
StoreIndex:  1  Feature: base   Version: 1.0
        License Type: Permanent
        License State: Active, Not in Use
        License Count: Non-Counted
        License Priority: Medium

StoreIndex:  3  Feature: base-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Active, In Use
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  3 days
        License Count: 250/0/0
        License Priority: High
```

- See the details for a particular license by entering this command:

  show license detail *license_name*

Information similar to the following appears:

```
Index:  1       Feature: base-ap-count   Version: 1.0
        License Type: Permanent
        License State: Active, Not in Use
        License Count: 12/0/0
        License Priority: Medium
        Store Index: 0
        Store Name: Primary License Storage

Index:  2       Feature: base-ap-count   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  4 days
        License Count: 250/0/0
        License Priority: Low
        Store Index: 3
           Store Name: Evaluation License Storage
```

- See all expiring, evaluation, permanent, or in-use licenses by entering this command:

  show license {**expiring** | **evaluation** | **permanent** | **in-use**}

  Information similar to the following appears for the **show license in-use** command:

```
StoreIndex:  2  Feature: base-ap-count   Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: 12/12/0
        License Priority: Medium
StoreIndex:  3  Feature: base Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted License Priority: Medium
```

Note Controller platforms do not support the status of "grace period" or "extension" as a license type. The license status will always show "evaluation" even if a grace period or an extension evaluation license is installed.

- See the maximum number of access points allowed for this license on the controller, the number of access points currently joined to the controller, and the number of access points that can still join the controller by entering this command:

  show license capacity

  Information similar to the following appears:

```
Licensed Feature    Max Count      Current Count       Remaining Count
----------------    ---------      -------------       ---------------
AP Count              250              4                    246
```

- See statistics for all licenses on the controller by entering this command:

  show license statistics

- See a summary of license-enabled features by entering this command:

  show license feature

Troubleshooting Licensing Issues

- Configure debugging of license agent by entering this command:
  debug license agent {**errors** | **all**} {**enable** | **disable**}
- Configure debugging of licensing core events and core errors by entering this command:
  debug license core {**all** | **errors** | **events**} {**enable** | **disable**}
- Configure debugging of licensing errors by entering this command:
  debug license errors {**enable** | **disable**}
- Configure debugging of licensing events by entering this command:
  debug license events {**enable** | **disable**}

Activating an AP-Count Evaluation License

Information About Activating an AP-Count Evaluation License

If you are considering upgrading to a license with a higher access point count, you can try an evaluation license before upgrading to a permanent version of the license. For example, if you are using a permanent license with a 50-access-point count and want to try an evaluation license with a 100-access-point count, you can try out the evaluation license for 60 days.

AP-count evaluation licenses are set to low priority by default so that the controller uses the ap-count permanent license. If you want to try an evaluation license with an increased access point count, you must change its priority to high. If you no longer want to have this higher capacity, you can lower the priority of the ap-count evaluation license, which forces the controller to use the permanent license.

Note To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the controller uses a permanent license at another level or an unexpired evaluation license.

Activating an AP-Count Evaluation License (GUI)

Step 1 Choose **Management** > **Software Activation** > **Licenses** to open the Licenses page.
The Status column shows which licenses are currently in use, and the Priority column shows the current priority of each license.

Step 2 Activate an ap-count evaluation license as follows:

a) Click the link for the ap-count evaluation license that you want to activate. The License Detail page appears.

b) Choose **High** from the Priority drop-down list and click **Set Priority**.

Note You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.

c) Click **OK** when prompted to confirm your decision about changing the priority of the license.
d) When the EULA appears, read the terms of the agreement and then click **Accept**.
e) When prompted to reboot the controller, click **OK**.
f) Reboot the controller in order for the priority change to take effect.
g) Click **Licenses** to open the Licenses page and verify that the ap-count evaluation license now has a high priority and is in use. You can use the evaluation license until it expires.

Step 3 If you decide to stop using the ap-count evaluation license and want to revert to using an ap-count permanent license, follow these steps:

a) On the Licenses page, click the link for the ap-count evaluation license that is in use.
b) Choose **Low** from the Priority drop-down list and click **Set Priority**.
Note You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.
c) Click **OK** when prompted to confirm your decision about changing the priority of the license.
d) When the EULA appears, read the terms of the agreement and then click **Accept**.
e) When prompted to reboot the controller, click **OK**.
f) Reboot the controller in order for the priority change to take effect.
g) Click **Licenses** to open the Licenses page and verify that the ap-count evaluation license now has a low priority and is not in use. Instead, the ap-count permanent license should be in use.

Activating an AP-Count Evaluation License (CLI)

Step 1 See the current status of all the licenses on your controller by entering this command:
show license all

Information similar to the following appears:

```
License Store: Primary License Storage
StoreIndex:  0  Feature: base-ap-count   Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: 12/0/0
        License Priority: Medium
StoreIndex:  1  Feature: base   Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
StoreIndex:  2  Feature: base   Version: 1.0
        License Type: Evaluation
        License State: Inactive
            Evaluation total period:  8 weeks  4 days
            Evaluation period left:  8 weeks  4 days
        License Count: Non-Counted
        License Priority: Low
StoreIndex:  3  Feature: base-ap-count   Version: 1.0
```

```
      License Type: Evaluation
License State: Inactive
          Evaluation total period:  8 weeks  4 days
          Evaluation period left:  8 weeks  4 days
      License Count: 250/0/0
          License Priority: Low
```

The **License State** text box shows the licenses that are in use, and the **License Priority** text box shows the current priority of each license.

Note In the 7.2.110.0 release, the command output displays the full in-use count for active base-ap-count license even though there are no APs connected.

Step 2 Activate an ap-count evaluation license as follows:

a) Raise the priority of the base-ap-count evaluation license by entering this command:
license modify priority *license_name* **high**

Note You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.

b) Reboot the controller in order for the priority change to take effect by entering this command:
reset system

c) Verify that the ap-count evaluation license now has a high priority and is in use by entering this command:
show license all

You can use the evaluation license until it expires.

Step 3 If you decide to stop using the ap-count evaluation license and want to revert to using an ap-count permanent license, follow these steps:

a) Lower the priority of the ap-count evaluation license by entering this command:
license modify priority *license_name* **low**

b) Reboot the controller in order for the priority change to take effect by entering this command:
reset system

c) Verify that the ap-count evaluation license now has a low priority and is not in use by entering this command:
show license all

Instead, the ap-count permanent license should be in use.

Configuring Right to Use Licensing

Information About Right to Use Licensing

Right to Use (RTU) licensing is a model in which licenses are not tied to a unique device identifier (UDI), product ID, or serial number. Use RTU licensing to enable a desired AP license count on the controller after you accept the End User License Agreement (EULA). This allows you to add AP counts on a controller interacting with external tools.

RTU licensing is supported only on Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers.

In the RTU licensing model, the following types of licenses are available:

- Permanent or base licenses—These licenses are programmed into the controller hardware at the time of manufacturing. These licenses are base count licenses that cannot be deleted or transferred.
- Adder licenses—These licenses are wireless access point count licenses that you can activate by accepting the RTU EULA. The EULA states that you are obliged to purchase the specified access point count licenses at the time of activation. You must activate these licenses for the purchased access points count and accept the EULA.

  You can remove an adder license from one controller and transfer the license to another controller in the same product family. For example, an adder license such as LIC-CT7500-100A can be transferred (partially or fully) from one Cisco Flex 7500 Series Controller to another Cisco Flex 7500 Series Controller.

  Note Licenses embedded in the controller at the time of shipment is not transferrable.

- Evaluation licenses—These licenses are demo or trial mode licenses that are valid for 90 days. Fifteen days prior to the expiry of the 90-day period, you are notified about the requirement to buy the permanent license. These evaluation licenses are installed with the license image. You can activate the evaluation licenses anytime with a command. A EULA is prompted after you run the activation command on the controller CLI. The EULA states that you are obligated to pay for the specified license count within 90 days of usage. The countdown starts after you accept the EULA.

Whenever you add or delete an access point adder license on the controller, you are prompted with an RTU EULA. You can either accept or decline the RTU EULA for each add or delete operation.

For high-availability (HA) controllers when you enable HA, the controllers synchronize with the enabled license count of the primary controller and support high availability for up to the license count enabled on the primary controller.

You can view the RTU licenses through the controller GUI or CLI. You can also view these licenses across multiple wireless controllers through Cisco Prime Infrastructure.

Configuring Right to Use Licensing (GUI)

Step 1 Choose **Management** > **Software Activation** > **Licenses** to open the Licenses page.

Step 2 In the Adder License area, choose to add or delete the number of APs that an AP license can support, enter a value, and click **Set Count**.

Step 3 Click **Save Configuration**.

Configuring Right to Use Licensing (CLI)

- Add or delete the number of APs that an AP license can support by entering this command:

  license {**add** | **delete**} **ap-count** *count*

- Add or delete a license for a feature by entering this command:

  license {**add** | **delete**} **feature** *license_name*

- Activate or deactivate an evaluation AP count license by entering this command:

  license {**activate** | **deactivate**} **ap-count eval**

Note When you activate the license, you are prompted to accept or reject the End User License Agreement (EULA) for the given license. If you activate a license that supports fewer number of APs than the current number of APs connected to the controller, the activation command fails.

- Activate or deactivate a feature license by entering this command:

  license {**activate** | **deactivate**} **feature** *license_name*

- See the licensing information by entering this command:

  show license all

Rehosting Licenses

This section describes how to rehost licenses.

Information About Rehosting Licenses

Revoking a license from one controller and installing it on another is called *rehosting*. You might want to rehost a license in order to change the purpose of a controller. For example, if you want to move your OfficeExtend or indoor mesh access points to a different controller, you could transfer the adder license from one controller to another controller of the same model (intramodel transfer). This can be done in the case of RMA or a network rearchitecture that requires you to transfer licenses from one appliance to another. It is not possible to rehost base licenses in normal scenarios of network rearchitecture. The only exception where the transfer of base licenses is allowed is for RMA when you get a replacement hardware when your existing appliance has a failure.

Evaluation licenses cannot be rehosted.

In order to rehost a license, you must generate credential information from the controller and use it to obtain a permission ticket to revoke the license from the Cisco licensing site. Next, you must obtain a rehost ticket and use it to obtain a license installation file for the controller on which you want to install the license.

Note A revoked license cannot be reinstalled on the same controller.

Note Starting in the release 7.3, the Right-to-Use licensing is supported on the Cisco Flex 7500 Series Controllers, thereby the rehosting behavior changes on these controllers. If you require to rehost licenses, you need to plan rehosting the installed adder licenses prior to an upgrade.

Rehosting a License

Rehosting a License (GUI)

Step 1 Choose **Management** > **Software Activation** > **Commands** to open the License Commands page.

Step 2 From the Action drop-down list, choose **Rehost**. The Revoke a License from the Device and Generate Rehost Ticket area appears.

Step 3 In the File Name to Save Credentials text box, enter the path on the TFTP server where you want the device credentials to be saved and click **Save Credentials**.

Step 4 To obtain a permission ticket to revoke the license, follow these steps:

a) Click **Cisco Licensing** (https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet).

b) On the Product License Registration page, click **Look Up a License** under Manage Licenses.

c) Enter the product ID and serial number for your controller.

Note To find the controller's product ID and serial number, choose **Controller** > **Inventory** on the controller GUI.

d) Open the device credential information file that you saved in Step 3 and copy and paste the contents of the file into the Device Credentials text box.

e) Enter the security code in the blank box and click **Continue**.

f) Choose the licenses that you want to revoke from this controller and click **Start License Transfer**.

g) On the Rehost Quantities page, enter the number of licenses that you want to revoke in the To Rehost text box and click **Continue**.

h) On the Designate Licensee page, enter the product ID and serial number of the controller for which you plan to revoke the license, read and accept the conditions of the End User License Agreement (EULA), complete the rest of the text boxes on this page, and click **Continue**.

i) On the Review and Submit page, verify that all information is correct and click **Submit**.

j) When a message appears indicating that the registration is complete, click **Download Permission Ticket**. The rehost permission ticket is e-mailed within 1 hour to the address that you specified.

k) After the e-mail arrives, copy the rehost permission ticket to your TFTP server.

Step 5 Use the rehost permission ticket to revoke the license from this controller and generate a rehost ticket as follows:

a) In the Enter Saved Permission Ticket File Name text box, enter the TFTP path and filename (*.lic) for the rehost permission ticket that you generated in Step 4.

b) In the Rehost Ticket File Name text box, enter the TFTP path and filename (*.lic) for the ticket that will be used to rehost this license on another controller.

c) Click **Generate Rehost Ticket**.

d) When the End User License Agreement (EULA) acceptance dialog box appears, read the agreement and click **Accept** to accept the terms of the agreement.

Step 6 Use the rehost ticket generated in Step 5 to obtain a license installation file, which can then be installed on another controller as follows:

a) Click **Cisco Licensing**.

b) On the Product License Registration page, click **Upload Rehost Ticket** under Manage Licenses.

c) On the Upload Ticket page, enter the rehost ticket that you generated in Step 5 in the Enter Rehost Ticket text box and click **Continue**.

d) On the Validate Features page, verify that the license information for your controller is correct, enter the rehost quantity, and click **Continue**.
e) On the Designate Licensee page, enter the product ID and serial number of the controller on which you plan to use the license, read and accept the conditions of the End User License Agreement (EULA), complete the rest of the text boxes on this page, and click **Continue**.
f) On the Review and Submit page, verify that all information is correct and click **Submit**.
g) When a message appears indicating that the registration is complete, click **Download License**. The rehost license key is e-mailed within 1 hour to the address that you specified.
h) After the e-mail arrives, copy the rehost license key to your TFTP server.
i) Follow the instructions in the Installing a License section to install this on another controller.

Rehosting a License (CLI)

Step 1 Save device credential information to a file by entering this command:
license save credential *url*

where *url* is tftp://*server_ip*/*path*/*filename*.

Step 2 Obtain a permission ticket to revoke the license as follows:

a) Go to https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet. The Product License Registration page appears.
b) Under Manage Licenses, click **Look Up a License**.
c) Enter the product ID and serial number for your controller.
Note To find the controller's product ID and serial number, enter the **show license udi** command on the controller CLI.
d) Open the device credential information file that you saved in Step 1 and copy and paste the contents of the file into the Device Credentials text box.
e) Enter the security code in the blank box and click **Continue**.
f) Choose the licenses that you want to revoke from this controller and click **Start License Transfer**.
g) On the Rehost Quantities page, enter the number of licenses that you want to revoke in the To Rehost text box and click **Continue**.
h) On the Designate Licensee page, enter the product ID and serial number of the controller for which you plan to revoke the license, read and accept the conditions of the End-User License Agreement (EULA), complete the rest of the text boxes on this page, and click **Continue**.
i) On the Review and Submit page, verify that all information is correct and click **Submit**.
j) When a message appears indicating that the registration is complete, click **Download Permission Ticket**. The rehost permission ticket is e-mailed within 1 hour to the address that you specified.
k) After the e-mail arrives, copy the rehost permission ticket to your TFTP server.

Step 3 Use the rehost permission ticket to revoke the license from this controller and generate a rehost ticket as follows:

a) Revoke the license from the controller by entering this command:
license revoke *permission_ticket_url*

where *permission_ticket_url* is tftp://*server_ip*/*path*/*filename*.

b) Generate the rehost ticket by entering this command:
license revoke rehost *rehost_ticket_url*

where *rehost_ticket_url* is tftp://*server_ip*/*path*/*filename*.

c) If prompted, read and accept the terms of the End-User License Agreement (EULA).

Step 4 Use the rehost ticket generated in Step 3 to obtain a license installation file, which can then be installed on another controller as follows:

a) Go to https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet.
b) On the Product License Registration page, click **Upload Rehost Ticket** under Manage Licenses.
c) On the Upload Ticket page, enter the rehost ticket that you generated in Step 3 in the Enter Rehost Ticket text box and click **Continue**.
d) On the Validate Features page, verify that the license information for your controller is correct, enter the rehost quantity, and click **Continue**.
e) On the Designate Licensee page, enter the product ID and serial number of the controller on which you plan to use the license, read and accept the conditions of the End-User License Agreement (EULA), complete the rest of the text boxes on this page, and click **Continue**.
f) On the Review and Submit page, verify that all information is correct and click **Submit**.
g) When a message appears indicating that the registration is complete, click **Download License**. The rehost license key is e-mailed within 1 hour to the address that you specified.
h) After the e-mail arrives, copy the rehost license key to your TFTP server.
i) Follow the instructions in the Installing a License (GUI), on page 58 section to install this license on another controller.

Transferring Licenses to a Replacement Controller after an RMA

Information About Transferring Licenses to a Replacement Controller after an RMA

If you return a Cisco 5500 Series Controller to Cisco as part of the Return Material Authorization (RMA) process, you must transfer that controller's licenses within 60 days to a replacement controller that you receive from Cisco.

Replacement controllers come preinstalled with the following licenses: permanent base and evaluation base, base-ap-count. No other permanent licenses are installed. The SKU for replacement controllers is AIR-CT5508-CA-K9.

Because licenses are registered to the serial number of a controller, you can use the licensing portal on Cisco.com to request that the license from your returned controller be revoked and authorized for use on the replacement controller. After your request is approved, you can install the old license on the replacement controller. Any additional ap-count licenses if installed in the returned controller has to be rehosted on the replacement controller. Before you begin, you need the product ID and serial number of both the returned controller and the replacement controller. This information is included in your purchase records.

Note The evaluation licenses on the replacement controller are designed for temporary use and expire after 60 days. To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. If the evaluation licenses expire before you transfer the permanent licenses from your defective controller to your replacement controller, the replacement controller remains up and running using the permanent base license, but access points are no longer able to join the controller.

Transferring a License to a Replacement Controller after an RMA

Step 1 Browse to http://cisco.com/go/license.

Step 2 On the Product License Registration page, choose **Transfer** > **License for RMA**.

Step 3 Click **Specify Device** and then choose the controller model from the Product Family drop-down list.

Step 4 Complete the on-screen instructions to generate the license file.
The license is provided online or in an e-mail.

Step 5 Copy the license file to the TFTP server.

Step 6 Install the license by choosing **Management** > **Software Activation** > **Commands** > **Action** > **Install License**.

Configuring the License Agent

Information About Configuring the License Agent

If your network contains various Cisco-licensed devices, you might want to consider using the Cisco License Manager (CLM) to manage all of the licenses using a single application. CLM is a secure client/server application that manages Cisco software licenses network wide.

The license agent is an interface module that runs on the controller and mediates between CLM and the controller's licensing infrastructure. CLM can communicate with the controller using various channels, such as HTTP, Telnet, and so on. If you want to use HTTP as the communication method, you must enable the license agent on the controller.

The license agent receives requests from CLM and translates them into license commands. It also sends notifications to CLM. It uses XML messages over HTTP or HTTPS to receive the requests and send the notifications. For example, CLM sends a **license install** command, and the agent notifies CLM after the license expires.

Note You can download the CLM software and access user documentation at http://www.cisco.com/go/clm.

Configuring the License Agent (GUI)

Step 1 Choose **Management** > **Software Activation** > **License Agent** to open the License Agent Configuration page.

Step 2 Select the **Enable Default Authentication** check box to enable the license agent, or leave it unselected to disable this feature. The default value is unselected.

Step 3 In the Maximum Number of Sessions text box, enter the maximum number of sessions for the license agent. The valid range is 1 to 25 sessions (inclusive).

Step 4 Configure the license agent to listen for requests from the CLM as follows:

a) Select the **Enable Listener** check box to enable the license agent to receive license requests from the CLM, or unselect this check box to disable this feature. The default value is unselected.

b) In the Listener Message Processing URL text box, enter the URL where the license agent receives license requests (for example, http://209.165.201.30/licenseAgent/custom). The Protocol parameter indicates whether the URL requires HTTP or HTTPS.

Note You can specify the protocol to use on the HTTP Configuration page.

c) Select the **Enable Authentication for Listener** check box to enable authentication for the license agent when it is receiving license requests, or unselect this check box to disable this feature. The default value is unselected.

d) In the Max HTTP Message Size text box, enter the maximum size for license requests. The valid range is 0 to 9999 bytes, and the default value is 0.

Step 5 Configure the license agent to send license notifications to the CLM as follows:

a) Select the **Enable Notification** check box to enable the license agent to send license notifications to the CLM, or unselect this check box to disable this feature. The default value is unselected.

b) In the URL to Send the Notifications text box, enter the URL where the license agent sends the notifications (for example, http://www.cisco.com/license/notify).

c) In the User Name text box, enter the username required in order to view the notification messages at this URL.

d) In the Password and Confirm Password text boxes, enter the password required in order to view the notification messages at this URL.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your changes.

Configuring the License Agent (CLI)

Step 1 Enable the license agent by entering one of these commands:

- **config license agent default authenticate—**Enables the license agent default listener with authentication.
- **config license agent default authenticate none—**Enables the license agent default listener without authentication.

Note To disable the license agent default listener, enter the **config license agent default disable command**. The default value is disabled.

Step 2 Specify the maximum number of sessions for the license agent by entering this command:
config license agent max-sessions *sessions*

The valid range for the *sessions* parameter is 1 to 25 (inclusive), and the default value is 9.

Step 3 Enable the license agent to receive license requests from the CLM and to specify the URL where the license agent receives the requests by entering this command:
config license agent listener http {**plaintext** | **encrypt**} *url* **authenticate** [**none**] [**max-message** *size*] [**acl** *acl*]

The valid range for the *size* parameter is 0 to 65535 bytes, and the default value is 0.

Note To prevent the license agent from receiving license requests from the CLM, enter the **config license agent listener http disable command**. The default value is disabled.

Step 4 Configure the license agent to send license notifications to the CLM and to specify the URL where the license agent sends the notifications by entering this command:
config license agent notify *url username password*

Note To prevent the license agent from sending license notifications to the CLM, enter the **config license agent notify disable** *username password command.* The default value is disabled.

Step 5 Enter the **save config** command to save your changes.

Step 6 See statistics for the license agent's counters or sessions by entering this command:
show license agent {**counters** | **sessions**}

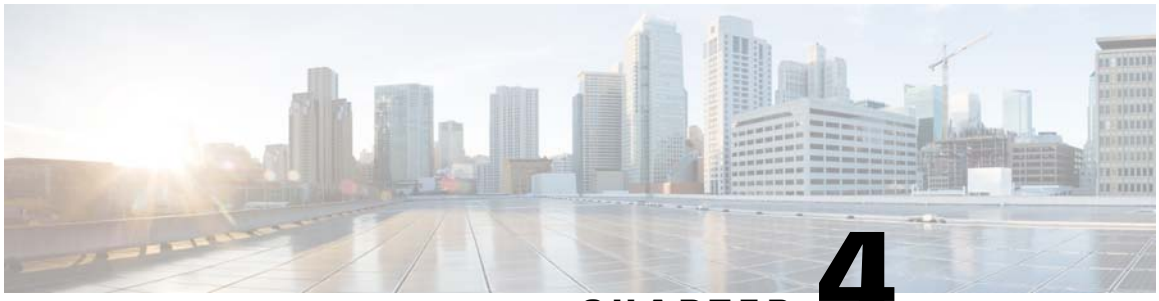
Information similar to the following appears for the **show license agent counters** command:

```
License Agent Counters
Request Messages Received:10: Messages with Errors:1
Request Operations Received:9: Operations with Errors:0
Notification Messages Sent:12: Transmission Errors:0: Soap Errors:0
```

Information similar to the following appears for the **show license agent sessions** command:

```
License Agent Sessions: 1 open, maximum is 9
```

Note To clear the license agent's counter or session statistics, enter the **clear license agent** {**counters** | **sessions**} command.



CHAPTER 4

Configuring 802.11 Bands

Configuring 802.11 Bands

Information About Configuring 802.11 Bands

You can configure the 802.11b/g/n (2.4-GHz) and 802.11a/n (5-GHz) bands for the controller to comply with the regulatory requirements in your country. By default, both 802.11b/g/n and 802.11a/n are enabled.

When a controller is configured to allow only 802.11g traffic, 802.11b client devices are able to successfully connect to an access point but cannot pass traffic. When you configure the controller for 802.11g traffic only, you must mark 11g rates as mandatory.

Configuring the 802.11 Bands (GUI)

Step 1 Choose **Wireless** > **802.11a/n** or **802.11b/g/n** > **Network** to open the Global Parameters page.

Step 2 Select the **802.11a** (or **802.11b/g**) **Network Status** check box to enable the 802.11a or 802.11b/g band. To disable the band, unselect the check box. The default value is enabled. You can enable both the 802.11a and 802.11b/g bands.

Step 3 If you enabled the 802.11b/g band in *Step 2*, select the **802.11g Support** check box if you want to enable 802.11g network support. The default value is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.

Step 4 Specify the period at which the SSID is broadcast by the access point by entering a value between 20 and 1000 milliseconds (inclusive) in the Beacon Period text box. The default value is 100 milliseconds.

Note The beacon period in controllers is listed in terms of milliseconds. The beacon period can also be measured in time units, where one time unit equals 1024 microseconds or 102.4 milliseconds. If a beacon interval is listed as 100 milliseconds in a controller, it is only a rounded off value for 102.4 milliseconds. Due to hardware limitation in certain radios, even though the beacon interval is, say 100 time units, it is adjusted to 102 time units, which roughly equals 104.448 milliseconds. When the beacon period is to be represented in terms of time units, the value is adjusted to the nearest multiple of 17.

Step 5 Specify the size at which packets are fragmented by entering a value between 256 and 2346 bytes (inclusive) in the Fragmentation Threshold text box. Enter a low number for areas where communication is poor or where there is a great deal of radio interference.

Step 6 Make access points advertise their channel and transmit power level in beacons and probe responses for CCX clients. Select the **DTPC Support** check box. Otherwise, unselect this check box. The default value is enabled.
Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.

Note On access points that run Cisco IOS software, this feature is called *world mode*.

Note DTPC and 801.11h power constraint cannot be enabled simultaneously.

Step 7 Specify the maximum allowed clients by entering a value between 1 to 200 in the Maximum Allowed Client text box. The default value is 200.

Step 8 Use the Data Rates options to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:

- 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps
- 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps

For each data rate, choose one of these options:

- **Mandatory**—Clients must support this data rate in order to associate to an access point on the controller.
- **Supported**—Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate.
- **Disabled**—The clients specify the data rates used for communication.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Configuring the 802.11 Bands (CLI)

Step 1 Disable the 802.11a band by entering this command:
config 802.11a disable network

Note The 802.11a band must be disabled before you can configure the 802.11a network parameters in this section.

Step 2 Disable the 802.11b/g band by entering this command:
config 802.11b disable network

Note The 802.11b band must be disabled before you can configure the 802.11b network parameters in this section.

Step 3 Specify the rate at which the SSID is broadcast by the access point by entering this command:
config {**802.11a** | **802.11b**} **beaconperiod** *time_unit*

where *time_unit* is the beacon interval in time units (TUs). One TU is 1024 microseconds. You can configure the access point to send a beacon every 20 to 1000 milliseconds.

Step 4 Specify the size at which packets are fragmented by entering this command:
config {**802.11a** | **802.11b**} **fragmentation** *threshold*

where *threshold* is a value between 256 and 2346 bytes (inclusive). Specify a low number for areas where communication is poor or where there is a great deal of radio interference.

Step 5 Make access points advertise their channel and transmit power level in beacons and probe responses by entering this command:
config {**802.11a** | **802.11b** } **dtpc** {**enable** | **disable**}

The default value is enabled. Client devices using dynamic transmit power control (DTPC) receive the channel and power level information from the access points and adjust their settings automatically. For example, a client device used primarily in Japan could rely on DTPC to adjust its channel and power settings automatically when it travels to Italy and joins a network there.

Note On access points that run Cisco IOS software, this feature is called *world mode*.

Step 6 Specify the maximum allowed clients that can be configured by entering this command:
config {**802.11a** | **802.11b**} **max-clients** *max_allow_clients*

The valid range is between 1 to 200.

Step 7 Specify the rates at which data can be transmitted between the controller and the client by entering this command:
config {**802.11a** | **802.11b**} **rate** {**disabled** | **mandatory** | **supported**} *rate*

where

- **disabled—**Clients specify the data rates used for communication.
- **mandatory—**Clients support this data rate in order to associate to an access point on the controller.
- **supported—**Any associated clients that support this data rate may communicate with the access point using that rate. However, the clients are not required to be able to use this rate in order to associate.
- *rate***—**The rate at which data is transmitted:
  - 6, 9, 12, 18, 24, 36, 48, and 54 Mbps (802.11a)
  - 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps (802.11b/g)

Step 8 Enable the 802.11a band by entering this command:
config 802.11a enable network

The default value is enabled.

Step 9 Enable the 802.11b band by entering this command:
config 802.11b enable network

The default value is enabled.

Step 10 Enable or disable 802.11g network support by entering this command:
config 802.11b 11gSupport {**enable** | **disable**}

The default value is enabled. You can use this command only if the 802.11b band is enabled. If you disable this feature, the 802.11b band is enabled without 802.11g support.

Step 11 Enter the **save config** command to save your changes.

Step 12 View the configuration settings for the 802.11a or 802.11b/g band by entering this command:
show {**802.11a** | **802.11b**}

Information similar to the following appears:

```
802.11a Network.............................. Enabled
11nSupport................................... Enabled
      802.11a Low Band....................... Enabled
      802.11a Mid Band....................... Enabled
      802.11a High Band...................... Enabled
802.11a Operational Rates
    802.11a 6M Rate........................... Mandatory
    802.11a 9M Rate........................... Supported
    802.11a 12M Rate.......................... Mandatory
    802.11a 18M Rate.......................... Supported
    802.11a 24M Rate.......................... Mandatory
    802.11a 36M Rate.......................... Supported
    802.11a 48M Rate.......................... Supported
    802.11a 54M Rate.......................... Supported
...
Beacon Interval.............................. 100
...
Default Channel.............................. 36
Default Tx Power Level....................... 1
DTPC Status.................................. Enabled
Fragmentation Threshold...................... 2346
Maximum Number of Clients per AP............. 200
```

Configuring Band Selection

Information About Configuring Band Selection

Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three nonoverlapping channels. To prevent these sources of interference and improve overall network performance, you can configure band selection on the controller.

Band selection is enabled globally by default.

Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels.

Restrictions on Band Selection

- Band-selection enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.
- Band selection can be used only with Cisco Aironet 1040, 1140, 1250, 1260, 3500, and the 3600 series access points.

Note OEAP 600 Series access points do not support band select.

- Band selection operates only on access points that are connected to a controller. A FlexConnect access point without a controller connection does not perform band selection after a reboot.
- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.
- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.
- It is not possible to enable or disable band selection and client load balancing globally through the controller GUI or CLI. You can, however, enable or disable band selection and client load balancing for a particular WLAN. Band selection and client load balancing are enabled globally by default.

Configuring Band Selection

Configuring Band Selection (GUI)

Step 1 Choose **Wireless** > **Advanced > Band Select** to open the **Band Select** page.

Step 2 In the **Probe Cycle Count** text box, enter a value between 1 and 10. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

Step 3 In the **Scan Cycle Period Threshold (milliseconds)** text box, enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.

Step 4 In the **Age Out Suppression (seconds)** text box, enter a value between 10 and 200 seconds. Age-out suppression sets the expiration time for pruning previously known 802.11b/g/n clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 5 In the **Age Out Dual Band (seconds)** text box, enter a value between 10 and 300 seconds. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 6 In the **Acceptable Client RSSI (dBm)** text box, enter a value between –20 and –90 dBm. This parameter sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

Step 7 Click **Apply**.

Step 8 Click **Save Configuration**.

Step 9 To enable or disable band selection on specific WLANs, choose **WLANs** > **WLAN ID**. The **WLANs > Edit** page appears.

Step 10 Click the **Advanced** tab.

Step 11 In the **Load Balancing and Band Select** text area, if you want to enable band selection, select the **Client Band Select** check box. If you want to disable band selection, leave the check box unselected. The default value is disabled.

Step 12 Click **Save Configuration**.

Configuring Band Selection (CLI)

Step 1 Set the probe cycle count for band select by entering this command:
config band-select cycle-count *cycle_count*

You can enter a value between 1 and 10 for the *cycle_count* parameter.

Step 2 Set the time threshold for a new scanning cycle period by entering this command:
config band-select cycle-threshold *milliseconds*

You can enter a value for threshold between 1 and 1000 for the *milliseconds* parameter.

Step 3 Set the suppression expire to the band select by entering this command:
config band-select expire suppression *seconds*

You can enter a value for suppression between 10 to 200 for the *seconds* parameter.

Step 4 Set the dual band expire by entering this command:
config band-select expire dual-band *seconds*

You can enter a value for dual band between 10 and 300 for the *seconds* parameter.

Step 5 Set the client RSSI threshold by entering this command:
config band-select client-rssi *client_rssi*

You can enter a value for minimum dBm of a client RSSI to respond to a probe between 20 and 90 for the *client_rssi* parameter.

Step 6 Enter the **save config** command to save your changes.

Step 7 Enable or disable band selection on specific WLANs by entering this command:
config wlan band-select allow {**enable** | **disable**} *wlan_ID*

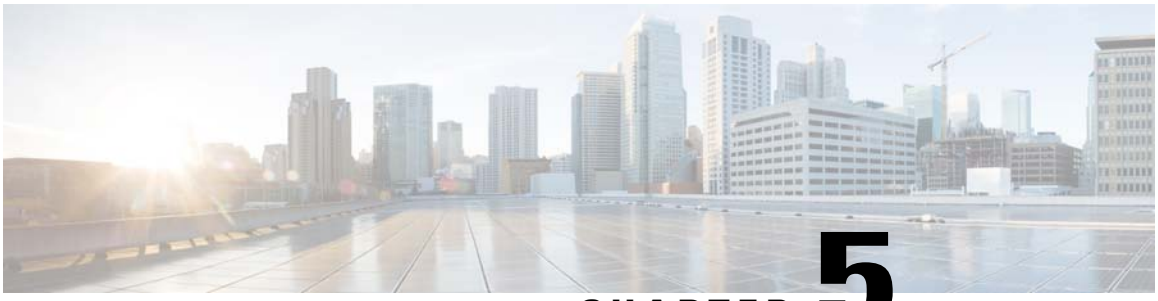
You can enter a value between 1 and 512 for *wlan_ID* parameter.

Step 8 Verify your settings by entering this command:
show band-select

Information similar to the following appears:

```
Band Select Probe Response..................... Enabled
   Cycle Count................................. 3 cycles
   Cycle Threshold............................. 300 milliseconds
   Age Out Suppression......................... 20 seconds
   Age Out Dual Band........................... 20 seconds
   Client RSSI................................. -30 dBm
```

Step 9 Enter the **save config** command to save your changes.



CHAPTER 5

Configuring 802.11 Parameters

Configuring the 802.11n Parameters

Information About Configuring the 802.11n Parameters

This section provides instructions for managing 802.11n devices such as the Cisco Aironet 1140 and 3600 Series Access Points on your network. The 802.11n devices support the 2.4- and 5-GHz bands and offer high-throughput data rates.

The 802.11n high-throughput rates are available on all 802.11n access points for WLANs using WMM with no Layer 2 encryption or with WPA2/AES encryption enabled.

Note Some Cisco 802.11n APs may intermittently emit incorrect beacon frames, which can trigger false wIPS alarms. We recommend that you ignore these alarms. The issue is observed in the following Cisco 802.11n APs: 1140, 1250, 2600, 3500, and 3600.

Configuring the 802.11n Parameters (GUI)

Step 1 Choose **Wireless** > **802.11a/n** or **802.11b/g/n** > **High Throughput** to open the (5 GHz or 2.4 GHz) High Throughput page.

Step 2 Select the **11n Mode** check box to enable 802.11n support on the network. The default value is enabled.

Step 3 Select the check boxes of the desired rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. These data rates, which are calculated for a 20-MHz channel width using a short guard interval, are available:

- 0 (7 Mbps)

- 1 (14 Mbps)
- 2 (21 Mbps)
- 3 (29 Mbps)
- 4 (43 Mbps)
- 5 (58 Mbps)
- 6 (65 Mbps)
- 7 (72 Mbps)
- 8 (14 Mbps)
- 9 (29 Mbps)
- 10 (43 Mbps)
- 11 (58 Mbps)
- 12 (87 Mbps)
- 13 (116 Mbps)
- 14 (130 Mbps)
- 15 (144 Mbps)

Any associated clients that support the selected rates may communicate with the access point using those rates. However, the clients are not required to be able to use this rate in order to associate. The MCS settings determine the number of spatial streams, the modulation, the coding rate, and the data rate values that are used.

Step 4 Click **Apply**.

Step 5 Use the 802.11n data rates that you configured by enabling WMM on the WLAN as follows:

a) Choose **WLANs** to open the WLANs page.
b) Click the ID number of the WLAN for which you want to configure WMM mode.
c) When the WLANs > Edit page appears, choose the **QoS** tab to open the WLANs > Edit (Qos) page.
d) From the WMM Policy drop-down list, choose **Required** or **Allowed** to require or allow client devices to use WMM. Devices that do not support WMM cannot join the WLAN.
If you choose **Allowed**, devices that cannot support WMM can join the WLAN but will not benefit from the 802.11n rates.
e) Click **Apply**.

Step 6 Click **Save Configuration**.

Note To determine if an access point supports 802.11n, look at the 11n Supported text box on either the 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page or the 802.11a/n (or 802.11b/g/n) AP Interfaces > Details page.

Configuring the 802.11n Parameters (CLI)

- Enable 802.11n support on the network by entering this command:
config {**802.11a** | **802.11b**} **11nsupport** {**enable** | **disable**}

- Specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client by entering this command:
  config {**802.11a** | **802.11b**} **11nsupport mcs tx** {**0-15**} {**enable** | **disable**}
- Use the 802.11n data rates that you configured by enabling WMM on the WLAN as follows:
  config wlan wmm {**allow** | **disable** | **require**} *wlan_id*

  The **require** parameter requires client devices to use WMM. Devices that do not support WMM cannot join the WLAN.

  If set to **allow**, devices that cannot support WMM can join the WLAN but do not benefit from 802.11n rates.
- Specify the aggregation method used for 802.11n packets as follows:
  a) Disable the network by entering this command:
  config {**802.11a** | **802.11b**} **disable network**
  b) Specify the aggregation method entering this command:
  config {**802.11a** | **802.11b**} **11nsupport** {**a-mpdu** | **a-msdu**} **tx priority** {**0-7** | **all**} {**enable** | **disable**}

  Aggregation is the process of grouping packet data frames together rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). A-MSDU is performed in hardware and therefore is the default method.

  You can specify the aggregation method for various types of traffic from the access point to the clients. This table defines the priority levels (0-7) assigned per traffic type.

Table 3: Traffic Type Priority Levels

User Priority	Traffic Type
0	Best effort
1	Background
2	Spare
3	Excellent effort
4	Controlled load
5	Video, less than 100-ms latency and jitter
6	Voice, less than 10-ms latency and jitter
7	Network control

You can configure each priority level independently, or you can use the **all** parameter to configure all of the priority levels at once. When you use the **enable** command, the traffic associated with that priority level uses A-MPDU transmission. When you use the **disable** command, the traffic associated with that priority level uses A-MSDU transmission. Configure the priority levels to match the

aggregation method used by the clients. By default, A-MPDU is enabled for priority level 0, 4 and 5 and the rest are disabled. By default, A-MSDU is enabled for all priorities except 6 and 7.

c) Reenable the network by entering this command:
config {**802.11a** | **802.11b**} **enable network**

- Configure the 802.11n-5 GHz A-MPDU transmit aggregation scheduler by entering this command:
config 802.11{**a** | **b**} **11nsupport a-mpdu tx scheduler** {**enable** | **disable** | **timeout rt** *timeout-value*}

  The timeout value is in milliseconds. The valid range is between 1 millisecond to 1000 milliseconds.
- Configure the guard interval for the network by entering this command:
config 802.11{**a** | **b**} **11nsupport guard_interval** {**any** | **long**}
- Configure the Reduced Interframe Space (RIFS) for the network by entering this command:
config 802.11{**a** | **b**} **11nsupport rifs rx** {**enable** | **disable**}
- Save your changes by entering this command:
save config
- View the configuration settings for the 802.11 networks by entering this command:
show {**802.11a** | **802.11b**}

Configuring 802.11h Parameters

Information About Configuring 802.11h Parameters

802.11h informs client devices about channel changes and can limit the transmit power of those client devices.

Configuring the 802.11h Parameters (GUI)

Step 1 Disable the 802.11 band as follows:
a) Choose **Wireless > 802.11a/n > Network** to open the 802.11a Global Parameters page.
b) Unselect the **802.11a Network Status** check box.
c) Click **Apply**.

Step 2 Choose **Wireless > 802.11a/n > DFS (802.11h)** to open the 802.11h Global Parameters page.

Step 3 In the Power Constraint area, enter the local power constraint. The valid range is between 0 dBm and 30 dBm.

Step 4 In the Channel Switch Announcement area, select the **Channel Announcement** check box if you want the access point to announce when it is switching to a new channel and the new channel number, or unselect this check box to disable the channel announcement. The default value is disabled.

Step 5 If you enabled the channel announcement, the **Channel Quiet Mode** check box appears. Select this check box if you want the access point to stop transmitting on the current channel, or unselect this check box to disable quiet mode. The default value is disabled.

Step 6 Click **Apply**.

Step 7 Reenable the 802.11a band as follows:
a) Choose **Wireless > 802.11a/n > Network** to open the 802.11a Global Parameters page.

b) Select the **802.11a Network Status** check box.
c) Click **Apply**.

Step 8 Click **Save Configuration**.

Configuring the 802.11h Parameters (CLI)

Step 1 Disable the 802.11a network by entering this command:
config 802.11a disable network

Step 2 Enable or disable an access point to announce when it is switching to a new channel, and the new channel number by entering this command:
config 802.11h channelswitch {**enable** | **disable**} *switch_mode*

Enter either 0 or 1 for the *switch_mode* parameter to specify whether transmissions are restricted until the actual channel switch (0), or are not restricted (1). By default, this feature is in disabled state.

Step 3 Configure a new channel using the 802.11h channel announcement by entering this command:
config 802.11h setchannel channel *channel*

Step 4 Configure the 802.11h power constraint value by entering this command:
config 802.11h powerconstraint *value*

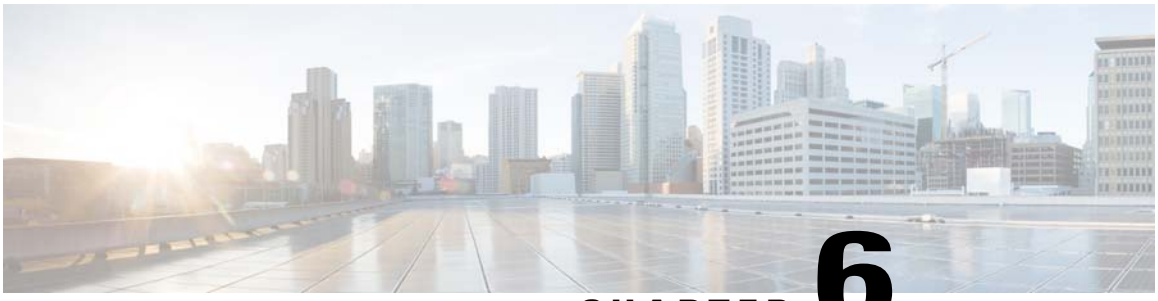
Use increments of 3 dB for the value so that the AP goes down one power level at a time.

Step 5 Reenable the 802.11a network by entering this command:
config 802.11a enable network

Step 6 View the status of the 802.11h parameters by entering this command:
show 802.11h

Information similar to the following appears:

```
Power Constraint.............................. 0
Channel Switch................................ Disabled
Channel Switch Mode........................... 0
```



CHAPTER 6

Configuring DHCP Proxy

Information About Configuring DHCP Proxy

When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. At least one DHCP server must be configured on either the interface associated with the WLAN or the WLAN itself.

When DHCP proxy is disabled on the controller, those DHCP packets transmitted to and from the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are removed from the CAPWAP tunnel and transmitted on the upstream VLAN. DHCP packets directed to the client are received on the upstream VLAN, converted to 802.11, and transmitted through a CAPWAP tunnel toward the client. As a result, the internal DHCP server cannot be used when DHCP proxy is disabled. The ability to disable DHCP proxy allows organizations to use DHCP servers that do not support Cisco's native proxy mode of operation. It should be disabled only when required by the existing infrastructure.

Note DHCP proxy is enabled by default.

Restrictions on Using DHCP Proxy

- DHCP proxy must be enabled in order for DHCP option 82 to operate correctly.
- All controllers that will communicate must have the same DHCP proxy setting.

Configuring DHCP Proxy (GUI)

Step 1 Choose **Controller** > **Advanced** > **DHCP** to open the DHCP Parameters page.

Step 2 Select the **Enable DHCP Proxy** check box to enable DHCP proxy on a global basis. Otherwise, unselect the check box. The default value is selected.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your changes.

Configuring DHCP Proxy (GUI)

Step 1 Choose **Controller > Interfaces**.

Step 2 Select the interface you want to configure the DHCP proxy.
You can configure the DHCP proxy on the management, virtual, ap manager, or dynamic interfaces in the controller. The **Interfaces > Edit** page is displayed with DHCP information on the primary and secondary DHCP servers configured in the controller. If the primary and secondary servers are not listed, you must enter values for the IP address of the DHCP servers in the text boxes displayed in this window.

Step 3 Select from the following option of the proxy mode drop-down to enable DHCP proxy on the selected management interface:Global—Uses the global DHCP proxy mode on the controller.Enabled—Enables the DHCP proxy mode on the interface. When you enable DHCP proxy on the controller; the controller unicasts the DHCP requests from the client to the configured servers. You must configure at least one DHCP server on either the interface associated with the WLAN or on the WLAN.Disabled—Disables the DHCP proxy mode on the interface. When you disable the DHCP proxy on the controller, the DHCP packets transmitted to and from the clients are bridged by the controller without any modification to the IP portion of the packet. Packets received from the client are removed from the CAPWAP tunnel and transmitted on the upstream VLAN. DHCP packets directed to the client are received on the upstream VLAN, converted to 802.11, and transmitted through a CAPWAP tunnel toward the client. As a result, the internal DHCP server cannot be used when DHCP proxy is disabled.

Step 4 Check the Enable DHCP option 82 checkbox to ensure additional security when DHCP is used to allocate network addresses, check the Enable DHCP option 82 checkbox.

Step 5 Click **Apply** to save the configuration.

Configuring DHCP Proxy (CLI)

Step 1 Enable or disable DHCP proxy by entering this command:
config dhcp proxy {**enable** | **disable**}

Step 2 View the DHCP proxy configuration by entering this command:

show dhcp proxy

Information similar to the following appears:

```
DHCP Proxy Behavior: enabled
```

Configuring DHCP Proxy (CLI)

Step 1 Configure the DHCP primary and secondary servers on the interface. To do this, enter the following commands:

- **config interface dhcp management primary** *primary-server*
- **config interface dhcp dynamic-interface** *interface-name* **primary primary-s**

Step 2 Configure DHCP proxy on the management or dynamic interface of the controller. To do this, enter the following command:

- **config interface dhcp management proxy-mode** enableglobaldisable
- **config interface dhcp dynamic-interface** *interface-name* **proxy-mode** enableglobaldisable.

Note To ensure additional security when DHCP is configured, use the **config interface dhcp***interface type***option-82 enable** command.

Step 3 Enter the **save config** command.

Step 4 To view the proxy settings of the controller interface enter the **show dhcp proxy** command.

Configuring a DHCP Timeout (GUI)

Step 1 Choose **Controller** > **Advanced** > **DHCP** to open the DHCP Parameters page.

Step 2 Select the **DHCP Timeout (5 - 120 seconds)** check box to enable a DHCP timeout on a global basis. Otherwise, unselect the check box. The valid range is 5 through 120 seconds.

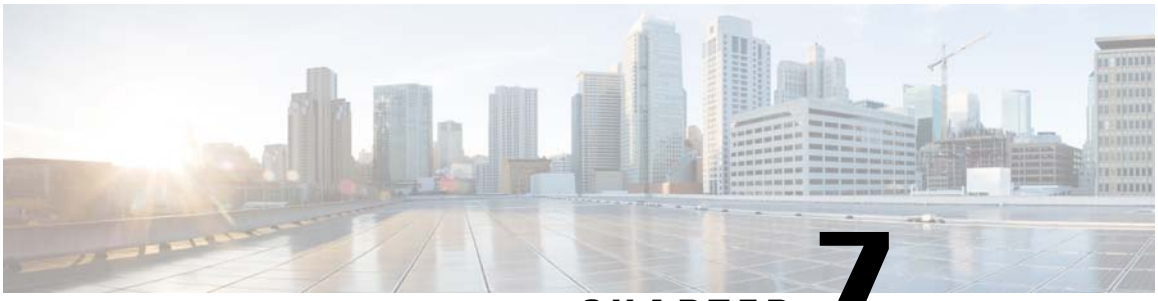
Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your changes.

Configuring a DHCP Timeout (CLI)

Configure a DHCP timeout by entering this command:

config dhcp timeout *seconds*



CHAPTER 7

Configuring SNMP

Configuring SNMP (CLI)

Note To view the controller trap log, choose **Monitor** and click **View All** under "Most Recent Traps" on the controller GUI.

- Create an SNMP community name by entering this command:
  config snmp community create *name*
- Delete an SNMP community name by entering this command:
  config snmp community delete *name*
- Configure an SNMP community name with read-only privileges by entering this command:
  config snmp community accessmode ro *name*
- Configure an SNMP community name with read-write privileges by entering this command:
  config snmp community accessmode rw *name*
- Configure an IP address and subnet mask for an SNMP community by entering this command:
  config snmp community ipaddr *ip-address ip-mask name*

Note This command behaves like an SNMP access list. It specifies the IP address from which the device accepts SNMP packets with the associated community. An AND operation is performed between the requesting entity's IP address and the subnet mask before being compared to the IP address. If the subnet mask is set to 0.0.0.0, an IP address of 0.0.0.0 matches to all IP addresses. The default value is 0.0.0.0.

Note The controller can use only one IP address range to manage an SNMP community.

- Enable or disable a community name by entering this command:
  config snmp community mode {**enable** | **disable**}
- Configure a destination for a trap by entering this command:
  config snmp trapreceiver create *name ip-address*
- Delete a trap by entering this command:
  config snmp trapreceiver delete *name*
- Change the destination for a trap by entering this command:
  config snmp trapreceiver ipaddr *old-ip-address name new-ip-address*
- Enable or disable the traps by entering this command:
  config snmp trapreceiver mode {**enable** | **disable**}
- Configure the name of the SNMP contact by entering this command:
  config snmp syscontact *syscontact-name*

  Enter up to 31 alphanumeric characters for the contact name.
- Configure the SNMP system location by entering this command:
  config snmp syslocation *syslocation-name*

  Enter up to 31 alphanumeric characters for the location.
- Verify that the SNMP traps and communities are correctly configured by entering these commands:
  show snmpcommunity

  show snmptrap
- See the enabled and disabled trap flags by entering this command:
  show trapflags

  If necessary, use the **config trapflags** command to enable or disable trap flags.
- Configure when the warning message should be displayed after the number of clients or RFID tags associated with the controller hover around the threshold level by entering this command:
  config trapflags {**client** | **rfid**} max-warning-threshold {*threshold-between-80-to-100* | **enable** | **disable**}

  The warning message is displayed at an interval of 600 seconds (10 minutes).
- Configure the SNMP engine ID by entering this command:
  config snmp engineID *engine-id-string*

Note The engine ID string can be a maximum of 24 characters.

- View the engine ID by entering this command:
  show snmpengineID
- Configure the SNMP version by entering this command:
  config snmp version {**v1** | **v2c** | **v3**} {**enable** | **disable**}

SNMP Community Strings

The controller has commonly known default values of "public" and "private" for the read-only and read-write SNMP community strings. Using these standard values presents a security risk. If you use the default community names, and since these are known, the community names could be used to communicate to the controller using SNMP. Therefore, we strongly advise that you change these values.

Changing the SNMP Community String Default Values (GUI)

Step 1 Choose **Management** and then **Communities** under SNMP. The SNMP v1 / v2c Community page appears.

Step 2 If “public” or “private” appears in the Community Name column, hover your cursor over the blue drop-down arrow for the desired community and choose **Remove** to delete this community.

Step 3 Click **New** to create a new community. The SNMP v1 / v2c Community > New page appears.

Step 4 In the Community Name text box, enter a unique name containing up to 16 alphanumeric characters. Do not enter “public” or “private.”

Step 5 In the next two text boxes, enter the IP address from which this device accepts SNMP packets with the associated community and the IP mask.

Step 6 Choose **Read Only** or **Read/Write** from the Access Mode drop-down list to specify the access level for this community.

Step 7 Choose **Enable** or **Disable** from the Status drop-down list to specify the status of this community.

Step 8 Click **Apply** to commit your changes.

Step 9 Click **Save Configuration** to save your settings.

Step 10 Repeat this procedure if a “public” or “private” community still appears on the SNMP v1 / v2c Community page.

Changing the SNMP Community String Default Values (CLI)

Step 1 See the current list of SNMP communities for this controller by entering this command:
show snmp community

Step 2 If "public" or "private" appears in the SNMP Community Name column, enter this command to delete this community:
config snmp community delete *name*

The *name* parameter is the community name (in this case, “public” or “private”).

Step 3 Create a new community by entering this command:
config snmp community create *name*

Enter up to 16 alphanumeric characters for the *name* parameter. Do not enter “public” or “private.”

Step 4 Enter the IP address from which this device accepts SNMP packets with the associated community by entering this command:
config snmp community ipaddr *ip_address ip_mask name*

Step 5 Specify the access level for this community by entering this command, where **ro** is read-only mode and **rw** is read/write mode:
config snmp community accessmode {**ro** | **rw**} *name*

Step 6 Enable or disable this SNMP community by entering this command:
config snmp community mode {**enable** | **disable**} *name*

Step 7 Save your changes by entering this command:
save config

Step 8 Repeat this procedure if you still need to change the default values for a "public" or "private" community string.

Configuring Real Time Statistics (CLI)

SNMP traps are defined for CPU and memory utilization of AP and controller. The SNMP trap is sent out when the threshold is crossed. The sampling period and statistics update interval can be configured using SNMP and CLI.

- Configure the sampling interval by entering this command:

  config service statistics sampling-interval *seconds*

- Configure the statistics interval by entering this command:

  config service statistics statistics-interval *seconds*

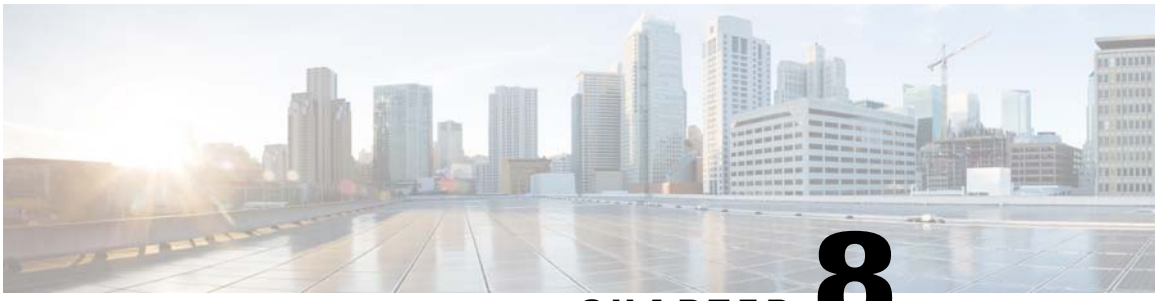
- See sampling and service interval statistics by entering this command:

  show service statistics interval

SNMP Trap Enhancements

This feature provides soaking of SNMP traps and resending of traps after a threshold that you can configure called the hold time. The hold time helps in suppressing false traps being generated. The traps that are supported are for CPU and memory utilization of AP and controller. The retransmission of the trap occurs until the trap is cleared.

- Configure the hold time after which the SNMP traps are to be resent by entering this command:
  config service alarm hold-time *seconds*
- Configure the retransmission interval of the trap by entering this command:
  config service alarm trap retransmit-interval *seconds*
- Configure debugging of the traps by entering this command:
  debug service alarm {**enable** | **disable**}



CHAPTER 8

Configuring Aggressive Load Balancing

Information About Configuring Aggressive Load Balancing

Enabling aggressive load balancing on the controller allows lightweight access points to load balance wireless clients across access points. You can enable aggressive load balancing using the controller.

Note Clients are load balanced between access points on the same controller. Load balancing does not occur between access points on different controllers.

When a wireless client attempts to associate to a lightweight access point, association response packets are sent to the client with an 802.11 response packet including status code 17. The code 17 indicates that the AP is busy. The AP responds with an association response bearing 'success' if the AP threshold is not met, and with code 17 (AP busy) if the AP utilization threshold is reached or exceeded and another less busy AP heard the client request.

For example, if the number of clients on AP1 is more than the number of clients on AP2 plus the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, it receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the controller to deny client associations up to 10 times (if a client attempted to associate 11 times, it would be allowed to associate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).

Passive scanning clients will be able to associate to an AP irrespective of whether load balancing is enabled or not.

Note Cisco 600 Series OfficeExtend Access Points do not support client load balancing.

With the 7.4 release, FlexConnect access points do support client load balancing.

You can configure the controller to analyze the WAN interface utilization of neighboring APs and then load balance the clients across the lightly loaded APs. You can configure this by defining a load balancing threshold. By defining the threshold, you can measure the WAN interface utilization percentage. For example, a threshold value of 50 triggers the load balancing upon detecting utilization of 50% or more on an AP-WAN interface.

Configuring Aggressive Load Balancing (GUI)

Step 1 Choose **Wireless** > **Advanced** > **Load Balancing** to open the Load Balancing page.

Step 2 In the Client Window Size text box, enter a value between 1 and 20.
The window size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

load-balancing window + client associations on AP with the lightest load = load-balancing threshold

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client window size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

Step 3 In the Maximum Denial Count text box, enter a value between 0 and 10.
The denial count sets the maximum number of association denials during load balancing.

Step 4 Click **Apply**.

Step 5 Click **Save Configuration**.

Step 6 To enable or disable aggressive load balancing on specific WLANs, do the following:

a) Choose **WLANs** > **WLAN ID**. The WLANs > Edit page appears.
b) In the **Advanced** tab, select or unselect the **Client Load Balancing** check box.
c) Click **Apply**.
d) Click **Save Configuration**.

Configuring Aggressive Load Balancing (CLI)

Step 1 Set the client window for aggressive load balancing by entering this command:
config load-balancing window *client_count*

You can enter a value between 0 and 20 for the *client_count* parameter.

Step 2 Set the denial count for load balancing by entering this command:

config load-balancing denial *denial_count*

You can enter a value between 1 and 10 for the *denial_count* parameter.

Step 3 Save your changes by entering this command:
save config

Step 4 Enable or disable aggressive load balancing on specific WLANs by entering this command:
config wlan load-balance allow {**enable** | **disable**} *wlan_ID*

You can enter a value between 1 and 512 for *wlan_ID* parameter.

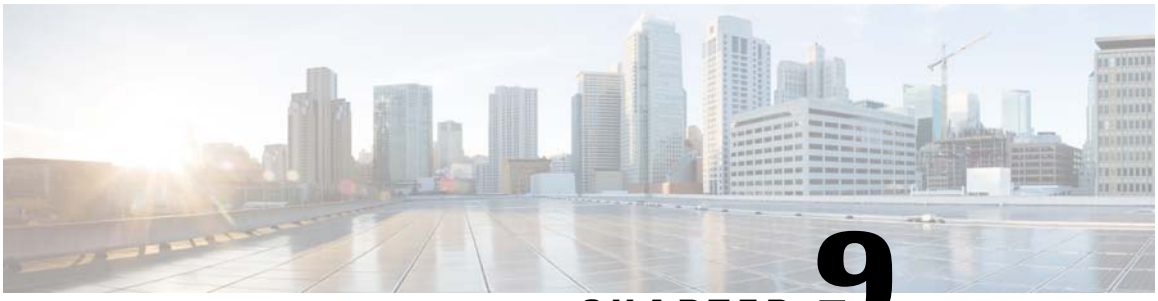
Step 5 Verify your settings by entering this command:
show load-balancing

Step 6 Save your changes by entering this command:
save config

Step 7 Configure the load balance mode on a WLAN by entering this command:
config wlan load-balance mode {*client-count* | *uplink-usage*} *wlan-id*

This feature requires the AP to upload its uplink usage statistics to the controller periodically. Check these statistics by entering this command:

show ap stats system *cisco-AP*



CHAPTER 9

Configuring Fast SSID Changing

Information About Configuring Fast SSID Changing

When fast SSID changing is enabled, the controller allows clients to move faster between SSIDs. When fast SSID is enabled, the client entry is not cleared and the delay is not enforced.

When fast SSID changing is disabled, the controller enforces a delay before clients are allowed to move to a new SSID. When fast SSID is disabled and the client sends a new association for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID.

Configuring Fast SSID Changing (GUI)

Step 1 Choose **Controller** to open the General page.

Step 2 From the Fast SSID Change drop-down list, choose **Enabled** to enable this feature or **Disabled** to disable it. The default value is disabled.

Step 3 Click **Apply** to commit your changes.

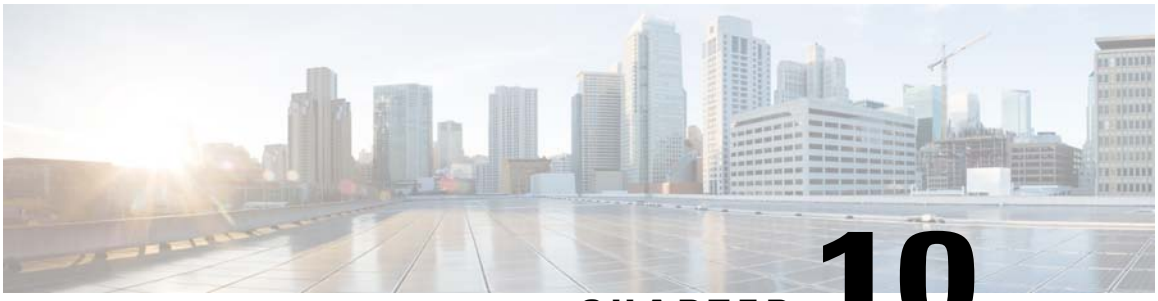
Step 4 Click **Save Configuration** to save your changes.

Configuring Fast SSID Changing (CLI)

Step 1 Enable or disable fast SSID changing by entering this command:

config network fast-ssid-change {**enable** | **disable**}

Step 2 Save your changes by entering this command:
save config



CHAPTER 10

Configuring 802.3 Bridging

Configuring 802.3 Bridging

Information About Configuring 802.3 Bridging

The controller supports 802.3 frames and the applications that use them, such as those typically used for cash registers and cash register servers. However, to make these applications work with the controller, the 802.3 frames must be bridged on the controller.

You can also configure 802.3 bridging using the Cisco Prime Network Control System. See the *Cisco Prime Network Control System Configuration Guide* for instructions.

Restrictions on 802.3 Bridging

- Support for raw 802.3 frames allows the controller to bridge non-IP frames for applications not running over IP.

  The raw 802.3 frame contains destination MAC address, source MAC address, total packet length, and payload.

- By default, Cisco 5500 Series Controllers bridge all non-IPv4 packets (such as AppleTalk, IPv6, and so on). You can also use ACLs to block the bridging of these protocols.

Configuring 802.3 Bridging

Configuring 802.3 Bridging (GUI)

Step 1 Choose **Controller** > **General** to open the General page.

Step 2 From the 802.3 Bridging drop-down list, choose **Enabled** to enable 802.3 bridging on your controller or **Disabled** to disable this feature. The default value is Disabled.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your changes.

Configuring 802.3 Bridging (CLI)

Step 1 See the current status of 802.3 bridging for all WLANs by entering this command:
show network

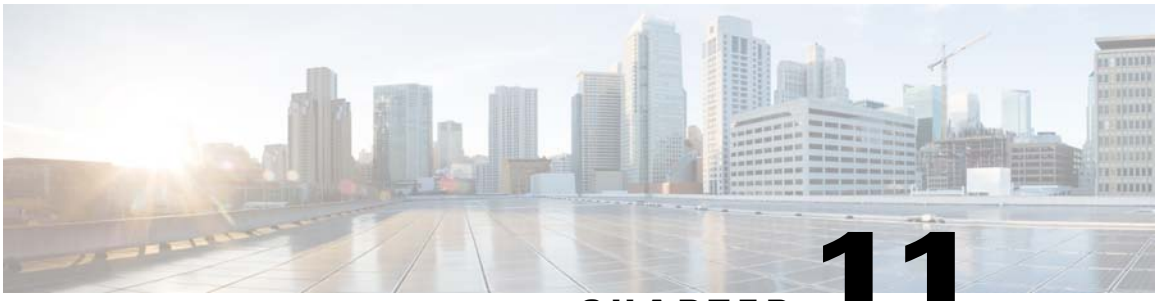
Step 2 Enable or disable 802.3 bridging globally on all WLANs by entering this command:
config network 802.3-bridging {**enable** | **disable**}

The default value is disabled.

Step 3 Save your changes by entering this command:
save config

Enabling 802.3X Flow Control

802.3X Flow Control is disabled by default. To enable it, enter the **config switchconfig flowcontrol enable** command.



CHAPTER 11

Configuring Multicast

Configuring Multicast Mode

Information About Multicast Mode

If your network supports packet multicasting, you can configure the multicast method that the controller uses. The controller performs multicasting in two modes:

- Unicast mode—In this mode, the controller unicasts every multicast packet to every access point associated to the controller. This mode is inefficient but might be required on networks that do not support multicasting.
- Multicast mode—In this mode, the controller sends multicast packets to a CAPWAP multicast group. This method reduces overhead on the controller processor and shifts the work of packet replication to your network, which is much more efficient than the unicast method.

When you enable multicast mode and the controller receives a multicast packet from the wired LAN, the controller encapsulates the packet using CAPWAP and forwards the packet to the CAPWAP multicast group address. The controller always uses the management interface for sending multicast packets. Access points in the multicast group receive the packet and forward it to all the BSSIDs mapped to the interface on which clients receive multicast traffic. From the access point perspective, the multicast appears to be a broadcast to all SSIDs.

The controller supports Multicast Listener Discovery (MLD) v1 snooping for IPv6 multicast. This feature keeps track of and delivers IPv6 multicast flows to the clients that request them. To support IPv6 multicast, you must enable Global Multicast Mode.

Note When you disable the Global Multicast Mode, the controller still forwards the IPv6 ICMP multicast messages, such as router announcements and DHCPv6 solicits, as these are required for IPv6 to work. As a result, enabling the Global Multicast Mode on the controller does not impact the ICMPv6 and the DHCPv6 messages. These messages will always be forwarded irrespective of whether or not the Global Multicast Mode is enabled.

In controller software 4.2 or later releases, Internet Group Management Protocol (IGMP) snooping is introduced to better direct multicast packets. When this feature is enabled, the controller gathers IGMP reports from the clients, processes them, creates unique multicast group IDs (MGIDs) from the IGMP reports after selecting the Layer 3 multicast address and the VLAN number, and sends the IGMP reports to the infrastructure switch. The controller sends these reports with the source address as the interface address on which it received the reports from the clients. The controller then updates the access point MGID table on the access point with the client MAC address. When the controller receives multicast traffic for a particular multicast group, it forwards it to all the access points, but only those access points that have active clients listening or subscribed to that multicast group send multicast traffic on that particular WLAN. IP packets are forwarded with an MGID that is unique for an ingress VLAN and the destination multicast group. Layer 2 multicast packets are forwarded with an MGID that is unique for the ingress interface.

When IGMP snooping is disabled, the following is true:

- The controller always uses Layer 2 MGID when it sends multicast data to the access point. Every interface created is assigned one Layer 2 MGID. For example, the management interface has an MGID of 0, and the first dynamic interface created is assigned an MGID of 8, which increments as each dynamic interface is created.
- The IGMP packets from clients are forwarded to the router. As a result, the router IGMP table is updated with the IP address of the clients as the last reporter.

When IGMP snooping is enabled, the following is true:

- The controller always uses Layer 3 MGID for all Layer 3 multicast traffic sent to the access point. For all Layer 2 multicast traffic, it continues to use Layer 2 MGID.
- IGMP report packets from wireless clients are consumed or absorbed by the controller, which generates a query for the clients. After the router sends the IGMP query, the controller sends the IGMP reports with its interface IP address as the listener IP address for the multicast group. As a result, the router IGMP table is updated with the controller IP address as the multicast listener.
- When the client that is listening to the multicast groups roams from one controller to another, the first controller transmits all the multicast group information for the listening client to the second controller. As a result, the second controller can immediately create the multicast group information for the client. The second controller sends the IGMP reports to the network for all multicast groups to which the client was listening. This process aids in the seamless transfer of multicast data to the client.
- If the listening client roams to a controller in a different subnet, the multicast packets are tunneled to the anchor controller of the client to avoid the reverse path filtering (RPF) check. The anchor then forwards the multicast packets to the infrastructure switch.

Note The MGIDs are controller specific. The same multicast group packets coming from the same VLAN in two different controllers may be mapped to two different MGIDs.

Note If Layer 2 multicast is enabled, a single MGID is assigned to all the multicast addresses coming from an interface.

Restrictions for Configuring Multicast Mode

- The Cisco Unified Wireless Network solution uses some IP address ranges for specific purposes, and you should keep these ranges in mind when configuring a multicast group:
  - 224.0.0.0 through 224.0.0.255—Reserved link local addresses
  - 224.0.1.0 through 238.255.255.255—Globally scoped addresses
  - 239.0.0.0 through 239.255.x.y /16—Limited scope addresses
- When you enable multicast mode on the controller, you also must configure a CAPWAP multicast group address. Access points subscribe to the CAPWAP multicast group using IGMP.
- Cisco 1100, 1130, 1200, 1230, and 1240 access points use IGMP versions 1, 2, and 3.
- Access points in monitor mode, sniffer mode, or rogue detector mode do not join the CAPWAP multicast group address.
- The CAPWAP multicast group configured on the controllers should be different for different controllers.
- Access points running recent Cisco IOS versions transmit multicast frames at the highest configured basic rate and management frames at the lowest basic mandatory rates, can cause reliability problems. Access points running LWAPP or autonomous Cisco IOS should transmit multicast and management frames at the lowest configured basic rate. Such behavior is necessary to provide good coverage at the cell's edge, especially for unacknowledged multicast transmissions where multicast wireless transmissions might fail to be received.

  Because multicast frames are not retransmitted at the MAC layer, clients at the edge of the cell might fail to receive them successfully. If reliable reception is a goal, multicast frames should be transmitted at a low data rate. If support for high data rate multicast frames is required, it might be useful to shrink the cell size and disable all lower data rates.

  Depending on your requirements, you can take the following actions:
  - If you need to transmit multicast data with the greatest reliability and if there is no need for great multicast bandwidth, then configure a single basic rate, that is low enough to reach the edges of the wireless cells.
  - If you need to transmit multicast data at a certain data rate in order to achieve a certain throughput, you can configure that rate as the highest basic rate. You can also set a lower basic rate for coverage of nonmulticast clients.
- Multicast mode does not operate across intersubnet mobility events such as guest tunneling. It does, however, operate with interface overrides using RADIUS (but only when IGMP snooping is enabled) and with site-specific VLANs (access point group VLANs).
- For LWAPP, the controller drops multicast packets sent to UDP control port 12223. For CAPWAP, the controller drops multicast packets sent to UDP control and data ports 5246 and 5247, respectively.

Therefore, you may want to consider not using these port numbers with the multicast applications on your network.

- We recommend that any multicast applications on your network not use the multicast address configured as the CAPWAP multicast group address on the controller.
- For multicast to work on 2500 series controller, you have to configure the multicast IP address.
- Multicast mode is not supported on Cisco Flex 7500 Series Controllers.

Enabling Multicast Mode (GUI)

Step 1 Choose **Controller** > **Multicast** to open the Multicast page.

Step 2 Select the **Enable Global Multicast Mode** check box to configure sending multicast packets. The default value is disabled.

Note FlexConnect supports unicast mode only.

Step 3 If you want to enable IGMP snooping, select the **Enable IGMP Snooping** check box. If you want to disable IGMP snooping, leave the check box unselected. The default value is disabled.

Step 4 To set the IGMP timeout, enter a value between 30 and 7200 seconds in the IGMP Timeout text box. The controller sends three queries in one timeout value at an interval of *timeout*/ 3 to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (that is, to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.

Step 5 Enter the IGMP Query Interval (seconds).

Step 6 Select the **Enable MLD Snooping** check box to support IPv6 forwarding decisions.

Note To enable MLD Snooping, you must enable Global Multicast Mode of the controller.

Step 7 In the MLD Timeout text box, enter a value between 30 and 7200 seconds to set the MLD timeout.

Step 8 Enter the MLD Query Interval (seconds). The valid range is between 15 and 2400 seconds.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Enabling Multicast Mode (CLI)

Step 1 Enable or disable multicasting on the controller by entering this command:
config network multicast global {**enable** | **disable**}

The default value is disabled.

Note The **config network broadcast** {**enable** | **disable**} command allows you to enable or disable broadcasting without enabling or disabling multicasting as well. This command uses the multicast mode currently on the controller to operate.

Step 2 Perform either of the following:

a) Configure the controller to use the unicast method to send multicast packets by entering this command:
config network multicast mode unicast

b) Configure the controller to use the multicast method to send multicast packets to a CAPWAP multicast group by entering this command:
config network multicast mode multicast *multicast_group_ip_address*

Step 3 Enable or disable IGMP snooping by entering this command:
config network multicast igmp snooping {**enable** | **disable**}

The default value is disabled.

Step 4 Set the IGMP timeout value by entering this command:
config network multicast igmp timeout *timeout*

You can enter a *timeout* value between 30 and 7200 seconds. The controller sends three queries in one timeout value at an interval of *timeout*/3 to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (that is, to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.

Step 5 Enable or disable MLD snooping by entering this command:
config network multicast mld snooping {**enable** | **disable**}

The default value is disabled.

Note To enable MLD snooping, you must enable global multicast mode of the controller.

Step 6 Set the MLD timeout value by entering this command:
config network multicast mld timeout *timeout*

Enter the MLD Query Interval (seconds). The valid range is between 15 and 2400 seconds.

Step 7 Save your changes by entering this command:
save config

Viewing Multicast Groups (GUI)

Step 1 Choose **Monitor > Multicast**. The Multicast Groups page appears.
This page shows all the multicast groups and their corresponding MGIDs.

Step 2 Click the link for a specific MGID (such as MGID 550) to see a list of all the clients joined to the multicast group in that particular MGID.

Viewing Multicast Groups (CLI)

Before You Begin

- See all the multicast groups and their corresponding MGIDs by entering this command:

  show network multicast mgid summary

  Information similar to the following appears:

```
Layer2 MGID Mapping:
--------------------
InterfaceName                    vlanId   MGID
-------------------------------- ------   ----
management                       0        0
test                             0        9
wired                            20       8

Layer3 MGID Mapping:
--------------------
Number of Layer3 MGIDs........................... 1

 Group address    Vlan  MGID
 ---------------  ----  ----
 239.255.255.250  0     550
```

- See all the clients joined to the multicast group in a specific MGID by entering this command:

  show network multicast mgid detail *mgid_value*

  where the *mgid_value* parameter is a number between 550 and 4095.

  Information similar to the following appears:

```
Mgid..................................... 550
Multicast Group Address..................... 239.255.255.250
Vlan..................................... 0
Rx Packet Count.......................... 807399588
No of clients............................ 1
Client List.............................
        Client MAC            Expire Time (mm:ss)
        00:13:02:23:82:ad     0:20
```

Viewing an Access Point's Multicast Client Table (CLI)

To help troubleshoot roaming events, you can view an access point's multicast client table from the controller by performing a remote debug of the access point.

Step 1 Initiate a remote debug of the access point by entering this command:
debug ap enable *Cisco_AP*

Step 2 See all of the MGIDs on the access point and the number of clients per WLAN by entering this command:
debug ap command "**show capwap mcast mgid all**" *Cisco_AP*

Step 3 See all of the clients per MGID on the access point and the number of clients per WLAN by entering this command:
debug ap command "**show capwap mcast mgid id** *mgid_value*" *Cisco_AP*

Configuring Multicast Domain Name System

Information About Multicast Domain Name System

Multicast Domain Name System (mDNS) service discovery provides a way to announce and discover the services on the local network. The mDNS service discovery enables wireless clients to access Apple services such as Apple Printer and Apple TV advertised in a different Layer 3 network. mDNS performs DNS queries over IP multicast. mDNS supports zero-configuration IP networking. As a standard, mDNS uses multicast IP address 224.0.0.251 as the destination address and 5353 as the UDP destination port.

Restrictions for Configuring Multicast DNS

- mDNS over IPv6 is not supported.
- mDNS is not supported on access points in FlexConnect mode in a locally switched WLAN and mesh access points.
- mDNS is not supported on remote LANs.
- mDNS is not supported on Cisco AP1240 and Cisco AP1130.
- Third-party mDNS servers or applications are not supported on the Cisco WLC using the mDNS feature. Devices that are advertised by the third-party servers or applications are not populated on the mDNS service or device table correctly on the Cisco WLC.
- Video is not supported on Apple iOS 6 with WMM in enabled state.

Configuring Multicast DNS (GUI)

Step 1 Configure the global mDNS parameters and the Master Services Database by following these steps:

a) Choose **Controller** > **mDNS** > **General**.

b) Select or unselect the **mDNS Global Snooping** check box to enable or disable snooping of mDNS packets, respectively.

c) Enter the mDNS query interval in minutes. The query interval is the frequency at which the controller queries for a service.

d) Choose a service from the **Select Service** drop-down list.

Note To add a new mDNS-supported service to the list, choose **Other**. Specify the service name and the service string. The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services Database. The controller can snoop and learn a maximum of 64 services.

e) Select or unselect the **Query Status** check box to enable or disable an mDNS query for a service, respectively.

f) Click **Add**.

g) Click **Apply**.

h) To view the details of an mDNS service, hover your cursor over the blue drop-down arrow of a service, and choose **Details**.

Step 2 Configure an mDNS profile by following these steps:

a) Choose **Controller** > **mDNS** > **Profiles**.
The controller has a default mDNS profile, which is default-mdns-profile. It is not possible to delete the default profile.

b) To create a new profile, click **New**, enter a profile name, and click **Apply**.

c) To edit a profile, click a profile name on the **mDNS Profiles** page; from the **Service Name** drop-down list, choose a service to be associated with the profile, and click **Apply**.
You can add multiple services to a profile.

Step 3 Click **Save Configuration**.

What to Do Next

After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN. Clients receive service advertisements only for the services associated with the profile. The highest priority is given to the profiles associated with interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority.

- Map an mDNS profile to an interface group by following these steps:
  1. Choose **Controller** > **Interface Groups**.
  2. Click the corresponding interface group name.
     The **Interface Groups > Edit** page is displayed.
  3. From the **mDNS Profile** drop-down list, choose a profile.

- Map an mDNS profile to an interface by following these steps:
  1. Choose **Controller** > **Interfaces**.
  2. Click the corresponding interface name.
     The **Interfaces > Edit** page is displayed.
  3. From the **mDNS Profile** drop-down list, choose a profile.

- Map an mDNS profile to a WLAN by following these steps:
  1. Choose **WLANs**. click the WLAN ID to open the WLANs > Edit page.
  2. Click the corresponding WLAN ID.
     The **WLANs > Edit** page is displayed.
  3. Click the **Advanced** tab.
  4. Select the **mDNS Snooping** check box.
  5. From the **mDNS Profile** drop-down list, choose a profile.

Configuring Multicast DNS (CLI)

- Configure mDNS snooping by entering this command:

  config mdns snooping {**enable** | **disable**}

- Configure an mDNS service by entering this command:

  config mdns service {{**create** *service-name service-string* **query** {**enable** | **disable**}} | **delete** *service-name*}

- Configure a query for an mDNS service by entering this command:

  config mdns service query {**enable** | **disable**} *service-name*

- Configure a query interval for mDNS services by entering this command:

  config mdns query interval *value-in-minutes*

- Configure an mDNS profile by entering this command:

  config mdns profile {**create** | **delete**} *profile-name*

  Note If you try to delete an mDNS profile that is already associated with an interface group, an interface, or a WLAN, an error message is displayed.

- Configure mDNS services to a profile by entering this command:

  config mdns profile service {**add** | **delete**} *profile-name service-name*

- Map an mDNS profile to an interface group by entering this command:

  config interface group mdns-profile {*interface-group-name* | **all**} {*mdns-profile-name* | **none**}

  Note If the mDNS profile name is **none**, no profiles are attached to the interface group. Any existing profile that is attached is removed.

- View information about an mDNS profile that is associated with an interface group by entering this command:

  show interface group detailed *interface-group-name*

- Map an mDNS profile to an interface by entering this command:

  config interface mdns-profile {**management** | {*interface-name* | **all**}} {*mdns-profile-name* | **none**}

- View information about the mDNS profile that is associated with an interface by entering this command:

  show interface detailed *interface-name*

- Configure mDNS for a WLAN by entering this command:

  config wlan mdns {**enable** | **disable**} {*wlan-id* | **all**}

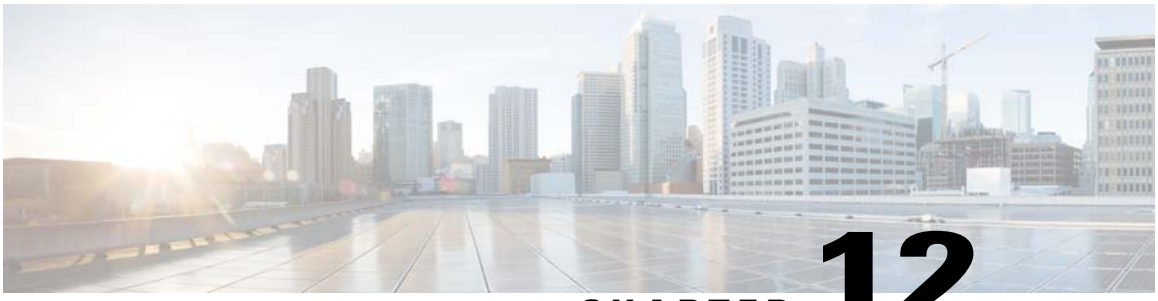
- Map an mDNS profile to a WLAN by entering this command:

  config wlan mdns profile {*wlan-id* | **all**} {*mdns-profile-name* | **none**}

- View information about an mDNS profile that is associated with a WLAN by entering this command:

show wlan *wlan-id*

- View information about all mDNS profiles or a particular mDNS profile by entering this command:
  show mdns profile {**summary** | **detailed** *mdns-profile-name*}
- View information about all mDNS services or a particular mDNS service by entering this command:
  show mdns service {**summary** | **detailed** *mdns-service-name*}
- View information about the mDNS domain names that are learned by entering this command:
  show mdns domain-name-ip summary
- View the mDNS profile for a client by entering this command:
  show client detail *client-mac-address*
- View the mDNS details for a network by entering this command:
  show network summary
- Clear the mDNS service database by entering this command:
  clear mdns service-database {**all** | *service-name*}
- View events related to mDNS by entering this command:
  debug mdns message {**enable** | **disable**}
- View mDNS details of the events by entering this command:
  debug mdns detail {**enable** | **disable**}
- View errors related to mDNS processing by entering this command:
  debug mdns error {**enable** | **disable**}
- Configure debugging of all mDNS details by entering this command:
  debug mdns all {**enable** | **disable**}



CHAPTER 12

Configuring Client Roaming

Information About Client Roaming

The Cisco UWN solution supports seamless client roaming across lightweight access points managed by the same controller, between controllers in the same mobility group on the same subnet, and across controllers in the same mobility group on different subnets. Also, in controller software release 4.1 or later releases, client roaming with multicast packets is supported.

You can adjust the default RF settings (RSSI, hysteresis, scan threshold, and transition time) to fine-tune the operation of client roaming using the controller GUI or CLI.

Inter-Controller Roaming

Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group and on the same subnet. This roaming is also transparent to the client because the session is sustained and a tunnel between controllers allows the client to continue using the same DHCP- or client-assigned IP address as long as the session remains active. The tunnel is torn down, and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP address or a 169.254.*.* client auto-IP address or when the operator-set session timeout is exceeded.

Intra-Controller Roaming

Each controller supports same-controller client roaming across access points managed by the same controller. This roaming is transparent to the client as the session is sustained, and the client continues using the same DHCP-assigned or client-assigned IP address. The controller provides DHCP functionality with a relay

function. Same-controller roaming is supported in single-controller deployments and in multiple-controller deployments.

Inter-Subnet Roaming

Multiple-controller deployments support client roaming across access points managed by controllers in the same mobility group on different subnets. This roaming is transparent to the client because the session is sustained and a tunnel between the controllers allows the client to continue using the same DHCP-assigned or client-assigned IP address as long as the session remains active. The tunnel is torn down, and the client must reauthenticate when the client sends a DHCP Discover with a 0.0.0.0 client IP address or a 169.254.*.* client auto-IP address or when the operator-set user timeout is exceeded.

Voice-over-IP Telephone Roaming

802.11 voice-over-IP (VoIP) telephones actively seek out associations with the strongest RF signal to ensure the best quality of service (QoS) and the maximum throughput. The minimum VoIP telephone requirement of 20-millisecond or shorter latency time for the roaming handover is easily met by the Cisco Unified Wireless Network (Cisco UWN) solution, which has an average handover latency of 5 or fewer milliseconds when open authentication is used. This short latency period is controlled by controllers rather than allowing independent access points to negotiate roaming handovers.

The Cisco UWN solution supports 802.11 VoIP telephone roaming across lightweight access points managed by controllers on different subnets, as long as the controllers are in the same mobility group. This roaming is transparent to the VoIP telephone because the session is sustained and a tunnel between controllers allows the VoIP telephone to continue using the same DHCP-assigned IP address as long as the session remains active. The tunnel is torn down, and the VoIP client must reauthenticate when the VoIP telephone sends a DHCP Discover with a 0.0.0.0 VoIP telephone IP address or a 169.254.*.* VoIP telephone auto-IP address or when the operator-set user timeout is exceeded.

CCX Layer 2 Client Roaming

The controller supports five CCX Layer 2 client roaming enhancements:

- Access point assisted roaming—This feature helps clients save scanning time. When a CCXv2 client associates to an access point, it sends an information packet to the new access point listing the characteristics of its previous access point. Roaming time decreases when the client recognizes and uses an access point list built by compiling all previous access points to which each client was associated and sent (unicast) to the client immediately after association. The access point list contains the channels, BSSIDs of neighbor access points that support the client's current SSID(s), and time elapsed since disassociation.
- Enhanced neighbor list—This feature focuses on improving a CCXv4 client's roam experience and network edge performance, especially when servicing voice applications. The access point provides its associated client information about its neighbors using a neighbor-list update unicast message.
- Enhanced neighbor list request (E2E)—The End-2-End specification is a Cisco and Intel joint program that defines new protocols and interfaces to improve the overall voice and roaming experience. It applies only to Intel clients in a CCX environment. Specifically, it enables Intel clients to request a neighbor list at will. When this occurs, the access point forwards the request to the controller. The controller receives the request and replies with the current CCX roaming sublist of neighbors for the access point to which the client is associated.

Note To see whether a particular client supports E2E, choose **Wireless** > **Clients** on the controller GUI, click the **Detail** link for the desired client, and look at the E2E Version text box in the Client Properties area.

- Roam reason report—This feature enables CCXv4 clients to report the reason why they roamed to a new access point. It also allows network administrators to build and monitor a roam history.
- Directed roam request—This feature enables the controller to send directed roam requests to the client in situations when the controller can better service the client on an access point different from the one to which it is associated. In this case, the controller sends the client a list of the best access points that it can join. The client can either honor or ignore the directed roam request. Non-CCX clients and clients running CCXv3 or below must not take any action. No configuration is required for this feature.

Guidelines and Limitations

- Controller software release 4.2 or later releases support CCX versions 1 through 5. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. The controller stores the CCX version of the client in its client database and uses it to generate and respond to CCX frames appropriately. Clients must support CCXv4 or v5 (or CCXv2 for access point assisted roaming) in order to utilize these roaming enhancements.

  The roaming enhancements mentioned above are enabled automatically, with the appropriate CCX support.
- FlexConnect access points in standalone mode do not support CCX Layer 2 roaming.
- Client roaming between 600 Series Access points is not supported.

Configuring CCX Client Roaming Parameters (GUI)

Step 1 Choose **Wireless** > **802.11a/n or 802.11b/g/n** > **Client Roaming**. The 802.11a (802.11b) > Client Roaming page appears.

Step 2 If you want to fine-tune the RF parameters that affect client roaming, choose **Custom** from the **Mode** drop-down list and go to *Step 3*. If you want to leave the RF parameters at their default values, choose **Default** and go to *Step 8*.

Step 3 In the **Minimum RSSI** text box, enter a value for the minimum received signal strength indicator (RSSI) required for the client to associate to an access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Therefore, clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached.
The range is –90 to –50 dBm.

The default is –85 dBm.

Step 4 In the **Hysteresis** text box, enter a value to indicate how much greater the signal strength of a neighboring access point must be in order for the client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between two access points.
The range is 3 to 20 dB.

The default is 3 dB.

Step 5 In the **Scan Threshold** text box, enter the minimum RSSI that is allowed before the client should roam to a better access point. When the RSSI drops below the specified value, the client must be able to roam to a better access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when the RSSI is below the threshold.
The range is –90 to –50 dBm.

The default is –72 dBm.

Step 6 In the **Transition Time** text box, enter the maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold.
The Scan Threshold and Transition Time parameters guarantee a minimum level of client roaming performance. Together with the highest expected client speed and roaming hysteresis, these parameters make it possible to design a wireless LAN network that supports roaming simply by ensuring a certain minimum overlap distance between access points.

The range is 1 to 5 seconds.

The default is 5 seconds.

Step 7 Click **Apply**.

Step 8 Click **Save Configuration**.

Step 9 Repeat this procedure if you want to configure client roaming for another radio band.

Configuring CCX Client Roaming Parameters (CLI)

Configure CCX Layer 2 client roaming parameters by entering this command:

config {**802.11a** | **802.11b**} **l2roam rf-params** {**default** | **custom** *min_rssi roam_hyst scan_thresh trans_time*}

Obtaining CCX Client Roaming Information (CLI)

Step 1 View the current RF parameters configured for client roaming for the 802.11a or 802.11b/g network by entering this command:
show {**802.11a** | **802.11b**} **l2roam rf-param**

Step 2 View the CCX Layer 2 client roaming statistics for a particular access point by entering this command:
show {**802.11a** | **802.11b**} **l2roam statistics** *ap_mac*

This command provides the following information:

- The number of roam reason reports received
- The number of neighbor list requests received
- The number of neighbor list reports sent

- The number of broadcast neighbor updates sent

Step 3 View the roaming history for a particular client by entering this command:
show client roam-history *client_mac*

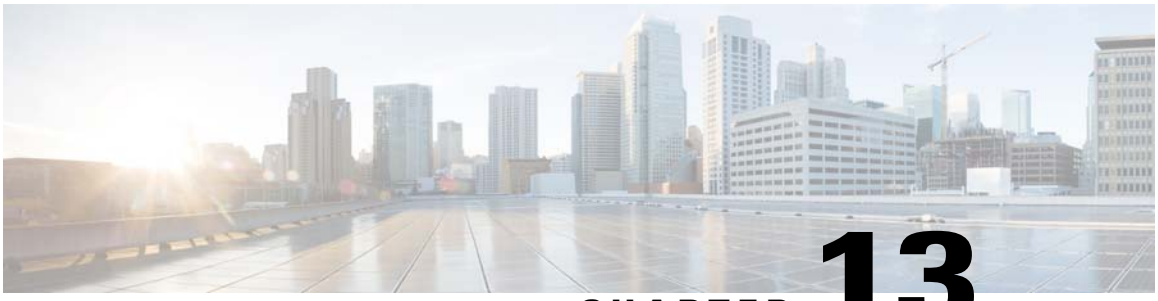
This command provides the following information:

- The time when the report was received
- The MAC address of the access point to which the client is currently associated
- The MAC address of the access point to which the client was previously associated
- The channel of the access point to which the client was previously associated
- The SSID of the access point to which the client was previously associated
- The time when the client disassociated from the previous access point
- The reason for the client roam

Debugging CCX Client Roaming Issues (CLI)

If you experience any problems with CCX Layer 2 client roaming, enter this command:

debug l2roam [**detail** | **error** | **packet** | **all**] {**enable** | **disable**}



CHAPTER 13

Configuring IP-MAC Address Binding

Information About Configuring IP-MAC Address Binding

In the controller software Release 5.2 or later releases, the controller enforces strict IP address-to-MAC address binding in client packets. The controller checks the IP address and MAC address in a packet, compares them to the addresses that are registered with the controller, and forwards the packet only if they both match. In previous releases, the controller checks only the MAC address of the client and ignores the IP address.

You must disable IP-MAC address binding to use an access point in sniffer mode if the access point is associated with a 5500 series controller, a 2500 series controller, or a controller network module. To disable IP-MAC address binding, enter the **config network ip-mac-binding disable**.

WLAN must be enabled to use an access point in sniffer mode if the access point is associated with a 5500 series controller, a 2500 series controller, or a controller network module. If WLAN is disabled, the access point cannot send packets.

Note If the IP address or MAC address of the packet has been spoofed, the check does not pass, and the controller discards the packet. Spoofed packets can pass through the controller only if both the IP and MAC addresses are spoofed together and changed to that of another valid client on the same controller.

Configuring IP-MAC Address Binding (CLI)

Step 1 Enable or disable IP-MAC address binding by entering this command:
config network ip-mac-binding {**enable** | **disable**}

The default value is enabled.

Note You might want to disable this binding check if you have a routed network behind a workgroup bridge (WGB).

Note You must disable this binding check in order to use an access point in sniffer mode if the access point is joined to a Cisco 5500 Series Controller.

Step 2 Save your changes by entering this command:
save config

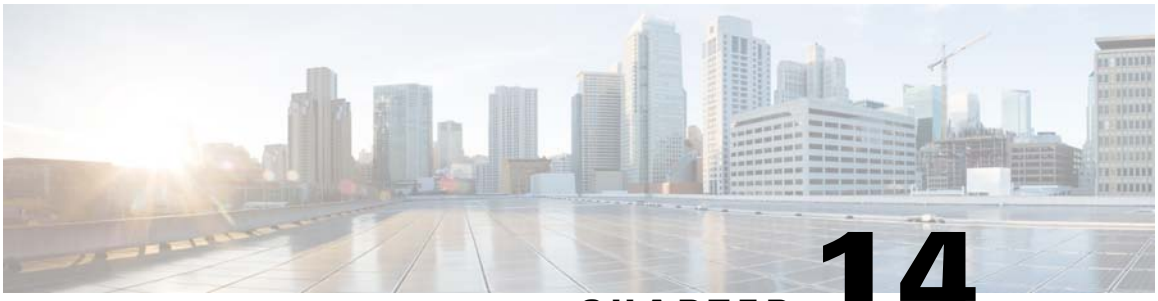
Step 3 View the status of IP-MAC address binding by entering this command:
show network summary

Information similar to the following appears:

```
RF-Network Name............................. ctrl4404
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Disable
...
```

IP/MAC Addr Binding Check ..... Enabled

```
...<?Line-Break?><?HardReturn?>
```



CHAPTER 14

Configuring Quality of Service

Configuring Quality of Service

Information About Quality of Service

Quality of service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics.

The controller supports four QoS levels:

- Platinum/Voice—Ensures a high quality of service for voice over wireless.
- Gold/Video—Supports high-quality video applications.
- Silver/Best Effort—Supports normal bandwidth for clients. This is the default setting.
- Bronze/Background—Provides the lowest bandwidth for guest services.

Note VoIP clients should be set to Platinum.

You can configure the bandwidth of each QoS level using QoS profiles and then apply the profiles to WLANs. The profile settings are pushed to the clients associated to that WLAN. In addition, you can create QoS roles to specify different bandwidth levels for regular and guest users. Follow the instructions in this section to configure QoS profiles and QoS roles. You can also define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN.

The wireless rate limits can be defined on both upstream and downstream traffic. Rate limits can be defined per SSID and/or specified as a maximum rate limit for all clients. These rate limits can be individually configured.

Configuring Quality of Service Profiles

You can configure the Platinum, Gold, Silver, and Bronze QoS profiles.

Configuring QoS Profiles (GUI)

Step 1 Disable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles.
To disable the radio networks, choose **Wireless > 802.11a/n** or **802.11b/g/n > Network**, unselect the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 2 Choose **Wireless > QoS > Profiles** to open the QoS Profiles page.

Step 3 Click the name of the profile that you want to configure to open the Edit QoS Profile page.

Step 4 Change the description of the profile by modifying the contents of the Description text box.

Step 5 Define the data rates on a per-user basis as follows:

a) Define the average data rate for TCP traffic per user by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

b) Define the peak data rate for TCP traffic per user by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Ensure that you configure the average data rate before you configure the burst data rate.

c) Define the average real-time rate for UDP traffic per user by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note Average Data Rate is used to measure TCP traffic while Average Real-time rate is used for UDP traffic. They are measured in kbps for all the entries. The values for Average Data Rate and Average Real-time rate can be different because they are applied to different upper layer protocols such as TCP and UDP. These different values for the rates do not impact the bandwidth.

d) Define the peak real-time rate for UDP traffic per user by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Step 6 Define the data rates on a per-SSID basis as follows:

a) Define the average data rate TCP traffic per SSID by entering the rate in Kbps in the Average Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

b) Define the peak data rate for TCP traffic per SSID by entering the rate in Kbps in the Burst Data Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic in the WLANs.

c) Define the average real-time rate for UDP traffic per SSID by entering the rate in Kbps in the Average Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

d) Define the peak real-time rate for UDP traffic per SSID by entering the rate in Kbps in the Burst Real-Time Rate text boxes. A value of 0 indicates that the value specified in the selected QoS profile will take effect.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic in the WLANs.

Step 7 Define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN.

a) From the Maximum Priority drop-down list, choose the maximum QoS priority for any data frames transmitted by the AP to any station in the WLAN.
For example, a QoS profile named 'gold' targeted for video applications has the maximum priority set to video by default.

b) From the Unicast Default Priority drop-down list, choose the QoS priority for unicast data frames transmitted by the AP to non-WMM stations in the WLAN

c) From the Multicast Default Priority drop-down list, choose the QoS priority for multicast data frames transmitted by the AP to stations in the WLAN,

Note The default unicast priority cannot be used for non-WMM clients in a mixed WLAN.

Step 8 Choose **802.1p** from the Protocol Type drop-down list and enter the maximum priority value in the 802.1p Tag text box to define the maximum value (0–7) for the priority tag associated with packets that fall within the profile.
The tagged packets include CAPWAP data packets (between access points and the controller) and packets sent toward the core network.

Note If a QoS profile has 802.1p tagging configured and if this QoS profile is assigned to a WLAN that uses an untagged interface on the controller, the client traffic will be blocked.

Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Step 11 Reenable the 802.11 networks.
To enable the radio networks, choose **Wireless > 802.11a/n** or **802.11b/g/n > Network**, select the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Configuring QoS Profiles (CLI)

Step 1 Disable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles by entering these commands:
config 802.11 {**a** | **b**} **disable network**

Step 2 Change the profile description by entering this command:
config qos description {**bronze** | **silver** | **gold** | **platinum** }*description*

Step 3 Define the average data rate for TCP traffic per user or per SSID by entering this command:
config qos average-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Note For the *rate* parameter, you can enter a value between 0 and 512,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Step 4 Define the peak data rate for TCP traffic per user or per SSID by entering this command:
config qos burst-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Step 5 Define the average real-time data rate for UDP traffic per user or per SSID by entering this command:
config qos average-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Step 6 Define the peak real-time data rate for UDP traffic per user or per SSID by entering this command:
config qos burst-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Step 7 Define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN by entering this command:
config qos priority {**bronze** | **gold** | **platinum** | **silver**} {*maximum priority*} {*default unicast priority*} {*default multicast priority*}

You choose from the following options for the *maximum priority*, *default unicast priority*, and *default multicast priority* parameters:

- besteffort
- background
- video
- voice

Step 8 Define the maximum value (0–7) for the priority tag associated with packets that fall within the profile, by entering these commands:
config qos protocol-type {**bronze** | **silver** | **gold** | **platinum**} **dot1p**

config qos dot1p-tag {**bronze** | **silver** | **gold** | **platinum**} *tag*

The tagged packets include CAPWAP data packets (between access points and the controller) and packets sent toward the core network.

Note The 802.1p tagging has impact only on wired packets. Wireless packets are impacted only by the maximum priority level set for a QoS profile.

Note If a QoS profile has 802.1p tagging configured and if this QoS profile is assigned to a WLAN that uses an untagged interface on the controller, the client traffic will be blocked.

Step 9 Reenable the 802.11a and 802.11b/g networks so that you can configure the QoS profiles by entering these commands:
config 802.11{**a** | **b**} **enable network**

Configuring Quality of Service Roles

Information About Quality of Service Roles

After you configure a QoS profile and apply it to a WLAN, it limits the bandwidth level of clients associated to that WLAN. Multiple WLANs can be mapped to the same QoS profile, which can result in bandwidth contention between regular users (such as employees) and guest users. In order to prevent guest users from using the same level of bandwidth as regular users, you can create QoS roles with different (and presumably lower) bandwidth contracts and assign them to guest users.

You can configure up to ten QoS roles for guest users.

Note If you choose to create an entry on the RADIUS server for a guest user and enable RADIUS authentication for the WLAN on which web authentication is performed rather than adding a guest user to the local user database from the controller, you need to assign the QoS role on the RADIUS server itself. To do so, a "guest-role" Airespace attribute needs to be added on the RADIUS server with a datatype of "string" and a return value of "11." This attribute is sent to the controller when authentication occurs. If a role with the name returned from the RADIUS server is found configured on the controller, the bandwidth associated to that role is enforced for the guest user after authentication completes successfully.

Configuring QoS Roles

Configuring QoS (GUI)

Step 1 Choose **Wireless** > **QoS > Roles** to open the QoS Roles for the Guest Users page.
This page shows any existing QoS roles for guest users.

Note If you want to delete a QoS role, hover your cursor over the blue drop-down arrow for that role and choose **Remove**.

Step 2 Click **New** to create a new QoS role. The **QoS Role Name > New** page appears.

Step 3 In the **Role Name** text box, enter a name for the new QoS role. The name should uniquely identify the role of the QoS user (such as Contractor, Vendor, and so on).

Step 4 Click **Apply**.

Step 5 Click the name of the QoS role to edit the bandwidth of a QoS role. The **Edit QoS Role Data Rates** page appears.

Note The values that you configure for the per-user bandwidth contracts affect only the amount of bandwidth going downstream (from the access point to the wireless client). They do not affect the bandwidth for upstream traffic (from the client to the access point).

Note The Access Points that support per-user bandwidth contracts for upstream (from the client to the access point) are - AP1140, AP1040, AP3500, AP3600, AP1250, and AP1260.

Step 6 Define the average data rate for TCP traffic on a per-user basis by entering the rate in Kbps in the **Average Data Rate** text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Step 7 Define the peak data rate for TCP traffic on a per-user basis by entering the rate in Kbps in the Burst Data Rate text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Ensure that you configure the average data rate before you configure the burst data rate.

Step 8 Define the average real-time rate for UDP traffic on a per-user basis by entering the rate in Kbps in the **Average Real-Time Rate** text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Step 9 Define the peak real-time rate for UDP traffic on a per-user basis by entering the rate in Kbps in the **Burst Real-Time Rate** text box. You can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

Step 10 Click **Apply**.

Step 11 Click **Save Configuration**.

Step 12 Apply a QoS role to a guest user by following the instructions in the Configuring Local Network Users for the Controller (GUI) section.

Configuring QoS Roles (CLI)

Step 1 Create a QoS role for a guest user by entering this command:
config netuser guest-role create *role_name*

Note If you want to delete a QoS role, enter the **config netuser guest-role delete** *role_name* command.

Step 2 Configure the bandwidth contracts for a QoS role by entering these commands:

- **config netuser guest-role qos data-rate average-data-rate** *role_name rate*—Configures the average data rate for TCP traffic on a per-user basis.
- **config netuser guest-role qos data-rate burst-data-rate** *role_name rate*—Configures the peak data rate for TCP traffic on a per-user basis.

  Note The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

- **config netuser guest-role qos data-rate average-realtime-rate** *role_name rate*—Configures the average real-time rate for UDP traffic on a per-user basis.
- **config netuser guest-role qos data-rate burst-realtime-rate** *role_name rate*—Configures the peak real-time rate for UDP traffic on a per-user basis.

  Note The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

  Note For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name should uniquely identify the role of the QoS user (such as Contractor, Vendor, and so on). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

Step 3 Apply a QoS role to a guest user by entering this command:
config netuser guest-role apply *username role_name*

For example, the role of *Contractor* could be applied to guest user *jsmith*.

Note If you do not assign a QoS role to a guest user, the Role text box in the User Details shows the role as "default." The bandwidth contracts for this user are defined in the QoS profile for the WLAN.

Note If you want to unassign a QoS role from a guest user, enter the **config netuser guest-role apply** *username* **default command**. This user now uses the bandwidth contracts defined in the QoS profile for the WLAN.

Step 4 Save your changes by entering this command:
save config

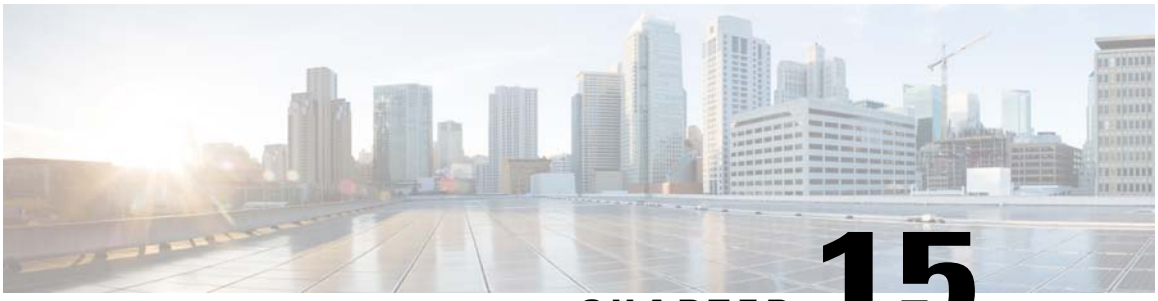
Step 5 See a list of the current QoS roles and their bandwidth parameters by entering this command:

show netuser guest-roles

Information similar to the following appears:

```
Role Name..................................... Contractor
     Average Data Rate........................ 10
     Burst Data Rate.......................... 10
     Average Realtime Rate.................... 100
     Burst Realtime Rate...................... 100

Role Name..................................... Vendor
     Average Data Rate........................ unconfigured
     Burst Data Rate.......................... unconfigured
     Average Realtime Rate.................... unconfigured
     Burst Realtime Rate..................... unconfigured
```



CHAPTER 15

Configuring Application Visibility and Control

Information About Application Visibility and Control

Application Visibility and Control (AVC) classifies applications using deep packet inspection techniques with the Network-Based Application Recognition (NBAR) engine, and provides application-level visibility and control into Wi-Fi networks. After the applications are recognized, the AVC feature enables you to either drop or mark the data traffic.

Using AVC, we can detect more than 1000 applications. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.

AVC is supported on the following controller platforms: Cisco 2500 Series Wireless LAN Controllers, Cisco 5500 Series Wireless LAN Controllers, Cisco Flex 7500 Series Wireless LAN Controllers in central switching mode, Cisco 8500 Series Wireless LAN Controllers, and Cisco Wireless Services Module 2 (WiSM2).

AVC DSCP marks only the DSCP of the original packet in the controller in both directions (upstream and downstream). It does not affect the outer CAPWAP DCSP. AVC DSCP is applicable only when the application is classified. For example, based on the AVC profile configuration, if an application is classified as ftp or http, the corresponding DSCP marking is applied irrespective of the WLAN QoS. For downstream, the DSCP value of outer CAPWAP header and inner packet's DSCP are taken from AVC DSCP. WLAN QoS is only applicable for all traffic from WLC to AP through CAPWAP. It does not change the DSCP of the original packet

Restrictions for Application Visibility and Control

- IPv6 packet classification is not supported.
- Layer 2 roaming is not supported across controllers.

- Multicast traffic is not supported.

Configuring Application Visibility and Control (GUI)

Step 1 Create and configure an AVC profile by following these steps:

a) Choose **Wireless** > **Application Visibility and Control** > **AVC Profiles**.
b) Click **New**.
c) Enter the AVC profile name.
d) Click **Apply**.
e) On the **AVC Profile Name** page, click the corresponding AVC profile name.
The **AVC Profile > Edit** page is displayed.
f) Click **Add New Rule**.
g) Choose the application group and the application name from the respective drop-down lists.
View the list of default AVC applications available by choosing **Wireless** > **Application Visibility and Control** > **AVC Applications**.
h) From the **Action** drop-down list, choose either of the following:

- **Drop—**Drops the upstream and downstream packets that correspond to the chosen application.
- **Mark—**Marks the upstream and downstream packets that correspond to the chosen application with the Differentiated Services Code Point (DSCP) value that you specify in the **DSCP (0 to 63)** drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.

Note The default action is to give permission to all applications.

i) If you choose **Mark** from the **Action** drop-down list, choose a DSCP value from the **DSCP (0 to 63)** drop-down list. The DSCP value is a packet header code that is used to define QoS across the Internet. The DSCP values are mapped to the following QoS levels:

- **Platinum (Voice)—**Assures a high QoS for Voice over Wireless.
- **Gold (Video)—**Supports high-quality video applications.
- **Silver (Best Effort)—**Supports normal bandwidth for clients.
- **Bronze (Background)—**Provides the lowest bandwidth for guest services.

You can also choose **Custom** and specify the DSCP value. The valid range is from 0 to 63.

j) Click **Apply**.
k) Click **Save Configuration**.

Step 2 Associate an AVC profile to a WLAN by following these steps:

a) Choose **WLANs** and click the corresponding WLAN ID.
The **WLANs > Edit** page is displayed.
b) Click the **QoS** tab.
c) Choose the AVC profile from the **AVC Profile** drop-down list.

d) Click **Apply**.
e) Click **Save Configuration**.

Configuring Application Visibility and Control (CLI)

- Create or delete an AVC profile by entering this command:

  config avc profile *avc-profile-name* {**create** | **delete**}

- Add a rule for an AVC profile by entering this command:

  config avc profile *avc-profile-name* **rule add application** *application-name* {**drop** | **mark** *dscp-value*}

- Remove a rule for an AVC profile by entering this command:

  config avc profile *avc-profile-name* **rule remove application** *application-name*

- Configure an AVC profile to a WLAN by entering this command:

  config wlan avc *wlan-id* **profile** *avc-profile-name* {**enable** | **disable**}

- Configure application visibility for a WLAN by entering this command:

  config wlan avc *wlan-id* **visibility** {**enable** | **disable**}

  Note Application visibility is the subset of an AVC profile. Therefore, visibility is automatically enabled when you configure an AVC profile on the WLAN.

- View information about all AVC profile or a particular AVC profile by entering this command:

  show avc profile {**summary** | **detailed** *avc-profile-name*}

- View information about AVC applications by entering this command:

  show avc applications [*application-group*]

- View various statistical information about AVC by entering this command:

  show avc statistics

- Configure troubleshooting for AVC events by entering this command:

  debug avc events {**enable** | **disable**}

- Configure troubleshooting for AVC errors by entering this command:

  debug avc error {**enable** | **disable**}

Configuring NetFlow

Information About NetFlow

NetFlow is a protocol that provides information about network users and applications, peak usage times, and traffic routing. The NetFlow protocol collects IP traffic information from network devices to monitor traffic. The NetFlow architecture consists of the following components:

- Collector—Entity that collects all the IP traffic information from various network elements.
- Exporter—Network entity that exports the template with the IP traffic information. The controller acts as an exporter.

Configuring NetFlow (GUI)

Step 1 Configure the Exporter by following these steps:

a) Choose **Wireless** > **Netflow** > **Exporter**.
b) Click **New**.
c) Enter the Exporter name, IP address, and the port number.
The valid range for the port number is from 1 to 65535.
d) Click **Apply**.
e) Click **Save Configuration**.

Step 2 Configure the NetFlow Monitor by following these steps:

a) Choose **Wireless** > **Netflow** > **Monitor**.
b) Click **New** and enter the Monitor name.
c) On the Monitor List page, click the Monitor name to open the Netflow Monitor > Edit page.
d) Choose the Exporter name and the Record name from the respective drop-down lists.
e) Click **Apply**.
f) Click **Save Configuration**.

Step 3 Associate a NetFlow Monitor to a WLAN by following these steps:

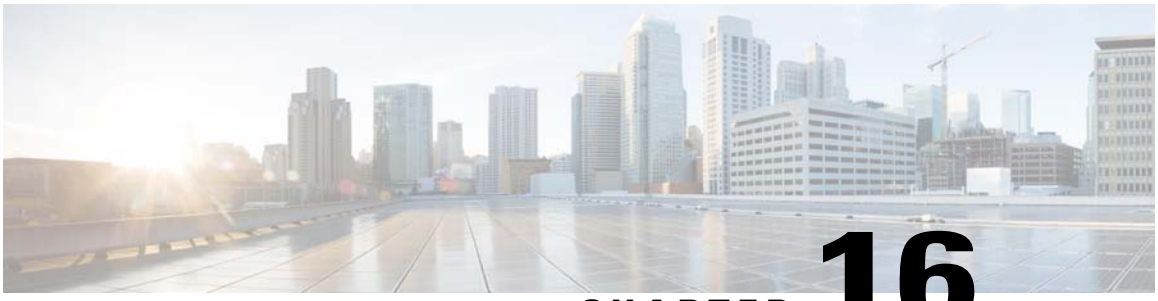
a) Choose **WLANs** and click the WLAN ID to open the WLANs > Edit page.
b) In the QoS tab, choose the NetFlow Monitor from the Netflow Monitor drop-down list.
c) Click **Apply**.
d) Click **Save Configuration**.

Configuring NetFlow (CLI)

- Create an Exporter by entering this command:

  config flow create exporter *exporter-name ip-addr port-number*

- Create a NetFlow Monitor by entering this command:
  config flow create monitor *monitor-name*
- Associate or dissociate a NetFlow Monitor with an Exporter by entering this command:
  config flow {**add** | **delete**} **monitor** *monitor-name* **exporter** *exporter-name*
- Associate or dissociate a NetFlow Monitor with a Record by entering this command:
  config flow {**add** | **delete**} **monitor** *monitor-name* **record ipv4_client_app_flow_record**
- Associate or dissociate a NetFlow Monitor with a WLAN by entering this command:
  config wlan flow *wlan-id* **monitor** *monitor-name* {**enable** | **disable**}
- See a summary of NetFlow Monitors by entering this command:
  show flow monitor summary
- See information about the Exporter by entering this command:
  show flow exporter {**summary** | **statistics**}
- Configure a debug of NetFlow by entering this command:
  debug flow {**detail** | **error** | **info**} {**enable** | **disable**}



CHAPTER 16

Configuring Media and EDCA Parameters

Configuring Voice and Video Parameters

Information About Configuring Voice and Video Parameters

Three parameters on the controller affect voice and/or video quality:

- Call admission control
- Expedited bandwidth requests
- Unscheduled automatic power save delivery

Each of these parameters is supported in Cisco Compatible Extensions (CCX) v4 and v5.

Note Traffic stream metrics (TSM) can be used to monitor and report issues with voice quality.

Call Admission Control

Call admission control (CAC) enables an access point to maintain controlled quality of service (QoS) when the wireless LAN is experiencing congestion. The Wi-Fi Multimedia (WMM) protocol deployed in CCXv3 ensures sufficient QoS as long as the wireless LAN is not congested. However, in order to maintain QoS under differing network loads, CAC in CCXv4 is required. Two types of CAC are available: bandwidth-based CAC and load-based CAC.

Bandwidth-Based CAC

Bandwidth-based, or static, CAC enables the client to specify how much bandwidth or shared medium time is required to accept a new call and in turn enables the access point to determine whether it is capable of accommodating this particular call. The access point rejects the call if necessary in order to maintain the maximum allowed number of calls with acceptable quality.

The QoS setting for a WLAN determines the level of bandwidth-based CAC support. To use bandwidth-based CAC with voice applications, the WLAN must be configured for Platinum QoS. To use bandwidth-based CAC with video applications, the WLAN must be configured for Gold QoS. Also, make sure that WMM is enabled for the WLAN. See the Information About Configuring 802.3 Bridging, on page 103 section for QoS and WMM configuration instructions.

Note You must enable admission control (ACM) for CCXv4 clients that have WMM enabled. Otherwise, bandwidth-based CAC does not operate properly.

Load-Based CAC

Load-based CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types (including that from clients), co-channel access point loads, and collocated channel interference, for voice applications. Load-based CAC also covers the additional bandwidth consumption resulting from PHY and channel impairment.

In load-based CAC, the access point continuously measures and updates the utilization of the RF channel (that is, the percentage of bandwidth that has been exhausted), channel interference, and the additional calls that the access point can admit. The access point admits a new call only if the channel has enough unused bandwidth to support that call. By doing so, load-based CAC prevents oversubscription of the channel and maintains QoS under all conditions of WLAN loading and interference.

Note Load-based CAC is supported only on lightweight access points. If you disable load-based CAC, the access points start using bandwidth-based CAC.

Expedited Bandwidth Requests

The expedited bandwidth request feature enables CCXv5 clients to indicate the urgency of a WMM traffic specifications (TSPEC) request (for example, an e911 call) to the WLAN. When the controller receives this request, it attempts to facilitate the urgency of the call in any way possible without potentially altering the quality of other TSPEC calls that are in progress.

You can apply expedited bandwidth requests to both bandwidth-based and load-based CAC. Expedited bandwidth requests are disabled by default. When this feature is disabled, the controller ignores all expedited requests and processes TSPEC requests as normal TSPEC requests.

This table lists examples of TSPEC request handling for normal TSPEC requests and expedited bandwidth requests.

Table 4: TSPEC Request Handling Examples

CAC Mode	Reserved bandwidth for voice calls[1]	Usage[2]	Normal TSPEC Request	TSPEC with Expedited Bandwidth Request
Bandwidth-based CAC	75% (default setting)	Less than 75%	Admitted	Admitted
		Between 75% and 90% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 90%	Rejected	Rejected
Load-based CAC		Less than 75%	Admitted	Admitted
		Between 75% and 85% (reserved bandwidth for voice calls exhausted)	Rejected	Admitted
		More than 85%	Rejected	Rejected

1 For bandwidth-based CAC, the voice call bandwidth usage is per access point and does not take into account co-channel access points. For load-based CAC, the voice call bandwidth usage is measured for the entire channel.

2 Bandwidth-based CAC (consumed voice and video bandwidth) or load-based CAC (channel utilization [Pb]).

Note Admission control for TSPEC g711-40ms codec type is supported.

Note When video ACM is enabled, the controller rejects a video TSPEC if the non-MSDU size in the TSPEC is greater than 149 or the mean data rate is greater than 1 Kbps.

U-APSD

Unscheduled automatic power save delivery (U-APSD) is a QoS facility defined in IEEE 802.11e that extends the battery life of mobile clients. In addition to extending battery life, this feature reduces the latency of traffic flow delivered over the wireless media. Because U-APSD does not require the client to poll each individual packet buffered at the access point, it allows delivery of multiple downlink packets by sending a single uplink trigger packet. U-APSD is enabled automatically when WMM is enabled.

Traffic Stream Metrics

In a voice-over-wireless LAN (VoWLAN) deployment, traffic stream metrics (TSM) can be used to monitor voice-related metrics on the client-access point air interface. It reports both packet latency and packet loss. You can isolate poor voice quality issues by studying these reports.

The metrics consist of a collection of uplink (client side) and downlink (access point side) statistics between an access point and a client device that supports CCX v4 or later releases. If the client is not CCX v4 or CCXv5 compliant, only downlink statistics are captured. The client and access point measure these metrics. The access point also collects the measurements every 5 seconds, prepares 90-second reports, and then sends the reports to the controller. The controller organizes the uplink measurements on a client basis and the downlink measurements on an access point basis and maintains an hour's worth of historical data. To store this data, the controller requires 32 MB of additional memory for uplink metrics and 4.8 MB for downlink metrics.

TSM can be configured through either the GUI or the CLI on a per radio-band basis (for example, all 802.11a radios). The controller saves the configuration in flash memory so that it persists across reboots. After an access point receives the configuration from the controller, it enables TSM on the specified radio band.

Note Access points support TSM entries in both local and FlexConnect modes.

This table shows the upper limit for TSM entries in different controller series.

TSM Entries	5500	7500
MAX AP TSM entries	100	100
MAX Client TSM entries	250	250
MAX TSM entries	100*250=25000	100*250=25000

Note Once the upper limit is reached, additional TSM entries cannot be stored and sent to Cisco Prime Infrastructure. If client TSM entries are full and AP TSM entries are available, then only the AP entries are stored, and vice versa. This leads to partial output. TSM cleanup occurs every one hour. Entries are removed only for those APs and clients that are not in the system.

Configuring Voice Parameters

Configuring Voice Parameters (GUI)

Step 1 Ensure that the WLAN is configured for WMM and the Platinum QoS level.

Step 2 Disable all WLANs with WMM enabled and click **Apply**.

Step 3 Choose **Wireless** and then **Network** under 802.11a/n or 802.11b/g/n, unselect the 802.11a (or 802.11b/g) Network Status check box, and click **Apply** to disable the radio network.

Step 4 Choose **Wireless** > **802.11a/n** or **802.11b/g/n** > **Media**. The 802.11a (or 802.11b) > Media page appears. The Voice tab is displayed by default.

Step 5 Select the **Admission Control (ACM)** check box to enable bandwidth-based CAC for this radio band. The default value is disabled.

Step 6 Select the **Admission Control (ACM)** you want to use by choosing from the following choices:

- **Load-based—**To enable channel-based CAC. This is the default option.
- **Static—**To enable radio-based CAC.

Step 7 In the **Max RF Bandwidth** text box, enter the percentage of the maximum bandwidth allocated to clients for voice applications on this radio band. Once the client reaches the value specified, the access point rejects new calls on this radio band.
The range is 5% to 85%. The sum of maximum bandwidth percentage of voice and video should not exceed 85%.

The default is 75%.

Step 8 In the **Reserved Roaming Bandwidth** text box, enter the percentage of maximum allocated bandwidth that is reserved for roaming voice clients. The controller reserves this bandwidth from the maximum allocated bandwidth for roaming voice clients.
The range is 0% to 25%.

The default is 6%.

Step 9 To enable expedited bandwidth requests, select the **Expedited Bandwidth** check box. By default, this text box is disabled.

Step 10 To enable SIP CAC support, select the **SIP CAC Support** check box. By default, SIP CAC support is disabled.

Step 11 From the **SIP Codec** drop-down list, choose one of the following options to set the codec name. The default value is G.711. The options are as follows:

- User Defined
- G.711
- G.729

Step 12 In the **SIP Bandwidth (kbps)** text box, enter the bandwidth in kilobits per second.
The possible range is 8 to 64.

The default value is 64.

Note The **SIP Bandwidth (kbps)** text box is highlighted only when you select the SIP codec as User-Defined. If you choose the SIP codec as G.711, the **SIP Bandwidth (kbps)** text box is set to 64. If you choose the SIP codec as G.729, the SIP Bandwidth (kbps) text box is set to 8.

Step 13 In the **SIP Voice Sample Interval (msecs)** text box, enter the value for the sample interval.

Step 14 In the **Maximum Calls** text box, enter the maximum number of calls that can be made to this radio. The maximum call limit includes both direct and roaming-in calls. If the maximum call limit is reached, the new or roaming-in calls result in failure.
The possible range is 0 to 25.

The default value is 0, which indicates that there is no check for maximum call limit.

Note If SIP CAC is supported and the CAC method is static, the Maximum Possible Voice Calls and Maximum Possible Roaming Reserved Calls fields appear.

Step 15 Select the **Metrics Collection** check box to collect traffic stream metrics. By default, this box is unselected. That is, the traffic stream metrics is not collected by default.

Step 16 Click **Apply**.

Step 17 Reenable all WMM WLANs and click **Apply**.

Step 18 Choose **Network** under 802.11a/n or 802.11b/g/n, select the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to reenable the radio network.

Step 19 Click **Save Configuration**.

Step 20 Repeat this procedure if you want to configure voice parameters for another radio band.

Configuring Voice Parameters (CLI)

Before You Begin

Ensure that you have configured SIP-based CAC.

Step 1 See all of the WLANs configured on the controller by entering this command:
show wlan summary

Step 2 Make sure that the WLAN that you are planning to modify is configured for WMM and the QoS level is set to Platinum by entering this command:
show wlan *wlan_id*

Step 3 Disable all WLANs with WMM enabled prior to changing the voice parameters by entering the command:
config wlan disable *wlan_id*

Step 4 Disable the radio network by entering this command:
config {**802.11a** | **802.11b**} **disable network**

Step 5 Save your settings by entering this command:
save config

Step 6 Enable or disable bandwidth-based voice CAC for the 802.11a or 802.11b/g network by entering this command:
config {**802.11a** | **802.11b**} **cac voice acm** {**enable** | **disable**}

Step 7 Set the percentage of maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network by entering this command:
config {**802.11a** | **802.11b**} **cac voice max-bandwidth** *bandwidth*

The *bandwidth* range is 5 to 85%, and the default value is 75%. Once the client reaches the value specified, the access point rejects new calls on this network.

Step 8 Set the percentage of maximum allocated bandwidth reserved for roaming voice clients by entering this command:
config {**802.11a** | **802.11b**} **cac voice roam-bandwidth** *bandwidth*

The *bandwidth* range is 0 to 25%, and the default value is 6%. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients.

Step 9 Configure the codec name and sample interval as parameters and to calculate the required bandwidth per call by entering this command:
config {**802.11a** | **802.11b**} **cac voice sip codec** {**g711** | **g729**} **sample-interval** *number_msecs*

Step 10 Configure the bandwidth that is required per call by entering this command:
config {**802.11a** | **802.11b**} **cac voice sip bandwidth** *bandwidth_kbps* **sample-interval** *number_msecs*

Step 11 Reenable all WLANs with WMM enabled by entering this command:
config wlan enable *wlan_id*

Step 12 Reenable the radio network by entering this command:
config {**802.11a** | **802.11b**} **enable network**

Step 13 View the TSM voice metrics by entering this command:
show [802.11a | 802.11b] cu-metrics *AP_Name*

The command also displays the channel utilization metrics.

Step 14 Enter the **save config** command to save your settings.

Step 15 Configure voice automatically for a WLAN by entering this command:
config auto-configure voice cisco *wlan-id* **radio** {**802.11a** | **802.11b** | **all**}

Step 16 Enter the **save config** command to save your settings.

Configuring Video Parameters

Configuring Video Parameters (GUI)

Step 1 Ensure that the WLAN is configured for WMM and the Gold QoS level.

Step 2 Disable all WLANs with WMM enabled and click **Apply**.

Step 3 Choose **Wireless** and then **Network** under 802.11a/n or 802.11b/g/n, unselect the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to disable the radio network.

Step 4 Choose **Wireless** > **802.11a/n** or **802.11b/g/n** > **Media**. The 802.11a (or 802.11b) > Media page appears.

Step 5 In the **Video** tab, select the **Admission Control (ACM)** check box to enable video CAC for this radio band. The default value is disabled.

Step 6 From the **CAC Method** drop-down list, choose between **Static** and **Load Based** methods.
The static CAC method is based on the radio and the load-based CAC method is based on the channel.

Note For TSpec and SIP based CAC for video calls, only Static method is supported.

Step 7 In the **Max RF Bandwidth** text box, enter the percentage of the maximum bandwidth allocated to clients for video applications on this radio band. When the client reaches the value specified, the access point rejects new requests on this radio band.
The range is 5% to 85%. The sum of maximum bandwidth percentage of voice and video should not exceed 85%. The default is 0%.

Step 8 In the Reserved Roaming Bandwidth text box, enter the percentage of the maximum RF bandwidth that is reserved for roaming clients for video.

Step 9 Configure the SIP CAC Support by selecting or unselecting the **SIP CAC Support** check box.
SIP CAC is supported only if SIP Snooping is enabled.

Note You cannot enable SIP CAC if you have selected the Load Based CAC method.

Step 10 Click **Apply**.

Step 11 Reenable all WMM WLANs and click **Apply**.

Step 12 Choose **Network** under 802.11a/n or 802.11b/g/n, select the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to reenable the radio network.

Step 13 Click **Save Configuration**.

Step 14 Repeat this procedure if you want to configure video parameters for another radio band.

Configuring Video Parameters (CLI)

Before You Begin

Ensure that you have configured SIP-based CAC.

Step 1 See all of the WLANs configured on the controller by entering this command:
show wlan summary

Step 2 Make sure that the WLAN that you are planning to modify is configured for WMM and the QoS level is set to Gold by entering this command:
show wlan *wlan_id*

Step 3 Disable all WLANs with WMM enabled prior to changing the video parameters by entering this command:
config wlan disable *wlan_id*

Step 4 Disable the radio network by entering this command:
config {**802.11a** | **802.11b**} **disable network**

Step 5 Save your settings by entering this command:
save config

Step 6 Enable or disable video CAC for the 802.11a or 802.11b/g network by entering this command:
config {**802.11a** | **802.11b**} **cac video acm** {**enable** | **disable**}

Step 7 To configure the CAC method as either static or load-based, enter this command:
config {**802.11a** | **802.11b**} **cac video cac-method** {**static** | **load-based**}

Step 8 Set the percentage of maximum bandwidth allocated to clients for video applications on the 802.11a or 802.11b/g network by entering this command:
config {**802.11a** | **802.11b**} **cac video max-bandwidth** *bandwidth*

The *bandwidth* range is 5 to 85%, and the default value is 5%. However, the maximum RF bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network.

Note If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests.

Step 9 To configure the percentage of the maximum RF bandwidth that is reserved for roaming clients for video, enter this command:
config {**802.11a** | **802.11b**} **cac video roam-bandwidth** *bandwidth*

Step 10 To configure the CAC parameters for SIP-based video calls, enter this command:
config {**802.11a** | **802.11b**} **cac video sip** {**enable** | **disable**}

Step 11 Process or ignore the TSPEC inactivity timeout received from an access point by entering this command:
config {**802.11a** | **802.11b**} **cac video tspec-inactivity-timeout** {**enable** | **ignore**}

Step 12 Reenable all WLANs with WMM enabled by entering this command:
config wlan enable *wlan_id*

Step 13 Reenable the radio network by entering this command:
config {**802.11a** | **802.11b**} **enable network**

Step 14 Enter the **save config** command to save your settings.

Viewing Voice and Video Settings

Viewing Voice and Video Settings (GUI)

Step 1 Choose **Monitor** > **Clients** to open the Clients page.

Step 2 Click the MAC address of the desired client to open the Clients > Detail page.
This page shows the U-APSD status (if enabled) for this client under Quality of Service Properties.

Step 3 Click **Back** to return to the Clients page.

Step 4 See the TSM statistics for a particular client and the access point to which this client is associated as follows:

a) Hover your cursor over the blue drop-down arrow for the desired client and choose **802.11aTSM** or **802.11b/g TSM**. The Clients > AP page appears.

b) Click the **Detail** link for the desired access point to open the Clients > AP > Traffic Stream Metrics page.
This page shows the TSM statistics for this client and the access point to which it is associated. The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Step 5 See the TSM statistics for a particular access point and a particular client associated to this access point, as follows:

a) Choose **Wireless** > **Access Points** > **Radios** > **802.11a/n** or **802.11b/g/n**. The 802.11a/n Radios or 802.11b/g/n Radios page appears.

b) Hover your cursor over the blue drop-down arrow for the desired access point and choose **802.11aTSM** or **802.11b/g TSM**. The AP > Clients page appears.

c) Click the **Detail** link for the desired client to open the AP > Clients > Traffic Stream Metrics page.
This page shows the TSM statistics for this access point and a client associated to it. The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Viewing Voice and Video Settings (CLI)

Step 1 See the CAC configuration for the 802.11 network by entering this command:
show ap stats {**802.11a** | **802.11b**}

Step 2 See the CAC statistics for a particular access point by entering this command:
show ap stats {802.11a | 802.11b} *ap_name*

Information similar to the following appears:

```
Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw)..... 0
Total channel MT free..................... 0
Total voice MT free....................... 0
Na Direct................................. 0
Na Roam................................... 0
  Video Bandwidth in use(% of config bw)..... 0
  Total num of voice calls in progress...... 0
  Num of roaming voice calls in progress..... 0
  Total Num of voice calls since AP joined..... 0
  Total Num of roaming calls since AP joined..... 0
 Total Num of exp bw requests received..... 5
  Total Num of exp bw requests admitted..... 2

Num of voice calls rejected since AP joined..... 0
  Num of roam calls rejected since AP joined..... 0
  Num of calls rejected due to insufficient bw....0
  Num of calls rejected due to invalid params.... 0
  Num of calls rejected due to PHY rate..... 0
  Num of calls rejected due to QoS policy..... 0
```

In the example above, “MT” is medium time, “Na” is the number of additional calls, and “exp bw” is expedited bandwidth.

Note Suppose an AP has to be rebooted when a voice client associated with the AP is on an active call. After the AP is rebooted, the client continues to maintain the call, and during the time the AP is down, the database is not refreshed by the controller. Therefore, we recommend that all active calls are ended before the AP is taken down.

Step 3 See the U-APSD status for a particular client by entering this command:
show client detail *client_mac*

Step 4 See the TSM statistics for a particular client and the access point to which this client is associated by entering this command:
show client tsm {**802.11a** | **802.11b**} *client_mac* {*ap_mac* | **all**}

The optional **all** command shows all access points to which this client has associated. Information similar to the following appears:

```
Client Interface Mac:              00:01:02:03:04:05
```

```
Measurement Duration:               90 seconds

  Timestamp                           1st Jan 2006, 06:35:80
    UpLink Stats
    ================
       Average Delay (5sec intervals).........................35
       Delay less than 10 ms..................................20
       Delay bet 10 - 20 ms...................................20
       Delay bet 20 - 40 ms...................................20
       Delay greater than 40 ms...............................20
      Total packet Count......................................80
      Total packet lost count (5sec)..........................10
      Maximum Lost Packet count(5sec).........................5
      Average Lost Packet count(5secs)........................2
    DownLink Stats
    ================
       Average Delay (5sec intervals).........................35
       Delay less than 10 ms..................................20
       Delay bet 10 - 20 ms...................................20
       Delay bet 20 - 40 ms...................................20
       Delay greater than 40 ms...............................20
      Total packet Count......................................80
      Total packet lost count (5sec)..........................10
      Maximum Lost Packet count(5sec).........................5
      Average Lost Packet count(5secs)........................2
```

Note The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Note Clear the TSM statistics for a particular access point or all the access points to which this client is associated by entering this **clear client tsm** {**802.11a** | **802.11b**} *client_mac* {*ap_mac* | **all**} command.

Step 5 See the TSM statistics for a particular access point and a particular client associated to this access point by entering this command:
show ap stats {**802.11a** | **802.11b**} *ap_name* **tsm** {*client_mac* | **all**}

The optional **all** command shows all clients associated to this access point. Information similar to the following appears:

```
AP Interface Mac:                   00:0b:85:01:02:03
Client Interface Mac:               00:01:02:03:04:05
Measurement Duration:               90 seconds

  Timestamp                           1st Jan 2006, 06:35:80
    UpLink Stats
    ================
       Average Delay (5sec intervals).........................35
       Delay less than 10 ms..................................20
       Delay bet 10 - 20 ms...................................20
       Delay bet 20 - 40 ms...................................20
       Delay greater than 40 ms...............................20
      Total packet Count......................................80
      Total packet lost count (5sec)..........................10
      Maximum Lost Packet count(5sec).........................5
      Average Lost Packet count(5secs)........................2
    DownLink Stats
```

```
================
   Average Delay (5sec intervals).............................35
   Delay less than 10 ms......................................20
   Delay bet 10 - 20 ms.......................................20
   Delay bet 20 - 40 ms.......................................20
   Delay greater than 40 ms...................................20
  Total packet Count..........................................80
  Total packet lost count (5sec).............................10
  Maximum Lost Packet count(5sec)............................5
  Average Lost Packet count(5secs)...........................2
```

Note The statistics are shown in 90-second intervals. The timestamp text box shows the specific interval when the statistics were collected.

Step 6 Enable or disable debugging for call admission control (CAC) messages, events, or packets by entering this command: **debug cac** {**all** | **event** | **packet**} {**enable** | **disable**}

where **all** configures debugging for all CAC messages, **event** configures debugging for all CAC events, and **packet** configures debugging for all CAC packets.

Step 7 Use the following command to perform voice diagnostics and to view the debug messages between a maximum of two 802.11 clients:
debug voice-diag {**enable** | **disable**} *mac-id mac-id2* [**verbose**]

The verbose mode is an optional argument. When the verbose option is used, all debug messages are displayed in the console. You can use this command to monitor a maximum of two 802.11 clients. If one of the clients is a non-WiFi client, only the 802.11 client is monitored for debug messages.

Note It is implicitly assumed that the clients being monitored are on call.

Note The debug command automatically stops after 60 minutes.

Step 8 Use the following commands to view various voice-related parameters:

- **show client voice-diag status**

  Displays information about whether voice diagnostics is enabled or disabled. If enabled, will also displays information about the clients in the watch list and the time remaining for the diagnostics of the voice call.

  If voice diagnostics is disabled when the following commands are entered, a message indicating that voice diagnostics is disabled appears.

- **show client voice-diag tspec**

  Displays the TSPEC information sent from the clients that are enabled for voice diagnostics.

- **show client voice-diag qos-map**

  Displays information about the QoS/DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed.

- **show client voice-diag avrg_rssi**

  Display the client's RSSI values in the last 5 seconds when voice diagnostics is enabled.

- **show client voice-diag roam-history**

  Displays information about the last three roaming calls. The output contains the timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, the reason for the roaming-failure.

- **show client calls {active | rejected} {802.11a | 802.11bg | all}**

  This command lists the details of active TSPEC and SIP calls on the controller.

Step 9 Use the following commands to troubleshoot video debug messages and statistics:

- **debug ap show stats {802.11b | 802.11a}** *ap-name* **multicast—**Displays the access point's supported multicast rates.
- **debug ap show stats {802.11b | 802.11a}** *ap-name* **load—**Displays the access point's QBSS and other statistics.
- **debug ap show stats {802.11b | 802.11a}** *ap-name* **tx-queue—**Displays the access point's transmit queue traffic statistics.
- **debug ap show stats {802.11b | 802.11a}** *ap-name* **client** {**all** | **video** | *client-mac*}**—**Displays the access point's client metrics.
- **debug ap show stats {802.11b | 802.11a}** *ap-name packet***—**Displays the access point's packet statistics.
- **debug ap show stats {802.11b | 802.11a}** *ap-name* **video metrics—**Displays the access point's video metrics.
- **debug ap show stats video** *ap-name* **multicast mgid** *number* **—**Displays an access point's Layer 2 MGID database number.
- **debug ap show stats video** *ap-name* **admission—**Displays an access point's admission control statistics.
- **debug ap show stats video** *ap-name* **bandwidth—**Displays an access point's video bandwidth.

Configuring SIP-Based CAC

Restrictions for SIP-Based CAC

- SIPs are available only on the Cisco 5500 Series Controllers, Cisco 8500 Series Controllers, and on the 1240, 1130, and 11n access points.
- SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
- SIP CAC will be supported only if SIP snooping is enabled.

Configuring SIP-Based CAC (GUI)

Before You Begin

- Ensure that you have set the voice to the platinum QoS level.
- Ensure that you have enabled call snooping for the WLAN.

- Ensure that you have enabled the Admission Control (ACM) for this radio.

Step 1 Choose **Wireless** > **Advanced** > **SIP Snooping** to open the SIP Snooping page.

Step 2 Specify the call-snooping ports by entering the starting port and the ending port.

Step 3 Click **Apply** and then click **Save Configuration**.

Configuring SIP-Based CAC (CLI)

Step 1 Set the voice to the platinum QoS level by entering this command:
config wlan qos *wlan-id* **Platinum**

Step 2 Enable the call-snooping feature for a particular WLAN by entering this command:
config wlan call-snoop enable *wlan-id*

Step 3 Enable the ACM to this radio by entering this command:
config {**802.11a** | **802.11b**} **cac** {**voice** | **video**} **acm enable**

Step 4 To configure the call snooping ports, enter this command:
config advanced sip-snooping-ports *starting-port ending-port*

Step 5 To troubleshoot SIP-based CAC events, enter this command:
debug sip event {**enable** | **disable**}

Configuring Media Parameters

Configuring Media Parameters (GUI)

Step 1 Ensure that the WLAN is configured for WMM and the Gold QoS level.

Step 2 Disable all WLANs with WMM enabled and click **Apply**.

Step 3 Choose **Wireless** and then **Network** under 802.11a/n or 802.11b/g/n, unselect the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to disable the radio network.

Step 4 Choose **Wireless** > **802.11a/n** or **802.11b/g/n** > **Media**. The 802.11a (or 802.11b) > Media > Parameters page appears.

Step 5 Choose the **Media** tab to open the Media page.

Step 6 Select the **Unicast Video Redirect** check box to enable Unicast Video Redirect. The default value is disabled.

Step 7 In the **Maximum Media Bandwidth (0-85%)** text box, enter the percentage of the maximum bandwidth to be allocated for media applications on this radio band. Once the client reaches the specified value, the access point rejects new calls on this radio band.
The default value is 85%; valid values are from 0 to 85%.

Step 8 In the **Client Phy Rate** text box, enter the value for the rate in kilobits per second at which the client operates.

Step 9 In the **Maximum Retry Percent (0-100%)** text box, enter the percentage of the maximum retry. The default value is 80.

Step 10 Select the **Multicast Direct Enable** check box to enable the **Multicast Direct Enable** text box. The default value is enabled.

Step 11 From the **Max Streams per Radio** drop-down list, choose the maximum number of allowed multicast direct streams per radio. Choose a value between 1 to 20 or No Limit. The default value is set to No Limit.

Step 12 From the **Max Streams per Client** drop-down list, choose the maximum number of allowed clients per radio. Choose a value between 1 to 20 or No Limit. The default value is set to No Limit.

Step 13 If you want to enable the best radio queue for this radio, select the **Best Effort QoS Admission** check box. The default value is disabled.

Configuring Voice Prioritization Using Preferred Call Numbers

Information About Configuring Voice Prioritization Using Preferred Call Numbers

You can configure a controller to support calls from clients that do not support TSPEC-based calls. This feature is known as voice prioritization. These calls are given priority over other clients utilizing the voice pool. Voice prioritization is available only for SIP-based calls and not for TSPEC-based calls. If the bandwidth is available, it takes the normal flow and allocates the bandwidth to those calls.

You can configure up to six preferred call numbers. When a call comes to one of the configured preferred numbers, the controller does not check on the maximum call limit. It invokes the CAC to allocate bandwidth for the preferred call. The bandwidth allocation is 85 percent of the entire bandwidth pool, not just from the maximum configured voice pool. The bandwidth allocation is the same even for roaming calls.

Prerequisites for Configuring Voice Prioritization Using Preferred Call Numbers

You must configure the following before configuring voice prioritization:

- Set WLAN QoS to platinum.
- Enable ACM for the radio.
- Enable SIP call snooping on the WLAN.

Configuring a Preferred Call Number (GUI)

Step 1 Set the WLAN QoS profile to Platinum.

Step 2 Enable ACM for the WLAN radio.

Step 3 Enable SIP call snooping for the WLAN.

Step 4 Choose **Wireless > Advanced > Preferred Call** to open the Preferred Call page.
All calls configured on the controller appear.

Note To remove a preferred call, hover your cursor over the blue drop-down arrow and choose **Remove**.

Step 5 Click **Add Number** to add a new preferred call.

Step 6 In the Call Index text box, enter the index that you want to assign to the call. Valid values are from 1 through 6.

Step 7 In the Call Number text box, enter the number.

Step 8 Click **Apply** to add the new number.

Configuring a Preferred Call Number (CLI)

Step 1 Set the voice to the platinum QoS level by entering this command:
config wlan qos wlan-id Platinum

Step 2 Enable the ACM to this radio by entering this command:
config {802.11a | 802.11b} cac {voice | video} acm enable

Step 3 Enable the call-snooping feature for a particular WLAN by entering this command:
config wlan call-snoop enable *wlan-id*

Step 4 Add a new preferred call by entering this command:
config advanced sip-preferred-call-no *call_index* {*call_number* | **none**}

Step 5 Remove a preferred call by entering this command:
config advanced sip-preferred-call-no *call_index* **none**

Step 6 View the preferred call statistics by entering the following command:
show ap stats {802.11{a | b} | wlan} *ap_name*

Step 7 Enter the following command to list the preferred call numbers:
show advanced sip-preferred-call-no

Configuring EDCA Parameters

Information About EDCA Parameters

Enhanced distributed channel access (EDCA) parameters are designed to provide preferential wireless channel access for voice, video, and other quality-of-service (QoS) traffic.

Configuring EDCA Parameters (GUI)

Step 1 Choose **Wireless** and then **Network** under 802.11a/n or 802.11b/g/n, unselect the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply** to disable the radio network.

Step 2 Choose **EDCA Parameters**under 802.11a/n or 802.11b/g/n. The 802.11a (or 802.11b/g) > EDCA Parameters page appears.

Step 3 Choose one of the following options from the **EDCA Profile** drop-down list:

- **WMM—**Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option when voice or video services are not deployed on your network.
- **Spectralink Voice Priority—**Enables SpectraLink voice priority parameters. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.
- **Voice Optimized—**Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than SpectraLink are deployed on your network.
- **Voice & Video Optimized—**Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.
- **Custom Voice—**Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied.

  Note If you deploy video services, admission control (ACM) must be disabled.

Step 4 If you want to enable MAC optimization for voice, select the **Enable Low Latency MAC** check box. Otherwise, leave this check box unselected, which is the default value. This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, which improves the number of voice calls serviced per access point.

Note We do not recommend you to enable low latency MAC. You should enable low latency MAC only if the WLAN allows WMM clients. If WMM is enabled, then low latency MAC can be used with any of the EDCA profiles.

Step 5 Click **Apply** to commit your changes.

Step 6 To reenable the radio network, choose **Network** under 802.11a/n or 802.11b/g/n, select the **802.11a** (or **802.11b/g**) **Network Status** check box, and click **Apply**.

Step 7 Click **Save Configuration**.

Configuring EDCA Parameters (CLI)

Step 1 Disable the radio network by entering this command:
config {**802.11a** | **802.11b**} **disable network**

Step 2 Save your settings by entering this command:
save config

Step 3 Enable a specific EDCA profile by entering this command:
config advanced {802.11a | 802.11b} edca-parameters {wmm-default | svp-voice| optimized-voice| optimzed-voice-video| custom-voice}

- wmm-default—Enables the Wi-Fi Multimedia (WMM) default parameters. This is the default value. Choose this option when voice or video services are not deployed on your network.
- svp-voice—Enables SpectraLink voice priority parameters. Choose this option if SpectraLink phones are deployed on your network to improve the quality of calls.
- optimized-voice—Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than SpectraLink are deployed on your network.
- optimized-video-voice—Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.
- custom-voice—Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied.

  Note If you deploy video services, admission control (ACM) must be disabled.

Step 4 View the current status of MAC optimization for voice by entering this command:
show {**802.11a** | **802.11b**}

Information similar to the following appears:

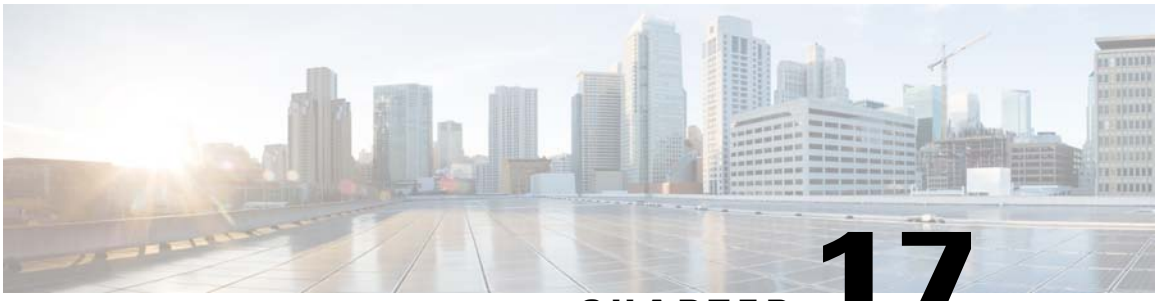
```
Voice-mac-optimization.................Disabled
```

Step 5 Enable or disable MAC optimization for voice by entering this command:
config advanced {**802.11a** | **802.11b**} **voice-mac-optimization** {**enable** | **disable**}

This feature enhances voice performance by controlling packet retransmits and appropriately aging out voice packets on lightweight access points, which improves the number of voice calls serviced per access point. The default value is disabled.

Step 6 Reenable the radio network by entering this command:
config {**802.11a** | **802.11b**} **enable network**

Step 7 Enter the **save config** command to save your settings.



CHAPTER 17

Configuring the Cisco Discovery Protocol

Information About Configuring the Cisco Discovery Protocol

The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco-manufactured equipment. A device enabled with CDP sends out periodic interface updates to a multicast address in order to make itself known to neighboring devices.

The default value for the frequency of periodic transmissions is 60 seconds, and the default advertised time-to-live value is 180 seconds. The second and latest version of the protocol, CDPv2, introduces new time-length-values (TLVs) and provides a reporting mechanism that allows for more rapid error tracking, which reduces downtime.

Note Cisco recommends that you disable Cisco Discovery Protocol on the controller and access point when connected to non-Cisco switches as CDP is unsupported on non-Cisco switches and network elements.

Restrictions for Configuring the Cisco Discovery Protocol

- CDPv1 and CDPv2 are supported on the following devices:
  - Cisco 5500 and 2500 Series Controllers
  - CAPWAP-enabled access points
  - An access point connected directly to a Cisco 5500 Series Controller

Note To use the Intelligent Power Management feature, ensure that CDPv2 is enabled on the Cisco 2500 Series Controllers. CDP v2 is enabled by default.

- The Cisco 600 Series OEAP access points do not support CDP.
- The support of CDPv1 and CDPv2 enables network management applications to discover Cisco devices.
- The following TLVs are supported by both the controller and the access point:
  - Device-ID TLV: 0x0001—The hostname of the controller, the access point, or the CDP neighbor.
  - Address TLV: 0x0002—The IP address of the controller, the access point, or the CDP neighbor.
  - Port-ID TLV: 0x0003—The name of the interface on which CDP packets are sent out.
  - Capabilities TLV: 0x0004—The capabilities of the device. The controller sends out this TLV with a value of Host: 0x10, and the access point sends out this TLV with a value of Transparent Bridge: 0x02.
  - Version TLV: 0x0005—The software version of the controller, the access point, or the CDP neighbor.
  - Platform TLV: 0x0006—The hardware platform of the controller, the access point, or the CDP neighbor.
  - Power Available TLV: 0x001a— The amount of power available to be transmitted by power sourcing equipment to permit a device to negotiate and select an appropriate power setting.
  - Full/Half Duplex TLV: 0x000b—The full- or half-duplex mode of the Ethernet link on which CDP packets are sent out.
- These TLVs are supported only by the access point:
  - Power Consumption TLV: 0x0010—The maximum amount of power consumed by the access point.
  - Power Request TLV:0x0019—The amount of power to be transmitted by a powerable device in order to negotiate a suitable power level with the supplier of the network power.
- Changing the CDP configuration on the controller does not change the CDP configuration on the access points that are connected to the controller. You must enable and disable CDP separately for each access point.
- You can enable or disable the CDP state on all or specific interfaces and radios. This configuration can be applied to all access points or a specific access point.
- The following is the behavior assumed for various interfaces and access points:
  - CDP is disabled on radio interfaces on indoor (nonindoor mesh) access points.
  - Nonmesh access points have CDPs disabled on radio interfaces when they join the controller. The persistent CDP configuration is used for the APs that had CDP support in its previous image.
  - CDP is enabled on radio interfaces on indoor-mesh and mesh access points.

- Mesh access points will have CDP enabled on their radio interfaces when they join the controller. The persistent CDP configuration is used for the access points that had CDP support in a previous image. The CDP configuration for radio interfaces is applicable only for mesh APs.

Configuring the Cisco Discovery Protocol

Configuring the Cisco Discovery Protocol (GUI)

Step 1 Choose **Controller** > **CDP** > **Global Configuration** to open the CDP > Global Configuration page.

Step 2 Select the **CDP Protocol Status** check box to enable CDP on the controller or unselect it to disable this feature. The default value is selected.

Note Enabling or disabling this feature is applicable to all controller ports.

Step 3 From the CDP Advertisement Version drop-down list, choose **v1** or **v2** to specify the highest CDP version supported on the controller. The default value is v1.

Step 4 In the Refresh-time Interval text box, enter the interval at which CDP messages are to be generated. The range is 5 to 254 seconds, and the default value is 60 seconds.

Step 5 In the Holdtime text box, enter the amount of time to be advertised as the time-to-live value in generated CDP packets. The range is 10 to 255 seconds, and the default value is 180 seconds.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your changes.

Step 8 Perform one of the following:

- To enable or disable CDP on a specific access point, follow these steps:

  Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

  Click the link for the desired access point.

  Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

  Select the **Cisco Discovery Protocol** check box to enable CDP on this access point or unselect it to disable this feature. The default value is enabled.

  Note If CDP is disabled in Step 2, a message indicating that the Controller CDP is disabled appears.

- Enable CDP for a specific Ethernet interface, radio, or slot as follows:

  Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

  Click the link for the desired access point.

  Choose the **Interfaces** tab and select the corresponding check boxes for the radios or slots from the CDP Configuration section.

  Note Configuration for radios is only applicable for mesh access points.

  Click **Apply** to commit your changes.

- To enable or disable CDP on all access points currently associated to the controller, follow these steps:

  Choose **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page.

  Select the **CDP State** check box to enable CDP on all access points associated to the controller or unselect it to disable CDP on all access points. The default value is selected. You can enable CDP on a specific Ethernet interface, radio, or slot by selecting the corresponding check box. This configuration will be applied to all access points associated with the controller.

  Click **Apply** to commit your changes.

Step 9 Click **Save Configuration** to save your changes.

Configuring the Cisco Discovery Protocol (CLI)

Step 1 Enable or disable CDP on the controller by entering this command:
config cdp {**enable** | **disable**}

CDP is enabled by default.

Step 2 Specify the interval at which CDP messages are to be generated by entering this command:
config cdp timer *seconds*

The range is 5 to 254 seconds, and the default value is 60 seconds.

Step 3 Specify the amount of time to be advertised as the time-to-live value in generated CDP packets by entering this command:
config cdp holdtime *seconds*

The range is 10 to 255 seconds, and the default value is 180 seconds.

Step 4 Specify the highest CDP version supported on the controller by entering this command:
config cdp advertise {**v1** | **v2**}

The default value is v1.

Step 5 Enable or disable CDP on all access points that are joined to the controller by entering the **config ap cdp** {**enable** | **disable**} **all** command.
The **config ap cdp disable all** command disables CDP on all access points that are joined to the controller and all access points that join in the future. CDP remains disabled on both current and future access points even after the controller or access point reboots. To enable CDP, enter the **config ap cdp enable all** command.

Note After you enable CDP on all access points joined to the controller, you may disable and then reenable CDP on individual access points using the command in Step 6. After you disable CDP on all access points joined to the controller, you may not enable and then disable CDP on individual access points.

Step 6 Enable or disable CDP on a specific access point by entering this command:
config ap cdp {**enable** | **disable**} *Cisco_AP*

Step 7 Configure CDP on a specific or all access points for a specific interface by entering this command:
config ap cdp {ethernet | radio} *interface_number slot_id* **{enable** | **disable} {all |** *Cisco_AP***}**

Note When you use the config ap cdp command to configure CDP on radio interfaces, a warning message appears indicating that the configuration is applicable only for mesh access points.

Step 8 Save your changes by entering this command:
save config

Viewing Cisco Discovery Protocol Information

Viewing Cisco Discovery Protocol Information (GUI)

Step 1 Choose **Monitor** > **CDP** > **Interface Neighbors** to open the CDP > Interface Neighbors page appears.
This page shows the following information:

- The controller port on which the CDP packets were received
- The name of each CDP neighbor
- The IP address of each CDP neighbor
- The port used by each CDP neighbor for transmitting CDP packets
- The time left (in seconds) before each CDP neighbor entry expires
- The functional capability of each CDP neighbor, defined as follows: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, or M - Remotely Managed Device
- The hardware platform of each CDP neighbor device

Step 2 Click the name of the desired interface neighbor to see more detailed information about each interface's CDP neighbor.
The CDP > Interface Neighbors > Detail page appears.
This page shows the following information:

- The controller port on which the CDP packets were received
- The name of the CDP neighbor
- The IP address of the CDP neighbor
- The port used by the CDP neighbor for transmitting CDP packets
- The CDP version being advertised (v1 or v2)
- The time left (in seconds) before the CDP neighbor entry expires
- The functional capability of the CDP neighbor, defined as follows: Router, Trans Bridge,?Source Route Bridge, Switch, Host, IGMP, Repeater, or Remotely Managed Device
- The hardware platform of the CDP neighbor device
- The software running on the CDP neighbor

Step 3 Choose **AP Neighbors** to see a list of CDP neighbors for all access points connected to the controller. The CDP AP Neighbors page appears.

Step 4 Click the **CDP Neighbors** link for the desired access point to see a list of CDP neighbors for a specific access point. The CDP > AP Neighbors page appears.
This page shows the following information:

- The name of each access point
- The IP address of each access point
- The name of each CDP neighbor
- The IP address of each CDP neighbor
- The port used by each CDP neighbor
- The CDP version being advertised (v1 or v2)

Step 5 Click the name of the desired access point to see detailed information about an access point's CDP neighbors. The CDP > AP Neighbors > Detail page appears.
This page shows the following information:

- The name of the access point
- The MAC address of the access point's radio
- The IP address of the access point
- The interface on which the CDP packets were received
- The name of the CDP neighbor
- The IP address of the CDP neighbor
- The port used by the CDP neighbor
- The CDP version being advertised (v1 or v2)
- The time left (in seconds) before the CDP neighbor entry expires
- The functional capability of the CDP neighbor, defined as follows: R - Router, T - Trans Bridge,?B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, or M - Remotely Managed Device
- The hardware platform of the CDP neighbor device
- The software running on the CDP neighbor

Step 6 Choose **Traffic Metrics** to see CDP traffic information. The CDP > Traffic Metrics page appears.
This page shows the following information:

- The number of CDP packets received by the controller
- The number of CDP packets sent from the controller
- The number of packets that experienced a checksum error
- The number of packets dropped due to insufficient memory
- The number of invalid packets

Viewing Cisco Discovery Protocol Information (CLI)

Step 1 See the status of CDP and to view CDP protocol information by entering this command:
show cdp

Step 2 See a list of all CDP neighbors on all interfaces by entering this command:
show cdp neighbors [detail]

The optional detail command provides detailed information for the controller's CDP neighbors.

Note This command shows only the CDP neighbors of the controller. It does not show the CDP neighbors of the controller's associated access points. Additional commands are provided below to show the list of CDP neighbors per access point.

Step 3 See all CDP entries in the database by entering this command:
show cdp entry all

Step 4 See CDP traffic information on a given port (for example, packets sent and received, CRC errors, and so on) by entering this command:
show cdp traffic

Step 5 See the CDP status for a specific access point by entering this command:
show ap cdp ap-name *Cisco_AP*

Step 6 See the CDP status for all access points that are connected to the controller by entering this command:
show ap cdp all

Step 7 See a list of all CDP neighbors for a specific access point by entering these commands:

- **show ap cdp neighbors ap-name** *Cisco_AP*
- **show ap cdp neighbors detail** *Cisco_AP*

Note The access point sends CDP neighbor information to the controller only when the information changes.

Step 8 See a list of all CDP neighbors for all access points connected to the controller by entering these commands:

- **show ap cdp neighbors all**
- **show ap cdp neighbors detail all**

Note The access point sends CDP neighbor information to the controller only when the information changes.

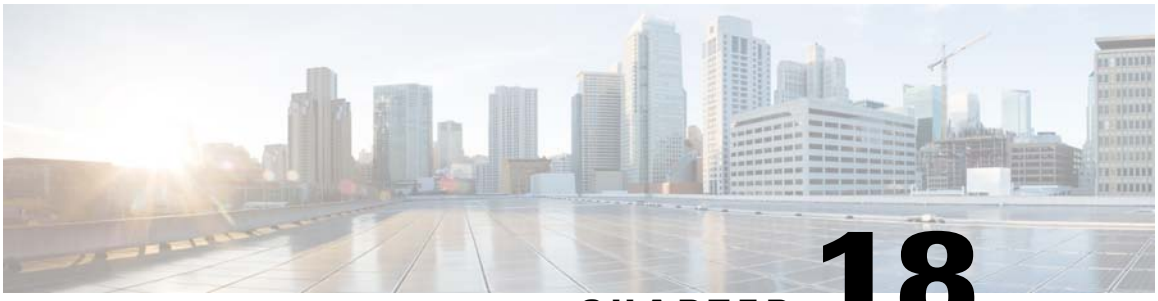
Getting CDP Debug Information

- Get debug information related to CDP packets by entering by entering this command:

debug cdp packets

- Get debug information related to CDP events by entering this command:

  debug cdp events



CHAPTER 18

Configuring Authentication for the Controller and NTP Server

Information About Configuring Authentication for the Controller and NTP Server

Starting in release 7.0.116.0, the controller software is now compliant with RFC 1305. As per this requirement, controllers must synonymize time with an NTP server by authentication. By default, an MD5 checksum is used.

Configuring the NTP Server for Authentication (GUI)

Step 1 Choose **Controller** > **NTP** > **Server** to open the NTP Severs page.

Step 2 Click **New** to add a new NTP Server.

Step 3 In the Server Index (Priority) text box, enter the NTP server index.
The controller tries Index 1 first, then Index 2 through 3, in a descending order. Set this to 1 if your network is using only one NTP server.

Step 4 Enter the server IP address.

Step 5 Enable or disable the NTP Authentication.

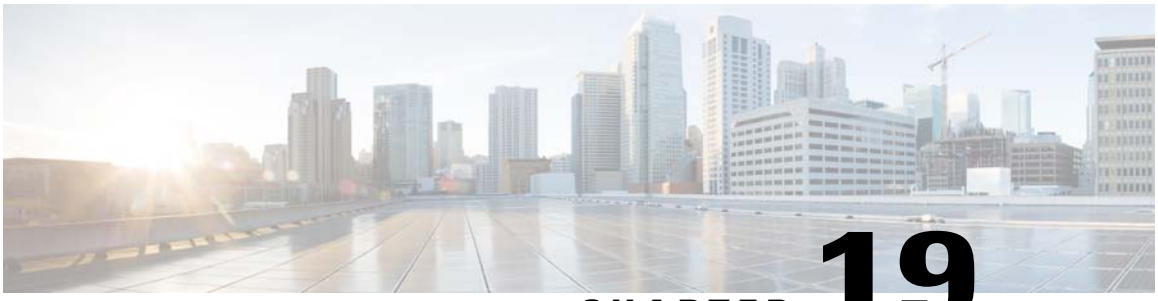
Step 6 If you enable the NTP Authentication, enter the Key Index.

Step 7 Click **Apply**.

Configuring the NTP Server for Authentication (CLI)

Before You Begin

- **config time ntp auth enable** *server-index key-index*—Enables NTP authentication on a given NTP server.
- **config time ntp key-auth add** *key-index* **md5** *key-format key*—Adds an authentication key. By default MD5 is used. The key format can be "ascii" or "hex".
- **config time ntp key-auth delete** *key-index*—Deletes authentication keys.
- **config time ntp auth disable** *server-index*—Disables NTP authentication.
- **show ntp-keys**—Displays the NTP authentication related parameter.



CHAPTER 19

Configuring RFID Tag Tracking

Information About Configuring RFID Tag Tracking

The controller enables you to configure radio-frequency identification (RFID) tag tracking. RFID tags are small wireless devices that are affixed to assets for real-time location tracking. They operate by advertising their location using special 802.11 packets, which are processed by access points, the controller, and the mobility services engine.

To know more about the tags supported by controller, see http://www.cisco.com/web/partners/pr46/pr147/ccx_wifi_tags.html. The mobility services engine receives telemetry and chokepoint information from tags that are compliant with this CCX specification.

Table 5: Cisco Compatible Extensions for RFID Tags Summary

Partners	**AeroScout**		**WhereNet**	**Pango (InnerWireless)**
Product Name	T2	T3	Wheretag IV	V3
Telemetry				
Temperature	X	X	—	X
Pressure	—	—	—	—
Humidity	—	—	—	—
Status	—	—	—	—
Fuel	—	—	—	—

Partners	AeroScout		WhereNet	Pango (InnerWireless)
Quantity	—	—	—	—
Distance	—	—	—	—
Motion Detection	X	X	—	X
Number of Panic Buttons	1	2	0	1
Tampering		X	X	X
Battery Information	X	X	X	X
Multiple-Frequency Tags[3]	X	X	X	

[3] For chokepoint systems, note that the tag can work only with chokepoints coming from the same vendor.

Note The Network Mobility Services Protocol (NMSP) runs on the mobility services engine. For NMSP to function, the TCP port (16113) over which the controller and the mobility services engine communicate must be open (not blocked) on any firewall that exists between these two devices.

The Cisco-approved tags support these capabilities:

- **Information notifications—**Enables you to view vendor-specific and emergency information.
- **Information polling—**Enables you to monitor battery status and telemetry data. Many telemetry data types provide support for sensory networks and a large range of applications for RFID tags.
- **Measurement notifications—**Enables you to deploy chokepoints at strategic points within your buildings or campuses. Whenever an RFID tag moves to within a defined proximity of a chokepoint, the tag begins transmitting packets that advertise its location in relation to the chokepoint.

You can configure and view RFID tag tracking information through the controller CLI.

Configuring RFID Tag Tracking (CLI)

Step 1 Enable or disable RFID tag tracking by entering this command:
config rfid status {**enable** | **disable**}

The default value is enabled.

Step 2 Specify a static timeout value (between 60 and 7200 seconds) by entering this command:
config rfid timeout *seconds*

The static timeout value is the amount of time that the controller maintains tags before expiring them. For example, if a tag is configured to beacon every 30 seconds, we recommend that you set the timeout value to 90 seconds (approximately three times the beacon value). The default value is 1200 seconds.

Step 3 Enable or disable RFID tag mobility for specific tags by entering these commands:

- **config rfid mobility** *vendor_name* **enable—**Enables client mobility for a specific vendor's tags. When you enter this command, tags are unable to obtain a DHCP address for client mode when attempting to select and/or download a configuration.
- **config rfid mobility** *vendor_name* **disable—**Disables client mobility for a specific vendor's tags. When you enter this command, tags can obtain a DHCP address. If a tag roams from one subnet to another, it obtains a new address rather than retaining the anchor state.

Note These commands can be used only for Pango tags. Therefore, the only valid entry for *vendor_name* is "pango" in all lowercase letters.

Viewing RFID Tag Tracking Information (CLI)

Step 1 See the current configuration for RFID tag tracking by entering this command:
show rfid config

Step 2 See detailed information for a specific RFID tag by entering this command:
show rfid detail *mac_address*

where *mac_address* is the tag's MAC address.

Step 3 See a list of all RFID tags currently connected to the controller by entering this command:
show rfid summary

Step 4 See a list of RFID tags that are associated to the controller as clients by entering this command:
show rfid client

Debugging RFID Tag Tracking Issues (CLI)

If you experience any problems with RFID tag tracking, use these debug commands.

- Configure MAC address debugging by entering this command:

  debug mac addr *mac_address*

Note We recommend that you perform the debugging on a per-tag basis. If you enable debugging for all of the tags, the console or Telnet screen is inundated with messages.

- Enable or disable debugging for the 802.11 RFID tag module by entering this command:

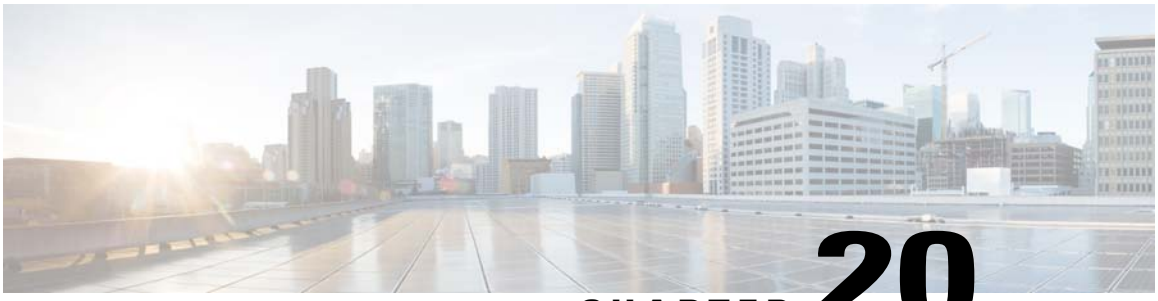
  debug dot11 rfid {**enable** | **disable**}

- Enable or disable RFID debug options by entering this command:

  debug rfid {**all** | **detail** | **error** | **nmsp** | **receive**} {**enable** | **disable**}

  where

  - **all** configures debugging of all RFID messages.
  - **detail** configures debugging of RFID detailed messages.
  - **error** configures debugging of RFID error messages.
  - **nmsp** configures debugging of RFID NMSP messages.
  - **receive** configures debugging of incoming RFID tag messages.



CHAPTER 20

Resetting the Controller to Default Settings

Information About Resetting the Controller to Default Settings

You can return the controller to its original configuration by resetting the controller to factory-default settings.

Resetting the Controller to Default Settings (GUI)

Step 1 Start your Internet browser.

Step 2 Enter the controller IP address in the browser address line and press **Enter**. An Enter Network Password dialog box appears.

Step 3 Enter your username in the User Name text box. The default username is *admin*.

Step 4 Enter the wireless device password in the Password text box and press **Enter**. The default password is *admin*.

Step 5 Choose **Commands** > **Reset to Factory Default**.

Step 6 Click **Reset**.

Step 7 When prompted, confirm the reset.

Step 8 Reboot the controller without saving the configuration.

Step 9 Use the configuration wizard to enter configuration settings. See the Configuring the Controller—Using the CLI Configuration Wizard section for more information.

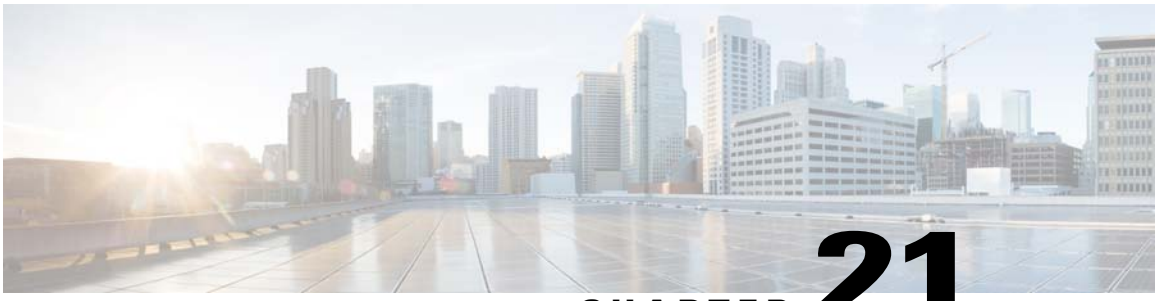
Resetting the Controller to Default Settings (CLI)

Step 1 Enter the **reset system** command. At the prompt that asks whether you need to save changes to the configuration, enter **N**. The unit reboots.

Step 2 When you are prompted for a username, enter the **recover-config** command to restore the factory-default configuration. The controller reboots and displays this message:

```
Welcome to the Cisco WLAN Solution Wizard Configuration Tool
```

Step 3 Use the configuration wizard to enter configuration settings. See the Configuring the Controller—Using the CLI Configuration Wizard section for more information.



CHAPTER 21

Managing Controller Software and Configurations

Upgrading the Controller Software

When you upgrade the controller software, the software on the access points associated with the controller is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession. Up to 10 access points can be concurrently upgraded from the controller.

Caution Do not power down the controller or any access point during this process; otherwise, you might corrupt the software image. Upgrading a controller with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent access point upgrades supported in the controller software release, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.

Restrictions for Upgrading Controller Software

- If you require a downgrade from one release to another, you might lose the configuration from your current release. The workaround is to reload the previous controller configuration files saved on the backup server or to reconfigure the controller.
- It is not possible to directly upgrade to this release from a release that is older than 6.0.182.0.

- You can upgrade or downgrade the controller software only between certain releases. In some instances, you must first install an intermediate release prior to upgrading to the latest software release.
- When you upgrade the controller to an intermediate software release, you must wait until all of the access points that are associated with the controller are upgraded to the intermediate release before you install the latest controller software. In large networks, it can take some time to download the software on each access point.
- When you upgrade to the latest software release, the software on the access points associated with the controller is also automatically upgraded. When an access point is loading software, each of its LEDs blinks in succession.
- We recommend that you access the controller GUI using Microsoft Internet Explorer 6.0 SP1 (or a later release) or Mozilla Firefox 2.0.0.11 (or a later release).
- Cisco controllers support standard SNMP Management Information Base (MIB) files. MIBs can be downloaded from the Software Center on Cisco.com.
- The controller software is factory installed on your controller and automatically downloaded to the access points after a release upgrade and whenever an access point joins a controller. We recommend that you install the latest software version available for maximum operational benefit.
- We recommend that you install Wireless LAN Controller Field Upgrade Software for Release 1.7.0.0-FUS, which is a special AES package that contains several system-related component upgrades. These include the bootloader, field recovery image, and FPGA/MCU firmware. Installing the FUS image requires special attention because it installs some critical firmware. The FUS image is independent of the runtime image. For more information, see http://www.cisco.com/en/US/docs/wireless/controller/release/notes/fus_rn_1_7_0_0.html.
- Ensure that you have a TFTP or FTP server available for the software upgrade. Follow these guidelines when setting up a TFTP or FTP server:
  - Ensure that your TFTP server supports files that are larger than the size of the controller software release. Some TFTP servers that support files of this size are tftpd32 and the TFTP server within the Cisco Prime Infrastructure. If you attempt to download the controller software and your TFTP server does not support files of this size, the following error message appears: “TFTP failure while storing in flash.”
  - If you are upgrading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable
- When you plug a controller into an AC power source, the bootup script and power-on self-test run to initialize the system. During this time, you can press Esc to display the bootloader Boot Options Menu. The menu options for the 5500 and Flex 7500 series controllers are different than for other controller platforms.

  Bootloader menu for 5500 Series Controllers:

```
Boot Options
Please choose an option from below:
 1. Run primary image
 2. Run backup image
 3. Change active boot image
 4. Clear Configuration
 5. Format FLASH Drive
 6. Manually update images
Please enter your choice:
```

Bootloader menu for other controller platforms:

```
Boot Options
Please choose an option from below:
 1. Run primary image
 2. Run backup image
 3. Manually update images
 4. Change active boot image
 5. Clear Configuration
Please enter your choice:
```

Enter **1** to run the current software, enter **2** to run the previous software, enter **4** (on a 5500 series controller), or enter **5** (on another controller platform) to run the current software and set the controller configuration to factory defaults. Do not choose the other options unless directed to do so.

Note See the Installation Guide or the Quick Start Guide for your controller for more details on running the bootup script and power-on self-test.

- Control which address(es) are sent in CAPWAP discovery responses when NAT is enabled on the Management Interface using the following command:

  config network ap-discovery nat-ip-only {**enable** | **disable**}

  where

  - **enable—**Enables use of NAT IP only in Discovery response. This is the default. Use this command if all APs are outside of the NAT gateway.
  - **disable—**Enables use of both NAT IP and non-NAT IP in discovery response. Use this command if APs are on the inside and outside of the NAT gateway; for example, Local Mode and OfficeExtend APs on the same controller.

  Note To avoid stranding APs, you must disable AP link-latency (if enabled) before you use the disable option for the **config network ap-discovery nat-ip-only** command. To disable AP link-latency, use the **config ap link-latency disable all** command.

- You can configure 802.1p tagging by using the **config qos dot1p-tag** {**bronze** | **silver** | **gold** | **platinum**} tag. For the 7.2.103.0 and later releases, if you tag 802.1p packets, the tagging has impact only on wired packets. Wireless packets are impacted only by the maximum priority level set for QoS.
- You can reduce the network downtime using the following options:
  - You can predownload the AP image.
  - For FlexConnect access points, use the FlexConnect Efficient AP upgrade feature to reduce traffic between the controller and the AP (main site and the branch).
- Do not power down the controller or any access point during the upgrade process; otherwise, you might corrupt the software image. Upgrading a controller with a large number of access points can take as long as 30 minutes, depending on the size of your network. However, with the increased number of concurrent access point upgrades supported, the upgrade time should be significantly reduced. The access points must remain powered, and the controller must not be reset during this time.
- If you want to downgrade to a previous release, do either of the following:

- Delete all WLANs that are mapped to interface groups and create new ones.
- Ensure that all WLANs are mapped to interfaces rather than interface groups.

- After you perform these functions on the controller, you must reboot the controller for the changes to take effect:
  - Enable or disable link aggregation (LAG)
  - Enable a feature that is dependent on certificates (such as HTTPS and web authentication)
  - Add new or modify existing SNMP v3 users
  - Modify an existing SNMP v3 engine ID
  - Add a new license or modify an existing license
  - Increase the priority for a license

- The controller bootloader stores a copy of the active primary image and the backup image. If the primary image becomes corrupted, you can use the bootloader to boot with the backup image.

  With the backup image stored before rebooting, be sure to choose **Option 2: Run Backup Image** from the boot menu to boot from the backup image. Then, upgrade with a known working image and reboot the controller.

- The recovery image provides a backup image that can be used if an access point power-cycles during an image upgrade. The best way to avoid the need for access point recovery is to prevent an access point from power-cycling during a system upgrade. If a power-cycle occurs during an upgrade to an oversized access point image, you can recover the access point using the TFTP recovery procedure.

  To recover the access point using the TFTP recovery procedure, follow these steps:

  1. Download the required recovery image from Cisco.com (c1100-rcvk9w8-mx, c1200-rcvk9w8-mx, or c1310-rcvk9w8-mx) and install it in the root directory of your TFTP server.
  2. Connect the TFTP server to the same subnet as the target access point and power-cycle the access point. The access point boots from the TFTP image and then joins the controller to download the oversized access point image and complete the upgrade procedure.
  3. After the access point has been recovered, you can remove the TFTP server.

- You can upgrade to a new release of the controller software or downgrade to an older release even if Federal Information Processing Standard (FIPS) is enabled.

Upgrading Controller Software (GUI)

Step 1 Upload your controller configuration files to a server to back them up.

Note We highly recommend that you back up your configuration files of the controller prior to upgrading the controller software. Otherwise, you must manually reconfigure the controller.

Step 2 Get the controller software image by following these steps:

a) Browse to the Cisco Software Center: http://www.cisco.com/cisco/software/navigator.html.

b) Choose **Wireless** > **Wireless LAN Controller**.

The following options are available: Integrated Controllers and Controller Modules and Standalone Controllers.

c) Depending on your controller platform, click one of the above options.
d) Click the controller model number or name. The Download Software page is displayed.
e) Click a controller software release. The software releases are labeled as follows to help you determine which release to download:
Early Deployment (ED)—These software releases provide new features, new hardware platform support, and bug fixes.

Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.

Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.

f) Choose a software release number.
g) Click the filename (*filename*.aes).
h) Click **Download**.
i) Read Cisco's End User Software License Agreement and then click **Agree**.
j) Save the file to your hard drive.
k) Repeat steps *a* through *k* to download the remaining file.

Step 3 Copy the controller software image (*filename*.aes) to the default directory on your TFTP or FTP server.

Step 4 (Optional) Disable the 802.11 networks.

Note For busy networks, controllers on high utilization, or small controller platforms, we recommend that you disable the 802.11 networks as a precautionary measure.

Step 5 Disable any WLANs on the controller.

Step 6 Choose **Commands > Download File** to open the Download File to Controller page.

Step 7 From the **File Type** drop-down list, choose **Code**.

Step 8 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 9 In the **IP Address** text box, enter the IP address of the server.
If you are using a TFTP server, the default values of 10 retries and 6 seconds for the **Maximum Retries** and **Timeout** text boxes should work correctly without any adjustment. However, you can change these values.

Step 10 If you are using a TFTP server, the default values of 10 retries for the Maximum Retries text field, and 6 seconds for the Timeout text field should work correctly without any adjustment. However, you can change these values if desired. To do so, enter the maximum number of times that the TFTP server attempts to download the software in the **Maximum Retries** text box and the amount of time (in seconds) that the TFTP server attempts to download the software in the **Timeout** text box.

Step 11 In the **File Path** text box, enter the directory path of the software.

Step 12 In the **File Name** text box, enter the name of the controller software file (*filename*.aes).

Step 13 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** text box, enter the username to log into the FTP server.
b) In the **Server Login Password** text box, enter the password to log into the FTP server.

c) In the **Server Port Number** text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 14 Click **Download** to download the software to the controller. A message appears indicating the status of the download.

Step 15 After the download is complete, click **Reboot**.

Step 16 If prompted to save your changes, click **Save and Reboot**.

Step 17 Click **OK** to confirm.

Step 18 After the controller reboots, repeat step 6 to step 17 to install the remaining file.

Step 19 Reenable the WLANs.

Step 20 For Cisco WiSM2, reenable the controller port channel on the Catalyst switch.

Step 21 If you have disabled the 802.11 networks in Step 4, reenable them.

Step 22 To verify the controller software version, choose **Monitor** on the controller GUI and see **Software Version** in the Controller Summary area.

Upgrading Controller Software (CLI)

Step 1 Upload your controller configuration files to a server to back them up.

Note We highly recommend that you back up your controller's configuration files prior to upgrading the controller software. Otherwise, you must manually reconfigure the controller.

Step 2 Get the controller software image by following these steps:

a) Browse to the Cisco Software Center: http://www.cisco.com/cisco/software/navigator.html.

b) Choose **Wireless** > **Wireless LAN Controller**.
The following options are available: Integrated Controllers and Controller Modules and Standalone Controllers.

c) Depending on your controller platform, click one of the above options.

d) Click the controller model number or name. The Download Software page is displayed.

e) Click a controller software release. The software releases are labeled as follows to help you determine which release to download:
Early Deployment (ED)—These software releases provide new features, new hardware platform support, and bug fixes.

Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.

Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.

f) Choose a software release number.

g) Click the filename (*filename*.aes).

h) Click **Download**.

i) Read Cisco's End User Software License Agreement and then click **Agree**.

j) Save the file to your hard drive.

k) Repeat steps *a* through *k* to download the remaining file.

Step 3 Copy the controller software image (*filename*.aes) to the default directory on your TFTP or FTP server.

Step 4 (Optional) Disable the 802.11 networks.

Note For busy networks, controllers on high utilization, or small controller platforms, we recommend that you disable the 802.11 networks as a precautionary measure.

Step 5 Disable any WLANs on the controller (using the **config wlan disable** *wlan_id* command).

Step 6 Log onto the controller CLI.

Step 7 Enter the **ping server-ip-address** command to verify that the controller can contact the TFTP or FTP server.

Step 8 View current download settings by entering the transfer download start command. Answer n to the prompt to view the current download settings.

Step 9 Change the download settings, if necessary by entering these commands:

- **transfer download mode** {**tftp** | **ftp** | **sftp**}
- **transfer download datatype code**
- **transfer download serverip server-ip-address**
- **transfer download filename filename**
- **transfer download path server-path-to-file**

  Note Pathnames on a TFTP or FTP server are relative to the server's default or root directory. For example, in the case of the Solaris TFTP server, the path is "/".

If you are using a TFTP server, also enter these commands:

- **transfer download tftpMaxRetries retries**
- **transfer download tftpPktTimeout timeout**

  Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

If you are using an FTP server, also enter these commands:

- **transfer download username username**
- **transfer download password password**
- **transfer download port port**

  Note The default value for the port parameter is 21.

Step 10 View the current updated settings by entering the transfer download start command. Answer y to the prompt to confirm the current download settings and start the software download.

Step 11 Save the code update to nonvolatile NVRAM and reboot the controller by entering this command:
reset system
The controller completes the bootup process.

Step 12 After the controller reboots, repeat Steps 6 through 11 to install the remaining file.

Step 13 Reenable the WLANs by entering this command:
config wlan enable *wlan_id*

Step 14 For Cisco WiSMs, re-enable the controller port channel on the Catalyst switch.

Step 15 If you have disabled the 802.11 networks in Step 4, renable them.

Step 16 To verify the controller software that is installed, enter the **show sysinfo** command and see Product Version.

Step 17 To verify the Cisco Unified Wireless Network Controller Boot Software file that is installed on the controller, enter the **show sysinfo** command on the controller CLI and see Recovery Image Version or Emergency Image Version.

Note If a Cisco Unified Wireless Network Controller Boot Software ER.aes file is not installed, Recovery Image Version or Emergency Image Version show 'N/A.'

Predownloading an Image to an Access Point

To minimize a network outages, you can now download an upgrade image to the access point from the controller without resetting the access point or losing network connectivity. Previously, you would download an upgrade image to the controller and reset it, which causes the access point to go into discovery mode. After the access point discovers the controller with the new image, the access point downloads the new image, resets, goes into discovery mode, and rejoins the controller.

You can now download the upgrade image to the controller and then download the image to the access point while the network is still up. You can also schedule a reboot of the controller and access points, either after a specified amount of time or at a specific date and time. When both devices are up, the access point discovers and rejoins the controller.

Access Point Predownload Process

The access point predownload feature works as follows:

- The controller image is downloaded.
  - The primary image becomes the backup image of the controller and the downloaded image becomes the new primary image. Change the current boot image as the backup image by using the **config boot backup** command to ensure that if a system failure occurs, the controller boots with the last working image of the controller.
  - To switch over to the new downloaded image, start predownload of the upgraded image using the **config ap image predownload primary all** command.
  - The upgrade image is downloaded as the backup image on the access points. You can verify this by using the **show ap image all** command.
  - Change the boot image to primary image manually using the **config boot primary** command and reboot the controller for the upgrade image to be activated.

    or
  - You issue a scheduled reboot with the **swap** keyword. The **swap** keyword has the following importance: The swapping occurs to the primary and backup images on the access point and the currently active image on controller with the backup image.
  - When the controller reboots, the access points are disassociated and eventually come up with an upgraded image. Once the controller responds to the discovery request sent by an access point with its discovery response packet, the access point sends a join request.

- The actual upgrade of the images occur. The following sequence of actions occur:
  - During boot time, the access point sends a join request.
  - The controller responds with the join response with the image version that the controller is running.
  - The access point compares its running image with the running image on the controller. If the versions match, the access point joins the controller.
  - If the versions do not match, the access point compares the version of the backup image and if they match, the access point swaps the primary and backup images and reloads and subsequently joins the controller.
  - If the primary image of the access point is the same as the controller image, the access point reloads and joins the controller.
  - If none of the above conditions are true, the access point sends an image data request to the controller, downloads the latest image, reloads, and joins the controller.

Restrictions for Predownloading an Image to an Access Point

- The maximum number of concurrent predownloads is limited to half the number of concurrent normal image downloads. This limitation allows new access points to join the controller during image downloading.

  If you reach the predownload limit, then the access points that cannot get an image sleep for a time between 180 to 600 seconds and then reattempt the predownload.
- Before you predownload, you should change the active controller boot image to the backup image to ensure that if the controller reboots for some reason, it comes back up with the earlier running image, not the partially downloaded upgrade image.
- Access points with 16-MB total available memory (1130 and 1240 access points) may not have enough free memory to download an upgrade image and may automatically delete crash info files, radio files, and any backup images to free up space. However, this limitation does not affect the predownload process because the predownload image replaces any backup image on the access point.
- When the system time is changed by using the **config time** command, the time set for a scheduled reset is not valid and the scheduled system reset is canceled. You are given an option either to cancel the scheduled reset before configuring the time or retain the scheduled reset and not configure the time.
- All the primary, secondary, and tertiary controllers should run the same images as the primary and backup images. That is, the primary image of all three controllers should be X and the secondary image of all three controllers should be Y or the feature is not effective.
- At the time of the reset, if any AP is downloading the controller image, the scheduled reset is canceled. The following message appears with the reason why the scheduled reset was canceled:

  ```
  %OSAPI-3-RESETSYSTEM_FAILED: osapi_task.c:4458 System will not reset as software is
  being upgraded.
  ```
- Predownloading a 7.2 or later version of image on a Cisco Aironet 1240 access point is not supported when upgrading from a previous controller release. If predownloading is attempted to the Cisco Aironet 1240 access point, the AP gets disconnected.

Predownloading an Image to Access Points—Global Configuration (GUI)

Step 1 Upload your controller configuration files to a server to back them up.

Note We highly recommend that you back up your controller's configuration files prior to upgrading the controller software. Otherwise, you must manually reconfigure the controller.

Step 2 Follow these steps to obtain the controller software:

a) Browse to the Cisco Software Center: http://www.cisco.com/cisco/software/navigator.html

b) Choose **Wireless** from the center selection window.

c) Click **Wireless LAN Controllers**.
The following options are available: Integrated Controllers and Controller Modules and Standalone Controllers.

d) Depending on your controller platform, click one of the above options.

e) Click the controller model number or name. The Download Software page is displayed.

f) Click a controller software release. The software releases are labeled as follows to help you determine which release to download:
Early Deployment (ED)—These software releases provide new features, new hardware platform support, and bug fixes.

Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.

Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.

g) Choose a software release number.

h) Click the filename (*filename.aes*).

i) Click **Download**.

j) Read Cisco's End User Software License Agreement and then click **Agree**.

k) Save the file to your hard drive.

l) Repeat steps a through k to download the remaining file.

Step 3 Copy the controller software file (*filename.aes*) to the default directory on your TFTP or FTP server.

Step 4 (Optional) Disable the controller 802.11X networks.

Note For busy networks, controllers on high utilization, or small controller platforms, we recommend that you disable the 802.11X networks as a precautionary measure.

Step 5 For Cisco WiSM2, shut down the controller port channel on the Catalyst switch to allow the controller to reboot before the access points start downloading the software.

Step 6 Disable any WLANs on the controller.

Step 7 Choose **Commands > Download File** to open the Download File to Controller page.

Step 8 From the **File Type** drop-down list, choose **Code**.

Step 9 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 10 In the **IP Address** text box, enter the IP address of the server.
If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

Step 11 Enter the maximum number of times that the TFTP server attempts to download the software in the **Maximum Retries** text box and the amount of time (in seconds) that the TFTP server attempts to download the software in the **Timeout** text box.

Step 12 In the **File Path** text box, enter the directory path of the software.

Step 13 In the **File Name** text box, enter the name of the controller software file (*filename*.aes).

Step 14 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** text box, enter the username to log into the FTP server.

b) In the **Server Login Password** text box, enter the password to log into the FTP server.

c) In the **Server Port Number** text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 15 Click **Download** to download the software to the controller. A message appears indicating the status of the download.

Step 16 To configure the predownloading of access point images globally, choose **Wireless > Access Points > Global Configuration** to open the Global Configuration page.

Step 17 In the AP Image Pre-download section, perform one of the following:

- To instruct all the access points to predownload a primary image from the controller, click **Download Primary** under the AP Image Pre-download.
- To instruct all the access points to swap their primary and backup images, click **Interchange Image**.
- To download an image from the controller and store it as a backup image, click **Download Backup**.
- To abort the predownload operation, click **Abort Predownload**.

Step 18 Click **OK**.

Step 19 Click **Apply**.

Configuring Predownload Image to an Access Point (GUI)

Step 1 Upload your controller configuration files to a server to back them up.

Note We highly recommend that you back up your controller's configuration files prior to upgrading the controller software. Otherwise, you must manually reconfigure the controller.

Step 2 Follow these steps to obtain the controller software:

a) Browse to the Cisco Software Center: http://www.cisco.com/cisco/software/navigator.html

b) Select **Wireless** from the center selection window.

c) Click **Wireless LAN Controllers**.
The following options are available: Integrated Controllers and Controller Modules and Standalone Controllers.

d) Depending on your controller platform, click one of the above options.

e) Click the controller model number or name. The **Download Software** page is displayed.

f) Click a controller software release. The software releases are labeled as follows to help you determine which release to download:
Early Deployment (ED)—These software releases provide new features, new hardware platform support, and bug fixes.

Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.

Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.

g) Choose a software release number.
h) Click the filename (*filename.aes*).
i) Click **Download**.
j) Read Cisco's End User Software License Agreement and then click **Agree**.
k) Save the file to your hard drive.
l) Repeat steps a through k to download the remaining file.

Step 3 Copy the controller software file (*filename.aes*) to the default directory on your TFTP or FTP server.

Step 4 (Optional) Disable the 802.11 networks.

Note For busy networks, controllers on high utilization, or small controller platforms, we recommend that you disable the 802.11 networks as a precautionary measure.

Step 5 For Cisco WiSM2, shut down the controller port channel on the Catalyst switch to allow the controller to reboot before the access points start downloading the software.

Step 6 Disable any WLANs on the controller.

Step 7 Choose **Commands > Download File** to open the Download File to Controller page.

Step 8 From the **File Type** drop-down list, choose **Code**.

Step 9 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available from the 7.4 release onwards

Step 10 In the **IP Address** text box, enter the IP address of the TFTP or FTP server.
If you are using a TFTP server, the default values of 10 retries and 6 seconds for the **Maximum Retries** and **Timeout** text boxes should work correctly without any adjustment. However, you can change these values.

Step 11 Enter the maximum number of times that the TFTP server attempts to download the software in the **Maximum Retries** text box and the amount of time (in seconds) that the TFTP server attempts to download the software in the **Timeout** text box.

Step 12 In the **File Path** text box, enter the directory path of the software.

Step 13 In the **File Name** text box, enter the name of the controller software file (*filename*.aes).

Step 14 If you are using an FTP server, follow these steps:

a) In the **Server Login Username** text box, enter the username to log into the FTP server.
b) In the **Server Login Password** text box, enter the password to log into the FTP server.
c) In the **Server Port Number** text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 15 Click **Download** to download the software to the controller. A message appears indicating the status of the download.

Step 16 To configure the predownloading of a specific access point, choose **Wireless > All APs > AP_Name** to open the All AP Details page for the selected AP.

Step 17 Click the **Advanced** tab.

Step 18 In the AP Image Pre-download section, perform one of the following:

- To instruct the access point to predownload a primary image from the controller, click **Download Primary** under the AP Image Pre-download.
- To instruct the access point to swap its primary and backup images, click **Interchange Image**.
- To download an image from the controller and store it as a backup image, click **Download Backup**.
- To abort the predownload operation, click **Abort Predownload**.

Step 19 Click **OK**.

Step 20 Click **Apply**.

Predownloading an Image to Access Points (CLI)

Using the CLI, you can predownload an image to a specific access point or to all access points.

Step 1 Follow these steps to obtain the controller software:

a) Browse to the Cisco Software Center: http://www.cisco.com/cisco/software/navigator.html
b) Select **Wireless** from the center selection window.
c) Click **Wireless LAN Controllers**.
The following options are available: Integrated Controllers and Controller Modules and Standalone Controllers.
d) Depending on your controller platform, click one of the above options.
e) Click the controller model number or name. The **Download Software** page is displayed.
f) Click a controller software release. The software releases are labeled as follows to help you determine which release to download:
Early Deployment (ED)—These software releases provide new features, new hardware platform support, and bug fixes.
Maintenance Deployment (MD)—These software releases provide bug fixes and ongoing software maintenance.
Deferred (DF)—These software releases have been deferred. We recommend that you migrate to an upgraded release.
g) Choose a software release number.
h) Click the filename (*filename.aes*).
i) Click **Download**.
j) Read Cisco's End User Software License Agreement and then click **Agree**.
k) Save the file to your hard drive.
l) Repeat steps a through n to download the remaining file.

Step 2 Copy the controller software file (*filename.aes*) to the default directory on your TFTP or FTP server.

Step 3 (Optional) Disable the 802.11 networks.

Note For busy networks, controllers on high utilization, or small controller platforms, we recommend that you disable the 802.11a/n or 802.11b/g/n networks as a precautionary measure.

Step 4 For Cisco WiSM2, shut down the controller port channel on the Catalyst switch to allow the controller to reboot before the access points start downloading the software.

Step 5 Disable any WLANs on the controller using the **config wlan disable** *wlan_id* command.

Step 6 Specify access points that will receive the predownload image.
Use one of these commands to specify access points for predownload:

- Specify access points for predownload by entering this command:

  config ap image predownload {**primary** | **backup**} {*ap_name* | **all**}

  The primary image is the new image; the backup image is the existing image. Access points always boot with the primary image.

- Swap an access point's primary and backup images by entering this command:

  config ap image swap {*ap_name* | **all**}

- Display detailed information on access points specified for predownload by entering this command:

  show ap image {**all** | *ap-name*}

The output lists access points that are specified for predownloading and provides for each access point, primary and secondary image versions, the version of the predownload image, the predownload retry time (if necessary), and the number of predownload attempts. The output also includes the predownload status for each device. The status of the access points is as follows:

- None—The access point is not scheduled for predownload.
- Predownloading—The access point is predownloading the image.
- Not supported—The access point (1120, 1230, and 1310) does not support predownloading.
- Initiated—The access point is waiting to get the predownload image because the concurrent download limit has been reached.
- Failed—The access point has failed 64 predownload attempts.
- Complete—The access point has completed predownloading.

Step 7 Set a reboot time for the controller and the access points.
Use one of these commands to schedule a reboot of the controller and access points:

- Specify the amount of time delay before the devices reboot by entering this command:

  reset system in *HH*:*MM*:*SS* **image** {**swap** | **no-swap**} **reset-aps** [**save-config**]

  Note The **swap** operand in the **reset** command will result in the swapping of the primary and backup images on both the controller and the access point.

  The controller sends a reset message to all joined access points, and then the controller resets.

- Specify a date and time for the devices to reboot by entering this command:

  reset system at *YYYY-MM-DD HH*:*MM*:*SS* **image** {**swap** | **no-swap**} **reset-aps** [**save-config**]

  The controller sends a reset message to all joined access points, and then the controller resets.

  Note The **swap** operand in the **reset** command will result in the swapping of the primary and backup images on both the controller and the access point.

- Set up an SNMP trap message that announces the upcoming reset by entering this command:

  reset system notify-time *minutes*

  The controller sends the announcement trap *the configured number of minutes* before the reset.

- Cancel the scheduled reboot by entering this command:

  reset system cancel

  Note If you configure reset times and then use the **config time** command to change the system time on the controller, the controller notifies you that any scheduled reset times will be canceled and must be reconfigured after you set the system time.

Use the **show reset** command to display scheduled resets.

Information similar to the following appears:

```
System reset is scheduled for Apr 08 01:01:01 2010.
Current local time and date is Apr 07 02:57:44 2010.
A trap will be generated 10 minutes before each scheduled system reset.
Use 'reset system cancel' to cancel the reset.
Configuration will be saved before the system reset.
```

Transferring Files to and from a Controller

Controllers have built-in utilities for uploading and downloading various files. Follow the instructions in these sections to import files using either the controller GUI or CLI:

- Downloading a Login Banner File
- Downloading Device Certificates
- Downloading CA Certificates
- Uploading PACs
- Uploading and Downloading Configuration Files

Downloading a Login Banner File

You can download a login banner file using either the GUI or the CLI. The login banner is the text that appears on the page before user authentication when you access the controller GUI or CLI using Telnet, SSH, or a console port connection.

You save the login banner information as a text (*.txt) file. The text file cannot be larger than 1296 characters and cannot have more than 16 lines of text.

Note The ASCII character set consists of printable and nonprintable characters. The login banner supports only printable characters.

Here is an example of a login banner:

```
Welcome to the Cisco Wireless Controller!
Unauthorized access prohibited.
Contact sysadmin@corp.com for access.
```

Follow the instructions in this section to download a login banner to the controller through the GUI or CLI. However, before you begin, make sure that you have a TFTP or FTP server available for the file download. Follow these guidelines when setting up a TFTP or FTP server:

- If you are downloading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP or FTP server cannot run on the same computer as Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

Note Clearing the controller configuration does not remove the login banner. See the Clearing the Login Banner (GUI) section for information about clearing the login banner using the controller GUI or CLI.

Note The controller can have only one login banner file. If you download another login banner file to the controller, the first login banner file is overwritten.

Downloading a Login Banner File (GUI)

Step 1 Copy the login banner file to the default directory on your server.

Step 2 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 3 From the File Type drop-down list, choose **Login Banner**.

Step 4 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**

- **SFTP** (available in 7.4 and later releases)

Step 5 In the IP Address text box, enter the IP address of the server type you chose in Step 4.
If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

Step 6 Enter the maximum number of times that the TFTP server attempts to download the certificate in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout text box.

Step 7 In the File Path text box, enter the directory path of the login banner file.

Step 8 In the File Name text box, enter the name of the login banner text (*.txt) file.

Step 9 If you are using an FTP server, follow these steps:

a) In the Server Login Username text box, enter the username to log into the FTP server.
b) In the Server Login Password text box, enter the password to log into the FTP server.
c) In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 10 Click **Download** to download the login banner file to the controller. A message appears indicating the status of the download.

Downloading a Login Banner File (CLI)

Step 1 Log into the controller CLI.

Step 2 Specify the transfer mode used to download the config file by entering this command:
transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Download the controller login banner by entering this command:
transfer download datatype login-banner

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:
transfer download serverip server-ip-address

Step 5 Specify the name of the config file to be downloaded by entering this command:
transfer download path server-path-to-file

Step 6 Specify the directory path of the config file by entering this command:
transfer download filename*filename***.txt**

Step 7 If you are using a TFTP server, enter these commands:

- **transfer download tftpMaxRetries retries**
- **transfer download tftpPktTimeout timeout**

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

Step 8 If you are using an FTP server, enter these commands:

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

Note The default value for the port parameter is 21.

Step 9 View the download settings by entering the **transfer download start** command. Enter y when prompted to confirm the current settings and start the download process.

Clearing the Login Banner (GUI)

Step 1 Choose **Commands** > **Login Banner** to open the Login Banner page.

Step 2 Click **Clear**.

Step 3 When prompted, click **OK** to clear the banner.
To clear the login banner from the controller using the controller CLI, enter the **clear login-banner** command.

Downloading Device Certificates

Each wireless device (controller, access point, and client) has its own device certificate. For example, the controller is shipped with a Cisco-installed device certificate. This certificate is used by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific device certificate, it must be downloaded to the controller.

Note For more information about configuring local EAP, see the Configuring Local EAP section.

Follow the instructions in this section to download a vendor-specific device certificate to the controller through the GUI or CLI. However, before you begin, make sure you have a TFTP or FTP server available for the certificate download. Follow these guidelines when setting up a TFTP or FTP server:

- If you are downloading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.

- A third-party TFTP or FTP server cannot run on the same computer as Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

Note All certificates downloaded to the controller must be in PEM format.

Downloading Device Certificates (GUI)

Step 1 Copy the device certificate to the default directory on your server.

Step 2 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 3 From the File Type drop-down list, choose **Vendor Device Certificate**.

Step 4 In the Certificate Password text box, enter the password that was used to protect the certificate.

Step 5 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 6 In the IP Address text box, enter the IP address of the server.
If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

Step 7 Enter the maximum number of times that the TFTP server attempts to download the certificate in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout text box.

Step 8 In the File Path text box, enter the directory path of the certificate.

Step 9 In the File Name text box, enter the name of the certificate.

Step 10 If you are using an FTP server, follow these steps:

a) In the Server Login Username text box, enter the username to log into the FTP server.
b) In the Server Login Password text box, enter the password to log into the FTP server.
c) In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 11 Click **Download** to download the device certificate to the controller. A message appears indicating the status of the download.

Step 12 After the download is complete, choose **Commands** > **Reboot** > **Reboot**.

Step 13 If prompted to save your changes, click **Save and Reboot**.

Step 14 Click **OK** to confirm your decision to reboot the controller.

Downloading Device Certificates (CLI)

Step 1 Log onto the controller CLI.

Step 2 Specify the transfer mode used to download the config file by entering this command:
transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Specify the type of the file to be downloaded by entering this command:
transfer download datatype eapdevcert

Step 4 Specify the certificate's private key by entering this command:
transfer download certpassword *password*

Step 5 Specify the IP address of the TFTP or FTP server by entering this command:
transfer download serverip *server-ip-address*

Step 6 Specify the name of the config file to be downloaded by entering this command:
transfer download path *server-path-to-file*

Step 7 Specify the directory path of the config file by entering this command:
transfer download filename *filename.pem*

Step 8 If you are using a TFTP server, enter these commands:

- **transfer download tftpMaxRetries retries**
- **transfer download tftpPktTimeout timeout**

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

Step 9 If you are using an FTP server, enter these commands:

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

Note The default value for the port parameter is 21.

Step 10 View the updated settings by entering the **transfer download start** command. Answer y when prompted to confirm the current settings and start the download process.

Step 11 Reboot the controller by entering this command:
reset system

Downloading CA Certificates

Controllers and access points have a Certificate Authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate may be used by EAP-FAST (when not using PACs), EAP-TLS, PEAP-GTC, and PEAP-MSCHAPv2 to authenticate wireless clients during local EAP authentication. However, if you want to use your own vendor-specific CA certificate, it must be downloaded to the controller.

Note For more information about configuring local EAP, see the Configuring Local EAP section.

Follow the instructions in this section to download CA certificates to the controller through the GUI or CLI. However, before you begin, make sure that you have a TFTP or FTP server available for the certificate download. Follow these guidelines when setting up a TFTP or FTP server:

- If you are downloading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP or FTP server cannot run on the same computer as Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

Note All certificates downloaded to the controller must be in PEM format.

Download CA Certificates (GUI)

Step 1 Copy the CA certificate to the default directory on your server.

Step 2 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 3 From the File Type drop-down list, choose **Vendor CA Certificate**.

Step 4 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 5 In the IP Address text box, enter the IP address of the server.
If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

Step 6 Enter the maximum number of times that the TFTP server attempts to download the certificate in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the certificate in the Timeout text box.

Step 7 In the File Path text box, enter the directory path of the certificate.

Step 8 In the File Name text box, enter the name of the certificate.

Step 9 If you are using an FTP server, follow these steps:

a) In the Server Login Username text box, enter the username to log on to the FTP server.
b) In the Server Login Password text box, enter the password to log on to the FTP server.
c) In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 10 Click **Download** to download the CA certificate to the controller. A message appears indicating the status of the download.

Step 11 After the download is complete, choose **Commands** > **Reboot** > **Reboot**.

Step 12 If prompted to save your changes, click **Save and Reboot**.

Step 13 Click **OK** to confirm your decision to reboot the controller.

Downloading CA Certificates (CLI)

Step 1 Log on to the controller CLI.

Step 2 Specify the transfer mode used to download the config file by entering this command:
transfer download mode {**tftp** | **ftp** | **sftp**}

Step 3 Specify the type of the file to be downloaded by entering this command:
transfer download datatype eapdevcert

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:
transfer download serverip *server-ip-address*

Step 5 Specify the directory path of the config file by entering this command:
transfer download path *server-path-to-file*

Step 6 Specify the name of the config file to be downloaded by entering this command:
transfer download filename *filename*.pem

Step 7 If you are using a TFTP server, enter these commands:

- **transfer download tftpMaxRetries** *retries*
- **transfer download tftpPktTimeout** *timeout*

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

Step 8 If you are using an FTP server, enter these commands:

- **transfer download username** *username*
- **transfer download password** *password*
- **transfer download port** *port*

Note The default value for the port parameter is 21.

Step 9 View the updated settings by entering the **transfer download start** command. Answer y when prompted to confirm the current settings and start the download process.

Step 10 Reboot the controller by entering the **reset system** command.

Uploading PACs

Protected access credentials (PACs) are credentials that are either automatically or manually provisioned and used to perform mutual authentication with a local EAP authentication server during EAP-FAST authentication. When manual PAC provisioning is enabled, the PAC file is manually generated on the controller.

Follow the instructions in this section to generate and load PACs from the controller through the GUI or CLI. However, before you begin, make sure you have a TFTP or FTP server available for the PAC upload. Follow these guidelines when setting up a TFTP or FTP server:

- If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are uploading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP or FTP server cannot run on the same computer as Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

Uploading PACs (GUI)

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, choose **PAC (Protected Access Credential)**.

Step 3 In the User text box, enter the name of the user who will use the PAC.

Step 4 In the Validity text box, enter the number of days for the PAC to remain valid. The default setting is zero (0).

Step 5 In the Password and Confirm Password text boxes, enter a password to protect the PAC.

Step 6 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**

- **SFTP** (available in 7.4 and later releases)

Step 7 In the IP Address text box, enter the IP address of the server.

Step 8 In the File Path text box, enter the directory path of the PAC.

Step 9 In the File Name text box, enter the name of the PAC file. PAC files have a .pac extension.

Step 10 If you are using an FTP server, follow these steps:

a) In the Server Login Username text box, enter the username to log into the FTP server.
b) In the Server Login Password text box, enter the password to log into the FTP server.
c) In the Server Port Number text box, enter the port number on the FTP server through which the upload occurs. The default value is 21.

Step 11 Click **Upload** to upload the PAC from the controller. A message appears indicating the status of the upload.

Step 12 Follow the instructions for your wireless client to load the PAC on your client devices. Make sure to use the password that you entered above.

Uploading PACs (CLI)

Step 1 Log on to the controller CLI.

Step 2 Specify the transfer mode used to upload the config file by entering this command:
transfer upload mode {**tftp** | **ftp** | **sftp**}

Step 3 Upload a Protected Access Credential (PAC) by entering this command:
transfer upload datatype pac

Step 4 Specify the identification of the user by entering this command:
transfer upload pac *username validity password*

Step 5 Specify the IP address of the TFTP or FTP server by entering this command:
transfer upload serverip *server-ip-address*

Step 6 Specify the directory path of the config file by entering this command:
transfer upload path *server-path-to-file*

Step 7 Specify the name of the config file to be uploaded by entering this command:
transfer upload filename *manual*.pac.

Step 8 If you are using an FTP server, enter these commands:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the port parameter is 21.

Step 9 View the updated settings by entering the **transfer upload start** command. Answer y when prompted to confirm the current settings and start the upload process.

Step 10 Follow the instructions for your wireless client to load the PAC on your client devices. Make sure to use the password that you entered above.

Uploading and Downloading Configuration Files

We recommend that you upload your controller's configuration file to a server to back it up. If you lose your configuration, you can then download the saved configuration to the controller.

Note Do not download a configuration file to your controller that was uploaded from a different controller platform. For example, a Cisco 5500 Series Controller does not support the configuration file from a Cisco 2500 Series Controller.

Follow these guidelines when working with configuration files:

- Any CLI with an invalid value is filtered out and set to default by the XML validation engine. Validation occurs during bootup. A configuration may be rejected if the validation fails. A configuration may fail if you have an invalid CLI. For example, if you have a CLI where you try to configure a WLAN without adding appropriate commands to add the WLAN.
- A configuration may be rejected if the dependencies are not addressed. For example, if you try to configure dependent parameters without using the add command. The XML validation may succeed but the configuration download infrastructure will immediately reject the configuration with no validation errors.
- An invalid configuration can be verified by using the **show invalid-config** command. The **show invalid-config** command reports the configuration that is rejected by the controller either as part of download process or by XML validation infrastructure.

Note You can also read and modify the configuration file.

Uploading Configuration Files

You can upload configuration files using either the GUI or the CLI.

Uploading the Configuration Files (GUI)

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, choose **Configuration**.

Step 3 Encrypt the configuration file by selecting the **Configuration File Encryption** check box and entering the encryption key in the Encryption Key text box.

Step 4 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 5 In the IP Address text box, enter the IP address of the server.

Step 6 In the File Path text box, enter the directory path of the configuration file.

Step 7 In the File Name text box, enter the name of the configuration file.

Step 8 If you are using an FTP server, follow these steps:

a) In the Server Login Username text box, enter the username to log into the FTP server.
b) In the Server Login Password text box, enter the password to log into the FTP server.
c) In the Server Port Number text box, enter the port number on the FTP server through which the upload occurs. The default value is 21.

Step 9 Click **Upload** to upload the configuration file to the server. A message appears indicating the status of the upload. If the upload fails, repeat this procedure and try again.

Uploading the Configuration Files (CLI)

Step 1 Specify the transfer mode used to upload the configuration file by entering this command:
transfer upload mode {**tftp** | **ftp** | **sftp**}

Step 2 Specify the type of file to be uploaded by entering this command:
transfer upload datatype config

Step 3 Encrypt the configuration file by entering these commands:

- **transfer encrypt enable**
- **transfer encrypt set-key** *key,* where *key* is the encryption key used to encrypt the file.

Step 4 Specify the IP address of the server by entering this command:
transfer upload serverip *server-ip-address*

Step 5 Specify the directory path of the configuration file by entering this command:
transfer upload path *server-path-to-file*

Step 6 Specify the name of the configuration file to be uploaded by entering this command:

transfer upload filename *filename*

Step 7 If you are using an FTP server, enter these commands to specify the username and password used to log into the FTP server and the port number through which the upload occurs:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the port parameter is 21.

Step 8 Initiate the upload process by entering this command:
transfer upload start

Step 9 When prompted to confirm the current settings, answer **y**.
Information similar to the following appears:

```
Mode..................................... TFTP
TFTP Server IP........................... 10.10.10.4
TFTP Path................................ Config/
TFTP Filename............................ AS_4402_4_2_55_8_Config.xml
Data Type................................ Config File
Encryption............................... Disabled

*********************************************
***  WARNING: Config File Encryption Disabled  ***
*********************************************

Are you sure you want to start? (y/N) Y
File transfer operation completed successfully.
```

If the upload fails, repeat this procedure and try again.

Downloading Configuration Files

You can download configuration files using either the GUI or the CLI.

Downloading the Configuration Files (GUI)

Step 1 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 2 From the File Type drop-down list, choose **Configuration**.

Step 3 If the configuration file is encrypted, select the **Configuration File Encryption** check box and enter the encryption key used to decrypt the file in the Encryption Key text box.

Note The key that you enter here should match the one entered during the upload process.

Step 4 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in 7.4 and later releases)

Step 5 In the IP Address text box, enter the IP address of the server.
If you are using a TFTP server, the default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.

Step 6 Enter the maximum number of times that the TFTP server attempts to download the configuration file in the Maximum Retries text box and the amount of time (in seconds) that the TFTP server attempts to download the configuration file in the Timeout text box.

Step 7 In the File Path text box, enter the directory path of the configuration file.

Step 8 In the File Name text box, enter the name of the configuration file.

Step 9 If you are using an FTP server, follow these steps:

a) In the Server Login Username text box, enter the username to log into the FTP server.
b) In the Server Login Password text box, enter the password to log into the FTP server.
c) In the Server Port Number text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 10 Click **Download** to download the file to the controller. A message appears indicating the status of the download, and the controller reboots automatically. If the download fails, repeat this procedure and try again.

Downloading the Configuration Files (CLI)

Note The controller does not support incremental configuration downloads. The configuration file contains all mandatory commands (all interface address commands, mgmtuser with read-write permission commands, and interface port or LAG enable or disable commands) required to successfully complete the download. For example, if you download only the **config time ntp server** *index server_address* command as part of the configuration file, the download fails. Only the commands present in the configuration file are applied to the controller, and any configuration in the controller prior to the download is removed.

Step 1 Specify the transfer mode used to download the configuration file by entering this command:
transfer download mode {**tftp** | **ftp** | **sftp**}

Step 2 Specify the type of file to be downloaded by entering this command:
transfer download datatype config

Step 3 If the configuration file is encrypted, enter these commands:

- **transfer encrypt enable**
- **transfer encrypt set-key** *key*, where *key* is the encryption key used to decrypt the file.

  Note The key that you enter here should match the one entered during the upload process.

Step 4 Specify the IP address of the TFTP or FTP server by entering this command:
transfer download serverip *server-ip-address*

Step 5 Specify the directory path of the configuration file by entering this command:
transfer download path *server-path-to-file*

Step 6 Specify the name of the configuration file to be downloaded by entering this command:
transfer download filename *filename*

Step 7 If you are using a TFTP server, enter these commands:

- **transfer download tftpMaxRetries** *retries*
- **transfer download tftpPktTimeout** *timeout*

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that the TFTP server attempts to download the software for the *retries* parameter and the amount of time (in seconds) that the TFTP server attempts to download the software for the *timeout* parameter.

Step 8 If you are using an FTP server, enter these commands to specify the username and password used to log into the FTP server and the port number through which the download occurs:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the port parameter is 21.

Step 9 View the updated settings by entering this command:
transfer download start

Step 10 When prompted to confirm the current settings and start the download process, answer y.
Information similar to the following appears:

```
Mode............................................. TFTP
TFTP Server IP................................... 10.10.10.4
TFTP Path........................................ Config/
TFTP Filename.................................... AS_4402_4_2_55_8_Config.xml
Data Type........................................ Config File
Encryption....................................... Disabled

************************************************
***  WARNING: Config File Encryption Disabled  ***
************************************************

Are you sure you want to start? (y/N) y

File transfer operation completed successfully.
```

If the download fails, repeat this procedure and try again.

Saving Configurations

Controllers contain two kinds of memory: volatile RAM and NVRAM. At any time, you can save the configuration changes from active volatile RAM to nonvolatile RAM (NVRAM) using one of these commands:

- **save config—**Saves the configuration from volatile RAM to NVRAM without resetting the controller.
- **reset system—**Prompts you to confirm that you want to save configuration changes before the controller reboots.
- **logout—**Prompts you to confirm that you want to save configuration changes before you log out.

Editing Configuration Files

When you save the controller's configuration, the controller stores it in XML format in flash memory. Controller software release 5.2 or later releases enable you to easily read and modify the configuration file by converting it to CLI format. When you upload the configuration file to a TFTP/FTP/SFTP server, the controller initiates the conversion from XML to CLI. You can then read or edit the configuration file in a CLI format on the server. When you are finished, you download the file back to the controller, where it is reconverted to an XML format and saved.

Step 1 Upload the configuration file to a TFTP/FTP/SFTP server by performing one of the following:

- Upload the file using the controller GUI.
- Upload the file using the controller CLI.

Step 2 Read or edit the configuration file on the server. You can modify or delete existing CLI commands and add new CLI commands to the file.

Note To edit the configuration file, you can use either Notepad or WordPad on Windows or the VI editor on Linux.

Step 3 Save your changes to the configuration file on the server.

Step 4 Download the configuration file to the controller by performing one of the following:

- Download the file using the controller GUI.
- Download the file using the controller CLI.

The controller converts the configuration file to an XML format, saves it to flash memory, and then reboots using the new configuration. CLI commands with known keywords and proper syntax are converted to XML while improper CLI commands are ignored and saved to flash memory. Any CLI commands that have invalid values are replaced with default values. To see any ignored commands or invalid configuration values, enter this command:

show invalid-config

Note You cannot execute this command after the **clear config** or **save config** command.

Step 5 If the downloaded configuration contains a large number of invalid CLI commands, you might want to upload the invalid configuration to the TFTP or FTP server for analysis. To do so, perform one of the following:

- Upload the invalid configuration using the controller GUI. Follow the instructions in the Uploading Configuration Files (GUI) section but choose **Invalid Config** from the File Type drop-down list in *Step 2* and skip *Step 3*.
- Upload the invalid configuration using the controller CLI. Follow the instructions in the Uploading Configuration Files (CLI) section but enter the transfer **upload datatype invalid-config command** in *Step 2* and skip *Step 3*.

Step 6 The controller does not support the uploading and downloading of port configuration CLI commands. If you want to configure the controller ports, enter these commands:

- **config port linktrap** {*port* | **all**} {**enable** | **disable**}—Enables or disables the up and down link traps for a specific controller port or for all ports.
- **config port adminmode** {*port* | **all**} {**enable** | **disable**}—Enables or disables the administrative mode for a specific controller port or for all ports.

Step 7 Save your changes by entering this command:
save config

Clearing the Controller Configuration

Step 1 Clear the configuration by entering this command:
clear config

Enter **y** at the confirmation prompt to confirm the action.

Step 2 Reboot the system by entering this command:
reset system

Enter n to reboot without saving configuration changes. When the controller reboots, the configuration wizard starts automatically.

Step 3 Follow the instructions in the Configuring the Controller-Using the Configuration Wizard section to complete the initial configuration.

Erasing the Controller Configuration

Step 1 Reset the configuration by entering this command:
reset system

At the confirmation prompt, enter y to save configuration changes to NVRAM. The controller reboots.

Step 2 When you are prompted for a username, restore the factory-default settings by entering this command:

recover-config

The controller reboots and the configuration wizard starts automatically.

Step 3 Follow the instructions in the Configuring the Controller-Using the Configuration Wizard section to complete the initial configuration.

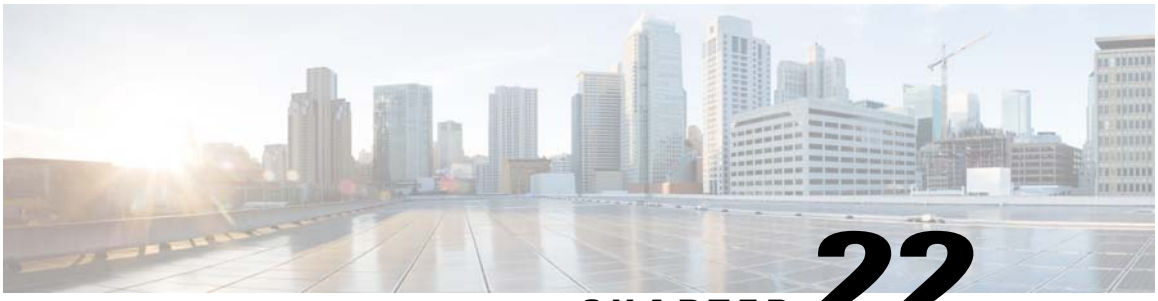
Resetting the Controller

You can reset the controller and view the reboot process on the CLI console using one of the following two methods:

- Turn the controller off and then turn it back on.
- On the CLI, enter reset system. At the confirmation prompt, enter y to save configuration changes to NVRAM. The controller reboots.

When the controller reboots, the CLI console displays the following reboot information:

- Initializing the system.
- Verifying the hardware configuration.
- Loading microcode into memory.
- Verifying the operating system software load.
- Initializing with its stored configurations.
- Displaying the login prompt.



CHAPTER 22

Managing User Accounts

Configuring Guest User Accounts

Information About Creating Guest Accounts

The controller can provide guest user access on WLANs. The first step in creating guest user accounts is to create a lobby administrator user, also known as a lobby ambassador account. Once this account has been created, a lobby ambassador can create and manage guest user accounts on the controller. The lobby ambassador has limited configuration privileges and access only to the web pages used to manage the guest accounts.

The lobby ambassador can specify the amount of time that the guest user accounts remain active. After the specified time elapses, the guest user accounts expire automatically.

Restrictions for Managing User Accounts

The local user database is limited to a maximum of 2048 entries, which is also the default value. This database is shared by local management users (including lobby ambassadors), local network users (including guest users), MAC filter entries, exclusion list entries, and access point authorization list entries. Together they cannot exceed the configured maximum value.

Creating a Lobby Ambassador Account

Creating a Lobby Ambassador Account (GUI)

Step 1 Choose **Management > Local Management Users** to open the Local Management Users page. This page lists the names and access privileges of the local management users.

Note If you want to delete any of the user accounts from the controller, hover your cursor over the blue drop-down arrow and choose **Remove**. However, deleting the default administrative user prohibits both GUI and CLI access to the controller. Therefore, you must create a user with administrative privileges (ReadWrite) before you remove the default user.

Step 2 Click **New** to create a lobby ambassador account. The Local Management Users > New page appears.

Step 3 In the User Name text box, enter a username for the lobby ambassador account.

Note Management usernames must be unique because they are stored in a single database.

Step 4 In the **Password** and **Confirm Password** text boxes, enter a password for the lobby ambassador account.

Note Passwords are case sensitive. The settings for the management User Details parameters depends on the settings that you make in the Password Policy page. The following requirements are enforced on the password

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password should not contain a management username or the reverse letters of a username.
- The password should not contain words like Cisco, oscic, admin, nimda, or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

Step 5 Choose **LobbyAdmin** from the User Access Mode drop-down list. This option enables the lobby ambassador to create guest user accounts.

Note The ReadOnly option creates an account with read-only privileges, and the ReadWrite option creates an administrative account with both read and write privileges.

Step 6 Click **Apply** to commit your changes. The new lobby ambassador account appears in the list of local management users.

Step 7 Click **Save Configuration** to save your changes.

Creating a Lobby Ambassador Account (CLI)

To create a lobby ambassador account use the following command:

config mgmtuser add *lobbyadmin_username lobbyadmin_pwd* **lobby-admin**

Note Replacing **lobby-admin** with **read-only** creates an account with read-only privileges. Replacing **lobby-admin** with **read-write** creates an administrative account with both read and write privileges.

Creating Guest User Accounts as a Lobby Ambassador (GUI)

Step 1 Log into the controller as the lobby ambassador, using the username and password. The Lobby Ambassador Guest Management > Guest Users List page appears.

Step 2 Click **New** to create a guest user account. The Lobby Ambassador Guest Management > Guest Users List > New page appears.

Step 3 In the User Name text box, enter a name for the guest user. You can enter up to 24 characters.

Step 4 Perform one of the following:

- If you want to generate an automatic password for this guest user, select the **Generate Password** check box. The generated password is entered automatically in the Password and Confirm Password text boxes.
- If you want to create a password for this guest user, leave the **Generate Password** check box unselected and enter a password in both the **Password** and **Confirm Password** text boxes.

  Note Passwords can contain up to 24 characters and are case sensitive.

Step 5 From the Lifetime drop-down lists, choose the amount of time (in days, hours, minutes, and seconds) that this guest user account is to remain active. A value of zero (0) for all four text boxes creates a permanent account.
Default: 1 day

Range: 5 minutes to 30 days

Note The smaller of this value or the session timeout for the guest WLAN, which is the WLAN on which the guest account is created, takes precedence. For example, if a WLAN session timeout is due to expire in 30 minutes but the guest account lifetime has 10 minutes remaining, the account is deleted in 10 minutes upon guest account expiry. Similarly, if the WLAN session timeout expires before the guest account lifetime, the client experiences a recurring session timeout that requires reauthentication.

Note You can change a guest user account with a nonzero lifetime to another lifetime value at any time while the account is active. However, to make a guest user account permanent using the controller GUI, you must delete the account and create it again. If desired, you can use the **config netuser lifetime** *user_name 0* command to make a guest user account permanent without deleting and recreating it.

Step 6 From the WLAN SSID drop-down list, choose the SSID that will be used by the guest user. The only WLANs that are listed are those WLANs for which Layer 3 web authentication has been configured.

Note We recommend that you create a specific guest WLAN to prevent any potential conflicts. If a guest account expires and it has a name conflict with an account on the RADIUS server and both are on the same WLAN, the users associated with both accounts are disassociated before the guest account is deleted.

Step 7 In the Description text box, enter a description of the guest user account. You can enter up to 32 characters.

Step 8 Click **Apply** to commit your changes. The new guest user account appears in the list of guest users on the Guest Users List page.
From this page, you can see all of the guest user accounts, their WLAN SSID, and their lifetime. You can also edit or remove a guest user account. When you remove a guest user account, all of the clients that are using the guest WLAN and are logged in using that account's username are deleted.

Step 9 Repeat this procedure to create any additional guest user accounts.

Viewing Guest User Accounts

Viewing the Guest Accounts (GUI)

To view guest user accounts using the controller GUI, choose **Security** > **AAA** > **Local Net Users**. The Local Net Users page appears.

From this page, you can see all of the local net user accounts (including guest user accounts) and can edit or remove them as desired. When you remove a guest user account, all of the clients that are using the guest WLAN and are logged in using that account's username are deleted.

Viewing the Guest Accounts (CLI)

To see all of the local net user accounts (including guest user accounts) using the controller CLI, enter this command:

show netuser summary

Configuring Administrator Usernames and Passwords

Information About Configuring Administrator Usernames and Passwords

You can configure administrator usernames and passwords to prevent unauthorized users from reconfiguring the controller and viewing configuration information. This section provides instructions for initial configuration and for password recovery.

Configuring Usernames and Passwords (GUI)

Step 1 Choose **Management** > **Local Management Users**.

Step 2 Click **New**.

Step 3 Enter the username and password, and confirm the password.
Usernames and passwords are case-sensitive and can contain up to 24 ASCII characters. Usernames and passwords cannot contain spaces.

Step 4 Choose the User Access Mode as one of the following:

- **ReadOnly**
- **ReadWrite**
- **LobbyAdmin**

Step 5 Click **Apply**.

Configuring Usernames and Passwords (CLI)

Step 1 Configure a username and password by entering one of these commands:

- **config mgmtuser add** *username password* **read-write—**Creates a username-password pair with read-write privileges.
- **config mgmtuser add** *username password* **read-only—**Creates a username-password pair with read-only privileges.

  Usernames and passwords are case-sensitive and can contain up to 24 ASCII characters. Usernames and passwords cannot contain spaces.

  Note If you ever need to change the password for an existing username, enter the **config mgmtuser password** *username new_password* command.

Step 2 List the configured users by entering this command:
show mgmtuser

Restoring Passwords

Before You Begin

Ensure that you are accessing the controller CLI through the console port.

Step 1 After the controller boots up, enter **Restore-Password** at the User prompt.
Note For security reasons, the text that you enter does not appear on the controller console.

Step 2 At the Enter User Name prompt, enter a new username.

Step 3 At the Enter Password prompt, enter a new password.

Step 4 At the Re-enter Password prompt, reenter the new password. The controller validates and stores your entries in the database.

Step 5 When the User prompt reappears, enter your new username.

Step 6 When the Password prompt appears, enter your new password. The controller logs you in with your new username and password.

Changing the Default Values for SNMP v3 Users

Information About Changing the Default Values for SNMP v3 Users

The controller uses a default value of "default" for the username, authentication password, and privacy password for SNMP v3 users. Using these standard values presents a security risk. Therefore, Cisco strongly advises that you change these values.

Note SNMP v3 is time sensitive. Ensure that you configure the correct time and time zone on your controller.

Changing the SNMP v3 User Default Values (GUI)

Step 1 Choose **Management** > **SNMP** > **SNMP V3 Users** to open the SNMP V3 Users page.

Step 2 If "default" appears in the User Name column, hover your cursor over the blue drop-down arrow for the desired user and choose **Remove** to delete this SNMP v3 user.

Step 3 Click **New** to add a new SNMP v3 user. The SNMP V3 Users > New page appears.

Step 4 In the User Profile Name text box, enter a unique name. Do not enter "default."

Step 5 Choose **Read Only** or **Read Write** from the Access Mode drop-down list to specify the access level for this user. The default value is Read Only.

Step 6 From the Authentication Protocol drop-down list, choose the desired authentication method: **None**, **HMAC-MD5** (Hashed Message Authentication Coding-Message Digest 5), or **HMAC-SHA** (Hashed Message Authentication Coding-Secure Hashing Algorithm). The default value is HMAC-SHA.

Step 7 In the Auth Password and Confirm Auth Password text boxes, enter the shared secret key to be used for authentication. You must enter at least 12 characters that include both letters and numbers.

Step 8 From the Privacy Protocol drop-down list, choose the desired encryption method: **None**, **CBC-DES** (Cipher Block Chaining-Digital Encryption Standard), or **CFB-AES-128** (Cipher Feedback Mode-Advanced Encryption Standard-128). The default value is CFB-AES-128.

Note In order to configure CBC-DES or CFB-AES-128 encryption, you must have selected either HMAC-MD5 or HMAC-SHA as the authentication protocol in Step 6.

Step 9 In the Priv Password and Confirm Priv Password text boxes, enter the shared secret key to be used for encryption. You must enter at least 12 characters that include both letters and numbers.

Step 10 Click **Apply**.

Step 11 Click **Save Configuration**.

Step 12 Reboot the controller so that the SNMP v3 user that you added takes effect.

Changing the SNMP v3 User Default Values (CLI)

Step 1 See the current list of SNMP v3 users for this controller by entering this command:
show snmpv3user

Step 2 If "default" appears in the SNMP v3 User Name column, enter this command to delete this user:
config snmp v3user delete *username*

The *username* parameter is the SNMP v3 username (in this case, "default").

Step 3 Create a new SNMP v3 user by entering this command:
config snmp v3user create *username* {**ro** | **rw**} {**none** | **hmacmd5** | **hmacsha**} {**none** | **des** | **aescfb128**} *auth_key encrypt_key*

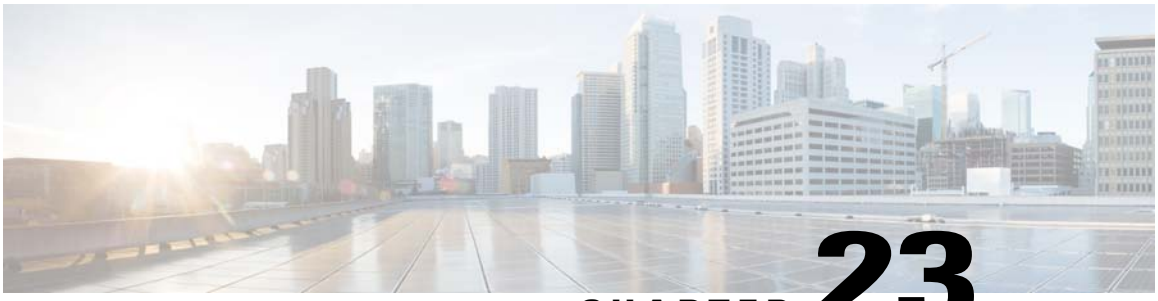
where

- *username* is the SNMP v3 username.
- **ro** is read-only mode and **rw** is read-write mode.
- **none**, **hmacmd5**, and **hmacsha** are the authentication protocol options.
- **none**, **des**, and **aescfb128** are the privacy protocol options.
- *auth_key is the authentication shared secret key.*
- *encrypt_key is the encryption shared secret key.*

  Do not enter "default" for the *username*, *auth_key*, and *encrypt_key* parameters.

Step 4 Enter the **save config** command.

Step 5 Reboot the controller so that the SNMP v3 user that you added takes effect by entering **reset system** command.



CHAPTER 23

Managing Web Authentication

Obtaining a Web Authentication Certificate

Information About Web Authentication Certificates

The operating system of the controller automatically generates a fully functional web authentication certificate, so you do not need to do anything in order to use certificates with Layer 3 web authentication. However, if desired, you can prompt the operating system to generate a new web authentication certificate, or you can download an externally generated SSL certificate.

Obtaining a Web Authentication Certificate (GUI)

Step 1 Choose **Security** > **Web Auth** > **Certificate** to open the Web Authentication Certificate page.
This page shows the details of the current web authentication certificate.

Step 2 If you want to use a new operating system-generated web authentication certificate, follow these steps:

a) Click **Regenerate Certificate**. The operating system generates a new web authentication certificate, and a successfully generated web authentication certificate message appears.

b) Reboot the controller to register the new certificate.

Step 3 If you prefer to use an externally generated web authentication certificate, follow these steps:

a) Verify that the controller can ping the TFTP server.

b) Select the **Download SSL Certificate** check box.
c) In the Server IP Address text box, enter the IP address of the TFTP server.
The default values of 10 retries and 6 seconds for the Maximum Retries and Timeout text boxes should work correctly without any adjustment. However, you can change these values.
d) Enter the maximum number of times that each download can be attempted in the Maximum Retries text box and the amount of time (in seconds) allowed for each download in the Timeout text box.
e) In the Certificate File Path text box, enter the directory path of the certificate.
f) In the Certificate File Name text box, enter the name of the certificate (**certname**.pem).
g) In the Certificate Password text box, enter the password for the certificate.
h) Click **Apply** to commit your changes. The operating system downloads the new certificate from the TFTP server.
i) Reboot the controller to register the new certificate.

Obtaining a Web Authentication Certificate (CLI)

Step 1 See the current web authentication certificate by entering this command:
show certificate summary

Information similar to the following appears:

```
Web Administration Certificate..................... Locally Generated
Web Authentication Certificate..................... Locally Generated
Certificate compatibility mode:................ off
```

Step 2 If you want the operating system to generate a new web authentication certificate, follow these steps:
a) To generate the new certificate, enter this command:
config certificate generate webauth
b) To reboot the controller to register the new certificate, enter this command:
reset system

Step 3 If you prefer to use an externally generated web authentication certificate, follow these steps:
Note We recommend that the Common Name (CN) of the externally generated web authentication certificate be 1.1.1.1 (or the equivalent virtual interface IP address) in order for the client's browser to match the domains of the web authentication URL and the web authentication certificate.

1 Specify the name, path, and type of certificate to be downloaded by entering these commands:

transfer download mode tftp

transfer download datatype webauthcert

transfer download serverip *server_ip_address*

transfer download path *server_path_to_file*

transfer download filename *certname*.pem

transfer download certpassword *password*

transfer download tftpMaxRetries *retries*

transfer download tftpPktTimeout *timeout*

Note The default values of 10 retries and a 6-second timeout should work correctly without any adjustment. However, you can change these values. To do so, enter the maximum number of times that each download can be attempted for the *retries* parameter and the amount of time (in seconds) allowed for each download for the *timeout* parameter.

2 Start the download process by entering this command:

transfer download start

3 Reboot the controller to register the new certificate by entering this command:

reset system

Web Authentication Process

Web authentication is a Layer 3 security feature that causes the controller to not allow IP traffic (except DHCP-related packets) from a particular client until that client has correctly supplied a valid username and password. When you use web authentication to authenticate clients, you must define a username and password for each client. When the clients attempt to join the wireless LAN, their users must enter the username and password when prompted by a login page.

Note If a client uses more than 20 DNS resolved addresses, the controller overwrites the 21st address in the first address space in the Mobile Station Control Block (MSCB) table, but the first address is still retained in the client. If the client again tries to use the first address, it will not be reachable because the controller does not have this address in the list of allowed addresses for the client's MSCB table.

Note One-Time Passwords (OTP) are not supported on web authentication.

Disabling Security Alert for Web Authentication Process

When web authentication is enabled (under Layer 3 Security), users might receive a web-browser security alert the first time that they attempt to access a URL.

Figure 19: Typical Web-Browser Security Alert

Note When clients connect to a WebAuth SSID with preauthorization ACL configured to allow VPN users, the clients will get disconnected from the SSID every few minutes. Webauth SSIDs must not connect without authenticating on the web page.

After the user clicks **Yes** to proceed (or if the client's browser does not display a security alert), the web authentication system redirects the client to a login page.

Step 1 Click **View Certificate** on the Security Alert page.

Step 2 Click **Install Certificate**.

Step 3 When the Certificate Import Wizard appears, click **Next**.

Step 4 Choose **Place all certificates in the following store** and click **Browse**.

Step 5 Choose **Place all certificates in the following store** and click **Browse**.

Step 6 Expand the **Trusted Root Certification Authorities** folder and choose **Local Computer**.

Step 7 Click **OK**.

Step 8 Click **Next** > **Finish**.

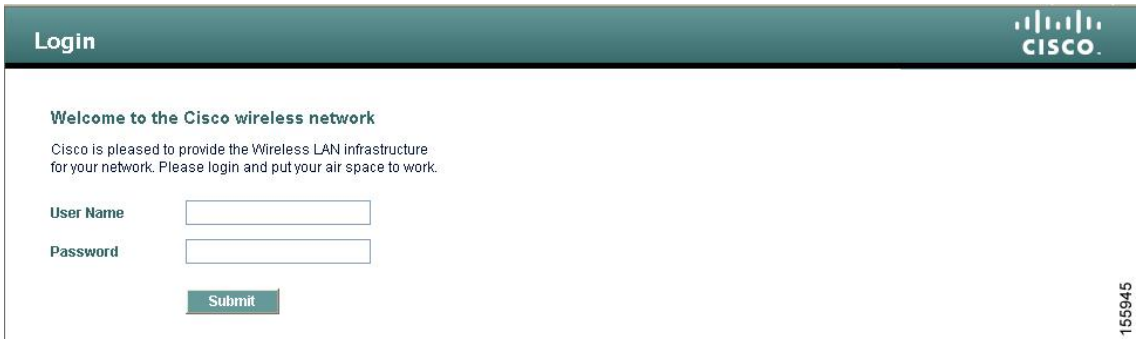
Step 9 When the "The import was successful" message appears, click **OK**.

Because the issuer text box is blank on the controller self-signed certificate, open Internet Explorer, choose **Tools** > **Internet Options** > **Advanced**, unselect the **Warn about Invalid Site Certificates** check box under Security, and click **OK**.

Step 10 Reboot the PC. On the next web authentication attempt, the login page appears.

The following figure shows the default web authentication login page.

Figure 20: Default Web Authentication Login Page



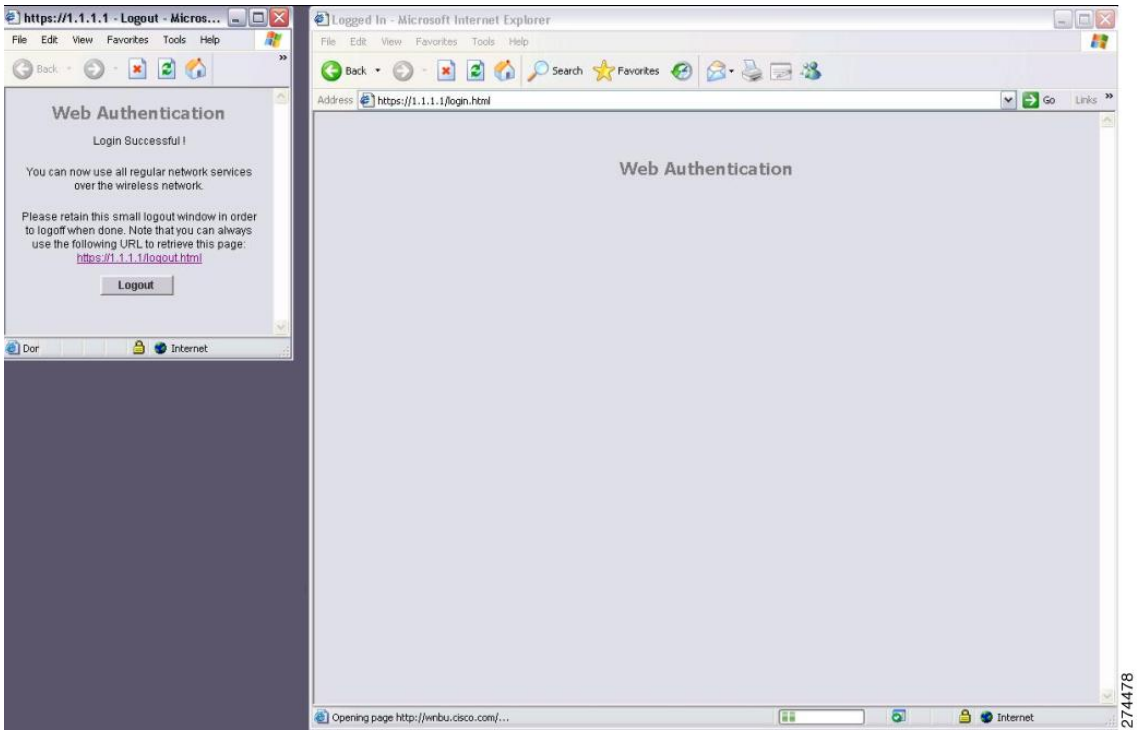
The default login page contains a Cisco logo and Cisco-specific text. You can choose to have the web authentication system display one of the following:

- The default login page
- A modified version of the default login page
- A customized login page that you configure on an external web server
- A customized login page that you download to the controller

The Choosing the Default Web Authentication Login Page section provides instructions for choosing how the web authentication login page appears.

When the user enters a valid username and password on the web authentication login page and clicks **Submit**, the web authentication system displays a successful login page and redirects the authenticated client to the requested URL.

Figure 21: Successful Login Page



The default successful login page contains a pointer to a virtual gateway address URL in the *https://<IP address>/logout.html* format. The IP address that you set for the controller virtual interface serves as the redirect address for the login page

Choosing the Default Web Authentication Login Page

Information About Default Web Authentication Login Page

If you are using a custom web-auth bundle that is served by the internal controller web server, the page should not contain more than 5 elements (including HTML, CSS, and Images). This is because the internal controller web server implements a DoS protection mechanism that limits each client to open a maximum of 5 (five) concurrent TCP connections depending on the load. Some browsers may try to open more than 5 TCP sessions at the same time (For example Firefox 4) if the page contains more elements and this may result in the page loading slowly depending on how the browser handles the DoS protection.

If you do not want users to connect to a web page using a browser that is configured with SSLv2 only, you can disable SSLv2 for web authentication by entering the **config network secureweb cipher-option sslv2**

disable command. If you enter this command, users must use a browser that is configured to use a more secure protocol such as SSLv3 or later releases. The default value is disabled.

Note Cisco TAC is not responsible for creating a custom webauth bundle.

If you have a complex custom web authentication module, it is recommended that you use an external web-auth config on the controller, where the full login page is hosted at an external web server.

Choosing the Default Web Authentication Login Page (GUI)

Step 1 Choose **Security** > **Web Auth** > **Web Login Page** to open the Web Login page.

Step 2 From the Web Authentication Type drop-down list, choose **Internal (Default)**.

Step 3 If you want to use the default web authentication login page as is, go to Step 8. If you want to modify the default login page, go to Step 4.

Step 4 If you want to hide the Cisco logo that appears in the top right corner of the default page, choose the Cisco Logo **Hide** option. Otherwise, click the **Show** option.

Step 5 If you want the user to be directed to a particular URL (such as the URL for your company) after login, enter the desired URL in the Redirect URL After Login text box. You can enter up to 254 characters.

Note The controller supports web authentication redirects only to HTTP (HTTP over TCP) servers. It does not support web authentication redirects to HTTPS (HTTP over SSL) servers.

Step 6 If you want to create your own headline on the login page, enter the desired text in the Headline text box. You can enter up to 127 characters. The default headline is "Welcome to the Cisco wireless network."

Step 7 If you want to create your own message on the login page, enter the desired text in the Message text box. You can enter up to 2047 characters. The default message is "Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work."

Step 8 Click **Apply** to commit your changes.

Step 9 Click **Preview** to view the web authentication login page.

Step 10 If you are satisfied with the content and appearance of the login page, click **Save Configuration** to save your changes. Otherwise, repeat any of the previous steps as necessary to achieve your desired results.

Choosing the Default Web Authentication Login Page (CLI)

Step 1 Specify the default web authentication type by entering this command:
config custom-web webauth_type internal

Step 2 If you want to use the default web authentication login page as is, go to Step 7. If you want to modify the default login page, go to Step 3.

Step 3 To show or hide the Cisco logo that appears in the top right corner of the default login page, enter this command:
config custom-web weblogo {**enable** | **disable**}

Step 4 If you want the user to be directed to a particular URL (such as the URL for your company) after login, enter this command:
config custom-web redirecturl *url*

You can enter up to 130 characters for the URL. To change the redirect back to the default setting, enter the **clear redirecturl** command.

Note The controller supports web authentication redirects only to HTTP (HTTP over TCP) servers. It does not support web authentication redirects to HTTPS (HTTP over SSL) servers.

Step 5 If you want to create your own headline on the login page, enter this command:
config custom-web webtitle *title*

You can enter up to 130 characters. The default headline is "Welcome to the Cisco wireless network." To reset the headline to the default setting, enter the **clear webtitle** command.

Step 6 If you want to create your own message on the login page, enter this command:
config custom-web webmessage *message*

You can enter up to 130 characters. The default message is "Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work." To reset the message to the default setting, enter the **clear webmessage** command.

Step 7 To enable or disable the web authentication logout popup window, enter this command:
config custom-web logout-popup {**enable** | **disable**}

Step 8 Enter the **save config** command to save your settings.

Step 9 Import your own logo into the web authentication login page as follows:

1. Make sure that you have a Trivial File Transfer Protocol (TFTP) server available for the file download. Follow these guidelines when setting up a TFTP server:
   - If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
   - If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
   - A third-party TFTP server cannot run on the same computer as the Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP server and the third-party TFTP server require the same communication port.
2. Ensure that the controller can contact the TFTP server by entering this command:
   ping ip-address
3. Copy the logo file (in .jpg, .gif, or .png format) to the default directory on your TFTP server. The maximum file size is 30 kilobits. For an optimal fit, the logo should be approximately 180 pixels wide and 360 pixels high.
4. Specify the download mode by entering this command:
   transfer download mode tftp
5. Specify the type of file to be downloaded by entering this command:
   transfer download datatype image
6. Specify the IP address of the TFTP server by entering this command:
   transfer download serverip *tftp-server-ip-address*

Note Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

7 Specify the download path by entering this command:

transfer download path *absolute-tftp-server-path-to-file*

8 Specify the file to be downloaded by entering this command:

transfer download filename {*filename.jpg* | *filename.gif* | *filename.png*}

9 View your updated settings and answer *y* to the prompt to confirm the current download settings and start the download by entering this command:

transfer download start

10 Save your settings by entering this command:

save config

Note If you ever want to remove this logo from the web authentication login page, enter the **clear webimage** command.

Step 10 Follow the instructions in the Verifying the Web Authentication Login Page Settings (CLI), on page 228 section to verify your settings.

Example: Creating a Customized Web Authentication Login Page

This section provides information on creating a customized web authentication login page, which can then be accessed from an external web server.

Here is a web authentication login page template. It can be used as a model when creating your own customized page:

```
<html>
<head>
<meta http-equiv="Pragma" content="no-cache">
<meta HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<title>Web Authentication</title>
<script>

function submitAction(){
 var link = document.location.href;
 var searchString = "redirect=";
 var equalIndex = link.indexOf(searchString);
 var redirectUrl = "";

 if (document.forms[0].action == "") {
  var url = window.location.href;
  var args = new Object();
  var query = location.search.substring(1);
  var pairs = query.split("&");
  for(var i=0;i<pairs.length;i++){
  var pos = pairs[i].indexOf('=');
   if(pos == -1) continue;
    var argname = pairs[i].substring(0,pos);
    var value = pairs[i].substring(pos+1);
    args[argname] = unescape(value);
  }
   document.forms[0].action = args.switch_url;
  }
```

```
      if(equalIndex >= 0) {
  equalIndex += searchString.length;
  redirectUrl = "";
  redirectUrl += link.substring(equalIndex);
  }
  if(redirectUrl.length > 255)
  redirectUrl = redirectUrl.substring(0,255);
  document.forms[0].redirect_url.value = redirectUrl;
  document.forms[0].buttonClicked.value = 4;
        document.forms[0].submit();
}

 function loadAction(){
      var url = window.location.href;
      var args = new Object();
      var query = location.search.substring(1);
      var pairs = query.split("&");
      for(var i=0;i<pairs.length;i++){
          var pos = pairs[i].indexOf('=');
          if(pos == -1) continue;
          var argname = pairs[i].substring(0,pos);
          var value = pairs[i].substring(pos+1);
          args[argname] = unescape(value);
      }
//alert( "AP MAC Address is " + args.ap_mac);
      //alert( "The Switch URL to post user credentials is " + args.switch_url);
      document.forms[0].action = args.switch_url;

      // This is the status code returned from webauth login action
      // Any value of status code from 1 to 5 is error condition and user
      // should be shown error as below or modify the message as it suits
      // the customer
      if(args.statusCode == 1){
        alert("You are already logged in. No further action is required on your part.");
      }
      else if(args.statusCode == 2){
       alert("You are not configured to authenticate against web portal. No further action
 is required on your part.");
      }
      else if(args.statusCode == 3){
        alert("The username specified cannot be used at this time. Perhaps the username is
 already logged into the system?");
      }
      else if(args.statusCode == 4){
        alert("The User has been excluded. Please contact the administrator.");
      }
      else if(args.statusCode == 5){
        alert("Invalid username and password. Please try again.");
      }
      else if(args.statusCode == 6){
        alert("Invalid email address format. Please try again.");
      }
}

</script>
</head>
<body topmargin="50" marginheight="50" onload="loadAction();">
<form method="post" action="https://209.165.200.225/login.html">
<input TYPE="hidden" NAME="buttonClicked" SIZE="16" MAXLENGTH="15" value="0">
<input TYPE="hidden" NAME="redirect_url" SIZE="255" MAXLENGTH="255" VALUE="">
<input TYPE="hidden" NAME="err_flag" SIZE="16" MAXLENGTH="15" value="0">

<div align="center">
<table border="0" cellspacing="0" cellpadding="0">
<tr> <td> </td></tr>

<tr align="center"> <td colspan="2"><font size="10" color="#336699">Web
Authentication</font></td></tr>

<tr align="center">

<td colspan="2"> User Name    <input type="TEXT" name="username" SIZE="25"
MAXLENGTH="63" VALUE="">
```

```
</td>
</tr>
<tr align="center" >
<td colspan="2"> Password      <input type="Password" name="password"
 SIZE="25" MAXLENGTH="24">
</td>
</tr>

<tr align="center">
<td colspan="2"><input type="button" name="Submit" value="Submit" class="button"
onclick="submitAction();">
</td>
</tr>
</table>
</div>

</form>
</body>
</html>
```

These parameters are added to the URL when the user's Internet browser is redirected to the customized login page:

- **ap_mac—**The MAC address of the access point to which the wireless user is associated.
- **switch_url—**The URL of the controller to which the user credentials should be posted.
- **redirect—**The URL to which the user is redirected after authentication is successful.
- **statusCode—**The status code returned from the controller's web authentication server.
- **wlan—**The WLAN SSID to which the wireless user is associated.

The available status codes are as follows:

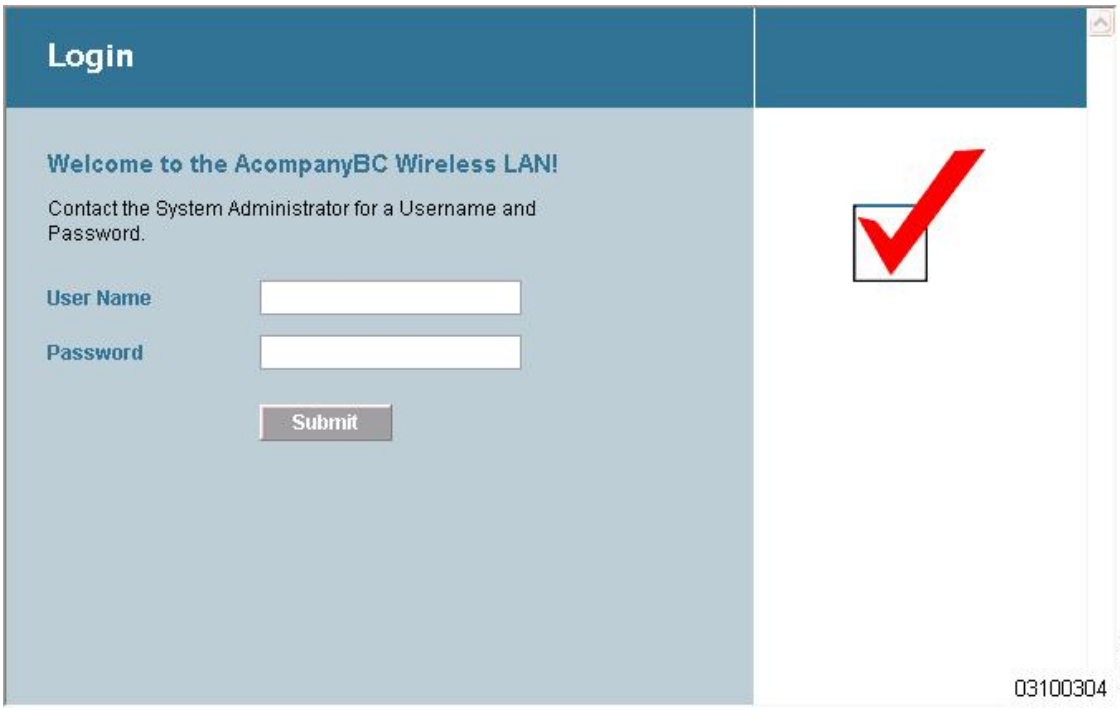
- Status Code 1: "You are already logged in. No further action is required on your part."
- Status Code 2: "You are not configured to authenticate against web portal. No further action is required on your part."
- Status Code 3: "The username specified cannot be used at this time. Perhaps the username is already logged into the system?"
- Status Code 4: "You have been excluded."
- Status Code 5: "The User Name and Password combination you have entered is invalid. Please try again."

Note For additional information, see the *External Web Authentication with Wireless LAN Controllers Configuration Example* at this URL: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008076f974.shtml

Example: Modified Default Web Authentication Login Page Example

This figure shows an example of a modified default web authentication login page.

Figure 22: Modified Default Web Authentication Login Page Example



These CLI commands were used to create this login page:

- **config custom-web weblogo** *disable*
- **config custom-web webtitle** *Welcome to the AcompanyBC Wireless LAN!*
- **config custom-web webmessage** *Contact the System Administrator for a Username and Password.*
- **transfer download** *start*
- **config custom-web redirecturl** *url*

Using a Customized Web Authentication Login Page from an External Web Server

Information About Customized Web Authentication Login Page

You can customize the web authentication login page to redirect to an external web server. When you enable this feature, the user is directed to your customized login page on the external web server.

You must configure a preauthentication access control list (ACL) on the WLAN for the external web server and then choose this ACL as the WLAN preauthentication ACL under Security Policies > Web Policy on the WLANs > Edit page.

Choosing a Customized Web Authentication Login Page from an External Web Server (GUI)

Step 1 Choose **Security** > **Web Auth** > **Web Login Page** to open the Web Login page.

Step 2 From the Web Authentication Type drop-down list, choose **External (Redirect to external server)**.

Step 3 In the Redirect URL after login text box, enter the URL that you want the user to be redirected after a login. For example, you may enter your company's URL here and the users will be directed to that URL after login. The maximum length is 254 characters. By default, the user is redirected to the URL that was entered in the user's browser before the login page was served. of the customized web authentication login page on your web server. You can enter up to 252 characters.

Step 4 In the External Webauth URL text box, enter the URL that is to be used for external web authentication.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Choosing a Customized Web Authentication Login Page from an External Web Server (CLI)

Step 1 Specify the web authentication type by entering this command:
config custom-web webauth_type external

Step 2 Specify the URL of the customized web authentication login page on your web server by entering this command:
config custom-web ext-webauth-url *url*

You can enter up to 252 characters for the URL.

Step 3 Specify the IP address of your web server by entering this command:
config custom-web ext-webserver {**add** | **delete**} *server_IP_address*

Step 4 Enter the **save config** command to save your settings.

Step 5 Follow the instructions in the Verifying the Web Authentication Login Page Settings (CLI), on page 228 section to verify your settings.

Downloading a Customized Web Authentication Login Page

You can compress the page and image files used for displaying a web authentication login page into a.tar file for download to a controller. These files are known as the webauth bundle. The maximum allowed size of the files in their uncompressed state is 1 MB. When the .tar file is downloaded from a local TFTP server, it enters the controller's file system as an untarred file.

You can download a login page example from Cisco Prime Infrastructure and use it as a starting point for your customized login page. For more information, see the Cisco Prime Infrastructure documentation.

Note If you load a webauth bundle with a .tar compression application that is not GNU compliant, the controller cannot extract the files in the bundle and the following error messages appear: "Extracting error" and "TFTP transfer failed." Therefore, we recommend that you use an application that complies with GNU standards, such as PicoZip, to compress the .tar file for the webauth bundle.

Note Configuration backups do not include extra files or components, such as the webauth bundle or external licenses, that you download and store on your controller, so you should manually save external backup copies of those files or components.

Note If the customized webauth bundle has more than 3 separated elements, we advise you to use an external server to prevent page load issues that may be caused because of TCP rate-limiting policy on the controller.

Prerequisites for Downloading a Customized Web Authentication Login Page

- Name the login page `login.html`. The controller prepares the web authentication URL based on this name. If the server does not find this file after the webauth bundle has been untarred, the bundle is discarded, and an error message appears.
- Include input text boxes for both a username and password.
- Retain the redirect URL as a hidden input item after extracting from the original URL.
- Extract and set the action URL in the page from the original URL.
- Include scripts to decode the return status code.
- Make sure that all paths used in the main page (to refer to images, for example).
- Ensure that no filenames within the bundle are greater than 30 characters.

Downloading a Customized Web Authentication Login Page (GUI)

Step 1 Copy the .tar file containing your login page to the default directory on your server.

Step 2 Choose **Commands** > **Download File** to open the Download File to Controller page.

Step 3 From the **File Type** drop-down list, choose **Webauth Bundle**.

Step 4 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**

- **SFTP** (available in the 7.4 and later releases)

Step 5 In the **IP Address** text box, enter the IP address of the server.

Step 6 If you are using a TFTP server, enter the maximum number of times the controller should attempt to download the .tar file in the Maximum Retries text box.
The range is 1 to 254.

The default is 10.

Step 7 If you are using a TFTP server, enter the amount of time in seconds before the controller times out while attempting to download the *.tar file in the Timeout text box.
The range is 1 to 254 seconds.

The default is 6 seconds.

Step 8 In the **File Path** text box, enter the path of the .tar file to be downloaded. The default value is "/."

Step 9 In the **File Name** text box, enter the name of the .tar file to be downloaded.

Step 10 If you are using an FTP server, follow these steps:

1. In the **Server Login Username** text box, enter the username to log into the FTP server.
2. In the **Server Login Password** text box, enter the password to log into the FTP server.
3. In the **Server Port Number** text box, enter the port number on the FTP server through which the download occurs. The default value is 21.

Step 11 Click **Download** to download the .tar file to the controller.

Step 12 Choose **Security** > **Web Auth** > **Web Login Page** to open the Web Login page.

Step 13 From the Web Authentication Type drop-down list, choose **Customized (Downloaded)**.

Step 14 Click **Apply**.

Step 15 Click **Preview** to view your customized web authentication login page.

Step 16 If you are satisfied with the content and appearance of the login page, click **Save Configuration**.

Downloading a Customized Web Authentication Login Page (CLI)

Step 1 Copy the .tar file containing your login page to the default directory on your server.

Step 2 Specify the download mode by entering this command:
transfer download mode {**tftp** | **ftp** | **sftp**

Step 3 Specify the type of file to be downloaded by entering this command:
transfer download datatype webauthbundle

Step 4 Specify the IP address of the TFTP server by entering this command:
transfer download serverip *tftp-server-ip-address*.

Note Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

Step 5 Specify the download path by entering this command:
transfer download path *absolute-tftp-server-path-to-file*

Step 6 Specify the file to be downloaded by entering this command:
transfer download filename *filename.tar*

Step 7 View your updated settings and answer **y** to the prompt to confirm the current download settings and start the download by entering this command:
transfer download start

Step 8 Specify the web authentication type by entering this command:
config custom-web webauth_type *customized*

Step 9 Enter the **save config** command to save your settings.

Example: Customized Web Authentication Login Page

This figure shows an example of a customized web authentication login page.

Figure 23: Customized Web Authentication Login Page Example

Verifying the Web Authentication Login Page Settings (CLI)

Verify your changes to the web authentication login page by entering this command:

show custom-web

Assigning Login, Login Failure, and Logout Pages per WLAN

Information About Assigning Login, Login Failure, and Logout Pages per WLAN

You can display different web authentication login, login failure, and logout pages to users per WLAN. This feature enables user-specific web authentication pages to be displayed for a variety of network users, such as guest users or employees within different departments of an organization.

Different login pages are available for all web authentication types (internal, external, and customized). However, different login failure and logout pages can be specified only when you choose customized as the web authentication type.

Assigning Login, Login Failure, and Logout Pages per WLAN (GUI)

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the ID number of the WLAN to which you want to assign a web login, login failure, or logout page.

Step 3 Choose **Security** > **Layer 3**.

Step 4 Make sure that **Web Policy** and **Authentication** are selected.

Step 5 To override the global authentication configuration web authentication pages, select the **Override Global Config** check box.

Step 6 When the Web Auth Type drop-down list appears, choose one of the following options to define the web authentication pages for wireless guest users:

- **Internal—**Displays the default web login page for the controller. This is the default value.
- **Customized—**Displays custom web login, login failure, and logout pages. If you choose this option, three separate drop-down lists appear for login, login failure, and logout page selection. You do not need to define a customized page for all three options. Choose **None** from the appropriate drop-down list if you do not want to display a customized page for that option.

  Note These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files.

- **External—**Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

  You can choose specific RADIUS or LDAP servers to provide external authentication on the WLANs > Edit (Security > AAA Servers) page. Additionally, you can define the priority in which the servers provide authentication.

Step 7 If you chose External as the web authentication type in Step 6, choose **AAA Servers** and choose up to three RADIUS and LDAP servers using the drop-down lists.

Note The RADIUS and LDAP external servers must already be configured in order to be selectable options on the WLANs > Edit (Security > AAA Servers) page. You can configure these servers on the RADIUS Authentication Servers page and LDAP Servers page.

Step 8 Establish the priority in which the servers are contacted to perform web authentication as follows:

Note The default order is local, RADIUS, LDAP.

1. Highlight the server type (local, RADIUS, or LDAP) that you want to be contacted first in the box next to the Up and Down buttons.
2. Click **Up** and **Down** until the desired server type is at the top of the box.
3. Click the **<** arrow to move the server type to the priority box on the left.
4. Repeat these steps to assign priority to the other servers.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Assigning Login, Login Failure, and Logout Pages per WLAN (CLI)

Step 1 Determine the ID number of the WLAN to which you want to assign a web login, login failure, or logout page by entering this command:
show wlan summary

Step 2 If you want wireless guest users to log into a customized web login, login failure, or logout page, enter these commands to specify the filename of the web authentication page and the WLAN for which it should display:

- **config wlan custom-web login-page** *page_name wlan_id—Defines a customized login page for a* given WLAN.
- **config wlan custom-web loginfailure-page** *page_name wlan_id—Defines a customized login* failure page for a given WLAN.

  Note To use the controller's default login failure page, enter the **config wlan custom-web loginfailure-page none** *wlan_id* command.

- **config wlan custom-web logout-page** *page_name wlan_id—Defines a customized logout page for* a given WLAN.

  Note To use the controller's default logout page, enter the **config wlan custom-web logout-page none** *wlan_id* command.

Step 3 Redirect wireless guess users to an external server before accessing the web login page by entering this command to specify the URL of the external server:
config wlan custom-web ext-webauth-url *ext_web_url wlan_id*

Step 4 Define the order in which web authentication servers are contacted by entering this command:
config wlan security web-auth server-precedence *wlan_id* {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**}

The default order of server web authentication is local, RADIUS and LDAP.

Note All external servers must be preconfigured on the controller. You can configure them on the RADIUS Authentication Servers page and the LDAP Servers page.

Step 5 Define which web authentication page displays for a wireless guest user by entering this command:
config wlan custom-web webauth-type {**internal** | **customized** | **external**} *wlan_id*

where

- **internal** displays the default web login page for the controller. This is the default value.
- **customized** displays the custom web login page that was configured in *Step 2*.

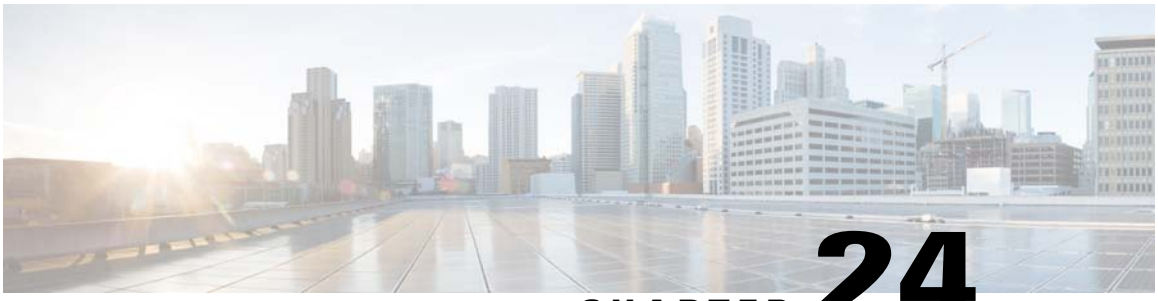
  Note You do not need to define the web authentication type in *Step 5* for the login failure and logout pages as they are always customized.

- **external** redirects users to the URL that was configured in *Step 3*.

Step 6 Use a WLAN-specific custom web configuration rather than a global custom web configuration by entering this command: **config wlan custom-web global disable** *wlan_id*

Note If you enter the **config wlan custom-web global enable** *wlan_id* command, the custom web authentication configuration at the global level is used.

Step 7 Save your changes by entering this command:
save config



CHAPTER 24

Configuring Wired Guest Access

Information About Wired Guest Access

Wired guest access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or through specific ports in a conference room. Like wireless guest user accounts, wired guest access ports are added to the network using the lobby ambassador feature.

Wired guest access can be configured in a standalone configuration or in a dual-controller configuration that uses both an anchor controller and a foreign controller. This latter configuration is used to further isolate wired guest access traffic but is not required for deployment of wired guest access.

Wired guest access ports initially terminate on a Layer 2 access switch or switch port configured with VLAN interfaces for wired guest access traffic. The wired guest traffic is then trunked from the access switch to a controller. This controller is configured with an interface that is mapped to a wired guest access VLAN on the access switch.

Note Although wired guest access is managed by anchor and foreign anchors when two controllers are deployed, mobility is not supported for wired guest access clients. In this case, DHCP and web authentication for the client are handled by the anchor controller.

Note You can specify the amount of bandwidth allocated to a wired guest user in the network by configuring a QoS role and a bandwidth contract.

You can create a basic peer to peer WLAN ACL and apply it to the wired guest WLAN. This will not block peer to peer traffic and the guest users can still communicate with each other.

Prerequisites for Configuring Wired Guest Access

To configure wired guest access on a wireless network, you must perform the following:

1. Configure a dynamic interface (VLAN) for wired guest user access
2. Create a wired LAN for guest user access
3. Configure the controller
4. Configure the anchor controller (if terminating traffic on another controller)
5. Configure security for the guest LAN
6. Verify the configuration

Restrictions for Configuring Wired Guest Access

- Wired guest access interfaces must be tagged.
- Wired guest access ports must be in the same Layer 2 network as the foreign controller.
- Up to five wired guest access LANs can be configured on a controller. Also in a wired guest access LAN, multiple anchors are supported.
- Layer 3 web authentication and web passthrough are supported for wired guest access clients. Layer 2 security is not supported.
- Do not trunk a wired guest VLAN to multiple foreign controllers, as it might produce unpredictable results.

Configuring Wired Guest Access (GUI)

Step 1 To create a dynamic interface for wired guest user access, choose **Controller** > **Interfaces**. The Interfaces page appears.

Step 2 Click **New** to open the **Interfaces > New** page.

Step 3 Enter a name and VLAN ID for the new interface.

Step 4 Click **Apply** to commit your changes.

Step 5 In the **Port Number** text box, enter a valid port number. You can enter a number between 0 and 25 (inclusive).

Step 6 Select the **Guest LAN** check box.

Step 7 Click **Apply** to commit your changes.

Step 8 To create a wired LAN for guest user access, choose **WLANs**.

Step 9 On the WLANs page, choose **Create New** from the drop-down list and click **Go**. The **WLANs** > **New page** appears.

Step 10 From the Type drop-down list, choose **Guest LAN**.

Step 11 In the **Profile Name** text box, enter a name that identifies the guest LAN. Do not use any spaces.

Step 12 From the WLAN ID drop-down list, choose the ID number for this guest LAN.

Note You can create up to five guest LANs, so the WLAN ID options are 1 through 5 (inclusive).

Step 13 Click **Apply** to commit your changes.

Step 14 Select the **Enabled** check box for the Status parameter.

Step 15 Web authentication (Web-Auth) is the default security policy. If you want to change this to web passthrough, choose the **Security** tab after completing *Step 16* and *Step 17*.

Step 16 From the Ingress Interface drop-down list, choose the VLAN that you created in *Step 3*. This VLAN provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 17 From the Egress Interface drop-down list, choose the name of the interface. This WLAN provides a path out of the controller for wired guest client traffic.

Step 18 If you want to change the authentication method (for example, from web authentication to web passthrough), choose **Security** > **Layer 3**. The **WLANs > Edit (Security > Layer 3)** page appears.

Step 19 From the Layer 3 Security drop-down list, choose one of the following:

- **None—**Layer 3 security is disabled.
- **Web Authentication—**Causes users to be prompted for a username and password when connecting to the wireless network. This is the default value.
- **Web Passthrough—**Allows users to access the network without entering a username and password.

  Note There should not be a Layer 3 gateway on the guest wired VLAN, as this would bypass the web authentication done through the controller.

Step 20 If you choose the Web Passthrough option, an **Email Input** check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

Step 21 To override the global authentication configuration set on the Web Login page, select the **Override Global Config** check box.

Step 22 When the Web Auth Type drop-down list appears, choose one of the following options to define the web authentication pages for wired guest users:

- **Internal—**Displays the default web login page for the controller. This is the default value.
- **Customized—**Displays custom web login, login failure, and logout pages. If you choose this option, three separate drop-down lists appear for login, login failure, and logout page selection. You do not need to define a customized page for all three options. Choose **None** from the appropriate drop-down list if you do not want to display a customized page for that option.

  Note These optional login, login failure, and logout pages are downloaded to the controller as webauth.tar files.
- **External—**Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

  You can choose specific RADIUS or LDAP servers to provide external authentication on the WLANs > Edit (Security > AAA Servers) page. Additionally, you can define the priority in which the servers provide authentication.

Step 23 If you chose External as the web authentication type in *Step 22*, choose **AAA Servers** and choose up to three RADIUS and LDAP servers using the drop-down lists.

Note The RADIUS and LDAP external servers must already be configured in order to be selectable options on the WLANs > Edit (Security > AAA Servers) page. You can configure these servers on the RADIUS Authentication Servers page and LDAP Servers page.

Step 24 To establish the priority in which the servers are contacted to perform web authentication as follows:

Note The default order is local, RADIUS,
LDAP.

1. Highlight the server type (local, RADIUS, or LDAP) that you want to be contacted first in the box next to the Up and Down buttons.
2. Click **Up** and **Down** until the desired server type is at the top of the box.
3. Click the **<** arrow to move the server type to the priority box on the left.
4. Repeat these steps to assign priority to the other servers.

Step 25 Click **Apply**.

Step 26 Click **Save Configuration**.

Step 27 Repeat this process if a second (anchor) controller is being used in the network.

Configuring Wired Guest Access (CLI)

Step 1 Create a dynamic interface (VLAN) for wired guest user access by entering this command:
config interface create *interface_name vlan_id*

Step 2 If link aggregation trunk is not configured, enter this command to map a physical port to the interface:
config interface port *interface_name primary_port* {*secondary_port*}

Step 3 Enable or disable the guest LAN VLAN by entering this command:
config interface guest-lan *interface_name* {**enable | disable}**

This VLAN is later associated with the ingress interface created in *Step 5*.

Step 4 Create a wired LAN for wired client traffic and associate it to an interface by entering this command:
config guest-lan create *guest_lan_id interface_name*

The guest LAN ID must be a value between 1 and 5 (inclusive).

Note To delete a wired guest LAN, enter the **config guest-lan delete** *guest_lan_id command.*

Step 5 Configure the wired guest VLAN's ingress interface, which provides a path between the wired guest client and the controller by way of the Layer 2 access switch by entering this command:
config guest-lan ingress-interface *guest_lan_id interface_name*

Step 6 Configure an egress interface to transmit wired guest traffic out of the controller by entering this command:
config guest-lan interface *guest_lan_id interface_name*

Note If the wired guest traffic is terminating on another controller, repeat *Step 4* and *Step 6* for the terminating (anchor) controller and *Step 1* through *Step 5* for the originating (foreign) controller. Additionally, configure the **config mobility group anchor add** {**guest-lan** *guest_lan_id* | **wlan** *wlan_id} IP_address* command for both controllers.

Step 7 Configure the security policy for the wired guest LAN by entering this command:
config guest-lan security {**web-auth enable guest_lan_id** | **web-passthrough enable** *guest_lan_id*}

Note Web authentication is the default setting.

Step 8 Enable or disable a wired guest LAN by entering this command:
config guest-lan {enable | disable} *guest_lan_id*

Step 9 If you want wired guest users to log into a customized web login, login failure, or logout page, enter these commands to specify the filename of the web authentication page and the guest LAN for which it should display:

- **config guest-lan custom-web login-page** *page_name guest_lan_id—Defines a web login page.*
- **config guest-lan custom-web loginfailure-page** *page_name guest_lan_id—Defines a web login failure* page.

  Note To use the controller's default login failure page, enter the **config guest-lan custom-web loginfailure-page none** *guest_lan_id* command.

- **config guest-lan custom-web logout-page** *page_name guest_lan_id*—Defines a web logout page.

  Note To use the controller's default logout page, enter the **config guest-lan custom-web logout-page none** *guest_lan_id* command.

Step 10 If you want wired guest users to be redirected to an external server before accessing the web login page, enter this command to specify the URL of the external server:
config guest-lan custom-web ext-webauth-url *ext_web_url guest_lan_id*

Step 11 If you want to define the order in which local (controller) or external (RADIUS, LDAP) web authentication servers are contacted, enter this command:
config wlan security web-auth server-precedence *wlan_id* {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**} {**local** | **ldap** | **radius**}

The default order of server web authentication is local, RADIUS, LDAP.

Note All external servers must be preconfigured on the controller. You can configure them on the RADIUS Authentication Servers page or the LDAP Servers page.

Step 12 Define the web login page for wired guest users by entering this command:

config guest-lan custom-web webauth-type {**internal** | **customized** | **external**} *guest_lan_id*

where

-
- **internal** displays the default web login page for the controller. This is the default value.
- **customized** displays the custom web pages (login, login failure, or logout) that were configured in *Step 9*.
- **external** redirects users to the URL that was configured in *Step 10*.

Step 13 Use a guest-LAN specific custom web configuration rather than a global custom web configuration by entering this command:
config guest-lan custom-web global disable *guest_lan_id*

Note If you enter the **config guest-lan custom-web global enable** *guest_lan_id* command, the custom web authentication configuration at the global level is used.

Step 14 Save your changes by entering this command:
save config

Note Information on the configured web authentication appears in both the **show run-config** and **show running-config** commands.

Step 15 Display the customized web authentication settings for a specific guest LAN by entering this command:
show custom-web {all | guest-lan guest_lan_id}

Note If internal web authentication is configured, the Web Authentication Type displays as internal rather than external (controller level) or customized (WLAN profile level).

Step 16 Display a summary of the local interfaces by entering this command:
show interface summary

Note The interface name of the wired guest LAN in this example is *wired-guest* and its VLAN ID is 236.

Display detailed interface information by entering this command:

show interface detailed *interface_name*

Step 17 Display the configuration of a specific wired guest LAN by entering this command:
show guest-lan *guest_lan_id*

Note Enter the **show guest-lan summary** command to see all wired guest LANs configured on the controller.

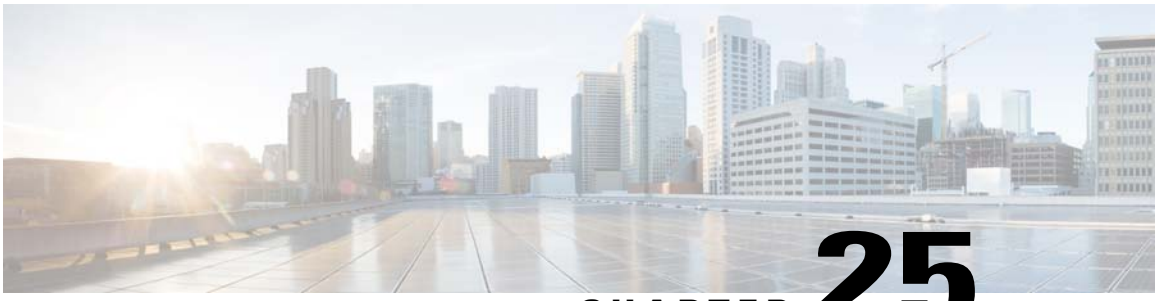
Step 18 Display the active wired guest LAN clients by entering this command:
show client summary guest-lan

Step 19 Display detailed information for a specific client by entering this command:
show client detail *client_mac*

Supporting IPv6 Client Guest Access

The client is in WebAuth Required state until the client is authenticated. The controller intercepts both IPv4 and IPv6 traffic in this state and redirects it to the virtual IP address of the controller. Once authenticated, the user's MAC address is moved to the run state and both IPv4 and IPv6 traffic is allowed to pass.

In order to support the redirection of IPv6-only clients, the controller automatically creates an IPv6 virtual address based on the IPv4 virtual address configured on the controller. The virtual IPv6 address follows the convention of [::ffff:<virtual IPv4 address>]. For example, a virtual IP address of 192.0.2.1 would translate into [::ffff:192.0.2.1]. For an IPv6 captive portal to be displayed, the user must request an IPv6 resolvable DNS entry such as ipv6.google.com which returns a DNSv6 (AAAA) record.



CHAPTER 25

Troubleshooting

Interpreting LEDs

Information About Interpreting LEDs

This section describes how to interpret controller LEDs and lightweight access point LEDs.

Interpreting Controller LEDs

See the quick start guide for your specific controller for a description of the LED patterns. See the list of controllers and the respective documentation at http://www.cisco.com/en/US/products/hw/wireless/index.html.

Interpreting Lightweight Access Point LEDs

See the quick start guide or hardware installation guide for your specific access point for a description of the LED patterns. See the list of access points and the respective documentation at http://www.cisco.com/en/US/products/hw/wireless/index.html.

System Messages

Information About System Messages

This table lists some common system messages and their descriptions. For a complete list of system messages, see the *Cisco Wireless LAN Controller System Message Guide, Release 7.0*.

Table 6: System Messages and Descriptions

Error Message	Description
apf_utils.c 680: Received a CIF field without the protected bit set from mobile xx:xx:xx:xx:xx:xx	A client is sending an association request on a security-enabled WLAN with the protected bit set to 0 (in the Capability field of the association request). As designed, the controller rejects the association request, and the client sees an association failure.
dtl_arp.c 480: Got an idle-timeout message from an unknown client xx:xx:xx:xx:xx:xx	The controller's network processing unit (NPU) sends a timeout message to the central processing unit (CPU) indicating that a particular client has timed out or aged out. This situation typically occurs when the CPU has removed a wireless client from its internal database but has not notified the NPU. Because the client remains in the NPU database, it ages out on the network processor and notifies the CPU. The CPU finds the client that is not present in its database and then sends this message.
STATION_DISASSOCIATE	The client may have intentionally terminated usage or may have experienced a service disruption.
STATION_DEAUTHENTICATE	The client may have intentionally terminated usage or this message could indicate an authentication issue.
STATION_AUTHENTICATION_FAIL	Check disable, key mismatch, or other configuration issues.
STATION_ASSOCIATE_FAIL	Check load on the Cisco radio or signal quality issues.
LRAD_ASSOCIATED	The associated lightweight access point is now managed by this controller.

Error Message	Description
LRAD_DISASSOCIATED	The lightweight access point may have associated to a different controller or may have become completely unreachable.
LRAD_UP	The lightweight access point is operational; no action required.
LRAD_DOWN	The lightweight access point may have a problem or is administratively disabled.
LRADIF_UP	The Cisco radio is UP.
LRADIF_DOWN	The Cisco radio may have a problem or is administratively disabled.
LRADIF_LOAD_PROFILE_FAILED	The client density may have exceeded system capacity.
LRADIF_NOISE_PROFILE_FAILED	The non-802.11 noise has exceeded the configured threshold.
LRADIF_INTERFERENCE_PROFILE_FAILED	802.11 interference has exceeded threshold on channel; check channel assignments.
LRADIF_COVERAGE_PROFILE_FAILED	A possible coverage hole has been detected. Check the lightweight access point history to see if it is a common problem and add lightweight access points if necessary.
LRADIF_LOAD_PROFILE_PASSED	The load is now within threshold limits.
LRADIF_NOISE_PROFILE_PASSED	The detected noise is now less than threshold.
LRADIF_INTERFERENCE_PROFILE_PASSED	The detected interference is now less than threshold.
LRADIF_COVERAGE_PROFILE_PASSED	The number of clients receiving a poor signal are within threshold.
LRADIF_CURRENT_TXPOWER_CHANGED	Informational message.
LRADIF_CURRENT_CHANNEL_CHANGED	Informational message.
LRADIF_RTS_THRESHOLD_CHANGED	Informational message.
LRADIF_ED_THRESHOLD_CHANGED	Informational message.
LRADIF_FRAGMENTATION_THRESHOLD_CHANGED	Informational message.
RRM_DOT11_A_GROUPING_DONE	Informational message.
RRM_DOT11_B_GROUPING_DONE	Informational message.
ROGUE_AP_DETECTED	May be a security issue. Use maps and trends to investigate.

Error Message	Description
ROGUE_AP_REMOVED	A detected rogue access point has timed out. The unit might have shut down or moved out of the coverage area.
AP_MAX_ROGUE_COUNT_EXCEEDED	The current number of active rogue access points has exceeded system threshold.
LINK_UP	Positive confirmation message.
LINK_DOWN	A port may have a problem or is administratively disabled.
LINK_FAILURE	A port may have a problem or is administratively disabled.
AUTHENTICATION_FAILURE	An attempted security breech has occurred. Investigate.
STP_NEWROOT	Informational message.
STP_TOPOLOGY_CHANGE	Informational message.
IPSEC_ESP_AUTH_FAILURE	Check WLAN IPsec configuration.
IPSEC_ESP_REPLAY_FAILURE	Check for an attempt to spoof an IP address.
IPSEC_ESP_POLICY_FAILURE	Check for a IPsec configuration mismatch between WLAN and client.
IPSEC_ESP_INVALID_SPI	Informational message.
IPSEC_OTHER_POLICY_FAILURE	Check for a IPsec configuration mismatch between WLAN and client.
IPSEC_IKE_NEG_FAILURE	Check for a IPsec IKE configuration mismatch between WLAN and client.
IPSEC_SUITE_NEG_FAILURE	Check for a IPsec IKE configuration mismatch between WLAN and client.
IPSEC_INVALID_COOKIE	Informational message.
RADIOS_EXCEEDED	The maximum number of supported Cisco radios has been exceeded. Check for a controller failure in the same Layer 2 network or add another controller.
SENSED_TEMPERATURE_HIGH	Check fan, air conditioning, and/or other cooling arrangements.
SENSED_TEMPERATURE_LOW	Check room temperature and/or other reasons for low temperature.
TEMPERATURE_SENSOR_FAILURE	Replace temperature sensor as soon as possible.

Error Message	Description
TEMPERATURE_SENSOR_CLEAR	The temperature sensor is operational.
POE_CONTROLLER_FAILURE	Check ports; a possible serious failure has been detected.
MAX_ROGUE_COUNT_EXCEEDED	The current number of active rogue access points has exceeded system threshold.
SWITCH_UP	The controller is responding to SNMP polls.
SWITCH_DOWN	The controller is not responding to SNMP polls; check controller and SNMP settings.
RADIUS_SERVERS_FAILED	Check network connectivity between RADIUS and the controller.
CONFIG_SAVED	The running configuration has been saved to flash; it will be active after a reboot.
MULTIPLE_USERS	Another user with the same username has logged in.
FAN_FAILURE	Monitor controller temperature to avoid overheating.
POWER_SUPPLY_CHANGE	Check for a power-supply malfunction.
COLD_START	The controller may have been rebooted.
WARM_START	The controller may have been rebooted.

Viewing System Resources

Information About Viewing System Resources

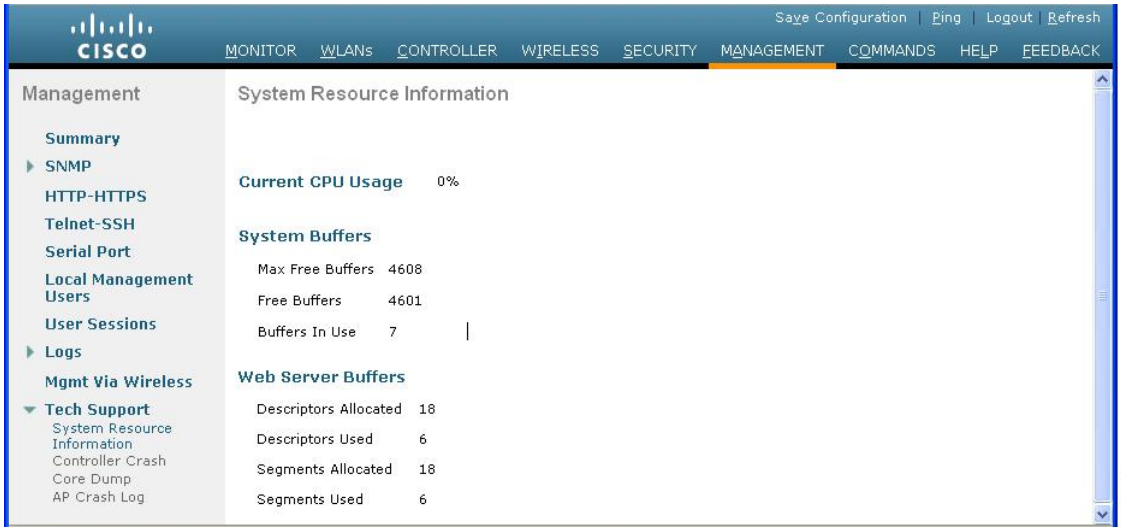
You can determine the amount of system resources being used by the controller. Specifically, you can view the current controller CPU usage, system buffers, and web server buffers.

The Cisco 5500 Series Controllers have multiple CPUs, so you can view individual CPU usage. For each CPU, you can see the percentage of the CPU in use and the percentage of the CPU time spent at the interrupt level (for example, 0%/3%).

Viewing System Resources (GUI)

On the controller GUI, choose **Management > Tech Support > System Resource Information**. The System Resource Information page appears.

Figure 24: System Resource Information Page



Viewing System Resources (CLI)

On the controller CLI, enter these commands:

- **show cpu**

  Where the first number is the CPU percentage that the controller spent on the user application and the second number is the CPU percentage that the controller spent on the OS services.

- **show tech-support**

Using the CLI to Troubleshoot Problems

If you experience any problems with your controller, you can use the commands in this section to gather information and debug issues.

- **show process cpu—**Shows how various tasks in the system are using the CPU at that instant in time. This command is helpful in understanding if any single task is monopolizing the CPU and preventing other tasks from being performed.
  The Priority field shows two values: 1) the original priority of the task that was created by the actual function call and 2) the priority of the task divided by a range of system priorities.

  The CPU Use field shows the CPU usage of a particular task.

  The Reaper field shows three values: 1) the amount of time for which the task is scheduled in user mode operation, 2) the amount of time for which the task is scheduled in system mode operation, and 3) whether the task is being watched by the reaper task monitor (indicated by a “T”). If the task is being watched

by the reaper task monitor, this field also shows the timeout value (in seconds) before which the task needs to alert the task monitor.

Note If you want to see the total CPU usage as a percentage, enter the **show cpu** command.

- **show process memory—**Shows the allocation and deallocation of memory from various processes in the system at that instant in time.
  In the example above, the following fields provide information:
  The Name field shows the tasks that the CPU is to perform.

  The Priority field shows two values: 1) the original priority of the task that was created by the actual function call and 2) the priority of the task divided by a range of system priorities.

  The BytesInUse field shows the actual number of bytes used by dynamic memory allocation for a particular task.

  The BlocksInUse field shows the chunks of memory that are assigned to perform a particular task.

  The Reaper field shows three values: 1) the amount of time for which the task is scheduled in user mode operation, 2) the amount of time for which the task is scheduled in system mode operation, and 3) whether the task is being watched by the reaper task monitor (indicated by a “T”). If the task is being watched by the reaper task monitor, this field also shows the timeout value (in seconds) before which the task needs to alert the task monitor.
- **show tech-support—**Shows an array of information related to the state of the system, including the current configuration, last crash file, CPU utilization, and memory utilization.
- **show run-config—**Shows the complete configuration of the controller. To exclude access point configuration settings, use the **show run-config no-ap** command.

Note If you want to see the passwords in clear text, enter the **config passwd-cleartext enable command**. To execute this command, you must enter an admin password. This command is valid only for this particular session. It is not saved following a reboot.

- **show run-config commands—**Shows the list of configured commands on the controller. This command shows only values configured by the user. It does not show system-configured default values.

Configuring System and Message Logging

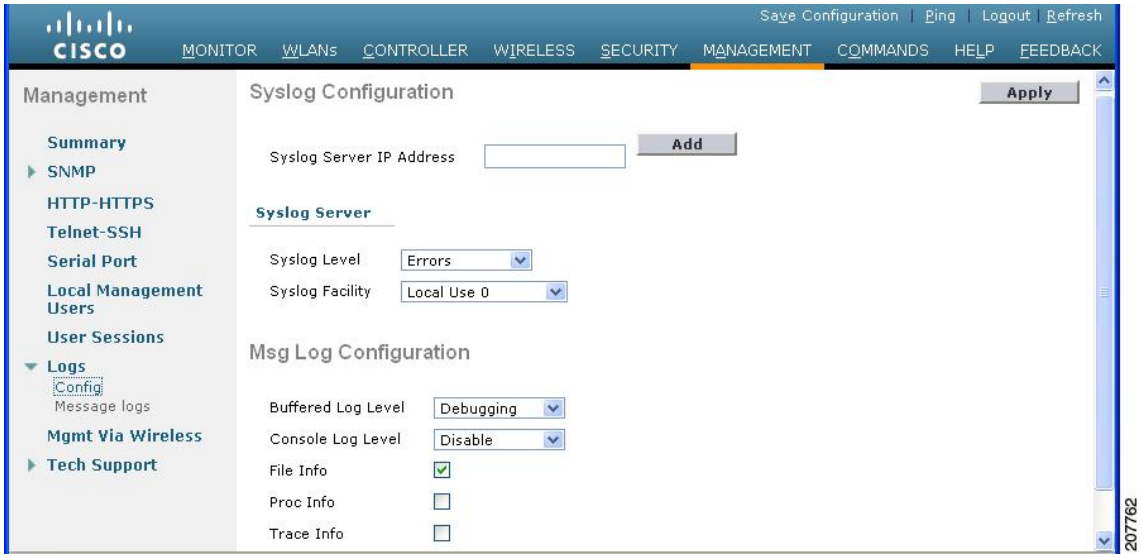
Information About System and Message Logging

System logging allows controllers to log their system events to up to three remote syslog servers. The controller sends a copy of each syslog message as it is logged to each syslog server configured on the controller. Being able to send the syslog messages to multiple servers ensures that the messages are not lost due to the temporary unavailability of one syslog server. Message logging allows system messages to be logged to the controller buffer or console.

Configuring System and Message Logging (GUI)

Step 1 Choose **Management > Logs > Config**. The Syslog Configuration page appears.

Figure 25: Syslog Configuration Page



Step 2 In the **Syslog Server IP Address** text box, enter the IP address of the server to which to send the syslog messages and click **Add**. You can add up to three syslog servers to the controller. The list of syslog servers that have already been added to the controller appears below this text box.

Note If you want to remove a syslog server from the controller, click **Remove** to the right of the desired server.

Step 3 To set the severity level for filtering syslog messages to the syslog servers, choose one of the following options from the **Syslog Level** drop-down list:

- **Emergencies** = Severity level 0
- **Alerts** = Severity level 1 (default value)
- **Critical** = Severity level 2
- **Errors** = Severity level 3
- **Warnings** = Severity level 4
- **Notifications** = Severity level 5
- **Informational** = Severity level 6
- **Debugging** = Severity level 7

If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the syslog servers. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the syslog servers.

Step 4 To set the facility for outgoing syslog messages to the syslog servers, choose one of the following options from the **Syslog Facility** drop-down list :

- **Kernel** = Facility level 0
- **User Process** = Facility level 1
- **Mail** = Facility level 2
- **System Daemons** = Facility level 3
- **Authorization** = Facility level 4
- **Syslog** = Facility level 5 (default value)
- **Line Printer** = Facility level 6
- **USENET** = Facility level 7
- **Unix-to-Unix Copy** = Facility level 8
- **Cron** = Facility level 9
- **FTP Daemon** = Facility level 11
- **System Use 1** = Facility level 12
- **System Use 2** = Facility level 13
- **System Use 3** = Facility level 14
- **System Use 4** = Facility level 15
- **Local Use 0** = Facility level 16
- **Local Use 2** = Facility level 17
- **Local Use 3** = Facility level 18
- **Local Use 4** = Facility level 19
- **Local Use 5** = Facility level 20
- **Local Use 5** = Facility level 21
- **Local Use 5** = Facility level 22
- **Local Use 5** = Facility level 23

Step 5 Click **Apply**.

Step 6 To set the severity level for logging messages to the controller buffer and console, choose one of the following options from both the **Buffered Log Level** and **Console Log Level** drop-down lists:

- **Emergencies** = Severity level 0
- **Alerts** = Severity level 1
- **Critical** = Severity level 2

- **Errors** = Severity level 3 (default value)
- **Warnings** = Severity level 4
- **Notifications** = Severity level 5
- **Informational** = Severity level 6
- **Debugging** = Severity level 7
- **Disable—** This option is available only for Console Log level. Select this option to disable console logging.

If you set a logging level, only those messages whose severity is equal to or less than that level are logged by the controller. For example, if you set the logging level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are logged.

Step 7 Select the **File Info** check box if you want the message logs to include information about the source file. The default value is enabled.

Step 8 Select the **Trace Info** check box if you want the message logs to include traceback information. The default is disabled.

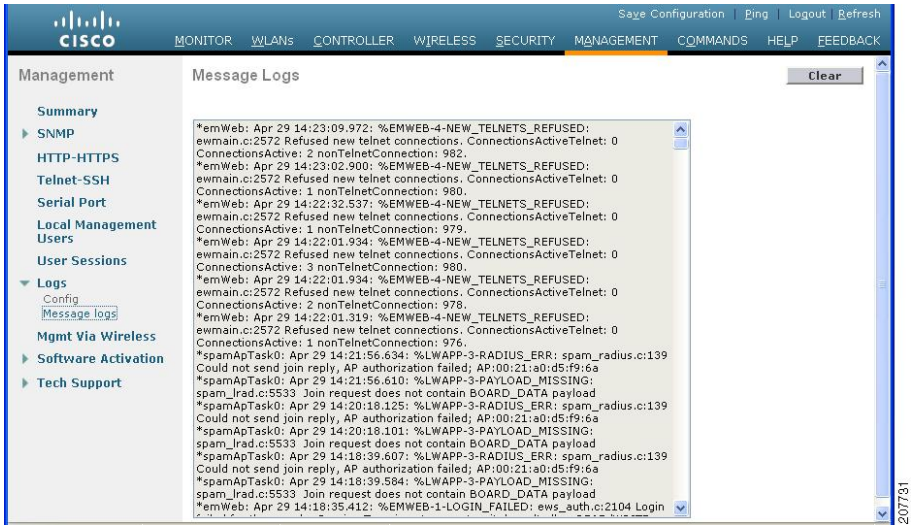
Step 9 Click **Apply**.

Step 10 Click **Save Configuration**.

Viewing Message Logs (GUI)

To view message logs using the controller GUI, choose **Management > Logs > Message Logs**. The Message Logs page appears.

Figure 26: Message Logs Page



Note To clear the current message logs from the controller, click **Clear**.

Configuring System and Message Logging (CLI)

Step 1 Enable system logging and set the IP address of the syslog server to which to send the syslog messages by entering this command:
config logging syslog host *server_IP_address*

You can add up to three syslog servers to the controller.

Note To remove a syslog server from the controller by entering this command: **config logging syslog host** *server_IP_address* **delete**

Step 2 Set the severity level for filtering syslog messages to the syslog server by entering this command:
config logging syslog level *severity_level*

where *severity_level* is one of the following:

- emergencies = Severity level 0
- alerts = Severity level 1
- critical = Severity level 2
- errors = Severity level 3
- warnings = Severity level 4
- notifications = Severity level 5
- informational = Severity level 6
- debugging = Severity level 7

Note As an alternative, you can enter a number from 0 through 7 for the *severity_level* parameter.

Note If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the syslog server. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the syslog server.

Step 3 Set the severity level for filtering syslog messages for a particular access point or for all access points by entering this command:
config ap logging syslog level *severity_level* {*Cisco_AP* | **all**}

where *severity_level* is one of the following:

- emergencies = Severity level 0
- alerts = Severity level 1
- critical = Severity level 2
- errors = Severity level 3
- warnings = Severity level 4

- notifications = Severity level 5
- informational = Severity level 6
- debugging = Severity level 7

Note If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the access point. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the access point.

Step 4 Set the facility for outgoing syslog messages to the syslog server by entering this command:
config logging syslog facility *facility_code*

where *facility_code* is one of the following:

- authorization = Authorization system. Facility level = 4.
- auth-private = Authorization system (private). Facility level = 10.
- cron = Cron/at facility. Facility level = 9.
- daemon = System daemons. Facility level = 3.
- ftp = FTP daemon. Facility level = 11.
- kern = Kernel. Facility level = 0.
- local0 = Local use. Facility level = 16.
- local1 = Local use. Facility level = 17.
- local2 = Local use. Facility level = 18.
- local3 = Local use. Facility level = 19.
- local4 = Local use. Facility level = 20.
- local5 = Local use. Facility level = 21.
- local6 = Local use. Facility level = 22.
- local7 = Local use. Facility level = 23.
- lpr = Line printer system. Facility level = 6.
- mail = Mail system. Facility level = 2.
- news = USENET news. Facility level = 7.
- sys12 = System use. Facility level = 12.
- sys13 = System use. Facility level = 13.
- sys14 = System use. Facility level = 14.
- sys15 = System use. Facility level = 15.
- syslog = The syslog itself. Facility level = 5.
- user = User process. Facility level = 1.

- uucp = Unix-to-Unix copy system. Facility level = 8.

Step 5 Set the severity level for logging messages to the controller buffer and console, enter these commands:

- **config logging buffered** *severity_level*
- **config logging console** *severity_level*

where *severity_level* is one of the following:

- emergencies = Severity level 0
- alerts = Severity level 1
- critical = Severity level 2
- errors = Severity level 3
- warnings = Severity level 4
- notifications = Severity level 5
- informational = Severity level 6
- debugging = Severity level 7

Note As an alternative, you can enter a number from 0 through 7 for the *severity_level* parameter.

Note If you set a logging level, only those messages whose severity is equal to or less than that level are logged by the controller. For example, if you set the logging level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are logged.

Step 6 Save debug messages to the controller buffer, the controller console, or a syslog server by entering these commands:

- **config logging debug buffered {enable | disable}**
- **config logging debug console {enable | disable}**
- **config logging debug syslog {enable | disable}**

By default, the console command is enabled, and the buffered and syslog commands are disabled.

Step 7 To cause the controller to include information about the source file in the message logs or to prevent the controller from displaying this information by entering this command:
config logging fileinfo {enable | disable}

The default value is enabled.

Step 8 Configure the controller to include process information in the message logs or to prevent the controller from displaying this information by entering this command:
config logging procinfo {**enable** | **disable**}

The default value is disabled.

Step 9 Configure the controller to include traceback information in the message logs or to prevent the controller from displaying this information by entering this command:
config logging traceinfo {enable | disable}

The default value is disabled.

Step 10 Enable or disable timestamps in log messages and debug messages by entering these commands:

- **config service timestamps log {datetime | disable}**
- **config service timestamps debug {datetime | disable}**

  where

  - **datetime** = Messages are timestamped with the standard date and time. This is the default value.
  - **disable** = Messages are not timestamped.

Step 11 Save your changes by entering this command:
save config

Viewing System and Message Logs (CLI)

To see the logging parameters and buffer contents, enter this command:

show logging

Viewing Access Point Event Logs

Information About Access Point Event Logs

Access points log all system messages (with a severity level greater than or equal to notifications) to the access point event log. The event log can contain up to 1024 lines of messages, with up to 128 characters per line. When the event log becomes filled, the oldest message is removed to accommodate a new event message. The event log is saved in a file on the access point flash, which ensures that it is saved through a reboot cycle. To minimize the number of writes to the access point flash, the contents of the event log are written to the event log file during normal reload and crash scenarios only.

Viewing Access Point Event Logs (CLI)

Use these CLI commands to view or clear the access point event log from the controller:

- To see the contents of the event log file for an access point that is joined to the controller, enter this command:

  show ap eventlog *Cisco_AP*

  Information similar to the following appears:

```
AP event log download has been initiated
Waiting for download to complete

AP event log download completed.
 ========================= AP Event log Contents =====================
*Sep 22 11:44:00.573: %CAPWAP-5-CHANGED: CAPWAP changed state to IMAGE
*Sep 22 11:44:01.514: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0,
```

```
changed state to down
*Sep 22 11:44:01.519: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1,
changed state to down
*Sep 22 11:44:53.539: *** Access point reloading. Reason: NEW IMAGE DOWNLOAD ***
*Mar 1 00:00:39.078: %CAPWAP-3-ERRORLOG: Did not get log server settings from DHCP.
*Mar 1 00:00:42.142: %CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source
*Mar 1 00:00:42.151: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Mar 1 00:00:42.158: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Mar 1 00:00:43.143: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1,
changed state to up
*Mar 1 00:00:43.151: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio0,
changed state to up
*Mar 1 00:00:48.078: %CAPWAP-3-ERRORLOG: Could Not resolve CISCO-CAPWAP-CONTROLLER
*Mar 1 00:01:42.144: %CDP_PD-4-POWER_OK: Full power - NEGOTIATED inline power source
*Mar 1 00:01:48.121: %CAPWAP-3-CLIENTERRORLOG: Set Transport Address: no more AP manager
 IP addresses remain
*Mar 1 00:01:48.122: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN
*Mar 1 00:01:48.122: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down
*Mar 1 00:01:48.122: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
administratively down
```

- To delete the existing event log and create an empty event log file for a specific access point or for all access points joined to the controller, enter this command:

  clear ap-eventlog {**specific** *Cisco_AP* | **all**}

Uploading Logs and Crash Files

Prerequisites to Upload Logs and Crash Files

- Follow the instructions in this section to upload logs and crash files from the controller. However, before you begin, ensure you have a TFTP or FTP server available for the file upload. Follow these guidelines when setting up a TFTP or FTP server:
  - If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are uploading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP or FTP server cannot run on the same computer as Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

Uploading Logs and Crash Files (GUI)

Step 1 Choose **Command > Upload File**. The Upload File from Controller page appears.

Step 2 From the **File Type** drop-down list, choose one of the following:

- **Event Log**

- **Message Log**
- **Trap Log**
- **Crash File**

Step 3 From the **Transfer Mode** drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in the 7.4 and later releases)

Step 4 In the **IP Address** text box, enter the IP address of the server.

Step 5 In the **File Path** text box, enter the directory path of the log or crash file.

Step 6 In the **File Name** text box, enter the name of the log or crash file.

Step 7 If you chose FTP as the Transfer Mode, follow these steps:

1. In the **Server Login Username** text box, enter the FTP server login name.
2. In the **Server Login Password** text box, enter the FTP server login password.
3. In the **Server Port Number** text box, enter the port number of the FTP server. The default value for the server port is 21.

Step 8 Click **Upload** to upload the log or crash file from the controller. A message appears indicating the status of the upload.

Uploading Logs and Crash Files (CLI)

Step 1 To transfer the file from the controller to a server, enter this command:
transfer upload mode {**tftp** | **ftp** | **sftp**}

Step 2 To specify the type of file to be uploaded, enter this command:
transfer upload datatype *datatype*

where *datatype* is one of the following options:

- **crashfile—**Uploads the system's crash file.
- **errorlog—**Uploads the system's error log.
- **panic-crash-file—**Uploads the kernel panic information if a kernel panic occurs.
- **systemtrace—**Uploads the system's trace file.
- **traplog—**Uploads the system's trap log.

- **watchdog-crash-file—**Uploads the console dump resulting from a software-watchdog-initiated reboot of the controller following a crash. The software watchdog module periodically checks the integrity of the internal software and makes sure that the system does not stay in an inconsistent or nonoperational state for a long period of time.

Step 3 To specify the path to the file, enter these commands:

- **transfer upload serverip** *server_ip_address*
- **transfer upload path** *server_path_to_file*
- **transfer upload filename** *filename*

Step 4 If you are using an FTP server, also enter these commands:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the port parameter is 21.

Step 5 To see the updated settings, enter this command:

transfer upload start

Step 6 When prompted to confirm the current settings and start the software upload, answer **y**.

Uploading Core Dumps from the Controller

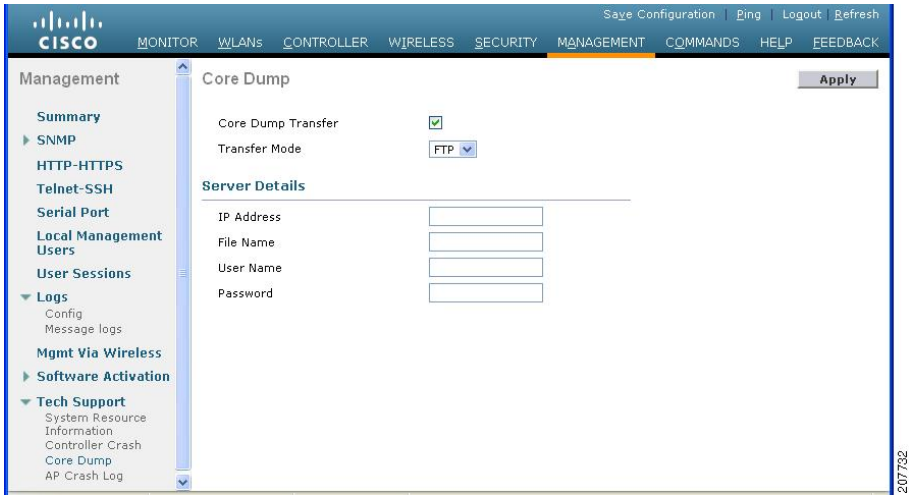
Information About Uploading Core Dumps from the Controller

To help troubleshoot controller crashes, you can configure the controller to automatically upload its core dump file to an FTP server after experiencing a crash. You cannot upload the core dump file directly to an FTP or TFTP server but you can upload a crash file to an FTP or TFTP server. The controllers save the core dump file to flash memory following a crash.

Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (GUI)

Step 1 Choose **Management > Tech Support > Core Dump** to open the Core Dump page.

Figure 27: Core Dump Page



Step 2 To enable the controller to generate a core dump file following a crash, select the **Core Dump Transfer** check box.

Step 3 To specify the type of server to which the core dump file is uploaded, choose **FTP** from the **Transfer Mode** drop-down list.

Step 4 In the **IP Address** text box, enter the IP address of the FTP server.

Note The controller must be able to reach the FTP server.

Step 5 In the **File Name** text box, enter the name that the controller uses to label the core dump file.

Step 6 In the **User Name** text box, enter the username for FTP login.

Step 7 In the **Password** text box, enter the password for FTP login.

Step 8 Click **Apply** to commit your changes.

Step 9 Click **Save Configuration** to save your changes.

Configuring the Controller to Automatically Upload Core Dumps to an FTP Server (CLI)

Step 1 To enable or disable the controller to generate a core dump file following a crash, enter this command:
config coredump {**enable** | **disable**}

Step 2 To specify the FTP server to which the core dump file is uploaded, enter this command:

config coredump ftp *server_ip_address filename*

where

- *server_ip_address* is the IP address of the FTP server to which the controller sends its core dump file.

  Note The controller must be able to reach the FTP server.

- *filename* is the name that the controller uses to label the core dump file.

Step 3 To specify the username and password for FTP login, enter this command:
config coredump username *ftp_username* **password** *ftp_password*

Step 4 To save your changes, enter this command:
save config

Step 5 To see a summary of the controller's core dump file, enter this command:

Example:
Information similar to the following appears:

show coredump summary

Information similar to the following appears:

```
Core Dump is enabled

FTP Server IP..................................... 10.10.10.17
FTP Filename...................................... file1
FTP Username...................................... ftpuser
FTP Password...................................... *********
```

Uploading Core Dumps from Controller to a Server (CLI)

Step 1 To see information about the core dump file in flash memory, enter this command:
show coredump summary

Information similar to the following appears:

```
Core Dump is disabled

Core Dump file is saved on flash

Sw Version..................................... 6.0.83.0
Time Stamp..................................... Wed Feb  4 13:23:11 2009
File Size...................................... 9081788
File Name Suffix........................... filename.gz
```

Step 2 To transfer the file from the controller to a server, enter these commands:

- **transfer upload mode** {**tftp** | **ftp** | **sftp**}
- **transfer upload datatype coredump**
- **transfer upload serverip** *server_ip_address*
- **transfer upload path** *server_path_to_file*
- **transfer upload filename** *filename*

Note After the file is uploaded, it ends with a .gz suffix. If desired, you can upload the same core dump file multiple times with different names to different servers.

Step 3 If you are using an FTP server, also enter these commands:

- **transfer upload username** *username*

  transfer upload password *password*
- **transfer upload port** *port*

Note The default value for the *port* parameter is 21.

Step 4 To view the updated settings, enter this command:
transfer upload start

Step 5 When prompted to confirm the current settings and start the software upload, answer y.

Uploading Packet Capture Files

Information About Uploading Packet Capture Files

When a Cisco 5500 Series Controller's data plane crashes, it stores the last 50 packets that the controller received in flash memory. This information can be useful in troubleshooting the crash.

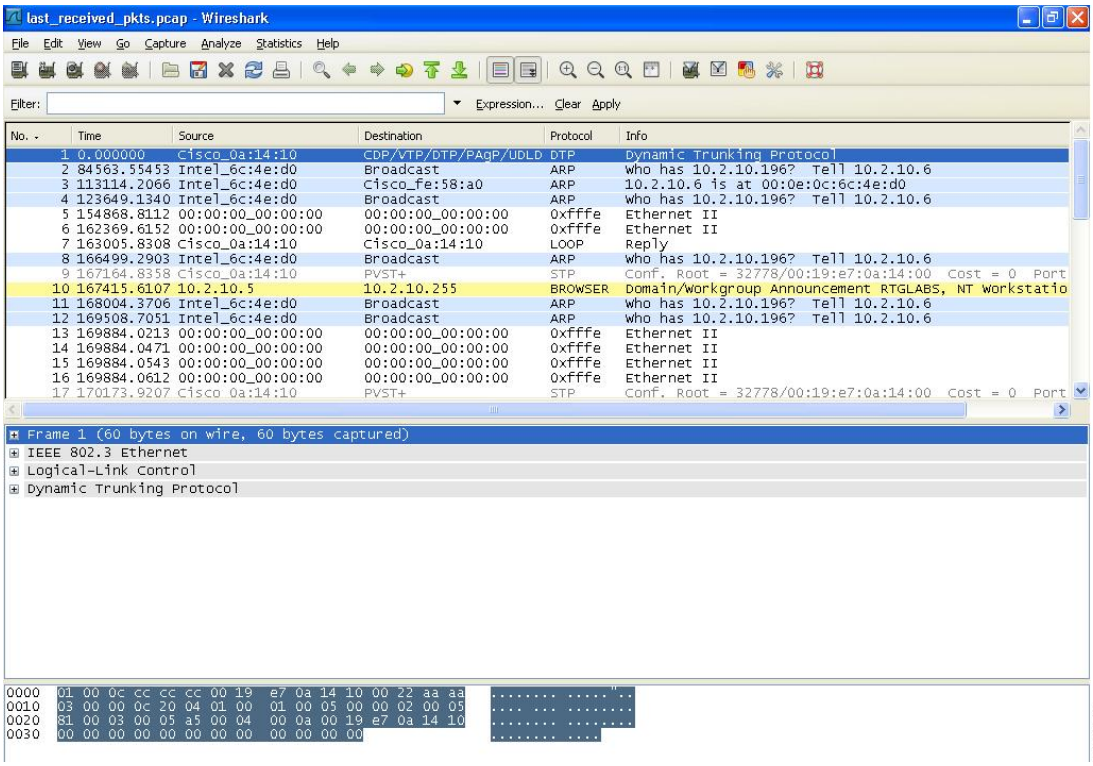
When a crash occurs, the controller generates a new packet capture file (*.pcap) file, and a message similar to the following appears in the controller crash file:

```
Last 5 packets processed at each core are stored in
 "last_received_pkts.pcap" captured file.
   - Frame 36,38,43,47,49, processed at core #0.
   - Frame 14,27,30,42,45, processed at core #1.
   - Frame 15,18,20,32,48, processed at core #2.
   - Frame 11,29,34,37,46, processed at core #3.
   - Frame 7,8,12,31,35, processed at core #4.
   - Frame 21,25,39,41,50, processed at core #5.
   - Frame 16,17,19,22,33, processed at core #6.
   - Frame 6,10,13,23,26, processed at core #7.
   - Frame 9,24,28,40,44, processed at core #8.
   - Frame 1,2,3,4,5, processed at core #9.
```

You can use the controller GUI or CLI to upload the packet capture file from the controller. You can then use Wireshark or another standard packet capture tool to view and analyze the contents of the file.

This figure shows a sample output of the packet capture in Wireshark.

Figure 28: Sample Output of Packet Capture File in Wireshark



Restrictions for Uploading Packet Capture Files

- Only Cisco 5500 Series Controllers generate packet capture files. This feature is not available on other controller platforms.
- Ensure that you have a TFTP or FTP server available for the file upload. Follow these guidelines when setting up a TFTP or FTP server:
  - If you are uploading through the service port, the TFTP or FTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
  - If you are uploading through the distribution system network port, the TFTP or FTP server can be on the same or a different subnet because the distribution system port is routable.
  - A third-party TFTP or FTP server cannot run on the same computer as Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP or FTP server and the third-party TFTP or FTP server require the same communication port.

Uploading Packet Capture Files (GUI)

Step 1 Choose **Commands > Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, choose **Packet Capture**.

Step 3 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**
- **SFTP** (available in the 7.4 and later releases)

Step 4 In the **IP Address** text box, enter the IP address of the server.

Step 5 In the **File Path** text box, enter the directory path of the packet capture file.

Step 6 In the **File Name** text box, enter the name of the packet capture file. These files have a .pcap extension.

Step 7 If you are using an FTP server, follow these steps:

a) In the **Server Login** Username text box, enter the username to log into the FTP server.
b) In the **Server Login Password** text box, enter the password to log into the FTP server.
c) In the **Server Port Number** text box, enter the port number on the FTP server through which the upload occurs. The default value is 21.

Step 8 Click **Upload** to upload the packet capture file from the controller. A message appears indicating the status of the upload.

Step 9 Use Wireshark or another standard packet capture tool to open the packet capture file and see the last 50 packets that were received by the controller.

Uploading Packet Capture Files (CLI)

Step 1 Log on to the controller CLI.

Step 2 Enter the **transfer upload mode** {**tftp** | **ftp** | **sftp**} command.

Step 3 Enter the **transfer upload datatype packet-capture** command.

Step 4 Enter the **transfer upload serverip** *server-ip-address* command.

Step 5 Enter the **transfer upload path** *server-path-to-file* command.

Step 6 Enter the **transfer upload filename** *last_received_pkts*.pcap command.

Step 7 If you are using an FTP server, enter these commands:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the *port* parameter is 21.

Step 8 Enter the **transfer upload start** command to see the updated settings and then answer y when prompted to confirm the current settings and start the upload process. This example shows the upload command output:

Step 9 Use Wireshark or another standard packet capture tool to open the packet capture file and see the last 50 packets that were received by the controller.

Monitoring Memory Leaks

This section provides instructions for troubleshooting hard-to-solve or hard-to-reproduce memory problems.

Caution The commands in this section can be disruptive to your system and should be run only when you are advised to do so by the Cisco Technical Assistance Center (TAC).

Monitoring Memory Leaks (CLI)

Step 1 To enable or disable monitoring for memory errors and leaks, enter this command:
config memory monitor errors {**enable** | **disable**}

The default value is disabled.

Note Your changes are not saved across reboots. After the controller reboots, it uses the default setting for this feature.

Step 2 If you suspect that a memory leak has occurred, enter this command to configure the controller to perform an auto-leak analysis between two memory thresholds (in kilobytes):
config memory monitor leaks *low_thresh high_thresh*

If the free memory is lower than the *low_thresh* threshold, the system crashes, generating a crash file. The default value for this parameter is 10000 kilobytes, and you cannot set it below this value.

Set the *high_thresh* threshold to the current free memory level or higher so that the system enters auto-leak-analysis mode. After the free memory reaches a level lower than the specified *high_thresh* threshold, the process of tracking and freeing memory allocation begins. As a result, the **debug memory events enable** command shows all allocations and frees, and the **show memory monitor detail** command starts to detect any suspected memory leaks. The default value for this parameter is 30000 kilobytes.

Step 3 To see a summary of any discovered memory issues, enter this command:
show memory monitor

Information similar to the following appears:

```
Memory Leak Monitor Status:
low_threshold(10000), high_threshold(30000), current status(disabled)

-----------------------------------------

Memory Error Monitor Status:
```

```
Crash-on-error flag currently set to (disabled)
No memory error detected.
```

Step 4 To see the details of any memory leaks or corruption, enter this command:
show memory monitor detail

Information similar to the following appears:

```
Memory error detected. Details:
-----------------------------------------------
-  Corruption detected at pmalloc entry address:        (0x179a7ec0)
-  Corrupt entry:headerMagic(0xdeadf00d),trailer(0xabcd),poison(0xreadceef),
entrysize(128),bytes(100),thread(Unknown task name, task id = (332096592)),
file(pmalloc.c),line(1736),time(1027)

Previous 1K memory dump from error location.
-----------------------------------------------
(179a7ac0): 00000000 00000000 00000000 ceeff00d readf00d 00000080 00000000 00000000
(179a7ae0): 17958b20 00000000 1175608c 00000078 00000000 readceef 179a7afc 00000001
(179a7b00): 00000003 00000006 00000001 00000004 00000001 00000009 00000009 0000020d
(179a7b20): 00000001 00000002 00000002 00000001 00000004 00000000 00000000 5d7b9aba
(179a7b40): cbddf004 192f465e 7791acc8 e5032242 5365788c a1b7cee6 00000000 00000000
(179a7b60): 00000000 00000000 00000000 00000000 00000000 ceeff00d readf00d 00000080
(179a7b80): 00000000 00000000 17958dc0 00000000 1175608c 00000078 00000000 readceef
(179a7ba0): 179a7ba4 00000001 00000003 00000006 00000001 00000004 00000001 00003763
(179a7bc0): 00000002 00000002 00000010 00000001 00000002 00000000 0000001e 00000013
(179a7be0): 0000001a 00000089 00000000 00000000 000000d8 00000000 00000000 17222194
(179a7c00): 1722246c 1722246c 00000000 00000000 00000000 00000000 00000000 ceeff00d
(179a7c20): readf00d 00000080 00000000 00000000 179a7b78 00000000 1175608c 00000078
```

Step 5 If a memory leak occurs, enter this command to enable debugging of errors or events during memory allocation:
debug memory {errors | events} {enable | disable}

Troubleshooting CCXv5 Client Devices

Information About Troubleshooting CCXv5 Client Devices

The controller supports three features designed to help troubleshoot communication problems with CCXv5 clients: diagnostic channel, client reporting, and roaming and real-time diagnostics.

Restrictions for CCXv5 Client Devices

Diagnostic channel, client reporting, and roaming and real-time diagnostics features are supported only on CCXv5 clients. They are not supported for use with non-CCX clients or with clients running an earlier version of CCX.

Configuring Diagnostic Channel

You can choose a diagnostic channel to troubleshoot why the client is having communication problems with a WLAN. You can test the client and access points to identify the difficulties that the client is experiencing and allow corrective measures to be taken to make the client operational on the network. You can use the controller GUI or CLI to enable the diagnostic channel, and you can use the controller CLI to run the diagnostic tests.

Note We recommend that you enable the diagnostic channel feature only for nonanchored SSIDs that use the management interface.

Configuring the Diagnostic Channel (GUI)

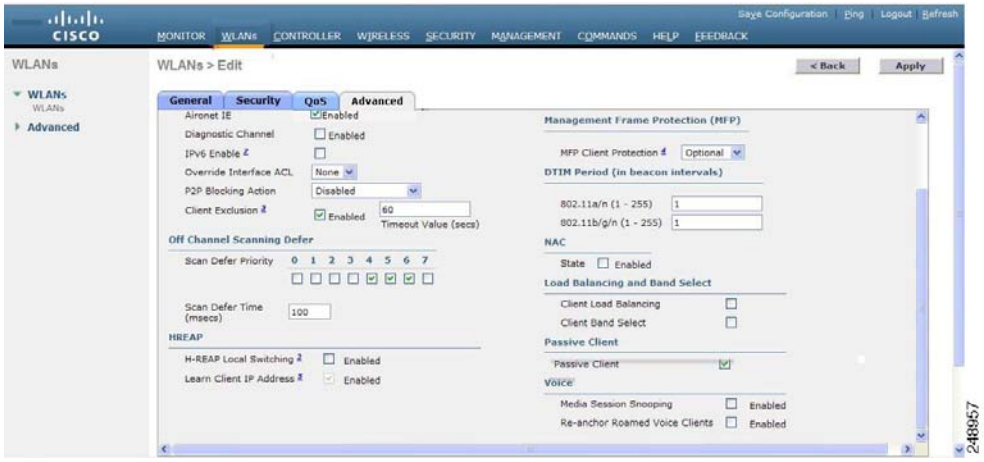
Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Create a new WLAN or click the ID number of an existing WLAN.

Note We recommend that you create a new WLAN on which to run the diagnostic tests.

Step 3 When the **WLANs > Edit** page appears, choose the **Advanced** tab to open the **WLANs > Edit (Advanced)** page.

Figure 29: WLANs > Edit (Advanced) Page



Step 4 If you want to enable diagnostic channel troubleshooting on this WLAN, select the **Diagnostic Channel** check box. Otherwise, leave this check box unselected, which is the default value.

Note You can use the CLI to initiate diagnostic tests on the client.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Configuring the Diagnostic Channel (CLI)

Step 1 To enable diagnostic channel troubleshooting on a particular WLAN, enter this command:
config wlan diag-channel {**enable** | **disable**} *wlan_id*

Step 2 To verify that your change has been made, enter this command:
show wlan *wlan_id*

Information similar to the following appears:

```
WLAN Identifier.................................. 1
Profile Name..................................... employee1
Network Name (SSID).............................. employee
Status........................................... Disabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
Exclusionlist Timeout............................ 60 seconds
Session Timeout.................................. Infinity
Interface........................................ virtual
WLAN ACL......................................... unconfigured
DHCP Server...................................... Default
DHCP Address Assignment Required................. Disabled
Quality of Service............................... Silver (best effort)
WMM.............................................. Disabled
CCX - AironetIe Support.......................... Enabled
CCX - Gratuitous ProbeResponse (GPR)............. Disabled
CCX - Diagnostics Channel Capability............. Enabled
...
```

Step 3 To send a request to the client to perform the DHCP test, enter this command:
config client ccx dhcp-test *client_mac_address*

Note This test does not require the client to use the diagnostic channel.

Step 4 To send a request to the client to perform the default gateway ping test, enter this command:
config client ccx default-gw-ping *client_mac_address*

Note This test does not require the client to use the diagnostic channel.

Step 5 To send a request to the client to perform the DNS server IP address ping test, enter this command:
config client ccx dns-ping *client_mac_address*

Note This test does not require the client to use the diagnostic channel.

Step 6 To send a request to the client to perform the DNS name resolution test to the specified host name, enter this command:
config client ccx dns-resolve *client_mac_address host_name*

Note This test does not require the client to use the diagnostic channel.

Step 7 To send a request to the client to perform the association test, enter this command:
config client ccx test-association *client_mac_address ssid bssid* {**802.11a | 802.11b | 802.11g**} *channel*

Step 8 To send a request to the client to perform the 802.1X test, enter this command:
config client ccx test-dot1x *client_mac_address profile_id bssid* {**802.11a** | **802.11b** | **802.11g**} *channel*

Step 9 To send a request to the client to perform the profile redirect test, enter this command:
config client ccx test-profile *client_mac_address profile_id*

The *profile_id* should be from one of the client profiles for which client reporting is enabled.

Note Users are redirected back to the parent WLAN, not to any other profile. The only profile shown is the user's parent profile. Note however that parent WLAN profiles can have one child diagnostic WLAN.

Step 10 Use these commands if necessary to abort or clear a test:

- To send a request to the client to abort the current test, enter this command:

  config client ccx test-abort *client_mac_address*

  Only one test can be pending at a time, so this command aborts the current pending test.

- To clear the test results on the controller, enter this command:

  config client ccx clear-results *client_mac_address*

Step 11 To send a message to the client, enter this command:

Example:
config client ccx send-message *client_mac_address message_id*
where *message_id* is one of the following:

- 1 = The SSID is invalid.
- 2 = The network settings are invalid.
- 3 = There is a WLAN credibility mismatch.
- 4 = The user credentials are incorrect.
- 5 = Please call support.
- 6 = The problem is resolved.
- 7 = The problem has not been resolved.
- 8 = Please try again later.
- 9 = Please correct the indicated problem.
- 10 = Troubleshooting is refused by the network.
- 11 = Retrieving client reports.
- 12 = Retrieving client logs.
- 13 = Retrieval complete.
- 14 = Beginning association test.
- 15 = Beginning DHCP test.

- 16 = Beginning network connectivity test.
- 17 = Beginning DNS ping test.
- 18 = Beginning name resolution test.
- 19 = Beginning 802.1X authentication test.
- 20 = Redirecting client to a specific profile.
- 21 = Test complete.
- 22 = Test passed.
- 23 = Test failed.
- 24 = Cancel diagnostic channel operation or select a WLAN profile to resume normal operation.
- 25 = Log retrieval refused by the client.
- 26 = Client report retrieval refused by the client.
- 27 = Test request refused by the client.
- 28 = Invalid network (IP) setting.
- 29 = There is a known outage or problem with the network.
- 30 = Scheduled maintenance period.
- 31 = The WLAN security method is not correct.
- 32 = The WLAN encryption method is not correct.
- 33 = The WLAN authentication method is not correct.

Step 12 To see the status of the last test, enter this command:
show client ccx last-test-status *client_mac_address*
Information similar to the following appears for the default gateway ping test:

```
Test Type..................................... Gateway Ping Test
Test Status................................... Pending/Success/Timeout

Dialog Token.................................. 15
Timeout....................................... 15000 ms
Request Time.................................. 1329 seconds since system boot
```

Step 13 To see the status of the last test response, enter this command:
show client ccx last-response-status *client_mac_address*

Information similar to the following appears for the 802.1X authentication test:

```
Test Status................................... Success

Response Dialog Token......................... 87
Response Status............................... Successful
Response Test Type............................ 802.1x Authentication Test
Response Time................................. 3476 seconds since system boot
```

Step 14 To see the results from the last successful diagnostics test, enter this command:
show client ccx results *client_mac_address*

Information similar to the following appears for the 802.1X authentication test:

```
dot1x Complete................................... Success
EAP Method....................................... *1,Host OS Login Credentials
dot1x Status..................................... 255
```

Step 15 To see the relevant data frames captured by the client during the previous test, enter this command: **show client ccx frame-data** *client_mac_address*

Information similar to the following appears:

```
LOG Frames:

Frame Number:.................................... 1
Last Frame Number:............................... 1120
Direction:....................................... 1
Timestamp:....................................... 0d 00h 50m 39s 863954us
Frame Length:.................................... 197
Frame Data:
00000000: 80 00 00 00 ff ff ff ff  ff ff 00 12 44 bd bd b0  ............D...
00000010: 00 12 44 bd bd b0 f0 af  43 70 00 f2 82 01 00 00  ..D.....Cp......
00000020: 64 00 11 08 00 01 00 01  08 8c 12 98 24 b0 48 60  d...........$.H`
00000030: 6c 05 04 01 02 00 00 85  1e 00 00 89 00 0f 00 ff  l...............
00000040: 03 19 00 41 50 32 33 2d  31 30 00 00 00 00 00 00  ...AP23-10......
00000050: 00 00 00 00 00 00 26 96  06 00 40 96 00 ff ff dd  ......&...@.....
00000060: 18 00 50 f2 01 01 00 00  50 f2 05 01 00 00 50 f2  ..P.....P.....P.
00000070: 05 01 00 00 40 96 00 28  00 dd 06 00 40 96 01 01  ....@..(....@...

00000080: 00 dd 05 00 40 96 03 04  dd 16 00 40 96 04 00 02  ....@......@....
00000090: 07 a4 00 00 23 a4 00 00  42 43 00 00 62 32 00 00  ....#...BC..b2..
000000a0: dd 05 00 40 96 0b 01 dd  18 00 50 f2 02 01 01 82  ...@......P.....
000000b0: 00 03 a4 00 00 27 a4 00  00 42 43 5e 00 62 32 2f  .....'...BC^.b2/

LOG Frames:

Frame Number:.................................... 2
Last Frame Number:............................... 1120
Direction:....................................... 1
Timestamp:....................................... 0d 00h 50m 39s 878289us
Frame Length:.................................... 147
Frame Data:
00000000: 80 00 00 00 ff ff ff ff  ff ff 00 0d ed c3 a0 22  ..............."
00000010: 00 0d ed c3 a0 22 00 bd  4d 50 a5 f7 78 08 00 00  ....."..MP..x...
00000020: 64 00 01 00 00 01 00 01  08 8c 12 98 24 b0 48 60  d...........$.H`
00000030: 6c 05 04 01 02 00 00 85  1e 00 00 84 00 0f 00 ff  l...............
00000040: 03 19 00 72 6f 67 75 65  2d 74 65 73 74 31 00 00  ...rogue-test1..
00000050: 00 00 00 00 00 00 23 96  06 00 40 96 00 10 00 dd  ......#...@.....
00000060: 06 00 40 96 01 01 00 dd  05 00 40 96 03 04 dd 05  ..@.......@.....
00000070: 00 40 96 0b 01 dd 18 00  50 f2 02 01 01 81 00 03  .@......P.......

00000080: a4 00 00 27 a4 00 00 42  43 5e 00 62 32 2f 00 d2  ...'...BC^.b2/..
00000090: b4 ab 84                                          ...

LOG Frames:

Frame Number:.................................... 3
Last Frame Number:............................... 1120
Direction:....................................... 1
Timestamp:....................................... 0d 00h 50m 39s 881513us
Frame Length:.................................... 189
Frame Data:
00000000: 80 00 00 00 ff ff ff ff  ff ff 00 12 44 bd 80 30  ............D..0
00000010: 00 12 44 bd 80 30 60 f7  46 c0 8b 4b d1 05 00 00  ..D..0`.F..K....
00000020: 64 00 11 08 00 01 00 01  08 8c 12 98 24 b0 48 60  d...........$.H`
00000030: 6c 05 04 00 02 00 00 85  1e 00 00 89 00 0f 00 ff  l...............
00000040: 03 19 00 41 50 34 30 2d  31 37 00 00 00 00 00 00  ...AP40-17......
00000050: 00 00 00 00 00 00 26 dd  18 00 50 f2 01 01 00 00  ......&...P.....
00000060: 50 f2 05 01 00 00 50 f2  05 01 00 00 40 96 00 28  P.....P.....@..(
00000070: 00 dd 06 00 40 96 01 01  00 dd 05 00 40 96 03 04  ....@.......@...
```

```
00000080: dd 16 00 40 96 04 00 05  07 a4 00 00 23 a4 00 00  ...@........#...
00000090: 42 43 00 00 62 32 00 00  dd 05 00 40 96 0b 01 dd  BC..b2.....@....
000000a0: 18 00 50 f2 02 01 01 85  00 03 a4 00 00 27 a4 00  ..P..........'..
000000b0: 00 42 43 5e 00 62 32 2f  00 0b 9a 1d 6f           .BC^.b2/....o
...
```

Configuring Client Reporting

The client reporting protocol is used by the client and the access point to exchange client information. Client reports are collected automatically when the client associates. You can use the controller GUI or CLI to send a client report request to any CCXv5 client any time after the client associates. There are four types of client reports:

- **Client profile—**Provides information about the configuration of the client.
- **Operating parameters—**Provides the details of the client's current operational modes.
- **Manufacturers' information—**Provides data about the wireless LAN client adapter in use.
- **Client capabilities—**Provides information about the client's capabilities.

Configuring Client Reporting (GUI)

Step 1 Choose **Monitor > Clients** to open the Clients page.

Step 2 Click the MAC address of the desired client. The **Clients > Detail** page appears.

Step 3 To send a report request to the client, click **Send CCXV5 Req**.

Note You must create a Trusted Profile using ACAU for Cisco CB21AG or equivalent software from your CCXv5 vendor.

Step 4 To view the parameters from the client, click **Display**. The Client Reporting page appears.

Step 5 Click the link for the desired client profile. The Profile Details page appears displaying the client profile details, including the SSID, power save mode, radio channel, data rates, and 802.11 security settings.

Configuring Client Reporting (CLI)

Step 1 To send a request to the client to send its profiles, enter this command:
config client ccx get-profiles *client_mac_address*

Step 2 To send a request to the client to send its current operating parameters, enter this command:
config client ccx get-operating-parameters *client_mac_address*

Step 3 To send a request to the client to send the manufacturer's information, enter this command:
config client ccx get-manufacturer-info *client_mac_address*

Step 4 To send a request to the client to send its capability information, enter this command:
config client ccx get-client-capability *client_mac_address*

Step 5 To clear the client reporting information, enter this command:
config client ccx clear-reports *client_mac_address*

Step 6 To see the client profiles, enter this command:
show client ccx profiles *client_mac_address*

Step 7 To see the client operating parameters, enter this command:
show client ccx operating-parameters *client_mac_address*

Step 8 To see the client manufacturer information, enter this command:
show client ccx manufacturer-info *client_mac_address*

Step 9 To see the client's capability information, enter this command:
show client ccx client-capability *client_mac_address*

Note This command displays the client's available capabilities, not current settings for the capabilities.

Configuring Roaming and Real-Time Diagnostics

You can use roaming and real-time logs and statistics to solve system problems. The event log enables you to identify and track the behavior of a client device. It is especially useful when attempting to diagnose difficulties that a user may be having on a WLAN. The event log provides a log of events and reports them to the access point. There are three categories of event logs:

- Roaming log—This log provides a historical view of the roaming events for a given client. The client maintains a minimum of five previous roaming events including failed attempts and successful roams.
- Robust Security Network Association (RSNA) log—This log provides a historical view of the authentication events for a given client. The client maintains a minimum of five previous authentication attempts including failed attempts and successful ones.
- Syslog—This log provides internal system information from the client. For example, it may indicate problems with 802.11 operation, system operation, and so on.

The statistics report provides 802.1X and security information for the client. You can use the controller CLI to send the event log and statistics request to any CCXv5 client any time after the client associates.

Configuring Roaming and Real-Time Diagnostics (CLI)

Step 1 To send a log request, enter this command:
config client ccx log-request *log_type client_mac_address*

where *log_type* is roam, rsna, or syslog.

Step 2 To view a log response, enter this command:

show client ccx log-response *log_type client_mac_address*

where *log_type* is roam, rsna, or syslog.

Information similar to the following appears for a log response with a *log_type* of roam:

```
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 13s 322396us
                         Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2, Transition
 Time=3125(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 16s 599006us
                         Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2, Transition
 Time=3235(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
                          Event Timestamp=0d 00h 00m 19s 882921us
                         Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:c2, Transition
 Time=3234(ms)
                          Transition Reason: Normal roam, poor link
                          Transition Result: Success
Tue Jun 26 18:28:48 2007  Roaming Response LogID=133: Status=Successful
                          Event Timestamp=0d 00h 00m 08s 815477us
                         Source BSSID=00:0b:85:81:06:c2, Target BSSID=00:0b:85:81:06:d2, Transition
 Time=3281(ms)
                          Transition Reason: First association to WLAN
                          Transition Result: Success
                          Event Timestamp=0d 00h 00m 26s 637084us
                         Source BSSID=00:0b:85:81:06:d2, Target BSSID=00:0b:85:81:06:c2, Transition
 Time=3313(ms)
```

Information similar to the following appears for a log response with a *log_type* of rsna:

```
Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
                          Event Timestamp=0d 00h 00m 00s 246578us
                          Target BSSID=00:14:1b:58:86:cd
                          RSNA Version=1
                          Group Cipher Suite=00-0f-ac-02
                          Pairwise Cipher Suite Count = 1
                              Pairwise Cipher Suite 0 = 00-0f-ac-04
                          AKM Suite Count = 1
                              AKM Suite 0 = 00-0f-ac-01
                          RSN Capability = 0x0
                          RSNA Result: Success
Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
                          Event Timestamp=0d 00h 00m 00s 246625us
                          Target BSSID=00:14:1b:58:86:cd
                          RSNA Version=1
                          Group Cipher Suite=00-0f-ac-02
                          Pairwise Cipher Suite Count = 1
                              Pairwise Cipher Suite 0 = 00-0f-ac-04
                          AKM Suite Count = 1
```

```
                            AKM Suite 0 = 00-0f-ac-01
                          RSN Capability = 0x0
                          RSNA Result: Success
Tue Jun 26 18:24:09 2007  RSNA Response LogID=132: Status=Successful
                          Event Timestamp=0d 00h 00m 01s 624375us
                          Target BSSID=00:14:1b:58:86:cd
                          RSNA Version=1
                          Group Cipher Suite=00-0f-ac-02
                          Pairwise Cipher Suite Count = 1
                              Pairwise Cipher Suite 0 = 00-0f-ac-04
                          AKM Suite Count = 1
                              AKM Suite 0 = 00-0f-ac-01
                          RSN Capability = 0x0
            RSNA Result: Success
```

Information similar to the following appears for a log response with a *log_type* of syslog:

```
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 278987us
                         Client SysLog = '<11> Jun 19 11:49:47 uraval3777 Mandatory elements missing
 in the OID response'
                          Event Timestamp=0d 00h 19m 42s 278990us
                         Client SysLog = '<11> Jun 19 11:49:50 uraval3777 Mandatory elements missing
 in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 278993us
                         Client SysLog = '<11> Jun 19 11:49:53 uraval3777 Mandatory elements missing
 in the OID response'
                          Event Timestamp=0d 00h 19m 42s 278996us
                         Client SysLog = '<11> Jun 19 11:49:56 uraval3777 Mandatory elements missing
 in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 279000us
                         Client SysLog = '<11> Jun 19 11:50:00 uraval3777 Mandatory elements missing
 in the OID response'
                          Event Timestamp=0d 00h 19m 42s 279003us
                         Client SysLog = '<11> Jun 19 11:50:03 uraval3777 Mandatory elements missing
 in the OID response'
Tue Jun 26 18:07:48 2007  SysLog Response LogID=131: Status=Successful
                          Event Timestamp=0d 00h 19m 42s 279009us
                         Client SysLog = '<11> Jun 19 11:50:09 uraval3777 Mandatory elements missing
 in the OID response'
                          Event Timestamp=0d 00h 19m 42s 279012us
                         Client SysLog = '<11> Jun 19 11:50:12 uraval3777 Mandatory elements missing
 in the OID response'
```

Step 3 To send a request for statistics, enter this command:
config client ccx stats-request *measurement_duration stats_name client_mac_address*

where *stats_name* is dot11 or security.

Step 4 To view the statistics response, enter this command:
show client ccx stats-report *client_mac_address*

Information similar to the following appears:

```
Measurement duration = 1

      dot11TransmittedFragmentCount       = 1
      dot11MulticastTransmittedFrameCount = 2
      dot11FailedCount                    = 3
      dot11RetryCount                     = 4
      dot11MultipleRetryCount             = 5
      dot11FrameDuplicateCount            = 6
      dot11RTSSuccessCount                = 7
      dot11RTSFailureCount                = 8
      dot11ACKFailureCount                = 9
      dot11ReceivedFragmentCount          = 10
      dot11MulticastReceivedFrameCount    = 11
      dot11FCSErrorCount                  = 12
      dot11TransmittedFrameCount          = 13
```

Using the Debug Facility

Information About Using the Debug Facility

The debug facility enables you to display all packets going to and from the controller CPU. You can enable it for received packets, transmitted packets, or both. By default, all packets received by the debug facility are displayed. However, you can define access control lists (ACLs) to filter packets before they are displayed. Packets not passing the ACLs are discarded without being displayed.

Each ACL includes an action (permit, deny, or disable) and one or more fields that can be used to match the packet. The debug facility provides ACLs that operate at the following levels and on the following values:

- Driver ACL
  - NPU encapsulation type
  - Port
- Ethernet header ACL
  - Destination address
  - Source address
  - Ethernet type
  - VLAN ID
- IP header ACL
  - Source address

- Destination address
- Protocol
- Source port (if applicable)
- Destination port (if applicable)

- EoIP payload Ethernet header ACL
  - Destination address
  - Source address
  - Ethernet type
  - VLAN ID
- EoIP payload IP header ACL
  - Source address
  - Destination address
  - Protocol
  - Source port (if applicable)
  - Destination port (if applicable)
- CAPWAP payload 802.11 header ACL
  - Destination address
  - Source address
  - BSSID
  - SNAP header type
- CAPWAP payload IP header ACL
  - Source address
  - Destination address
  - Protocol
  - Source port (if applicable)
  - Destination port (if applicable)

At each level, you can define multiple ACLs. The first ACL that matches the packet is the one that is selected.

Configuring the Debug Facility (CLI)

Step 1 To enable the debug facility, enter this command:

- **debug packet logging enable** {**rx** | **tx** | **all**} *packet_count display_size*

  where

  - **rx** displays all received packets, **tx** displays all transmitted packets, and **all** displays both transmitted and received packets.
  - *packet_count* is the maximum number of packets to log. You can enter a value between 1 and 65535 packets, and the default value is 25 packets.
  - *display_size* is the number of bytes to display when printing a packet. By default, the entire packet is displayed.

  Note To disable the debug facility, enter this command: **debug packet logging disable**.

- **debug packet logging acl driver** *rule_index action npu_encap port*

  where

  - *rule_index* is a value between 1 and 6 (inclusive).
  - *action* is permit, deny, or disable.
  - *npu_encap* specifies the NPU encapsulation type, which determines how packets are filtered. The possible values include dhcp, dot11-mgmt, dot11-probe, dot1x, eoip-ping, iapp, ip, lwapp, multicast, orphan-from-sta, orphan-to-sta, rbcp, wired-guest, or any.
  - *port* is the physical port for packet transmission or reception.

- Use these commands to configure packet-logging ACLs:

  debug packet logging acl eth *rule_index action dst src type vlan*

  where

  - *rule_index* is a value between 1 and 6 (inclusive).
  - *action* is permit, deny, or disable.
  - *dst* is the destination MAC address.
  - *src* is the source MAC address.
  - *type* is the two-byte type code (such as 0x800 for IP, 0x806 for ARP). This parameter also accepts a few common string values such as “ip” (for 0x800) or “arp” (for 0x806).
  - *vlan* is the two-byte VLAN ID.

- **debug packet logging acl ip** *rule_index action src dst proto src_port dst_port*

  where

  - *proto* is a numeric or any string recognized by getprotobyname(). The controller supports the following strings: ip, icmp, igmp, ggp, ipencap, st, tcp, egp, pup, udp, hmp, xns-idp, rdp, iso-tp4, xtp, ddp, idpr-cmtp, rspf, vmtp, ospf, ipip, and encap.
  - *src_port* is the UDP/TCP two-byte source port (for example, telnet, 23) or “any.” The controller accepts a numeric or any string recognized by getservbyname(). The controller supports the following strings: tcpmux, echo, discard, systat, daytime, netstat, qotd, msp, chargen, ftp-data, ftp, fsp, ssh, telnet, smtp, time, rlp, nameserver, whois, re-mail-ck, domain, mtp, bootps, bootpc, tftp, gopher, rje, finger, www, link, kerberos,

supdup, hostnames, iso-tsap, csnet-ns, 3com-tsmux, rtelnet, pop-2, pop-3, sunrpc, auth, sftp, uucp-path, nntp, ntp, netbios-ns, netbios-dgm, netbios-ssn, imap2, snmp, snmp-trap, cmip-man, cmip-agent, xdmcp, nextstep, bgp, prospero, irc, smux, at-rtmp, at-nbp, at-echo, at-zis, qmtp, z3950, ipx, imap3, ulistserv, https, snpp, saft, npmp-local, npmp-gui, and hmmp-ind.

- *dst_port* is the UDP/TCP two-byte destination port (for example, telnet, 23) or "any." The controller accepts a numeric or any string recognized by getservbyname(). The controller supports the same strings as those for the *src_port*.

- **debug packet logging acl eoip-eth** *rule_index action dst src type vlan*
- **debug packet logging acl eoip-ip** *rule_index action src dst proto src_port dst_port*
- **debug packet logging acl lwapp-dot11** *rule_index action dst src bssid snap_type*

  where

  - *bssid* is the Basic Service Set Identifier.
  - *snap_type* is the Ethernet type.

- **debug packet logging acl lwapp-ip** *rule_index action src dst proto src_port dst_port*

Note To remove all configured ACLs, enter this command: **debug packet logging acl clear-all**.

Step 2 To configure the format of the debug output, enter this command:
debug packet logging format {**hex2pcap** | **text2pcap**}

The debug facility supports two output formats: hex2pcap and text2pcap. The standard format used by IOS supports the use of hex2pcap and can be decoded using an HTML front end. The text2pcap option is provided as an alternative so that a sequence of packets can be decoded from the same console log file.

This figure shows an example of hex2pcap output.

Figure 30: Sample Hex2pcap Output

```
tx len=118, encap=n/a, port=1
[0000]: 000C316E 7F80000B 854008c0 08004500 ..1n.....@.@..E.
[0010]: 00680000 40004001 5FBE0164 6C0E0164 .h..@.@._>.dl..d
[0020]: 6C010800 08D9E500 00000000 00000000 l....Ye.........
[0030]: 00000000 00000000 00000000 00001C1D ................
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789:;<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253                      NOPQRS
rx len=118, encap=ip, port=1
[0000]: 000B8540 08C0000C 316E7F80 08004500 ...@.@..1n....E.
[0010]: 00680000 4000FF01 A0BD0164 6C010164 .h..@....=.dl..d
[0020]: 6C0E0000 10D9E500 00000000 00000000 l....Ye.........
[0030]: 00000000 00000000 00000000 00001C1D ................
[0040]: 1E1F2021 22232425 26272829 2A2B2C2D ...!"#$%&'()*+,-
[0050]: 2E2F3031 32333435 36373839 3A3B3C3D ./0123456789:;<=
[0060]: 3E3F4041 42434445 46474849 4A4B4C4D >?@ABCDEFGHIJKLM
[0070]: 4E4F5051 5253                      NOPQRS
```

212235

This figure shows an example of text2pcap output.

Figure 31: Sample Text2pcap Output

```
tx len=118, encap=n/a, port=1
0000 00 0C 31 6E 7F 80 00 0B 85 40 08 c0 08 00 45 00 ..1n.....@.@..E.
0010 00 68 00 00 40 00 40 01 5F BE 01 64 6C 0E 01 64 .h..@.@._>.dl..d
0020 6C 01 08 00 08 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.........
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 1D ................
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53                              NOPQRS
rx len=118, encap=ip, port=1
0000 00 0B 85 40 08 C0 00 0C 31 6E 7F 80 08 00 45 00 ...@.@..1n....E.
0010 00 68 00 00 40 00 FF 01 A0 BD 01 64 6C 01 01 64 .h..@....=.dl..d
0020 6C 0E 00 00 10 D9 E5 00 00 00 00 00 00 00 00 00 l....Ye.........
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1C 1D ................
0040 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D ...!"#$%&'()*+,-
0050 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D ./0123456789:;<=
0060 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D >?@ABCDEFGHIJKLM
0070 4E 4F 50 51 52 53                              NOPQRS
```

232343

Step 3 To determine why packets might not be displayed, enter this command:
debug packet error {**enable** | **disable**}

Step 4 To display the status of packet debugging, enter this command:
show debug packet

Information similar to the following appears:

```
Status..................................... disabled
Number of packets to display..................... 25
Bytes/packet to display.......................... 0
Packet display format............................ text2pcap

Driver ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   IP ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
      [5]: disabled
      [6]: disabled
   EoIP-Ethernet ACL:
      [1]: disabled
      [2]: disabled
      [3]: disabled
      [4]: disabled
```

```
   [5]: disabled
   [6]: disabled
EoIP-IP ACL:
   [1]: disabled
   [2]: disabled
   [3]: disabled
   [4]: disabled
   [5]: disabled
   [6]: disabled
LWAPP-Dot11 ACL:
   [1]: disabled
   [2]: disabled
   [3]: disabled
   [4]: disabled
   [5]: disabled
   [6]: disabled
LWAPP-IP ACL:
   [1]: disabled
   [2]: disabled
   [3]: disabled
   [4]: disabled
   [5]: disabled
   [6]: disabled?
```

Configuring Wireless Sniffing

Information About Wireless Sniffing

The controller enables you to configure an access point as a network "sniffer," which captures and forwards all the packets on a particular channel to a remote machine that runs packet analyzer software. These packets contain information on time stamps, signal strength, packet sizes, and so on. Sniffers allow you to monitor and record network activity and to detect problems.

Prerequisites for Wireless Sniffing

To perform wireless sniffing, you need the following hardware and software:

- A dedicated access point—An access point configured as a sniffer cannot simultaneously provide wireless access service on the network. To avoid disrupting coverage, use an access point that is not part of your existing wireless network.
- A remote monitoring device—A computer capable of running the analyzer software.
- Windows XP or Linux operating system—The controller supports sniffing on both Windows XP and Linux machines.
- Software and supporting files, plug-ins, or adapters—Your analyzer software may require specialized files before you can successfully enable

Restrictions for Wireless Sniffing

- Supported third-party network analyzer software applications are as follows:

- Wildpackets Omnipeek or Airopeek
- AirMagnet Enterprise Analyzer
- Wireshark

- The latest version of Wireshark can decode the packets by going to the Analyze mode. Select **decode as**, and switch UDP5555 to decode as AIROPEEK.
- You must disable IP-MAC address binding in order to use an access point in sniffer mode if the access point is joined to a Cisco 5500 Series Controller. To disable IP-MAC address binding, enter the **config network ip-mac-binding disable** command in the controller CLI.
- You must enable WLAN 1 in order to use an access point in sniffer mode if the access point is joined to a Cisco 5500 Series Controller. If WLAN 1 is disabled, the access point cannot send packets.

Prerequisites for Wireless Sniffing

Configuring Sniffing on an Access Point (GUI)

Step 1 Choose **Wireless > Access Points > All APs** to open the **All APs** page.

Step 2 Click the name of the access point that you want to configure as the sniffer. The All APs > Details for page appears.

Step 3 From the **AP Mode** drop-down list, choose **Sniffer**.

Step 4 Click **Apply**.

Step 5 Click **OK** when prompted that the access point will be rebooted.

Step 6 Choose **Wireless > Access Points > Radios > 802.11a/n (or 802.11b/g/n)** to open the 802.11a/n (or 802.11b/g/n) Radios page.

Step 7 Hover your cursor over the blue drop-down arrow for the desired access point and choose **Configure**. The 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page appears.

Step 8 Select the **Sniff** check box to enable sniffing on this access point, or leave it unselected to disable sniffing. The default value is unchecked.

Step 9 If you enabled sniffing in Step 8, follow these steps:

a) From the Channel drop-down list, choose the channel on which the access point sniffs for packets.

b) In the **Server IP Address** text box, enter the IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark.

Step 10 Click **Apply**.

Step 11 Click **Save Configuration**.

Configuring Sniffing on an Access Point (CLI)

Step 1 Configure the access point as a sniffer by entering this command:
config ap mode sniffer *Cisco_AP*

where *Cisco_AP* is the access point configured as the sniffer.

Step 2 When warned that the access point will be rebooted and asked if you want to continue, enter **Y**. The access point reboots in sniffer mode.

Step 3 Enable sniffing on the access point by entering this command:
config ap sniff {802.11a | 802.11b} enable *channel server_IP_address Cisco_AP*

where

- *channel* is the radio channel on which the access point sniffs for packets. The default values are 36 (802.11a/n) and 1 (802.11b/g/n).
- *server_IP_address* is the IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark.
- *Cisco_AP* is the access point configured as the sniffer.

Note To disable sniffing on the access point, enter the **config ap sniff** {**802.11a | 802.11b**} **disable** *Cisco_AP* command.

Step 4 Save your changes by entering this command:
save config

Step 5 See the sniffer configuration settings for an access point by entering this command:
show ap config {**802.11a | 802.11b**} *Cisco_AP*

Troubleshooting Access Points Using Telnet or SSH_old

The controller supports the use of the Telnet and Secure Shell (SSH) protocols to troubleshoot lightweight access points. Using these protocols makes debugging easier, especially when the access point is unable to connect to the controller.

- To avoid potential conflicts and security threats to the network, the following commands are unavailable while a Telnet or SSH session is enabled: **config terminal, telnet, ssh, rsh, ping, traceroute, clear, clock, crypto, delete, fsck, lwapp, mkdir, radius, release, reload, rename, renew, rmdir, save, set, test, upgrade**.
- Commands available during a Telnet or SSH session include **debug, disable, enable, help, led, login, logout, more, no debug, show, systat, undebug** and **where**.

Note For instructions on configuring Telnet or SSH SSH sessions on the controller, see the Configuring Telnet and Secure Shell Sessions section.

Information About Troubleshooting Access Points Using Telnet or SSH

The controller supports the use of the Telnet and Secure Shell (SSH) protocols to troubleshoot lightweight access points. Using these protocols makes debugging easier, especially when the access point is unable to connect to the controller.

- To avoid potential conflicts and security threats to the network, the following commands are unavailable while a Telnet or SSH session is enabled: **config terminal, telnet, ssh, rsh, ping, traceroute, clear, clock, crypto, delete, fsck, lwapp, mkdir, radius, release, reload, rename, renew, rmdir, save, set, test, upgrade**.
- Commands available during a Telnet or SSH session include **debug, disable, enable, help, led, login, logout, more, no debug, show, systat, undebug** and **where**.

Note For instructions on configuring Telnet or SSH SSH sessions on the controller, see the Configuring Telnet and Secure Shell Sessions section.

You can configure Telnet or SSH by using the controller CLI in software release 5.0 or later releases or using the controller GUI in software release 6.0 or later releases.

Troubleshooting Access Points Using Telnet or SSH (GUI)

Step 1 Choose **Wireless > Access Points > All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to enable Telnet or SSH.

Step 3 Choose the **Advanced** tab to open the **All APs > Details for (Advanced)** page.

Step 4 Select the **Telnet** check box to enable Telnet connectivity on this access point. The default value is unchecked.

Step 5 Select the **SSH** check box to enable SSH connectivity on this access point. The default value is unchecked.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Troubleshooting Access Points Using Telnet or SSH (CLI)

Step 1 Enable Telnet or SSH connectivity on an access point by entering this command:
config ap {**telnet** | **ssh**} **enable** *Cisco_AP*

The default value is disabled.

Note Disable Telnet or SSH connectivity on an access point by entering this command: **config ap** {**telnet** | **ssh**} **disable** *Cisco_AP*

Step 2 Save your changes by entering this command:
save config

Step 3 See whether Telnet or SSH is enabled on an access point by entering this command:
show ap config general *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 5
```

```
Cisco AP Name..................................... AP33
Country code...................................... Multiple Countries:US,AE,AR,AT,AU,BH
Reg. Domain allowed by Country.................... 802.11bg:-ABCENR 802.11a:-ABCEN
AP Country code................................... US - United States
AP Regulatory Domain.............................. 802.11bg:-A 802.11a:-A
Switch Port Number ............................... 2
MAC Address....................................... 00:19:2f:11:16:7a
IP Address Configuration.......................... Static IP assigned
IP Address........................................ 10.22.8.133
IP NetMask........................................ 255.255.248.0
Gateway IP Addr................................... 10.22.8.1
Domain.........................................
Name Server.....................................
Telnet State...................................... Enabled
Ssh State......................................... Enabled
...
```

Debugging the Access Point Monitor Service

Information About Debugging the Access Point Monitor Service

The controller sends access point status information to the Cisco 3300 Series Mobility Services Engine (MSE) using the access point monitor service.

The MSE sends a service subscription and an access point monitor service request to get the status of all access points currently known to the controller. When any change is made in the status of an access point, a notification is sent to the MSE.

Debugging Access Point Monitor Service Issues (CLI)

If you experience any problems with the access point monitor service, enter this command:

debug service ap-monitor {all | error | event | nmsp | packet} {enable | disable}

where

- **all** configures debugging of all access point status messages.
- **error** configures debugging of access point monitor error events.
- **event** configures debugging of access point monitor events.
- **nmsp** configures debugging of access point monitor NMSP events.
- **packet** configures debugging of access point monitor packets.
- **enable** enables the debub service ap-monitor mode.
- **disable** disables the debug service ap-monitor mode.

Troubleshooting OfficeExtend Access Points

Information About Troubleshooting OfficeExtend Access Points

This section provides troubleshooting information if you experience any problems with your OfficeExtend access points.

Interpreting OfficeExtend LEDs

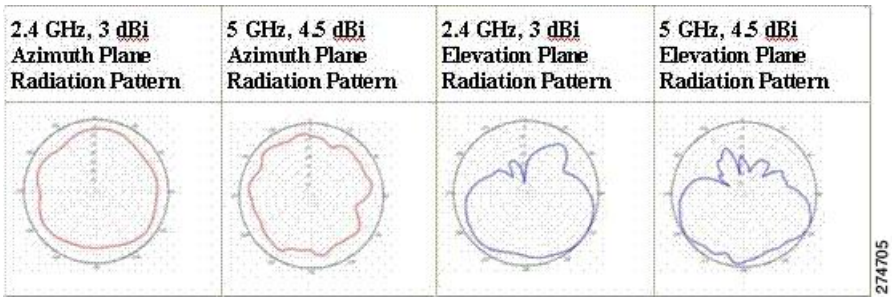
The LED patterns are different for 1130 series and 1140 series OfficeExtend access points. See the *Cisco OfficeExtend Access Point Quick Start Guide* for a description of the LED patterns. You can find this guide at this URL:

http://www.cisco.com/en/US/products/hw/wireless/index.html

Positioning OfficeExtend Access Points for Optimal RF Coverage

When positioning your OfficeExtend access point, consider that its RF signals are emitted in a cone shape spreading outward from the LED side of the access point. Ensure to mount the access point so that air can flow behind the metal back plate and prevent the access point from overheating.

Figure 32: OfficeExtend Access Point Radiation Patterns



Troubleshooting Common Problems

Most of the problems experienced with OfficeExtend access points are one of the following:

- The access point cannot join the controller because of network or firewall issues.
  Resolution: Follow the instructions in the Viewing Access Point Join Information section to see join statistics for the OfficeExtend access point, or find the access point's public IP address and perform pings of different packet sizes from inside the company.
- The access point joins but keeps dropping off. This behavior usually occurs because of network problems or when the network address translation (NAT) or firewall ports close because of short timeouts.

  Resolution: Ask the teleworker for the LED status.
- Clients cannot associate because of NAT issues.

  Resolution: Ask the teleworker to perform a speed test and a ping test. Some servers do not return big packet pings.

- Clients keep dropping data. This behavior usually occurs because the home router closes the port because of short timeouts.

  Resolution: Perform client troubleshooting in Cisco Prime Infrastructure to determine if the problem is related to the OfficeExtend access point or the client.

- The access point is not broadcasting the enterprise WLAN.

  Resolution: Ask the teleworker to check the cables, power supply, and LED status. If you still cannot identify the problem, ask the teleworker to try the following:

  - Connect to the home router directly and see if the PC is able to connect to an Internet website such as http://www.cisco.com/. If the PC cannot connect to the Internet, check the router or modem. If the PC can connect to the Internet, check the home router configuration to see if a firewall or MAC-based filter is enabled that is blocking the access point from reaching the Internet.
  - Log on to the home router and check to see if the access point has obtained an IP address. If it has, the access point's LED normally blinks orange.

- The access point cannot join the controller, and you cannot identify the problem.

  Resolution: A problem could exist with the home router. Ask the teleworker to check the router manual and try the following:

  - Assign the access point a static IP address based on the access point's MAC address.
  - Put the access point in a demilitarized zone (DMZ), which is a small network inserted as a neutral zone between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.
  - If problems still occur, contact your company's IT department for assistance.

- The teleworker experiences problems while configuring a personal SSID on the access point.

  Resolution: Clear the access point configuration and return it to factory default settings by clicking **Clear Config** on the access point GUI or by entering the clear ap config Cisco_AP command and then configuring a personal SSID on an OfficeExtend Access Point. If problems still occur, contact your company's IT department for assistance.

- The home network needs to be rebooted.

  Resolution: Ask the teleworker to follow these steps:

  Leave all devices networked and connected, and then power down all the devices.

  Turn on the cable or DSL modem, and then wait for 2 minutes. (Check the LED status.)

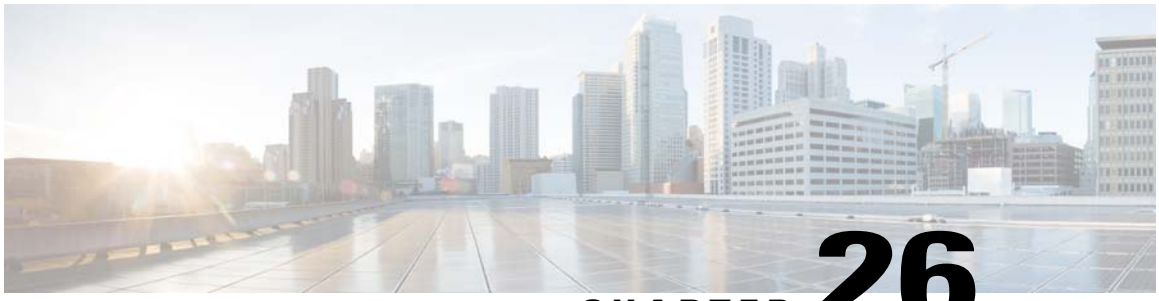
  Turn on the home router, and then wait for 2 minutes. (Check the LED status.)

  Turn on the access point, and then wait for 5 minutes. (Check the LED status.)

  Turn on the client.

PART II

Configuring Ports and Interfaces



CHAPTER 26

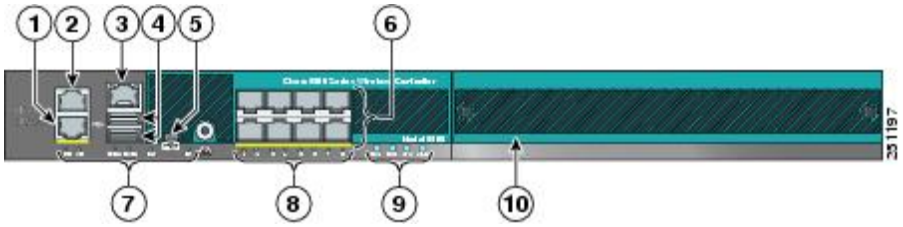
Overview of Ports and Interfaces

Three concepts are key to understanding how controllers connect to a wireless network: ports, interfaces, and WLANs.

Information About Ports

A port is a physical entity that is used for connections on the controller platform. Controllers have two types of ports: distribution system ports and a service port.

Figure 33: Ports on the Cisco 5500 Series Wireless LAN Controllers



1	Redundant port (RJ-45)	6	SFP distribution system ports 1–8
2	Service port (RJ-45)	7	Management port LEDs
3	Console port (RJ-45)	8	SFP distribution port Link and Activity LEDs

4	USB ports 0 and 1 (Type A)	9	Power supply (PS1 and PS2), System (SYS), and Alarm (ALM) LEDs
5	Console port (Mini USB Type B) **Note** You can use only one console port (either RJ-45 or mini USB). When you connect to one console port, the other is disabled.	10	Expansion module slot

Information About Distribution System Ports

A distribution system port connects the controller to a neighbor switch and serves as the data path between these two devices.

Restrictions for Configuring Distribution System Ports

- Cisco 5508 Controllers have eight Gigabit Ethernet distribution system ports, through which the Controller can manage multiple access points. The 5508-12, 5508-25, 5508-50, 5508-100, and 5508-250 models allow a total of 12, 25, 50, 100, or 250 access points to join the controller. Cisco 5508 controllers have no restrictions on the number of access points per port. However, we recommend using link aggregation (LAG) or configuring dynamic AP-manager interfaces on each Gigabit Ethernet port to automatically balance the load. If more than 100 access points are connected to the Cisco 5500 Series Controller, make sure that more than one Gigabit Ethernet interface is connected to the upstream switch.

Note The Gigabit Ethernet ports on the Cisco 5508 Controllers accept these SX/LC/T small form-factor plug-in (SFP) modules: - 1000BASE-SX SFP modules, which provide a 1000-Mbps wired connection to a network through an 850nM (SX) fiber-optic link using an LC physical connector - 1000BASE-LX SFP modules, which provide a 1000-Mbps wired connection to a network through a 1300nM (LX/LH) fiber-optic link using an LC physical connector - 1000BASE-T SFP modules, which provide a 1000-Mbps wired connection to a network through a copper link using an RJ-45 physical connector

- Each distribution system port is, by default, an 802.1Q VLAN trunk port. The VLAN trunking characteristics of the port are not configurable.

Note Some controllers support link aggregation (LAG), which bundles all of the controller's distribution system ports into a single 802.3ad port channel. Cisco 5500 Series Controllers support LAG, and LAG is enabled automatically on the controllers within the Cisco WiSM2.

- In Cisco Flex 7500 and 8500 Series Controllers:

- If a port is unresponsive after a soaking period of 5 seconds, all the interfaces for which the port is the primary and the active port, fail over to the backup port, if a backup is configured and is operational. Similarly, if the unresponsive port is the backup port, then all the interfaces fail over to the primary port if it is operational.
- After the unresponsive port is restored, there is a soaking period of 60 seconds after which if the port is still operational, then all the interfaces fall back to this port, which was the primary port. If the port was the backup port, then no change is done.

Information About Service Port

Cisco 5500 Series Controllers also have a 10/100/1000 copper Ethernet service port. The service port is controlled by the service-port interface and is reserved for out-of-band management of the controller and system recovery and maintenance in the event of a network failure. It is also the only port that is active when the controller is in boot mode. The service port is not capable of carrying 802.1Q tags, so it must be connected to an access port on the neighbor switch. Use of the service port is optional.

Note The service port is not autosensing. You must use the correct straight-through or crossover Ethernet cable to communicate with the service port.

Caution Do not configure wired clients in the same VLAN or subnet of the service port of the controller on the network. If you configure wired clients on the same subnet or VLAN as the service port, it is not possible to access the management interface of the controller.

Information About Interfaces

An interface is a logical entity on the controller. An interface has multiple parameters associated with it, including an IP address, default gateway (for the IP subnet), primary physical port, secondary physical port, VLAN identifier, and DHCP server.

These five types of interfaces are available on the controller. Four of these are static and are configured at setup time:

- Management interface (static and configured at setup time; mandatory)
- AP-manager interface (static and configured at setup time; mandatory)

Note You are not required to configure an AP-manager interface on Cisco 5500 Series Controllers.

- Virtual interface (static and configured at setup time; mandatory)
- Service-port interface (static and configured at setup time; optional)
- Dynamic interface (user-defined)

Note Typically, you define the management, AP-manager, virtual, and service-port interface parameters using the Startup Wizard. However, you can display and configure interface parameters through either the GUI or CLI after the controller is running.

When LAG is disabled, each interface is mapped to at least one primary port, and some interfaces (management and dynamic) can be mapped to an optional secondary (or backup) port. If the primary port for an interface fails, the interface automatically moves to the backup port. In addition, multiple interfaces can be mapped to a single controller port.

Note Interfaces that are quarantined are not displayed on the Controller > Interfaces page. For example, if there are 6 interfaces and one of them is quarantined, the quarantined interface is not displayed and the details of the other 5 interfaces are displayed on the GUI. You can get the total number of interfaces that is inclusive of quarantined interfaces through the count displayed on the top-right corner of the GUI.

Restrictions for Configuring Interfaces

- Each physical port on the wireless controller can have only one AP-manager configured with it. For the Cisco 5500 Series Controllers, the management interface with AP-management enabled cannot fail over to the backup port, which is primary for the AP-manager on the management or dynamic VLAN interface.
- Cisco 5500 Series Controllers do not support fragmented pings on any interface.

Information About Dynamic AP Management

A dynamic interface is created as a WLAN interface by default. However, any dynamic interface can be configured as an AP-manager interface, with one AP-manager interface allowed per physical port. A dynamic interface with the Dynamic AP Management option enabled is used as the tunnel source for packets from the controller to the access point and as the destination for CAPWAP packets from the access point to the controller. The dynamic interfaces for AP management must have a unique IP address and are usually configured on the same subnet as the management interface.

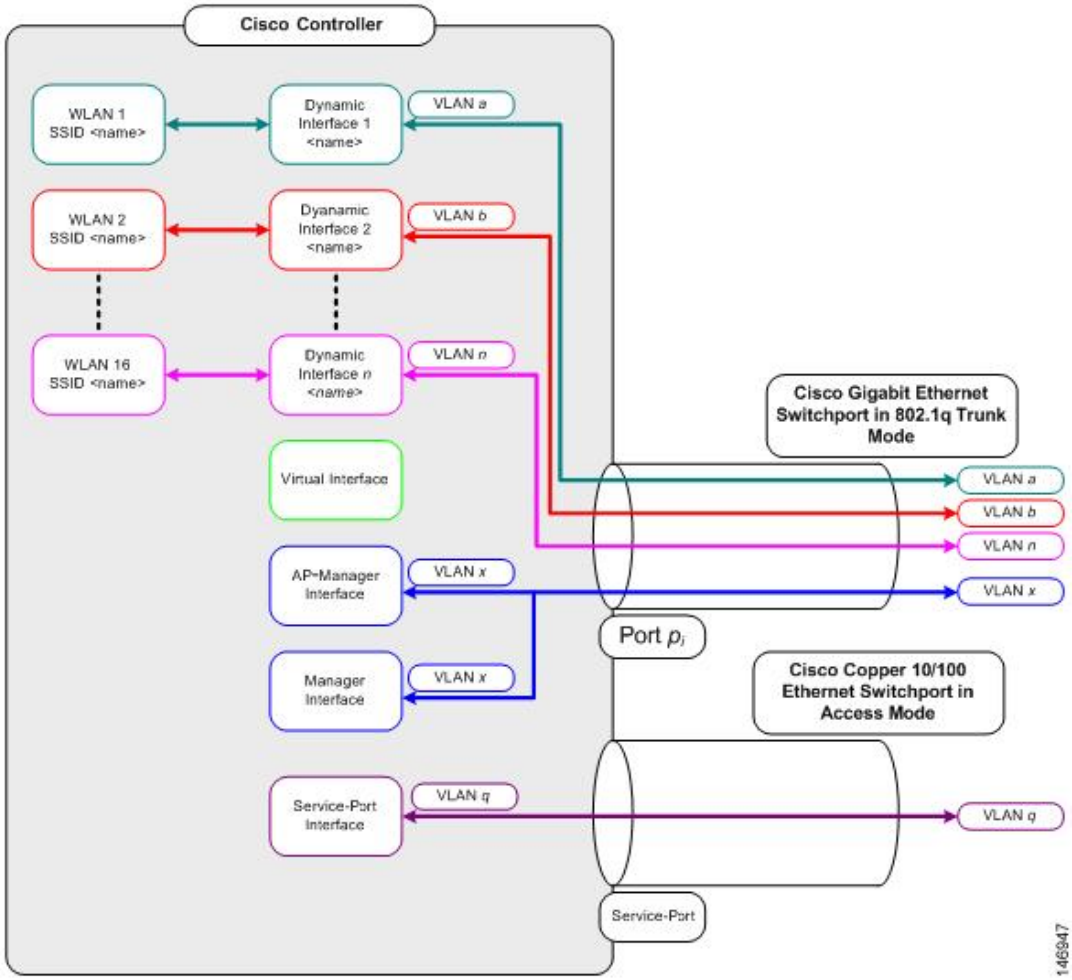
Note If link aggregation (LAG) is enabled, there can be only one AP-manager interface.

We recommend having a separate dynamic AP-manager interface per controller port.

Information About WLANs

A WLAN associates a service set identifier (SSID) to an interface or an interface group. It is configured with security, quality of service (QoS), radio policies, and other wireless network parameters. Up to 512 WLANs can be configured per controller.

Figure 34: Relationship between Ports, Interfaces, and WLANs



Each controller port connection is an 802.1Q trunk and should be configured as such on the neighbor switch. On Cisco switches, the native VLAN of an 802.1Q trunk is an untagged VLAN. If you configure an interface to use the native VLAN on a neighboring Cisco switch, make sure you configure the interface on the controller to be untagged.

Note A zero value for the VLAN identifier (on the **Controller > Interfaces** page) means that the interface is untagged.

The default (untagged) native VLAN on Cisco switches is VLAN 1. When controller interfaces are configured as tagged (meaning that the VLAN identifier is set to a nonzero value), the VLAN must be allowed on the 802.1Q trunk configuration on the neighbor switch and not be the native untagged VLAN.

We recommend that tagged VLANs be used on the controller. You should also allow only relevant VLANs on the neighbor switch's 802.1Q trunk connections to controller ports. All other VLANs should be disallowed or pruned in the switch port trunk configuration. This practice is extremely important for optimal performance of the controller.

Note We recommend that you assign one set of VLANs for WLANs and a different set of VLANs for management interfaces to ensure that controllers properly route VLAN traffic.