Cisco IOS Configuration Guide for Autonomous Cisco Aironet Access Points

Cisco IOS Release 15.3(3)JBB

First Published: May 28, 2015

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Text Part Number:

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco IOS Configuration Guide for Autonomous Cisco Aironet Access Points

CONTENTS

CHAPTER 7

CHAPTER 8

Preface

Audience

This guide is for the networking professional who installs and manages Cisco Aironet Access Points in Autonomous mode. To use this guide, you should have experience working with the Cisco IOS software and be familiar with the concepts and terminology of wireless local area networks.

The guide covers Cisco IOS Release 15.3(3)JA for Cisco Aironet Autonomous Access Points.

The following access point platforms are supported:

- AP 802
- AP 702I
- AP 700W
- AP 1040
- AP 1140
- AP 1260
- AP 1530
- AP 1550 (128 MB only supported)
- AP 1570
- AP 1600
- AP 1700
- AP 2600
- AP 2700
- AP 3500
- AP 3600 (AIR-RM3000AC-*x*-K9 802.11ac module is not supported)
- AP 3700 (AIR-RM3000AC-*x*-K9 802.11ac module is not supported)

Note This guide does not cover lightweight access points. Configuration for these devices can be found in the appropriate installation and configuration guides on Cisco.com.

Purpose

This guide provides the information you need to install and configure your access point. This guide provides procedures for using the Cisco IOS software commands that have been created or changed for use with the access point. It does not provide detailed information about these commands. For detailed information about these commands, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release. For information about the standard Cisco IOS software commands, refer to the Cisco IOS software documentation set available from the Cisco.com home page at **Support > Documentation**.

This guide also includes an overview of the access point web-based interface (APWI), which contains all the functionality of the command-line interface (CLI). This guide does not provide field-level descriptions of the APWI windows nor does it provide the procedures for configuring the access point from the APWI. For all APWI window descriptions and procedures, refer to the access point online help, which is available from the Help buttons on the APWI pages.

Configuration Procedures and Examples

The procedures and examples given in this guide have been documented as seen on the Cisco Aironet 3600 Series Access Points.

To view the latest configuration examples, visit Cisco Tech Zone(https://techzone.cisco.com). In the Tech Zone **Navigator**, browse to **Wireless LAN > Autonomous APs (IOS)** - Knowledge base for Autonomous (IOS) Wireless Deployments.

Note You need to have an account on Cisco.com to access Cisco Tech Zone. If you do not have an account, you can create one by clicking **Register Now** on the Log In page.

Organization

This guide is organized into these chapters:

Chapter 1, "Overview of Access Point Features," lists the software and hardware features of the access point and describes the access point role in your network.

Chapter 2, "Using the Web-Browser Interface," describes how to use the web-browser interface to configure the access point.

Chapter 3, "Using the Command-Line Interface," describes how to use the command-line interface (CLI) to configure the access point.

Chapter 4, "Configuring the Access Point for the First Time,"describes how to configure basic settings on a new access point.

Chapter 5, "Administrating the Access Point," describes how to perform one-time operations to administer your access point, such as preventing unauthorized access to the access point, setting the system date and time, and setting the system name and prompt.

Chapter 6, "Configuring Radio Settings," describes how to configure settings for the access point radio such as the role in the radio network, transmit power, channel settings, and others.

Chapter 7, "Configuring Multiple SSIDs," describes how to configure and manage multiple Service Set Identifiers (SSIDs) and multiple basic SSIDs (BSSIDs) on your access point. You can configure up to 16 SSIDs and up to eight BSSIDs on your access point.

Chapter 8, "Configuring Spanning Tree Protocol,"describes how to configure Spanning Tree Protocol (STP) on your access point, bridge, or access point operating in a bridge mode. STP prevents bridge loops from occurring in your network.

Chapter 9, "Configuring an Access Point as a Local Authenticator," describes how to configure the access point to act as a local RADIUS server for your wireless LAN. If the WAN connection to your main RADIUS server fails, the access point acts as a backup server to authenticate wireless devices.

Chapter 10, "Configuring WLAN Authentication and Encryption," describes how to configure the cipher suites required to use authenticated key management, Wired Equivalent Privacy (WEP), and WEP features including MIC, CMIC, TKIP, CKIP, and broadcast key rotation.

Chapter 11, "Configuring Authentication Types," describes how to configure authentication types on the access point. Client devices use these authentication methods to join your network.

Chapter 12, "Configuring Other Services," describes how to configure the access point to participate in WDS, to allow fast reassociation of roaming client services, and to participate in radio management.

Chapter 13, "Configuring RADIUS and TACACS+ Servers," describes how to enable and configure the RADIUS and Terminal Access Controller Access Control System Plus (TACACS+), which provide detailed accounting information and flexible administrative control over authentication and authorization processes.

Chapter 14, "Configuring VLANs," describes how to configure your access point to interoperate with the VLANs set up on your wired LAN.

Chapter 15, "Configuring QoS," describes how to configure and manage MAC address, IP, and EtherType filters on the access point using the web-browser interface.

Chapter 16, "Configuring Filters," describes how to configure and manage MAC address, IP, and EtherType filters on the access point using the web-browser interface.

Chapter 17, "Configuring CDP," describes how to configure Cisco Discovery Protocol (CDP) on your access point. CDP is a device-discovery protocol that runs on all Cisco network equipment.

Chapter 18, "Configuring SNMP," describes how to configure the Simple Network Management Protocol (SNMP) on your access point.

Chapter 19, "Configuring Repeater and Standby Access Points and Workgroup Bridge Mode," describes how to configure your access point as a hot standby unit or as a repeater unit.

Chapter 20, "Managing Firmware and Configurations," describes how to manipulate the Flash file system, how to copy configuration files, and how to archive (upload and download) software images.

Chapter 21, "Configuring L2TPv3 Over UDP/IP," describes how to configure the Layer 2 Tunneling Protocol (L2TPv3), which is a tunneling protocol that enables tunneling of Layer 2 packets over IP core networks.

Chapter 22, "Configuring Ethernet over GRE," describes Ethernet over GRE (EoGRE), which is a tunneling protocol that enables tunneling of Layer 2 packets encapsulated in GRE header over IP core networks.

Chapter 23, "Configuring System Message Logging," describes how to configure system message logging on your access point.

Chapter 25, "Miscellaneous AP-Specific Configurations," contains miscellaneous configurations that are specific to certain access points.

Appendix A, "Protocol Filters," lists some of the protocols that you can filter on the access point.

Appendix B, "Supported MIBs," lists the Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) that the access point supports for this software release.

Appendix C, "Error and Event Messages," lists the CLI error and event messages and provides an explanation and recommended action for each message.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface text**.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and timesavers use these conventions and symbols:

Note Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means reader be careful. In this situation, you might do something that could result equipment damage or loss of data.

Tip Means the following will help you solve a problem. The tips information might not be troubleshooting or even an action, but could be useful information.

Related Publications

- *Release Notes for Cisco Aironet Access Points and Bridges for Cisco IOS Release 15.3(3)JBB.*
- For each of the supported access points, the following types of guides have been provided as required on its respective support page on Cisco.com:
  - Access Point Getting Started Guide

- Access Point Hardware Installation Guide (Only in cases where hardware installation is not covered in the Getting Started Guide)
- Installation Instructions for Cisco Aironet Power Injectors
- Access Point Deployment Guide
- Cisco Aironet 802.11 a/b/g/n/ac Radio Installation and Upgrade Instructions

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Overview of Access Point Features

Cisco Aironet Access Points (hereafter called *access points*, or abbreviated as *APs*) provide a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking professionals. With a management system based on Cisco IOS software, Cisco Aironet access points are Wi-Fi certified, and depending on the specific model are 802.11a-compliant, 802.11b-compliant, 802.11g-compliant, 802.11n-compliant, and 802.11ac-compliant wireless LAN transceivers.

Note When booting up a 1530, 1700, or a 2700 series AP for the first time, it will boot up with a unified mode software image. To deploy the AP in an autonomous network, use following command from the AP console or telnet to force AP to reboot using autonomous mode software image.
capwap ap autonomous
For more information on software images on the AP, see Working with Software Images, page 20-20.

You can configure and monitor the wireless device using the command-line interface (CLI), the browser-based management system, or Simple Network Management Protocol (SNMP).

Radios in Access Points

An access point serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In large installations, wireless users within the radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

Each access point platform contains one, two, or three radios. For more information on the radios supported by each access point model, see the corresponding *Access Point Data Sheet*.

New Features and Platforms in this Release

For full information on the new features and updates to existing features in this release, see the *Release Notes for Autonomous Cisco Aironet Access Points and Bridges,* for this release at the following URL:

For the full list of CLI commands supported in this release, see the *Cisco IOS Command Reference for Autonomous Cisco Aironet Access Points and Bridges,* for this release at the following URL:

Note The proxy Mobile-IP feature is not supported in Cisco IOS Release 12.3(2)JA and later.

Support for Cisco Aironet 700W Series access points

- This AP supports 802.11n dual-radio 2 x 2 multiple-input multiple-output (MIMO) technology. It comes with integrated antennas, and supports 802.11a,b,g,n.
- Supported model is 702W.
- Supported operating modes are:
  - Root
  - Root Bridge
  - Non Root Bridge
  - Workgroup Bridge
  - Scanner
  - Spectrum
  - Repeater

For more information about this access point, visit:

http://www.cisco.com/c/en/us/products/wireless/aironet-700w-series/index.html.

Cisco Aironet 1570 Series

- This advanced carrier-grade outdoor access point supports 4x4 multiple-input and multiple-output (MIMO) smart antenna technology and three spatial streams for optimum performance. It comes with integrated and external antenna options, and supports 802.11a,b,g,n,ac.
- Supported models are 1572IC, 1572EC, and 1572 EAC
- Supported operating modes are:
  - Root
  - Root Bridge
  - Non Root Bridge
  - Workgroup Bridge

- Scanner
- Spectrum
- Repeater

For more information about this access point, visit:

http://www.cisco.com/go/ap1570.

New Features and Commands

Wi-Fi Certified Passpoint

This release features basic support for Wi-Fi Certified Passpoint, also known as Hotspot 2.0.

Wi-Fi Certified Passpoint, also known as Hotspot 2.0, streamlines network access in hotspots and eliminates the need for users to find and authenticate a network each time they connect. In Wi-Fi networks that do not support Passpoint, users must search for and choose a network, request the connection to the access point each time, and in many cases, must re-enter their authentication credentials. Passpoint automates that entire process, enabling a seamless connection between hotspot networks and mobile devices, with the highest WPA2 security.

In the current release Auto Discovery, 802.1x Authentication and Secure Connectivity are supported.

For configuration information, see Configuring 802.11u Hotspot and Hotspot 2.0, page 12-29.

Spectrum Expert on Cisco Aironet 1600 and 1570 series access points

This release supports Spectrum Expert mode on Cisco Aironet 1600 series access points. This allows the AP to connect to Cisco Spectrum Expert console (version 4.1 or later). You can configure the AP as a dedicated Spectrum Sensor that allows connection to Cisco Spectrum Expert.

For more information on Cisco Spectrum Expert, go to the following URL:

http://www.cisco.com/c/en/us/support/wireless/spectrum-expert/tsd-products-support-series-home.html

Ethernet over GRE (EoGRE)

Ethernet over GRE (EoGRE), is a tunneling protocol that enables tunneling of Layer 2 packets encapsulated in GRE header over IP core networks. Generic Routing Encapsulation (GRE) is a tunneling protocol that encapsulates a wide variety of network layer protocols inside virtual point-to-point links over a Layer 3 IPv4 or Layer 3 IPv6 access network. This release provides Ethernet over GRE (EoGRE) configuration. See Chapter 22, “Configuring Ethernet over GRE”.

Configuring Workgroup Bridges for High-Speed Roaming

For information on configuring workgroup bridges for high-speed roaming scenarios, such as in high-speed rail coaches, see Configuring Workgroup Bridges for High-Speed Roaming, page 19-24.

Note Configuring workgroup bridges for high-speed roaming scenarios is currently supported only on the Cisco Aironet 3600 and 3700 series access points.

Limiting Clients per Radio

You can now set the number of clients allowed for association with an interface. See Limiting Clients per Radio, page 6-9.

Configuring a Non-native VLAN as a Management VLAN

For information on configuring a non-native VLAN as a management VLAN, see Configuring a Non-native VLAN as a Management VLAN, page 14-10.

Downloading Configuration File Always from TFTP Server

You can set the AP to download the configuration file (config.txt) always from the TFTP server, even when the NVRAM (flash) has a configuration file stored on it. For more information, see Downloading Configuration File Always from TFTP Server, page 20-19.

Downloading Software Image Always from TFTP Server

You can set the AP to download the software image file, always from the TFTP server, even when an image exists on the NVRAM (flash). For more information, see Downloading Software Image Always from TFTP Server, page 20-34.

Commands for Cisco Aironet 1570 Series Access Points

The following commands have been introduced to support the Global Positioning System (GPS) module and the cable modem for AP 1570.

Command	Description
show cmodemstatus	Shows the following information about the cable modem: • Software version • AP MAC address • Cable Modem MAC address • Ethernet speed • Ethernet status • Data Over Cable Service Interface Specification (DOCSIS) Registration Status • Upstream Channel status • Downstream Channel status
show gps location	Shows the following information from the GPS module: • GPS location co-ordinates • Collection Time • Position Flags • Latitude • Longitude • Altitude • East Velocity • North Velocity • Up Velocity

Management Options

You can use the wireless device management system through the following interfaces:

- The Cisco IOS command-line interface (CLI), which you use through a console port or Telnet session. Use the **interface dot11radio** global configuration command to place the wireless device into the radio configuration mode. Most of the examples in this manual are taken from the CLI. Chapter 3, “Using the Command-Line Interface,” provides a detailed description of the CLI.
- A web-browser interface, which you use through a Web browser. Chapter 2, “Using the Web-Browser Interface,” provides a detailed description of the web-browser interface.
- Simple Network Management Protocol (SNMP). Chapter 18, “Configuring SNMP,” explains how to configure the wireless device for SNMP management.

Roaming Client Devices

If you have more than one wireless device in your wireless LAN, wireless client devices can roam seamlessly from one wireless device to another. The roaming functionality is based on signal quality, not proximity. When signal quality drops from a client, it roams to another access point.

Wireless LAN users are sometimes concerned when a client device stays associated to a distant access point instead of roaming to a closer access point. However, if a client signal to a distant access point remains strong and the signal quality is high, the client will not roam to a closer access point. Checking constantly for closer access points would be inefficient, and the extra radio traffic would slow throughput on the wireless LAN.

Using Cisco Centralized Key Management (CCKM) or 802.11r, with a device providing wireless distribution system (WDS), client devices can roam from one access point to another so quickly that there is no perceptible delay in voice or other time-sensitive applications.

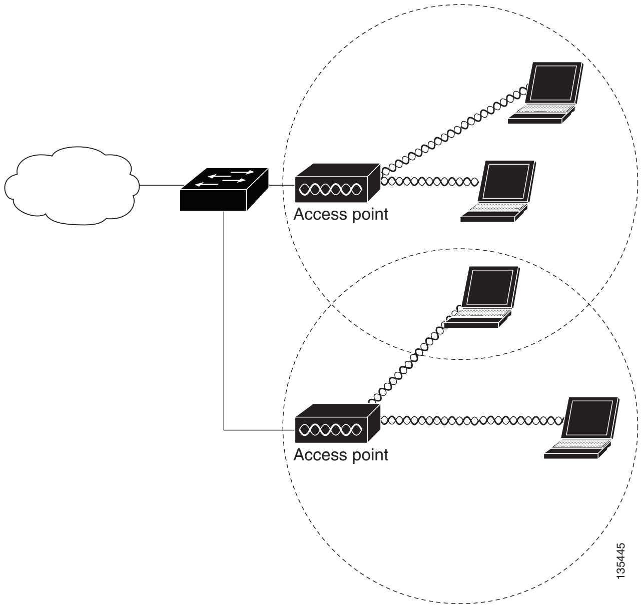
Network Configuration Examples

This section describes the role of an access point in common wireless network configurations. The access point default configuration is as a root unit connected to a wired LAN or as the central unit in an all-wireless network. Access points can also be configured as repeater access points, bridges, and workgroup bridges. These roles require specific configurations.

Root Access Point

An access point connected directly to a wired LAN provides a connection point for wireless users. If more than one access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. Figure 1-1 shows access points acting as root units on a wired LAN.

Figure 1-1 Access Points as Root Units on a Wired LAN

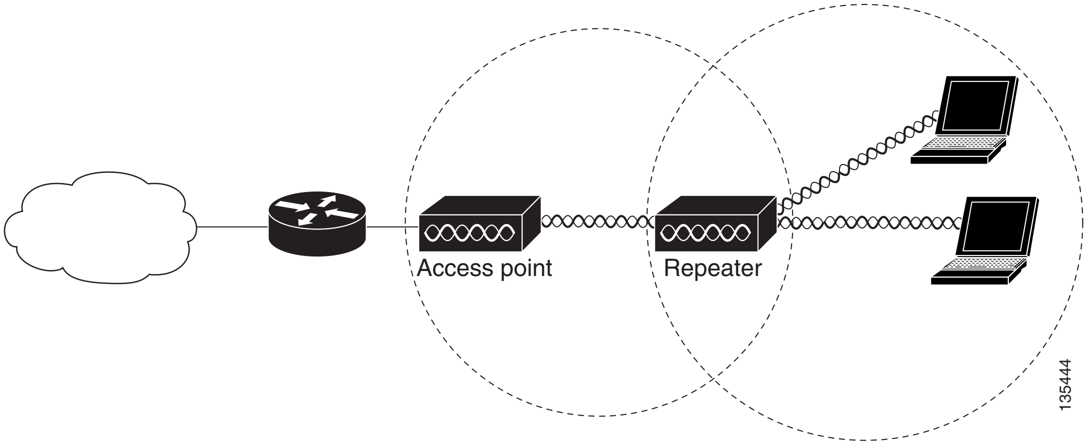


Repeater Access Point

An access point can be configured as a stand-alone repeater to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client. Figure 1-2 shows an access point acting as a repeater. Consult the "Configuring a Repeater Access Point" section on page 19-3 for instructions on setting up an access point as a repeater.

Note Non-Cisco client devices might have difficulty communicating with repeater access points.

Figure 1-2 Access Point as Repeater



Bridges

Access points can be configured as root or non-root bridges. In this role, an access point establishes a wireless link with a non-root bridge. Traffic is passed over the link to the wired LAN. Access points in root and non-root bridge roles can be configured to accept associations from clients. Figure 1-3 shows an access point configured as a root bridge with clients. Figure 1-4 shows two access points configured as a root and non-root bridge, both accepting client associations. Consult the "Configuring the Role in Radio Network" section on page 6-3 for instructions on setting up an access point as a bridge.

When wireless bridges are used in a point-to-multipoint configuration the throughput is reduced depending on the number of non-root bridges that associate with the root bridge. With a link data rate at 54 Mbps, the maximum throughput is about 25 Mbps in a point-to-point link. The addition of three bridges to form a point-to-multipoint network reduces the throughput to about 12.5 Mbps.

Figure 1-3 Access Point as a Root Bridge with Clients

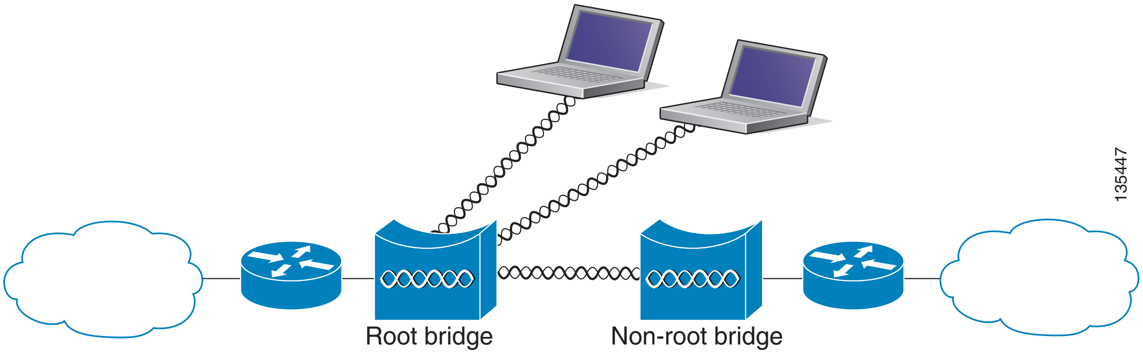
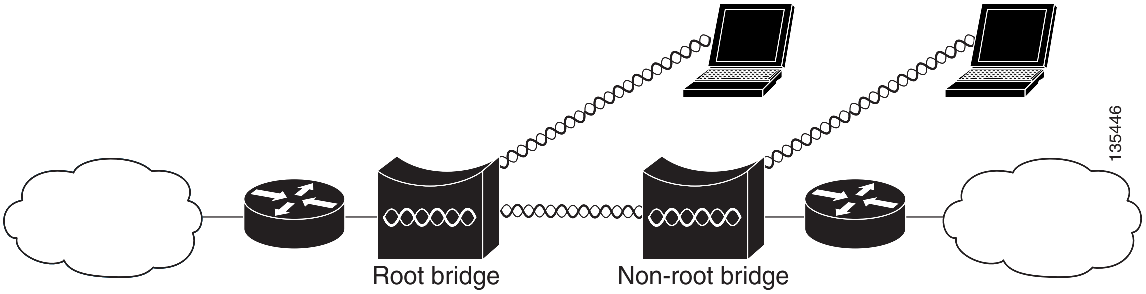


Figure 1-4 Access Points as Root and Non-root Bridges with Clients



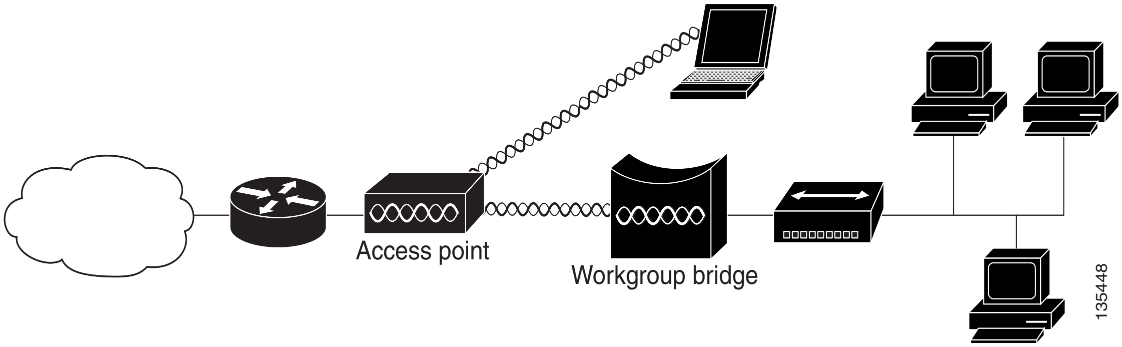
Workgroup Bridge

You can configure access points as workgroup bridges. In workgroup bridge mode, the unit associates to another access point as a client and provides a network connection for the devices connected to its Ethernet port. For example, if you need to provide wireless connectivity for a group of network printers, you can connect the printers to a hub or to a switch, connect the hub or switch to the access point Ethernet port, and configure the access point as a workgroup bridge. The workgroup bridge associates to an access point on your network.

If your access point has multiple radios, either radio can function in workgroup bridge mode..

Figure 1-5 shows an access point configured as a workgroup bridge. Consult the "Understanding Workgroup Bridge Mode" section on page 19-13 and the "Configuring Workgroup Bridge Mode" section on page 19-17 for information on configuring your access point as a workgroup bridge.

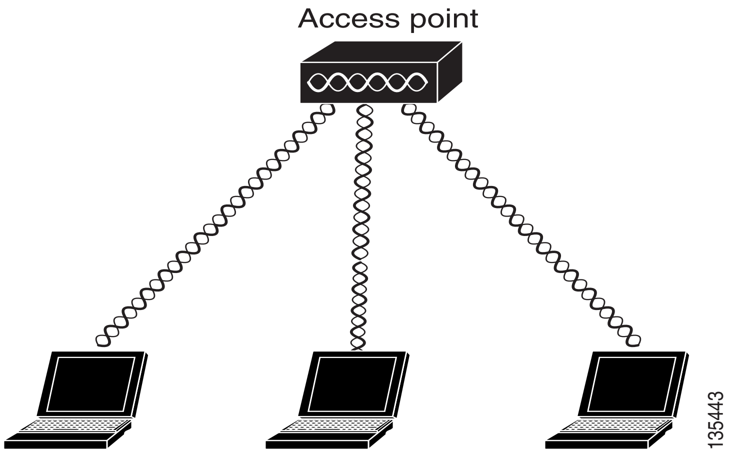
Figure 1-5 Access Point as a Workgroup Bridge



Central Unit in an All-Wireless Network

In an all-wireless network, an access point acts as a stand-alone root unit. The access point is not attached to a wired LAN; it functions as a hub linking all stations together. The access point serves as the focal point for communications, increasing the communication range of wireless users. Figure 1-6 shows an access point in an all-wireless network.

Figure 1-6 Access Point as Central Unit in All-Wireless Network



CHAPTER 2

Using the Web-Browser Interface

This chapter describes the web-browser interface that you can use to configure the wireless device.

The web-browser interface contains management pages that you use to change the wireless device settings, upgrade firmware, and monitor and configure other wireless devices on the network.

Note The wireless device web-browser interface is fully compatible with Microsoft Internet Explorer version 9.0 and Mozilla Firefox version 17.

Note Avoid using both the CLI and the web-browser interfaces to configure the wireless device. If you configure the wireless device using the CLI, the web-browser interface might display an inaccurate interpretation of the configuration. However, the inaccuracy does not necessarily mean that the wireless device is misconfigured.

Using the Web-Browser Interface for the First Time

Use the wireless device IP address to browse to the management system. See the "Logging into the Access Point" section on page 4-3 for instructions on assigning an IP address to the wireless device. Follow these steps to begin using the web-browser interface:

Step 1 Start the browser.

Step 2 Enter the wireless device IP address in the address bar of the and press **Enter**.
The Summary Status page appears.

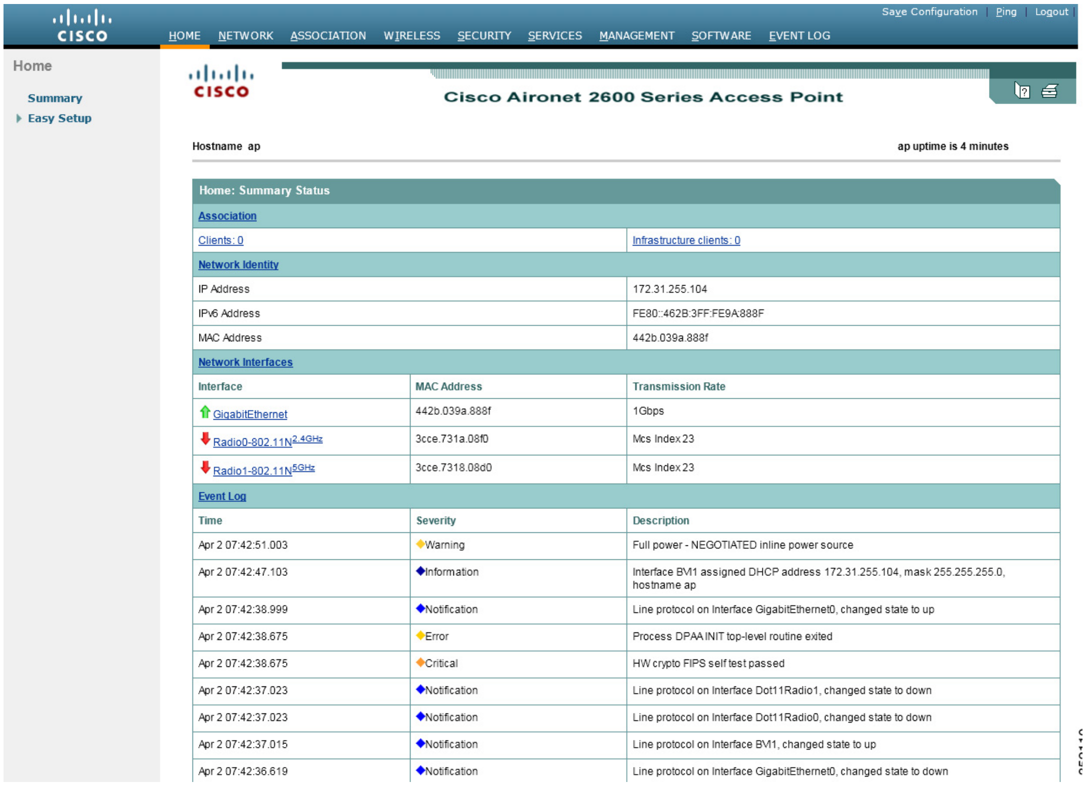
Using the Management Pages in the Web-Browser Interface

The system management pages use consistent techniques to present and save configuration information. You can use the navigation bar present at the top of a page to select the main menu options. Another navigation bar is present on the left side of the page, to use for navigating through the sub menus. You can use the navigation bar to browse to other management pages, and use the configuration action buttons to save or cancel changes to the configuration.

Note It is important to remember that clicking your web-browser **Back** button returns you to the previous page without saving any changes you have made. Clicking **Cancel** cancels any changes you made in the page and keeps you on that page. Changes are only applied when you click **Apply**.

Figure 2-1 shows the web-browser interface home page.

Figure 2-1 Web-Browser Interface Home Page


Save Configuration | Ping | Logout
HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
Home
Summary
Easy Setup
Cisco Aironet 2600 Series Access Point

Hostname ap

ap uptime is 4 minutes

Home: Summary Status

Association	
Clients: 0	Infrastructure clients: 0

Network Identity	
IP Address	172.31.255.104
IPv6 Address	FE80::462B:3FF:FE9A:888F
MAC Address	442b.039a.888f

Network Interfaces

Interface	MAC Address	Transmission Rate
↑ GigabitEthernet	442b.039a.888f	1Gbps
↓ Radio0-802.11N$^{2.4GHz}$	3cce.731a.08f0	Mcs Index 23
↓ Radio1-802.11N^{5GHz}	3cce.7318.08d0	Mcs Index 23

Event Log

Time	Severity	Description
Apr 2 07:42:51.003	◆Warning	Full power - NEGOTIATED inline power source
Apr 2 07:42:47.103	◆Information	Interface BVI1 assigned DHCP address 172.31.255.104, mask 255.255.255.0, hostname ap
Apr 2 07:42:38.999	◆Notification	Line protocol on Interface GigabitEthernet0, changed state to up
Apr 2 07:42:38.675	◆Error	Process DPAA INIT top-level routine exited
Apr 2 07:42:38.675	◆Critical	HW crypto FIPS self test passed
Apr 2 07:42:37.023	◆Notification	Line protocol on Interface Dot11Radio1, changed state to down
Apr 2 07:42:37.023	◆Notification	Line protocol on Interface Dot11Radio0, changed state to down
Apr 2 07:42:37.015	◆Notification	Line protocol on Interface BVI1, changed state to up
Apr 2 07:42:36.619	◆Notification	Line protocol on Interface GigabitEthernet0, changed state to down

Using Action Buttons

Table 2-1 lists the page links and buttons that appear on the management page.

Table 2-1 Buttons and Links on the Management Page

Button/Link	Description
Navigation Links	
Home	Displays wireless device status page with information on the number of radio devices associated to the wireless device, the status of the Ethernet and radio interfaces, and a list of recent wireless device activity.
Easy Setup	Displays the Easy Setup page that includes basic settings such as system name, IP address, and role in radio network.
Network	Displays a list of infrastructure devices on your wireless LAN. Provides configuration submenus for the access point interfaces (radio and Ethernet).
Association	Displays a list of all devices on your wireless LAN, listing their system names, network roles, and parent-client relationships.
Wireless	Displays a summary of wireless Domain services configuration and devices, and provides links to WDS configuration pages.
Security	Displays a summary of security settings and provides links to security configuration pages.

Table 2-1 Buttons and Links on the Management Page (continued)

Button/Link	Description
Services	Displays status for several wireless device features and links to configuration pages for Telnet/SSH, CDP, domain name server, filters, QoS, SNMP, SNTP, and VLANs.
Management	Displays a list of current guest users and provides links to configuration pages for guest users and web authentication pages.
Software	Displays the Version number of the firmware that the wireless device is running and provides links to configuration pages for upgrading and managing firmware.
Event Log	Displays the wireless device event log and provides links to configuration pages where you can select events to be included in traps, set event severity levels, and set notification methods.
Configuration Action Buttons	
Apply	Saves changes made on the page and remains on the page.
Refresh	Updates status information or statistics displayed on a page.
Cancel	Discards changes to the page and remains on the page.
Back	Discards any changes made to the page and returns to the previous page.
Logout	Exits the AP configuration web interface without saving.
Ping	Pings an IPv4 or IPv6 address
Save Configuration	Saves the AP's current configuration to NVRAM.

Character Restrictions in Entry Fields

You cannot use the following characters in the entry fields on the web-browser interface. This is true for all access points using Cisco IOS software.

“
]
+
/

Tab

Trailing space

Enabling HTTPS for Secure Browsing

You can protect the communication with the access point web-browser interface by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Socket Layer (SSL) protocol.

Note When you enable HTTPS, your browser might lose its connection to the access point. If you lose the connection, change the URL in your browser address line from http://*ip_address* to **https://*ip_address*** and log into the access point again.

Note When you enable HTTPS, most browsers prompt you for approval each time you browse to a device that does not have a fully qualified domain name (FQDN). To avoid the approval prompts, create an FQDN for the access point as detailed in the following procedure.

Follow these steps to create an FQDN and enable HTTPS:

Step 1 If your browser uses popup-blocking software, disable the popup-blocking feature.

Step 2 Choose **Easy Setup > Network Configuration**.

The Network Configuration page appears.

Step 3 Enter a name for the access point in the **Host Name** field, and then click **Apply**.

Step 4 Choose **Services > DNS** page.

The Services: DNS - Domain Name Service page appears.

Step 5 In the **Domain Name System (DNS)** field, click the **Enable** radio button.

Step 6 In the **Domain Name** field, enter your company's domain name.

Step 7 Enter at least one IP address for your DNS server in the **Name Server IPv4/IPv6 Addresses** fields.

Step 8 Click **Apply**.

The access point FQDN is a combination of the system name and the domain name. For example, if your system name is *ap3600* and your domain name is *company.com*, the FQDN is *ap3600.company.com*.

Step 9 Enter the FQDN on your DNS server.

Tip If you do not have a DNS server, you can register the access point FQDN with a dynamic DNS service. Search the Internet for *dynamic DNS* to find a fee-based DNS service.

Step 10 Choose **Services > HTTP**.

The Services: HTTP - Web Server page is displayed.

Step 11 In the **Web-based Configuration Management** field, select the **Enable Secure (HTTPS) Browsing** check box.

Step 12 In the **Domain Name** field, enter a domain name, and then click **Apply**.

Note Enabling HTTPS automatically disables HTTP. To maintain HTTP access with HTTPS enabled, check the **Enable Secure (HTTPS) Browsing** check box, and then check the **Enable Standard (HTTP) Browsing** check box. Although you can enable both standard HTTP and HTTPS, we recommend that you enable only one.

A warning appears stating that you will now use secure HTTP to browse to the access point. The warning also displays the new URL containing *https*, which you will need to use to browse to the access point.

Step 13 In the warning box, click **OK**.

The address in your browser address line changes from *http://*<ip-address> to *https://*<ip-address>.

Step 14 Another warning appears stating that the access point security certificate was not issued by a trusted certificate authority. However, you can ignore this warning. Click **Continue to this Website (not recommended).**

Note The following steps assume that you are using Microsoft Internet Explorer. If you are not, please refer to your browser documentation for more information on how to access web sites using self signed certificates.

Step 15 The access point login window appears and you must log in to the access point again. The default username is *Cisco* (case-sensitive) and the default password is *Cisco* (case-sensitive).

Step 16 To display the access point's security certificate, click the **Certificate error** icon in the address bar.

Step 17 Click **View Certificates**.

Step 18 In the Certificate window, click **Install Certificate**.
The Microsoft Windows Certificate Import Wizard appears.

Step 19 Click **Next**.
The next screen asks where you want to store the certificate. We recommend that you use the default storage area on your system.

Step 20 Click **Next** to accept the default storage area.
You have now successfully imported the certificate.

Step 21 Click **Finish**.
A security warning is displayed.

Step 22 Click **Yes**.
A message box stating that the installation is successful is displayed.

Step 23 Click **OK**.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Enabling HTTPS for Secure Browsing" section on page 2-5:

```
AP# configure terminal
AP(config)# hostname ap3600
AP(config)# ip domain name company.com
AP(config)# ip name-server 10.91.107.18
AP(config)# ip http secure-server
AP(config)# end
```

In this example, the access point system name is *ap3600*, the domain name is *company.com*, and the IP address of the DNS server is 10.91.107.18.

For complete descriptions of the commands used in this example, consult the Cisco IOS Commands Master List, Release 12.4. Click this link to browse to the master list of commands:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124mindx/124htnml.htm

Deleting an HTTPS Certificate

The access point generates a certificate automatically when you enable HTTPS. However, if you need to change the fully qualified domain name (FQDN) for an access point, or you need to add an FQDN after enabling HTTPS, you might need to delete the certificate. Follow these steps:

Step 1 Browse to the Services: HTTP Web Server page.

Step 2 Uncheck the **Enable Secure (HTTPS) Browsing** check box to disable HTTPS.

Step 3 Click **Delete Partial SSL certificate** to delete the certificate.

Step 4 Click **Apply**. The access point generates a new certificate using the new FQDN.

CLI Commands for Deleting an HTTPS Certificate

In the global configuration mode, use the following commands for deleting an HTTPS certificate.

	Command	Purpose
Step 1	**no ip http secure-server**	Disables HTTPS
Step 2	**crypto key zeroize rsa** *name-of-rsa-key*	Deletes the RSA key for the http server. Along with this all the router certificates (HTTPS certificates) issued using these keys will also be removed.

Using Online User Guides

In the web-browser interface, click the help icon at the top of the Home page to the online version of this guide (Cisco IOS Configuration Guide for Autonomous Cisco Aironet Access Points). You can choose view the guide online or you can also download a PDF version of the guide for offline reference. The online guide is periodically updated and hence will give you more up to date information.

Disabling the Web-Browser Interface

To prevent all use of the web-browser interface, select the **Disable Web-Based Management** check box on the Services: HTTP-Web Server page and click **Apply**.

To re-enable the web-browser interface, enter this global configuration command on the access point CLI:

```
ap(config)# ip http server
```

Using the Command-Line Interface

This chapter describes the Cisco IOS command-line interface (CLI) that you can use to configure the wireless device.

Cisco IOS Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

When you start a session on the wireless device, you begin in user mode, often called *user EXEC mode*. A subset of the Cisco IOS commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the wireless device reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you must enter privileged EXEC mode before you can enter the global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the wireless device reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

Table 3-1 describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the host name *ap*.

Table 3-1 Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with the wireless device.	`ap>`	Enter **logout** or **quit**.	Use this mode to: • Change terminal settings • Perform basic tests • Display system information
Privileged EXEC	While in user EXEC mode, enter the **enable** command.	`ap#`	Enter **disable** to exit.	Use this mode to verify commands. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`ap(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to the entire wireless device.
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface).	`ap(config-if)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the Ethernet and radio interfaces. The 2.4-GHz radio and the 802.11n 2.4-GHz radio is radio 0, The 5-GHz radio and the 802.11n 5-GHz radio is radio 1.

Getting Help

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command, as shown in Table 3-2.

Table 3-2 Help Summary

Command	Purpose
help	Obtains a brief description of the help system in any command mode.

abbreviated-command-entry?	Obtains a list of commands that begin with a particular character string.
	For example:
	`ap# di?`
	`dir  disable  disconnect`

abbreviated-command-entry<**Tab**>	Completes a partial command name.
	For example:
	`ap# sh conf<tab>`
	`ap# show configuration`

?	Lists all commands available for a particular command mode. For example: `ap> ?`
command **?**	Lists the associated keywords for a command. For example: `ap> show ?`

command keyword **?**	Lists the associated arguments for a keyword.
	For example:
	`ap(config)# cdp holdtime ?`
	`  <10-255>  Length of time (in sec) that receiver must keep this packet`

Abbreviating Commands

You have to enter only enough characters for the wireless device to recognize the command as unique. This example shows how to enter the **show configuration** privileged EXEC command:

```
ap# show conf
```

Using the no and Default Forms of Commands

Most configuration commands also have a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a *default* form. The default form of a command returns the command setting to its default. Most commands are disabled by default, so the default form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the default command enables the command and sets variables to their default values.

Understanding CLI Messages

Table 3-3 lists some error messages that you might encounter while using the CLI to configure the wireless device.

Table 3-3 Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for the wireless device to recognize the command.	Re-enter the command followed by a question mark (**?**) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`% Incomplete command.`	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (**?**) with a space between the command and the question mark. The possible keywords that you can enter with the command are displayed.
`% Invalid input detected at '^' marker.`	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (**?**) to display all the commands that are available in this command mode. The possible keywords that you can enter with the command are displayed.

Using Command History

The CLI provides a history or record of commands that you have entered. This feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize the command history feature to suit your needs as described in these sections:

- Changing the Command History Buffer Size, page 3-5
- Recalling Commands, page 3-5
- Disabling the Command History Feature, page 3-5

Changing the Command History Buffer Size

By default, the wireless device records ten command lines in its history buffer. Beginning in privileged EXEC mode, enter this command to change the number of command lines that the wireless device records during the current terminal session:

```
ap# terminal history [size number-of-lines]
```

The range is from 0 to 256.

Beginning in line configuration mode, enter this command to configure the number of command lines the wireless device records for all sessions on a particular line:

```
ap(config-line)# history [size number-of-lines]
```

The range is from 0 to 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in Table 3-4.

Table 3-4 Recalling Commands

Action[1]	Result
Press **Ctrl-P** or the up arrow key.	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press **Ctrl-N** or the down arrow key.	Return to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the up arrow key. Repeat the key sequence to recall successively more recent commands.
show history	While in privileged EXEC mode, list the last several commands that you just entered. The number of commands that are displayed is determined by the setting of the **terminal history** global configuration command and **history** line configuration command.

[1] The arrow keys function only on ANSI-compatible terminals such as VT100s.

Disabling the Command History Feature

The command history feature is automatically enabled.

To disable the feature during the current terminal session, enter the **terminal no history** privileged EXEC command.

To disable command history for the line, enter the **no history** line configuration command.

Using Editing Features

This section describes the editing features that can help you manipulate the command line. It contains these sections:

- Enabling and Disabling Editing Features, page 3-6
- Editing Commands Through Keystrokes, page 3-6
- Editing Command Lines that Wrap, page 3-7

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it.

To re-enable the enhanced editing mode for the current terminal session, enter this command in privileged EXEC mode:

```
ap# terminal editing
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
ap(config-line)# editing
```

To globally disable enhanced editing mode, enter this command in line configuration mode:

```
ap(config-line)# no editing
```

Editing Commands Through Keystrokes

Table 3-5 shows the keystrokes that you need to edit command lines.

Table 3-5 Editing Commands Through Keystrokes

Capability	Keystroke[1]	Purpose
Move around the command line to make changes or corrections.	**Ctrl-B** or the left arrow key	Move the cursor back one character.
	Ctrl-F or the right arrow key	Move the cursor forward one character.
	Ctrl-A	Move the cursor to the beginning of the command line.
	Ctrl-E	Move the cursor to the end of the command line.
	Esc B	Move the cursor back one word.
	Esc F	Move the cursor forward one word.
	Ctrl-T	Transpose the character to the left of the cursor with the character located at the cursor.
Recall commands from the buffer and paste them in the command line. The wireless device provides a buffer with the last ten items that you deleted.	**Ctrl-Y**	Recall the most recent entry in the buffer.
	Esc Y	Recall the next buffer entry. The buffer contains only the last 10 items that you have deleted or cut. If you press **Esc Y** more than ten times, you cycle to the first buffer entry.

Table 3-5 Editing Commands Through Keystrokes (continued)

Capability	Keystroke[1]	Purpose
Delete entries if you make a mistake or change your mind.	**Delete** or **Backspace**	Erase the character to the left of the cursor.
	Ctrl-D	Delete the character at the cursor.
	Ctrl-K	Delete all characters from the cursor to the end of the command line.
	Ctrl-U or **Ctrl-X**	Delete all characters from the cursor to the beginning of the command line.
	Ctrl-W	Delete the word to the left of the cursor.
	Esc D	Delete from the cursor to the end of the word.
Capitalize or lowercase words or capitalize a set of letters.	**Esc C**	Capitalize at the cursor.
	Esc L	Change the word at the cursor to lowercase.
	Esc U	Capitalize letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	**Ctrl-V** or **Esc Q**	
Scroll down a line or screen on displays that are longer than the terminal screen can display. **Note** The `More` prompt appears for output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the **Return** and **Space** bar keystrokes whenever you see the `More` prompt.	**Return**	Scroll down one line.
	Space	Scroll down one screen.
Redisplay the current command line if the wireless device suddenly sends a message to your screen.	**Ctrl-L** or **Ctrl-R**	Redisplay the current command line.

[1] The arrow keys function only on ANSI-compatible terminals such as VT100s.

Editing Command Lines that Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

In this example, the **access-list** global configuration command entry extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

```
ap(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
ap(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
ap(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
ap(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

After you complete the entry, press **Ctrl-A** to check the complete syntax before pressing the **Return** key to execute the command. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right:

```
ap(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

The software assumes you have a terminal screen that is 80 columns wide. If you have a width other than that, use the **terminal width** privileged EXEC command to set the width of your terminal.

Use line wrapping with the command history feature to recall and modify previous complex command entries. For information about recalling previous command entries, see the "Editing Commands Through Keystrokes" section on page 3-6.

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** or **more** command followed by the *pipe* character (|), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search for or filter out:

command **|** {**begin** | **include** | **exclude**} *regular-expression*

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

This example shows how to include in the output display only lines where the expression *protocol* appears:

```
ap# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet0/1 is up, line protocol is down
GigabitEthernet0/2 is up, line protocol is up
```

Accessing the CLI

You can open the wireless device CLI using Telnet or Secure Shell (SSH).

Opening the CLI with Telnet

Follow these steps to open the CLI with Telnet. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

Step 1 Select **Start** > **Programs** > **Accessories** > **Telnet**.

If Telnet is not listed in your Accessories menu, select **Start > Run**, type **Telnet** in the entry field, and press **Enter**.

Step 2 In the Telnet window, type **open** followed by the wireless device IP address, and press **Enter**.

Step 3 At the username and password prompts, enter your administrator username and password. The default username is **Cisco**, and the default password is **Cisco**. The default enable password is also **Cisco**. Usernames and passwords are case-sensitive.

Opening the CLI with Secure Shell

Secure Shell Protocol is a protocol that provides a secure, remote connection to networking devices set up to use it. Secure Shell (SSH) is a software package that provides secure login sessions by encrypting the entire session. SSH features strong cryptographic authentication, strong encryption, and integrity protection. For detailed information on SSH, visit the homepage of SSH Communications Security, Ltd. at this URL: http://www.ssh.com/

SSH provides more security for remote connections than Telnet by providing strong encryption when a device is authenticated. SSH versions 1 and 2 are supported in this release. See the "Configuring the Access Point for Secure Shell" section on page 5-27 for detailed instructions on setting up the wireless device for SSH access.

CHAPTER 4

Configuring the Access Point for the First Time

This chapter describes how to configure basic settings on the wireless device for the first time. The contents of this chapter are similar to the instructions in the quick start guide that shipped with the wireless device. You can configure all the settings described in this chapter using the CLI, but it might be simplest to browse to the wireless device web-browser interface to complete the initial configuration and then use the CLI to enter additional settings for a more detailed configuration.

Note The access point radio interfaces are disabled by default.

Before You Start

Before you install the wireless device, make sure you are using a computer connected to the same network as the wireless device, and obtain the following information from your network administrator:

- A system name for the wireless device
- The case-sensitive wireless service set identifier (SSID) for your radio network
- If not connected to a DHCP server, a unique IP address for the wireless device (such as 172.17.255.115)
- If the wireless device is not on the same subnet as your PC, a default gateway address and subnet mask
- A Simple Network Management Protocol (SNMP) community name and the SNMP file attribute (if SNMP is in use)
- If you use IPSU to find the wireless device IP address, the access point MAC address. The MAC address can be found on the label on the bottom of the access point (such as 00164625854c).

Resetting the Device to Default Settings

If you need to start over during the initial setup process, you can reset the access point to factory default settings.

Resetting to Default Settings Using the MODE Button

Note Using the MODE button for resetting to default settings applies only to autonomous mode access points and not to lightweight mode access points.

Follow these steps to reset the access point to factory default settings using the access point MODE button:

Step 1 Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

Step 2 Press and hold the MODE button while you reconnect power to the access point.

Step 3 Hold the MODE button until the Status LED turns amber (approximately 1 to 2 seconds), and release the button. All access point settings return to factory defaults.

Resetting to Default Settings Using the GUI

Follow these steps to return to the default settings using the access point GUI:

Step 1 Open your Internet browser.
The wireless device web-browser interface is fully compatible with Microsoft Internet Explorer version 9.0 and Mozilla Firefox version 17.

Step 2 Enter the wireless device IP address in the browser address line and press **Enter**. An Enter Network Password window appears.

Step 3 Enter your username in the User Name field. The default username is **Cisco**.

Step 4 Enter the wireless device password in the Password field and press **Enter**. The default password is **Cisco**. The Summary Status page appears.

Step 5 Click **Software** and the System Software screen appears.

Step 6 Click **System Configuration** and the System Configuration screen appears.

Step 7 Click the **Reset to Defaults** button to reset all settings, including the IP address, to factory defaults. To reset all settings except the IP address to defaults, click the **Reset to Defaults (Except IP)** button.

Resetting to Default Settings Using the CLI

Caution You should never delete any of the system files prior to resetting defaults or reloading software.

If you want to reset the access point to its default settings and a static IP address, use the *write erase* or *erase /all nvram* command. If you want to erase everything including the static IP address, in addition to the above commands, use the *erase* and *erase boot static-ipaddr static-ipmask* command.

From the privileged EXEC mode, you can reset the access point/bridge configuration to factory default values using the CLI by following these steps:

Step 1 Enter **erase nvram:** to erase all NVRAM files including the startup configuration.

Note The **erase nvram** command does not erase a static IP address.

Step 2 Follow the step below to erase a static IP address and subnet mask. Otherwise, go to step 3.

a. Enter **write default-config**.

Step 3 Enter **Y** when the following CLI message displays: *Erasing the nvram filesystem will remove all configuration files! Continue? [confirm].*

Step 4 Enter **reload** when the following CLI message displays: *Erase of nvram: complete*. This command reloads the operating system.

Step 5 Enter **Y** when the following CLI message displays: *Proceed with reload? [confirm].*

Caution Do not interrupt the boot process to avoid damaging the configuration file. Wait until the access point/bridge Install Mode LED begins to blink green before continuing with CLI configuration changes. You can also see the following CLI message when the load process has finished: *Line protocol on Interface Dot11Radio0, changed state to up*.

Step 6 After the access point/bridge reboots, you can reconfigure the access point by using the Web-browser interface if you previously assigned a static IP address, or the CLI if you did not.

The access point is configured with the factory default values including the IP address (set to receive an IP address using DHCP), from privileged EXEC mode. To obtain the new IP address for an access point/bridge, you can use the *show interface bvi1* CLI command.

Logging into the Access Point

A user can login to the access point using one of the following methods:

- graphical user interface (GUI)
- Telnet (if the AP is configured with an IP address)
- console port

Note Not all models of Cisco Aironet Access Points have the console port. If the access point does not have a console port, use either the GUI or the Telnet for access.

For information on logging into the AP through the GUI, refer to Using the Web-Browser Interface for the First Time, page 2-2.

For information on logging into the AP through the CLI refer to Accessing the CLI, page 3-9.

For information on logging into the AP through a console port refer to Connecting to an Access Point Locally, page 4-5.

Obtaining and Assigning an IP Address

To browse to the wireless device Express Setup page, you must either obtain or assign the wireless device IP address using one of the following methods:

- Connect to the access point console port and assign a static IP address. Follow the steps in the appropriate section to connect to the device console port:
  - Connecting to an Access Point Locally, page 4-5.
  - Connecting to the 1550 Series Access Point Locally, page 4-5

Note In some terminal emulator applications you may need to set the Flow control parameter to Xon/Xoff. If you are not able to console into the device with the flow control value set to none, try changing the flow control value to Xon/Xoff.

- Use a DHCP server (if available) to automatically assign an IP address. You can find out the DHCP-assigned IP address using one of the following methods:
  - Connect to the wireless device console port and use the **show ip interface brief** command to display the IP address.

    Follow the steps in the "Connecting to an Access Point Locally" section on page 4-5 to connect to the console port.
  - Provide your network administrator with the wireless device Media Access Control (MAC) address. Your network administrator will query the DHCP server using the MAC address to identify the IP address. The access point MAC address is on label attached to the bottom of the access point.

Default IP Address Behavior

When you connect a 1040, 1140, 1260, 2600 access point with a default configuration to your LAN, the access point requests an IP address from your DHCP server and, if it does not receive an address, continues to send requests indefinitely.

Connecting to an Access Point Locally

Note The following applies to all APs except the 1550 series APs.

If you need to configure the access point locally (without connecting the access point to a wired LAN), you can connect a PC to its console port using a DB-9 to RJ-45 serial cable. Follow these steps to open the CLI by connecting to the access point console port:

Step 1 Connect a nine-pin, female DB-9 to RJ-45 serial cable to the RJ-45 serial port on the access point and to the COM port on a computer. The Cisco part number for the DB-9 to RJ-45 serial cable is AIR-CONCAB1200. Browse to http://www.cisco.com/go/marketplace to order a serial cable.

Step 2 Set up a terminal emulator to communicate with the access point. Use the following settings for the terminal emulator connection: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Note If xon/xoff flow control does not work, use no flow control.

Step 3 When connected, press **enter** or type **en** to access the command prompt. Pressing **enter** takes you to the user exec mode. Entering **en** prompts you for a password, then takes you to the privileged exec mode. The default password is *Cisco* and is case-sensitive.

Note When your configuration changes are completed, you must remove the serial cable from the access point.

Connecting to the 1550 Series Access Point Locally

If you need to configure the access point locally (without connecting to a wired LAN), you can connect a PC to the Ethernet port on the long-reach power injector using a Category 5 Ethernet cable. You can use a local connection to the power injector Ethernet port the same as you would use a serial port connection.

Note You do not need a special crossover cable to connect your PC to the power injector; you can use either a straight-through cable or a crossover cable.

Follow these steps to connect to the bridge locally:

Step 1 Make sure that the PC you intend to use is configured to obtain an IP address automatically, or manually assign it an IP address within the same subnet as the access point/bridge IP address. For example, if you assigned the access point/bridge an IP address of 10.0.0.1, assign the PC an IP address of 10.0.0.20.

Step 2 With the power cable disconnected from the power injector, connect your PC to the power injector using a Category 5 Ethernet cable. You can use either a crossover cable or a straight-through cable.

Note Communication takes place between the power injector and the access point/bridge using Ethernet Port 0. Do not attempt to change any of the Ethernet Port 0 settings.

Step 3 Connect the power injector to the access point/bridge using dual coaxial cables.

Step 4 Connect the power injector power cable and power on the access point/bridge.

Step 5 Follow the steps in the "Assigning Basic Settings" section on page 4-6. If you make a mistake and need to start over, follow the steps in the "Resetting the Device to Default Settings" procedure on page 4-1.

Step 6 After configuring the access point/bridge, remove the Ethernet cable from your PC and connect the power injector to your wired LAN.

Note When you connect your PC to the access point/bridge or reconnect your PC to the wired LAN, you might need to release and renew the IP address on the PC. On most PCs, you can perform a release and renew by rebooting your PC or by entering **ipconfig /release** and **ipconfig /renew** commands in a command prompt window. Consult your PC operating instructions for detailed instructions.

Default Radio Settings

Beginning with Cisco IOS Release 12.3(8)JA, access point radios are disabled and no default SSID is assigned. This was done in order to prevent unauthorized users to access a customer wireless network through an access point having a default SSID and no security settings. You must create an SSID before you can enable the access point radio interfaces.

Assigning Basic Settings

After you determine or assign the wireless device IP address, you can browse to the wireless device Express Setup page and perform an initial configuration:

Step 1 Open your Internet browser.

Step 2 Enter the wireless device IP address in the browser address line and press **Enter**.
An Enter Network Password screen appears.

Step 3 Press **Tab** to bypass the Username field and advance to the Password field.

Step 4 Enter the case-sensitive password *Cisco* and press **Enter**.
The Summary Status page appears.

Step 5 Click **Easy Setup**.
The Express Setup screen appears.

Step 6 Click **Network Configuration**.

Step 7 Enter the **Network Configuration** settings which you obtained from your system administrator. The configurable settings include:

- **Host Name**—The host name, while not an essential setting, helps identify the wireless device on your network. The host name appears in the titles of the management system pages.

  Note You can enter up to 32 characters for the system name. However, when the wireless device identifies itself to client devices, it uses only the first 15 characters in the system name. If it is important for client users to distinguish between wireless devices, make sure that a unique portion of the system name appears in the first 15 characters.

  Note When you change the system name, the wireless device resets the radios, causing associated client devices to disassociate and quickly reassociate.

- **Server Protocol**—Click the radio button that matches the network method of IP address assignment.
  - **DHCP**—IP addresses are automatically assigned by your network DHCP server.
  - **Static IP**—The wireless device uses a static IP address that you enter in the IP address field.
- **IP Address**—Use this setting to assign or change the wireless device IP address. If DHCP is enabled for your network, leave this field blank.

Note If the wireless device IP address changes while you are configuring the wireless device using the web-browser interface or a Telnet session over the wired LAN, you lose your connection to the wireless device. If you lose your connection, reconnect to the wireless device using its new IP address. Follow the steps in the "Resetting the Device to Default Settings" section on page 4-1 if you need to start over.

- **IP Subnet Mask**—Enter the IP subnet mask provided by your network administrator so the IP address can be recognized on the LAN. If DHCP is enabled, leave this field blank.
- **Default Gateway**—Enter the default gateway IP address provided by your network administrator. If DHCP is enabled, leave this field blank.
- **IPv6 ProtocolP**—Specify the protcols to be applied, by selecting the required check boxes. You can select:
  - DHCP
  - Autoconfig
  - Static IP
- **IPv6 Address**—Enter the IPv6 address
- **Username**—Enter the username required to access the network.
- **Password**—Enter the password corresponding to the username required to access the network.
- **SNMP Community**—If your network is using SNMP, enter the SNMP Community name provided by your network administrator and select the attributes of the SNMP data (also provided by your network administrator).
- **Current SSID List (Read Only)**

Step 8 Enter the following **Radio Configuration** settings for the radio bands supported by the access point. Both the 2.4 GHz and 5 GHz radios have the following options:

- **SSID**—Type the SSID in the SSID entry field. The SSID can contain up to 32 alphanumeric characters.
  - **Broadcast SSID in Beacon**—To allow devices without a specified SSID to associate with the access point, select this check box. If this check box is selected, the access point will respond to Broadcast SSID probe requests and also broadcast its own SSID with its Beacons.
    When you broadcast the SSID, devices that do not specify an SSID can associate to the wireless device. This is a useful option for an SSID used by guests or by client devices in a public space. If you do not broadcast the SSID, client devices cannot associate to the wireless device unless their SSID matches this SSID. Only one SSID can be included in the wireless device beacon.
- **VLAN**—To enableVLAN for the radio, click the **Enable VLAN ID** radio button and then enter a VLAN identifier ranging from 1- 4095. To specify this as the native VLAN, check the **Native VLAN** check box. To disable VLAN, click the **No VLAN** radio button.
- **Security**—Select the security setting for the SSID. The settings are listed in order of robustness, from No Security to WPA, which is the most secure setting. If you select EAP Authentication or WPA, enter the IP address (the RADIUS Server IP address) and shared secret (RADIUS Server Secret) for the authentication server on your network.

Note If you do not use VLANs on your wireless LAN, the security options that you can assign to multiple SSIDs are limited. See the "Using VLANs" section on page 4-11 for details.

  - **No Security**—This security setting does not use an encryption key or key management, and uses open authentication.
  - **WEP Key**—This security setting uses mandatory WEP encryption, no key management and open authentication. You can specify up to four WEP keys, i.e. Key 1, 2, 3, and 4. Enter each key value, and specify whether it is 128 bit or 40 bit.
  - **EAP Authentication**—The Extensible Authentication Protocols (EAP) Authentication permits wireless access to users authenticated against a database through the services of an authentication server then encrypts the authenticated and authorized traffic. Use this setting for LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-GTC, EAP-SIM, and other 802.1x/EAP based protocols. This setting uses mandatory encryption WEP, open authentication + EAP, network EAP authentication, no key management, RADIUS server authentication port 1645. Specify the RADIUS Server and the RADIUS Server Secret.
  - **WPA**—The Wi-Fi Protected Access (WPA) security setting permits wireless access to users authenticated against a database through the services of an authentication server, then encrypts their authenticated and authorized IP traffic with stronger algorithms than those used in WEP. Make sure clients are WPA certified before selecting this option. This setting uses encryption ciphers tkip, open authentication + EAP, network EAP authentication, key management WPA mandatory, and RADIUS server authentication port 1645. Specify the RADIUS Server and the RADIUS Server Secret.

Note To better understand the security settings used here, see "Understanding the Security Settings" section on page 4-11.

- **Role in Radio Network**—Click the button that describes the role of the wireless device on your network. Select **Access Point (Root)** if the wireless device is connected to the wired LAN. Select **Repeater (Non-Root)** if it is not connected to the wired LAN. The only role supported on the

Airlink is root. For information on the roles supported by different APs in a radio network, see Configuring the Role in Radio Network, page 6-3. The following roles are available in a radio network:

  - **Access Point**—A root device. Accepts associations from clients and bridges wireless traffic from the clients to the wireless LAN. This setting can be applied to any access point.
  - **Repeater**—A non-root device. Accepts associations from clients and bridges wireless traffic from the clients to root access point connected to the wireless LAN. This setting can be applied to any access point.
  - **Root Bridge**—Establishes a link with a non-root bridge. In this mode, the device also accepts associations from clients.
  - **Non-Root Bridge**—In this mode, the device establishes a link with a root bridge.
  - **Install Mode**—Places the access point/bridge in auto installation mode so you can align and adjust a bridge link for optimum efficiency.
  - **Workgroup Bridge**—In the Workgroup bridge mode, the access point functions as a client device that associates with a Cisco Aironet access point or bridge. A workgroup bridge can have a maximum of 254 clients, presuming that no other wireless clients are associated to the root bridge or access point.
  - **Universal Workgroup Bridge**—Configures the access point as a workgroup bridge capable of associating with non-Cisco access points.
  - **Client MAC:**—The Ethernet MAC address of the client connected to the universal workgroup bridge. This field appears only in the universal workgroup bridge mode.
  - **Scanner**—Functions as a network monitoring device. In the Scanner mode, the access point does not accept associations from clients. It continuously scans and reports wireless traffic it detects from other wireless devices on the wireless LAN. All access points can be configured as a scanner.

- **Optimize Radio Network for**—Use this setting to select either preconfigured settings for the wireless device radio or customized settings for the wireless device radio.
  - **Throughput**—Maximizes the data volume handled by the wireless device, but might reduce its range.
  - **Range**—Maximizes the wireless device range but might reduce throughput.
  - **Default**—Sets the default values for the access point.
  - **Custom**—The wireless device uses the settings you enter on the Network Interfaces. Clicking **Custom** takes you to the Network Interfaces.
- **Aironet Extensions**—Enable this setting if there are only Cisco Aironet wireless devices on your wireless LAN.
- **Channel**—The default channel setting for the wireless device radios is least congested; at startup, the wireless device scans for and selects the least-congested channel. For the most consistent performance after a site survey, however, we recommend that you assign a static channel setting for each access point.
  - For the 2.4 GHz radio, the relevant options are Least-Congested, channel 1-2412, channel 2-2417, channel 3-2422, channel 4-2427, channel 5-2432, channel 6-2437, channel 7-2442, channel 8-2447, channel 9-2452, channel 10-2457, and channel 11-2462.
  - For the 5 GHz radio, the relevant options are Dynamic Frequency selection, channel 36-5180, channel 40-5200, channel 44-5220, channel 48-5240, channel 149-5745, channel 153-5765, channel 157-5785, channel 161-5805, and channel 165-5825.

- **Power**—Choose the power level from the **Power** drop-down list.
  - For the 2.4 GHz radio, the relevant options are Maximum, 22, 19, 16, 13, 10, 7, and 4.
  - For the 5 GHz radio, the relevant options are Maximum, 14, 11, 8, 5, and 2.

Step 9 Click **Apply** to save your settings.

Step 10 Click **Network Interfaces** to browse to the Network Interfaces Summary page.

Step 11 Click the radio interface to browse to the Network Interfaces: Radio Status page.

Step 12 Click the **Settings** tab to browse to the Settings page for the radio interface.

Step 13 Click **Enable** to enable the radio.

Step 14 Click **Apply**.

Your wireless device is now running but probably requires additional configuring to conform to your network operational and security requirements. Consult the chapters in this manual for the information you need to complete the configuration.

Note You can restore access points to factory defaults by unplugging the power jack and plugging it back in while holding down the Mode button for a few seconds, or until the Status LED turns amber.

Default Settings on the Easy Setup Page

Table 4-1 lists the default settings for the settings on the Express Setup page.

Table 4-1 Default Settings on the Express Setup Page

Setting	Default
Host Name	ap
Configuration Server Protocol	DHCP
IP Address	Assigned by DHCP by default; see the "Default IP Address Behavior" section on page 4-4 for a description of default IP address behavior on the access point
IP Subnet Mask	Assigned by DHCP by default; if DHCP is disabled, the default setting is 255.255.255.224
Default Gateway	Assigned by DHCP by default; if DHCP is disabled, the default setting is 0.0.0.0
IPv6 Protocol	DHCP and Autoconfig
SNMP Community	defaultCommunity (Read-only)
VLAN	No VLAN
Security	No Security
Role in Radio Network (for each radio installed)	Access point
Optimize Radio Network for	Default

Table 4-1 Default Settings on the Express Setup Page (continued)

Setting	Default
Aironet Extensions	Enable
Channel	Least-Congested (for 2.4GHz) and Dynamic Frequency Selection (for 5GHz)
Power	Maximum

Understanding the Security Settings

You can configure basic security settings in the **Easy Setup > Radio Configuration** section. You can use the options given in this section to create unique SSIDs and assign one of four security types to them.

You can create up to 16 SSIDs on the wireless device. The created SSIDs appear in the **Current SSID List**. On dual-radio wireless devices, the SSIDs that you create are enabled by default on both radio interfaces.

Note In Cisco IOS Release 12.4(23c)JA and 12.xxx, there is no default SSID. You must configure an SSID before client devices can associate to the access point.

The SSID can consist of up to 32 alphanumeric, case-sensitive, characters.

The first character can not contain the following characters:

- Exclamation point (!)
- Pound sign (#)
- Semicolon (;)

The following characters are invalid and cannot be used in an SSID:

- Plus sign (+)
- Right bracket (])
- Front slash (/)
- Quotation mark (")
- Tab
- Trailing spaces

Using VLANs

If you use VLANs on your wireless LAN and assign SSIDs to VLANs, you can create multiple SSIDs using any of the four security settings on the Express Security page. However, if you do not use VLANs on your wireless LAN, the security options that you can assign to SSIDs are limited because on the Express Security page encryption settings and authentication types are linked. Without VLANs, encryption settings (WEP and ciphers) apply to an interface, such as the 2.4-GHz radio, and you cannot use more than one encryption setting on an interface. For example, when you create an SSID with static WEP with VLANs disabled, you cannot create additional SSIDs with WPA authentication because they use different encryption settings. If you find that the security setting for an SSID conflicts with another SSID, you can delete one or more SSIDs to eliminate the conflict.

Security Types for an SSID

Table 4-2 describes the four security types that you can assign to an SSID.

Table 4-2 Security Types on Express Security Setup Page

Security Type	Description	Security Features Enabled
No Security	This is the least secure option. You should use this option only for SSIDs used in a public space and assign it to a VLAN that restricts access to your network.	None.
Static WEP Key	This option is more secure than no security. However, static WEP keys are vulnerable to attack. If you configure this setting, you should consider limiting association to the wireless device based on MAC address (see the Chapter 16, "Using MAC Address ACLs to Block or Allow Client Association to the Access Point" or, if your network does not have a RADIUS server, consider using an access point as a local authentication server (see Chapter 9, "Configuring an Access Point as a Local Authenticator").	Mandatory WEP. Client devices cannot associate using this SSID without a WEP key that matches the wireless device key.

Table 4-2 Security Types on Express Security Setup Page (continued)

Security Type	Description	Security Features Enabled
EAP Authentication	This option enables 802.1X authentication (such as LEAP, PEAP, EAP-TLS, EAP-FAST, EAP-TTLS, EAP-GTC, EAP-SIM, and other 802.1X/EAP based products) This setting uses mandatory encryption, WEP, open authentication + EAP, network EAP authentication, no key management, RADIUS server authentication port 1645. You are required to enter the IP address and shared secret for an authentication server on your network (server authentication port 1645). Because 802.1X authentication provides dynamic encryption keys, you do not need to enter a WEP key.	Mandatory 802.1X authentication. Client devices that associate using this SSID must perform 802.1X authentication. If radio clients are configured to authenticate using EAP-FAST, open authentication with EAP should also be configured. If you do not configure open authentication with EAP, the following GUI warning message appears: WARNING: Network EAP is used for LEAP authentication only. If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured. If you are using the CLI, this warning message appears: SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.
WPA	Wi-Fi Protected Access (WPA) permits wireless access to users authenticated against a database through the services of an authentication server, then encrypts their IP traffic with stronger algorithms than those used in WEP. This setting uses encryption ciphers, TKIP, open authentication + EAP, network EAP authentication, key management WPA mandatory, and RADIUS server authentication port 1645. As with EAP authentication, you must enter the IP address and shared secret for an authentication server on your network (server authentication port 1645).	Mandatory WPA authentication. Client devices that associate using this SSID must be WPA-capable. If radio clients are configured to authenticate using EAP-FAST, open authentication with EAP should also be configured. If you do not configure open authentication with EAP, the following GUI warning message appears: WARNING: Network EAP is used for LEAP authentication only. If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured. If you are using the CLI, this warning message appears: SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.

Limitations of Security Settings

The security settings in the Easy Setup Radio Configuration section are designed for simple configuration of basic security. The options available are a subset of the wireless device security capabilities. Keep these limitations in mind when using the Express Security page:

- If the **No VLAN** option is selected, the static WEP key can be configured once. If you select **Enable VLAN,** the static WEP key should be disabled.
- You cannot edit SSIDs. However, you can delete SSIDs and re-create them.
- You cannot configure multiple authentication servers. To configure multiple authentication servers, use the Security Server Manager page.
- You cannot configure multiple WEP keys. To configure multiple WEP keys, use the Security Encryption Manager page.
- You cannot assign an SSID to a VLAN that is already configured on the wireless device. To assign an SSID to an existing VLAN, use the Security SSID Manager page.
- You cannot configure combinations of authentication types on the same SSID (for example, MAC address authentication and EAP authentication). To configure combinations of authentication types, use the Security SSID Manager page.

CLI Configuration Examples

The examples in this section show the CLI commands that are equivalent to creating SSIDs using each security type. This section contains these example configurations:

- Example: No Security for Radio 2.4GHz, page 4-15
- Example: Static WEP for Radio 2.4 GHz, page 4-16
- Example: EAP Authentication, page 4-17
- Example: WPA2 for Radio 2.4GHz, page 4-19

Example: No Security for Radio 2.4GHz

This example shows a part of the resulting configuration when an SSID called *no_security_ssid* is created, the SSID is included in the beacon, assigned to VLAN 10, and then VLAN 10 is selected as the native VLAN:

```
!
dot11 ssid no_security_ssid
   vlan 10
   authentication open
   guest-mode
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 shutdown
 !
 ssid no_security_ssid
 !
 antenna gain 0
 station-role root
!
interface Dot11Radio0.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 station-role root
!
interface Dot11Radio1.10
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
```

Example: Static WEP for Radio 2.4 GHz

This example shows a part of the configuration that results from creating an SSID called *static_wep_ssid*, excluding the SSID from the beacon, assigning the SSID to VLAN 20, selecting 3 as the key slot, and entering a 128-bit key:

```
!
dot11 ssid static_wep_ssid
   vlan 20
   authentication open
!
!
!
encryption vlan 20 key 3 size 128bit 7 76031220D71D63394A6BD63DE57F transmit-key
encryption vlan 20 mode wep mandatory
 !
ssid static_wep_ssid
!
!
interface Dot11Radio0.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 subscriber-loop-control
bridge-group 20 spanning-disabled
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding
!
interface Dot11Radio0.31
encapsulation dot1Q 31 native
no ip route-cache
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
no ip address
no ip route-cache
!
encryption vlan 20 key 3 size 128bit 7 E55F05382FE2064B7C377B164B73 transmit-key
encryption vlan 20 mode wep mandatory
 !
ssid static_wep_ssid
!
!
interface Dot11Radio1.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 subscriber-loop-control
bridge-group 20 spanning-disabled
bridge-group 20 block-unknown-source
no bridge-group 20 source-learning
no bridge-group 20 unicast-flooding
!
interface Dot11Radio1.31
encapsulation dot1Q 31 native
```

```
no ip route-cache
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 spanning-disabled
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface GigabitEthernet0.20
encapsulation dot1Q 20
no ip route-cache
bridge-group 20
bridge-group 20 spanning-disabled
no bridge-group 20 source-learning
!
interface GigabitEthernet0.31
encapsulation dot1Q 31 native
no ip route-cache
bridge-group 1
bridge-group 1 spanning-disabled
no bridge-group 1 source-learning
!
```

Example: EAP Authentication

This example shows a part of the configuration that results from creating an SSID called *eap_ssid*, excluding the SSID from the beacon, and assigning the SSID to VLAN 30:

Note The following warning message appears if your radio clients are using EAP-FAST and you do not include open authentication with EAP as part of the configuration:

SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.

```
dot11 ssid eap_ssid
   vlan 30
   authentication open eap eap_methods
   authentication network-eap eap_methods
!
dot11 guest
!
username apuser password 7 096F471A1A0A
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 shutdown
 !
 encryption vlan 30 mode wep mandatory
 !
 ssid eap_ssid
 !
 antenna gain 0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 spanning-disabled
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 spanning-disabled
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 spanning-disabled
 no bridge-group 30 source-learning
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
!
radius server 10.10.11.100
 address ipv4 10.10.11.100 auth-port 1645 acct-port 1646
 key 7 00271A150754
!
bridge 1 route ip
```

Example: WPA2 for Radio 2.4GHz

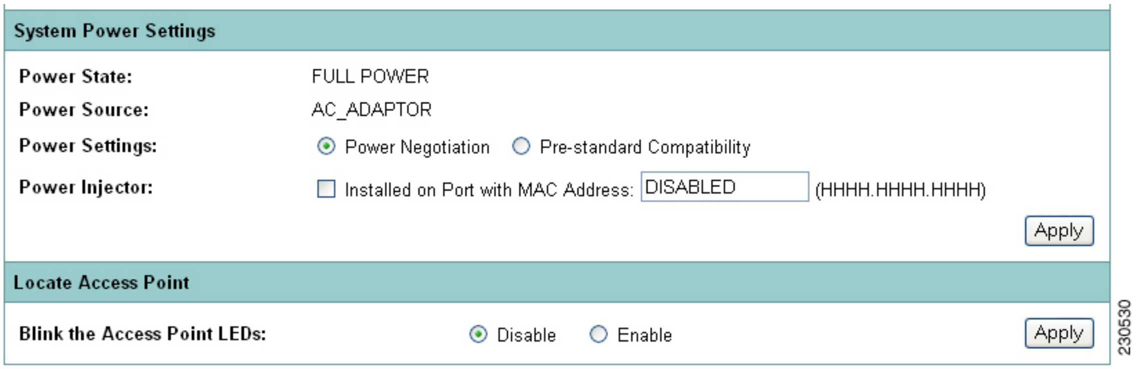
This example shows a part of the configuration that results from creating an SSID called *wpa_ssid*, excluding the SSID from the beacon, and assigning the SSID to VLAN 40:

```
aaa new-model
!
aaa group server radius rad_eap
 server name 10.10.11.100
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
aaa session-id common
!
dot11 ssid wpa_ssid
   vlan 40
   authentication open eap eap_methods
   authentication network-eap eap_methods
    authentication key-management wpa version 2
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 shutdown
 !
encryption vlan 40 mode ciphers aes-ccm
 !
 ssid wpa_ssid
 !
 antenna gain 0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 subscriber-loop-control
 bridge-group 40 spanning-disabled
 bridge-group 40 block-unknown-source
 no bridge-group 40 source-learning
 no bridge-group 40 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 subscriber-loop-control
 bridge-group 40 spanning-disabled
 bridge-group 40 block-unknown-source
 no bridge-group 40 source-learning
 no bridge-group 40 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 spanning-disabled
 no bridge-group 40 source-learning
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
!
radius-server attribute 32 include-in-access-req format %h
radius-server vsa send accounting
!
radius server 10.10.11.100
 address ipv4 10.10.11.100 auth-port 1645 acct-port 1646
 key 7 0....F175804
!
```

Configuring System Power Settings Access Points

The AP 1040, AP 802, AP 1140, AP 1550, AP 1600, AP 2600, AP 3500, AP 3600 and AP 1260 disable the radio interfaces when the unit senses that the power source to which it is connected does not provide enough power. Depending on your power source, you might need to enter the power source type in the access point configuration. Choose the **Software > System Configuration** page on the web-browser interface, and then select a power option. Figure 4-1 shows the System Power Settings section of the System Configuration page.

Figure 4-1 Power Options on the System Software: System Configuration Page



System Power Settings

Power State: FULL POWER

Power Source: AC_ADAPTOR

Power Settings: ● Power Negotiation ○ Pre-standard Compatibility

Power Injector: □ Installed on Port with MAC Address: DISABLED (HHHH.HHHH.HHHH)

Locate Access Point

Blink the Access Point LEDs: ● Disable ○ Enable

Using the AC Power Adapter

If you use the AC power adapter to provide power access point, you do not need to adjust the access point configuration.

Using a Switch Capable of IEEE 802.3af Power Negotiation

If you use a switch to provide Power over Ethernet (PoE) to the 1040, 1140, and 1260 access point, and the switch supports the IEEE 802.3af power negotiation standard, select **Power Negotiation** on the System Software: System Configuration page.

Using a Switch That Does Not Support IEEE 802.3af Power Negotiation

If you use a switch to provide Power over Ethernet (PoE) to the 1040, or 1140 access point, and the switch does not support the IEEE 802.3af power negotiation standard, select **Pre-Standard Compatibility** on the System Software: System Configuration page.

Using a Power Injector

If you use a power injector to provide power to the 1040, 1140, or 1260 access point, select **Power Injector** on the System Software: System Configuration page and enter the MAC address of the switch port to which the access point is connected.

dot11 extension power native Command

When enabled, the **dot11 extension power native** shifts the power tables the radio uses from the IEEE 802.11 tables to the native power tables. The radio derives the values for this table from the NativePowerTable and NativePowerSupportedTable of the CISCO-DOT11-1F-MIB. The Native Power tables were designed specifically to configure powers as low as -1dBm for Cisco Aironet radios that support these levels.

Support for 802.11ac

802.11ac is the next generation wireless standard of 802.11. It is designed to provide high throughput and operate in the 5 GHz band. 802.11ac is supported on the 3700, 2700, and 1700 series access points. The 802.11ac radio depends on the 802.11n radio to be fully functional. Shutting down the 802.11n radio will affect the 802.11ac functionalities.

Channel Widths for 802.11ac

802.11n and 802.11ac radios operate in the same band. However the channel widths can be independently configured with the restriction that it should be above the channel width configured on 802.11n. Please see Table 4-3 for more details on the supported channel width combinations.

Table 4-3 Supported Channel Width Combinations

802.11n Channel Bandwidth	802.11ac Channel Bandwidth
20	20
20	40
20	80
40	40
40	80

Off channel scanning or transmissions are not supported. The 802.11ac radio depends on 802.11n radios for the off channel scanning functionality.

For example, to configure 80 Mhz channel width:

```
ap# configure terminal
ap(config)# interface dot11Radio 1
ap(config-if)# channel width 80
ap(config-if)# end
```

Power Management for 802.11ac

The 3700, 2700, and 1700 802.11ac series access points can be powered by a Power-over-Ethernet (PoE) sources, local power, or a power injector. If the AP is powered by PoE, based on the whether the source is PoE+ (802.3at) or PoE (802.3af), the AP will adjust certain radio configurations as it may require more power than provided by the inline power source.

For example, a 3700 series AP which is powered by PoE+ (802.3at) will provide 4x4:3 configuration on both radios, and when powered by PoE (802.3af) it will provide a 3x3:3 configuration on both radios. Please refer to the below table.

Tip Radio configurations such as 4x4:3 imply 4 transmitters and 4 receivers capable of 3 spatial streams

Note To determine whether the AP is running at high PoE power or reduced (15.4W) power, in the AP's GUI, got to the Home page. If the AP is running on reduced power, under **Home:Summary Status**, the following warning is displayed:

Due to insufficient inline power. Upgrade inline power source or install power injector.

All access points except outdoor mesh products can be powered over Ethernet. Access points with two radios powered over Ethernet are fully functional and support all the features. See Table 4-4 for the various power management options available.

Table 4-4 Inline Power Options based on Power Sources

Power Draw	Description	AP Functionality	PoE Budget (Watts)[1]	802.3af	E-PoE	802.3at PoE+ PWRINJ4
PoE + 802.3at	AP3700 Out of the box	4x4:3 on 2.4/5 GHz	16.1	No	Yes	Yes
PoE 802.3af	AP3700 Out of the box	3x3:3 on 2.4/5 GHz	15.4	Yes	N/A	N/A
PoE 802.3at	AP2700 Out of the Box	3x4:3 on 2.4/5 GHz and Auxillary Ethernet Port Enabled	16.8	No	No	Yes
PoE 802.3af	AP2700 Out of the Box	3x4:3 on 5 GHz and 2x2:2 on 2.4 GHz and Auxiliary Ethernet Port Enabled	15.4	Yes	Yes	N/A

[1] This is the power required at the PSE, which is either a switch or an injector.

802.11n and 802.11ac use the power levels configured on 802.11n. You cannot configure power levels independently for 802.11ac.

Assigning an IP Address Using the CLI

When you connect the wireless device to the wired LAN, the wireless device links to the network using a bridge virtual interface (BVI) that it creates automatically. Instead of tracking separate IP addresses for the wireless device Ethernet and radio ports, the network uses the BVI.

When you assign an IP address to the wireless device using the CLI, you must assign the address to the BVI. Beginning in privileged EXEC mode, follow these steps to assign an IP address to the wireless device BVI:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface bvi1**	Enters interface configuration mode for the BVI.
Step 3	**ip address** *address mask*	Assigns an IP address and address mask to the BVI. **Note** If you are connected to the wireless device using a Telnet session, you lose your connection to the wireless device when you assign a new IP address to the BVI. If you need to continue configuring the wireless device using Telnet, use the new IP address to open another Telnet session to the wireless device.

Using a Telnet Session to Access the CLI

Follow these steps to access the CLI by using a Telnet session. These steps are for a PC running Microsoft Windows with a Telnet terminal application. Check your PC operating instructions for detailed instructions for your operating system.

Step 1 Choose **Start > Programs > Accessories > Telnet**.

If Telnet is not listed in your Accessories menu, select **Start > Run**, type **Telnet** in the entry field, and press **Enter**.

Step 2 When the Telnet window appears, click **Connect** and select **Remote System**.

Note In Windows 2000, the Telnet window does not contain drop-down lists. To start the Telnet session in Windows 2000, type **open** followed by the wireless device IP address.

Step 3 In the Host Name field, type the wireless device IP address and click **Connect**.

Configuring the 802.1X Supplicant

Traditionally, the dot1x authenticator/client relationship has always been a network device and a PC client respectively, as it was the PC user that had to authenticate to gain access to the network. However, wireless networks introduce unique challenges to the traditional authenticator/client relationship. First, access points can be placed in public places, inviting the possibility that they could be unplugged and their network connection used by an outsider. Second, when a repeater access point is incorporated into a wireless network, the repeater access point must authenticate to the root access point in the same way as a client does.

The supplicant is configured in two phases:

- Create and configure a credentials profile
- Apply the credentials to an interface or SSID

You can complete the phases in any order, but they must be completed before the supplicant becomes operational.

Creating a Credentials Profile

Beginning in privileged EXEC mode, follow these steps to create an 802.1X credentials profile:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot1x credentials** *profile*	Creates a dot1x credentials profile and enters the dot1x credentials configuration submode.
Step 3	**anonymous-id** *description*	(Optional)—Enter the anonymous identity to be used.
Step 4	**description** *description*	(Optional)—Enter a description for the credentials profile
Step 5	**username** *username*	Enter the authentication user id.
Step 6	**password {0 | 7 | LINE}**	Enter an unencrypted password for the credentials. **0**—An unencrypted password will follow. **7**—A hidden password will follow. Hidden passwords are used when applying a previously saved configuration. **LINE**—An unencrypted (clear text) password. **Note** Unencrypted and clear text are the same. You can enter a 0 followed by the clear text password, or omit the 0 and enter the clear text password.
Step 7	**pki-trustpoint** *pki-trustpoint*	(Optional and only used for EAP-TLS)—Enter the default pki-trustpoint.
Step 8	**end**	Return to the privileged EXEC mode.
Step 9	**copy running config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the **dot1x credentials** command to negate a parameter.

The following example creates a credentials profile named *test* with the username *Cisco* and a the unencrypted password *Cisco*:

```
ap>enable
Password:xxxxxxx
ap#config terminal
Enter configuration commands, one per line. End with CTRL-Z.
ap(config)# dot1x credentials test
ap(config-dot1x-creden)#username Cisco
ap(config-dot1x-creden)#password Cisco
ap(config-dot1x-creden)#exit
ap(config)#
```

Applying the Credentials to an Interface or SSID

Credential profiles are applied to an interface or an SSID in the same way.

Applying the Credentials Profile to the Wired Port

Beginning in the privileged EXEC mode, follow these steps to apply the credentials to the access point wired port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gigabitethernet 0**	Enter the interface configuration mode for the access point Gigabit Ethernet port. **Note** You can also use **interface fa0** to enter the Gigabit Ethernet configuration mode.
Step 3	**dot1x credentials** *profile name*	Enter the name of a previously created credentials profile.
Step 4	**end**	Return to the privileged EXEC mode
Step 5	**copy running config startup-config**	(Optional) Save your entries in the configuration file.

The following example applies the credentials profile *test* to the access point gigabit Ethernet port:

```
ap>enable
Password:xxxxxxx
ap#config terminal
Enter configuration commands, one per line. End with CTRL-Z.
ap(config)#interface Gig0
ap(config-if)#dot1x credentials test
ap(config-if)#end
```

Applying the Credentials Profile to an SSID Used For the Uplink

If you have a repeater access point in your wireless network and are using the 802.1X supplicant on the root access point, you must apply the 802.1X supplicant credentials to the SSID the repeater uses to associate with and authenticate to the root access point.

Beginning in the privileged EXEC mode, follow these steps to apply the credentials to an SSID used for the uplink:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ssid** *ssid*	Enter the 802.11 SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. **Note** The first character cannot contain the !, #, or; character. +,], /, “, TAB, and trailing spaces are invalid characters for SSIDs.
Step 3	**dot1x credentials** *profile*	Enter the name of a preconfigured credentials profile.
Step 4	**end**	Exits the dot1x credentials configuration submode
Step 5	**copy running config startup-config**	(Optional) Save your entries in the configuration file.

The following example applys the credentials profile *test* to the ssid *testap1 on a* repeater access point.

```
repeater-ap>enable
Password:xxxxxxx
repeater-ap#config terminal
Enter configuration commands, one per line. End with CTRL-Z.
repeater-ap(config-if)#dot11 ssid testap1
repeater-ap(config-ssid)#dot1x credentials test
repeater-ap(config-ssid)#end
repeater-ap(config)
```

Creating and Applying EAP Method Profiles

You can optionally configure an EAP method list to enable the supplicant to recognize a particular EAP method. See the “Creating and Applying EAP Method Profiles for the 802.1X Supplicant” section on page 11-17.

Configuring IPv6

IPv6 is the latest Internet protocol for IPv, developed to provide an extremely large number of addresses. It uses 128 bit addresses instead of the 32 bit addresses that are used in IPv4.

As deployments in wireless networks use greater number of IP wireless devices and smart phones, IPv6 with its 128-bit address format can support 3.4 x 1038 address space.

IPv6 addresses are represented as a series of 16-bit hexadecimal fields separated by colons (:) in the format: x:x:x:x:x:x:x:x.

There are three types of IPv6 address types:

- Unicast

  The Cisco IOS software supports these IPv6 unicast address types:

  - Aggregatable Global Address

    Aggregatable global unicast addresses are globally routable and reachable on the IPv6 portion of the Internet. These global addresses are identified by the format prefix of 001.

  - Link-Local Address

Link-Local Addressses are automatically configured on interface using link-local prefix FE80::/10 (1111 1110 10). The interface identifier is in the modified EUI-64 format.

- Anycast can be used only by a router and not the host. Anycast addresses must not be used as the source address of an IPv6 packet.
- Multicast address is a logical identifier for a group of hosts that process frames intended to be multicast for a designated network service. Multicast addresses in IPv6 use a prefix of FF00::/8 (1111 1111)

  IPv6 configuration uses these multicast groups:

  - Solicited-node multicast group FF02:0:0:0:0:1:FF00::/104
  - All-nodes link-local multicast group FF02::1
  - All-routers link-local multicast group FF02::2

Table 4-5 lists the IPv6 address types and formats.

Table 4-5 IPv6 Address Formats

IPv6 Address Type	Preferred Format	Compressed Format
Unicast	2001:0:0:0:DB8:800:200C:417A	2001::DB8:800:200C:417A
Multicast	FF01:0:0:0:0:0:0:101	FF01::101
Loopback	0:0:0:0:0:0:0:1	::1
Unspecified	0:0:0:0:0:0:0:0	::

The following modes are supported

- Root
- Root bridge
- Non Root bridge
- Repeater
- WGB

The following modes are not supported

- Spectrum mode
- Monitor mode

Beginning in privileged EXEC mode, use these commands to enable tie ipv6 address

- ap(config)# **int bv1**
- ap(config-if)# **ipv6 address**

A link-local address, based on the Modified EUI-64 interface ID, is automatically generated for the interface when stateless autoconfiguration is enabled.

Beginning in privileged EXEC mode, use the following command to enable stateless autoconfiguration:

ap(config-if)# **ipv6 address autoconfig**

Beginning in privileged EXEC mode, use the following command to configure a link local addreess without assigning any other IPv6 addressesto the interface:

ap(config-if)# **ipv6 address ipv6-address link-local**

Beginning in privileged EXEC mode, use the following command to assign a site-local or global address to the interface:

```
ap(config-if)# ipv6 address ipv6-address [eui-64]
```

Note The optional eui-64 keyword is used to utilize the Modified EUI-64 interface ID in the low order 64 bits of the address.

Configuring DHCPv6 address

DHCPv6 is a network protocol that is used for configuring IPv6 hosts with IP addresses, IP prefixes and other configuration required to operate on an IPv6 network. The DHCPv6 client obtains configuration parameters from a server either through a rapid two-message exchange (solicit, reply), or through a normal four-message exchange (solicit, advertise, request, reply). By default, the four-message exchange is used. When the rapid-commit option is enabled by both client and server, the two-message exchange is used.

Beginning in privileged EXEC mode, use these commands to enable the DHCPv6 client in an Access Point:

- ap# c**onf t**
- ap(config)**# int bv1**
- ap(config)**# ipv6 address dhcp rapid-commit(optional)**

Autonomous AP supports both DHCPv6 stateful and stateless addressing.

Stateful addressing

Stateful addressing uses a DHCP server. DHCP clients use stateful DHCPv6 addressing to obtain an IP address.

Beginning in privileged EXEC mode, use this command to configure stateful addressing:

```
ap(config)# ipv6 address dhcp
```

Stateless addressing

Stateless addressing does not use a DHCP server to obtain IP addresses. The DHCP clients autoconfigure their own IP addresses based on router advertisments.

Beginning in privileged EXEC mode, use this command to configure stateless addressing:

```
ap(config)# ipv6 address autoconfig
```

IPv6 Neighbor Discovery

The IPv6 neighbor discovery process uses ICMP messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network.

Beginning in privileged EXEC mode, use these commands to configure IPv6 neighbor discovery:

Command	Purpose
ipv6 nd ?	Configures neighbor discovery protocol.
ipv6 nd ns-interval *value*	This command is available only on bridge group virtual interface (BVI). Sets the interval between IPv6 neighbor solicitation retransmissions on an interface.
ipv6 nd reachable-time *value*	Sets the amount of time that a remote IPv6 node is reachable.
ipv6 nd dad attempts *value*	This command is available only on bridge group virtual interface (BVI). Configures the number of consecutive neighbor solicitation messages sent when duplicate address detection is performed on the unicast IPv6 addresses.
ipv6 nd dad time *value*	Configures the interval between IPv6 neighbor solicit transmissions for duplicate address detection.
ipv6 nd autoconfig default-router	This command is available only on bridge group virtual interface (BVI). Configures a default route to the Neighbor Discovery-derived default router.
ipv6 nd autoconfig prefix	This command is available only on bridge group virtual interface (BVI). Configures router solicitation message to solicit a router advertisement to eliminate any delay in waiting for the next periodic router advertisement.
ipv6 nd cache expire *expire-time-in-seconds*	Configures the length of time before the IPv6 neighbor discovery cache entry expires.
ipv6 nd cache interface-limit size [log rate]	Configures a neighbor discovery cache limit on a specified interface.
ipv6 nd na glean	This command is available only on bridge group virtual interface (BVI). Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement.
ipv6 nd nsf {**convergence** *time-in-seconds*| **dad** [**suppress**]| **throttle** *resolutions*}	Configures IPv6 neighbor discovery non-stop forwarding. You can specify the covergence time in seconds (10 to 600 seconds), suppress duplicate address detection (DAD), or set the number of resolutions to use with non-stop forwarding (NSF).
ipv6 nd nud limit *limit*	Configures the number of neighbor unreachability detection (NUD) resends, and set a limit to the number of unresolved resends.
ipv6 nd resolution data limit *limit-in-packets*	Configures a limit to the number of data packets in queue awaiting neighbor discovery (ND) resolution.
ipv6 nd route-owner	Inserts Neighbor Discovery-learned routes into the routing table with "ND" status and enables ND autoconfiguration behavior.

Configuring IPv6 Access Lists

IPv6 access lists (ACL) are used to filter traffic and restrict access to the router. IPv6 prefix lists are used to filter routing protocol updates.

Beginning in privileged EXEC mode, use these commands to to configure the access list globally and assign it to interface:

- ap(config)# **ipv6 access-list** *acl-name*

Beginning in privileged EXEC mode, you can use the command given in Table 4-6 for IPv6 Access List configuration.

Table 4-6 IPv6 Access List configuration commands

Command	Purpose
default	Set a command to its defaults.
deny	Specify packets to reject.
evaluate	Evaluate an access list.
exit	Exit from access-list configuration mode.
no	Negate a command or set its defaults.
permit	Specify packets to forward.
remark	Set an access list entry comment.
sequence	Set a sequence number for this entry.

Beginning in privileged EXEC mode, use these commands to assign the globally configured ACL to the outbound and inbound traffic on layer3 interface:

- ap(config)# **interface** *interface*
- ap(config)# **ipv6 traffic-filter** *acl-name* **in/out**

RADIUS Configuration

RADIUS server is a background process serving three functions:

- Authenticate users before granting them access to the network
- Authorize users for certain network services
- Account for the usage of certain network services

See Controlling Access Point Access with RADIUS, page 5-12.

IPv6 WDS Support

The WDS and the infrastructure access points communicate over a multicast protocol called WLAN Context Control Protocol (WLCCP).

Cisco IOS Release 15.2(4)JA supports communication between the WDS and Access Point through IPv6 addresses. The WDS works on a Dual Stack; that is, it accepts both IPv4 and IPv6 registeration.

IPv6 WDS AP registration

The first active IPv6 address is used to register the WDS. Table 4-7 shows different scenarios in the IPv6 WDS AP registration process.

Table 4-7 IPv6 WDS–AP Registration

	WDS			AP			
Scenario	**Dual**	**IPv6**	**IPv4**	**Dual**	**IPv6**	**IPv4**	**Mode of Communication**
1	Yes			yes			IPv6
2	Yes				yes		IPv6
3	Yes					yes	IPv4
4		yes		yes			IPv6
5		yes			yes		IPv6
6		yes				yes	Fails
7			yes	yes			IPv4
8			yes		yes		Fails
9			yes			yes	IPv4

Note 11r roaming between IPv4 and IPv6 access points is not supported because the MDIE is different. Both AP and WDS use the first active IPv6 address in BV1 to register and advertise. Link-local is not used for registration.

CDPv6 Support:

CDP is a layer2 protocol used to get information on the immediate neighbor's device-ID, capabilities, mac address, ip address or duplex. Each CDP enabled device sends information about itself to its immediate neighbor. As part of native IPv6, the access point sends its IPv6 address as well as part of the address TLV in the cdp message; it also parses the IPv6 address information it gets from the neighboring switch.

This command shows the connected IPv6 neighbor:

```
ap# show cdp neighbors detail
```

RA filtering

RA filtering increases the security of the IPv6 network by dropping RAs coming from wireless clients. RA filtering prevents misconfigured or malicious IPv6 clients from connecting to the network, often with a high priority that takes precedence over legitimate IPv6 routers. In all cases, the IPv6 RA is dropped at some point, protecting other wireless devices and upstream wired network from malicious or misconfigured IPv6 devices.

However, RA filtering is not supported in the uplink direction.

Automatic Configuring of the Access Point

The Autoconfig feature of autonomous access points allows the AP to download its configuration, periodically, from a Secure Copy Protocol (SCP) server. If the Autoconfig feaure is enabled, the AP downloads a configuration information file from the server at a pre-configured time and applies this configuration. The next configuration download is also scheduled along with this.

Note The AP does not apply a configuration if it is the same as the last downloaded configuration.

Enabling Autoconfig

To enable Autoconfig:

Step 1 Prepare a Configuration Information File

Step 2 Enable environmental variables

Step 3 Schedule the Configuration Information File Download

Prepare a Configuration Information File

An Autoconfig-enabled AP downloads the configuration information file from the SCP server. The configuration information file is an XML file, containing the following information:

- The new startup-configuration.
- An Absolute time and a Range value. The AP schedules the next information file download at this absolute time plus a random value between 0 and the range value.

The configuration information file has the following format:

```
<?xml version="1.0" encoding="UTF-8"?>
<l2tp_cfg>
    <cfg_fetch_start_time>Absolute Time</cfg_fetch_start_time>
    <cfg_fetch_time_range>Random Jitter</cfg_fetch_time_range>
    <cfg_fetch_config>
        <![CDATA[
        <Startup config>
        ]]>
    </cfg_fetch_config>
```

```
</l2tp_cfg>
```

The xml tags used in the configuration information file are described below.

XML Tags	Purpose
cfg_fetch_start_time	This tag contains the Absolute Time in the format DAY HH:MM, where: • DAY can be any of these values–Sun, Mon, Tue, Wed, Thu, Fri, Sat, All. • HH, indicates the hour, and can be a number from 0 to 23. • MM, indicates the minute, and can be a number from 0 to 59. Example: “Sun 10:30”, “Thu 00:00”, “All 12:40”
cfg_fetch_time_range	A random number of seconds between 0 to this value is added to the start time, to randomize the time when next information file is downloaded.
cfg_fetch_config	This tag contains the AP’s next startup configuration.

Enable environmental variables

After you have the configuration information file ready and hosted on the SCP server, you need to configure the following environmental variables.

Environmental Variable	Purpose
AUTO_CONFIG_AP_FUNCTIONALITY	To enable Autoconfig, this variable must be set ‘YES’.
AUTO_CONFIG_USER	Username for accessing the SCP server
AUTO_CONFIG_PASSWD	Password for accessing the SCP server
AUTO_CONFIG_SERVER	Hostname/IP of SCP server
AUTO_CONFIG_INF_FILE	Name of the configuration information file to be fetched from the SCP server

You can configure the environmental variables by using the following command in global configuration mode:

dot11 autoconfig add *environment-variable-name* **val** *value.*
For example:

```
dot11 autoconfig add AUTO_CONFIG_SERVER val 206.59.246.199
```

Schedule the Configuration Information File Download

After setting the environmental variables, you need to schedule the download of the configuration information file from the SCP server. Follow these steps:

Step 1 The AP's clock time must be in sync with a SNTP (Simple Network Time Protocol) server. You can set the SNTP server using the command, **sntp server** *sntp-server-ip,* where *sntp-server-ip* is the IP address of the SNTP server.

Step 2 You need to set the correct time zone for the AP to have the correct time, This can be done using the command **clock timezone** *TIMEZONE HH MM,* where:

- TIMEZONE is name of timezone like IST, UTC, or others.
- HH is the Hours offset from the timezone
- MM is the Minutes offset from timezone

Step 3 For instances where the download of the configuration information file from the SCP server fails, you can set a time interval after which the AP retries to download it again. This retry interval can be set using the command **dot11 autoconfig download retry interval min** *MIN* **max** *MAX***,** where:

- MIN is minimum number of seconds
- MAX is maximum number of seconds between retries. After every failed download, the retry interval doubles, but the retires stop the interval when becomes larger than MAX.

Enabling Autoconfig via a Boot File

You can enable Autoconfig by also providing the following commands in a boot file as a part of the DHCP IP configuration.

The format of the contents of the boot file returned by the DHCP/BootTP server should be as shown in the following example:

```
dot11 autoconfig add env var AUTO_CONFIG_AP_FUNCTIONALITY val YES
dot11 autoconfig add env var AUTO_CONFIG_USER val someusername
dot11 autoconfig add env var AUTO_CONFIG_PASSWD val somepasswd
dot11 autoconfig add env var AUTO_CONFIG_SERVER val scp.someserver.com
dot11 autoconfig add env var AUTO_CONFIG_INF_FILE val some_inf_file.xml
sntp server 208.210.12.199
clock timezone IST 5 30
dot11 autoconfig download retry interval min 100 max 400
end
```

Checking the Autoconfig Status

To know the Autoconfig status, use the **show dot11 autoconfig status** command.

Examples

```
AP1600-ATT# show dot11 autoconfig status
Dot11 l2tp auto config is disabled

1600-89-absim# show dot11 autoconfig status
Auto configuration download will occur after
45 seconds

1600-89-absim# show dot11 autoconfig status
Trying to download information file from server
```

Debugging Autoconfig

You can use the following debugging commands as required:

- Debug commands to see Autoconfig state machine transition:
  Deb dot11 autoconfigsm
- Debug commands to see Autoconfig events:
  Deb dot11 autoconfigev

CHAPTER 5

Administrating the Access Point

This chapter describes how to administrate the wireless device.

Disabling the Mode Button

You can disable the mode button on access points having a console port by using the global configuration **[no] boot mode-button** command. This command prevents password recovery and is used to prevent unauthorized users from gaining access to the access point CLI.

Caution This command disables password recovery. If you lose the privileged EXEC mode password for the access point after entering this command, you will need to contact the Cisco Technical Assistance Center (TAC) to regain access to the access point CLI.

The mode button is enabled by default. Beginning in the privilege EXEC mode, follow these steps to disable the access point mode button.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no boot mode-button**	Disables the access point mode button.
Step 3	**end**	**Note** It is not necessary to save the configuration.

You can check the status of the mode-button by executing the **show boot** or **show boot mode-button** commands in the privileged EXEC mode. The status does not appear in the running configuration. The following shows a typical response to the **show boot** and **show boot mode-button** commands:

```
ap#show boot
BOOT path-list:      flash:/ap3g2-k9w7-mx.152-4.JA1/ap3g2-k9w7-mx.152-4.JA1
Config file:         flash:/config.txt
Private Config file: flash:/private-config
Enable Break:        yes
Manual Boot:         no
Enable IOS Break:    no
HELPER path-list:
NVRAM/Config file
      buffer size:   32768
      Mode Button:    on
Radio Core TFTP:
ap#
```

Note As long as the privileged EXEC password is known, you can restore the mode button to normal operation using the global configuration **boot mode-button** command.

Preventing Unauthorized Access to Your Access Point

You can prevent unauthorized users from reconfiguring the wireless device and viewing configuration information. Typically, you want network administrators to have access to the wireless device while you restrict access to users who connect through a terminal or workstation from within the local network.

To prevent unauthorized access to the wireless device, you should configure one of these security features:

- Username and password pairs, which are locally stored on the wireless device. These pairs authenticate each user before that user can access the wireless device. You can also assign a specific privilege level (read only or read/write) to each username and password pair. For more information, see the "Configuring Username and Password Pairs" section on page 5-7. The default username is *Cisco*, and the default password is *Cisco*. Usernames and passwords are case-sensitive.

Note Characters TAB, ?, $, +, and [are invalid characters for passwords.

- Username and password pairs stored centrally in a database on a RADIUS or TACACS+ security server. For more information, see the "Controlling Access Point Access with RADIUS" section on page 5-12 and the "Controlling Access Point Access with TACACS+" section on page 5-17.

Protecting Access to Privileged EXEC Commands

A simple way of providing terminal access control in your network is to use passwords and assign privilege levels. Password protection restricts access to a network or network device. Privilege levels define what commands users can issue after they have logged into a network device.

Note For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Security Command Reference for Release 12.3*.

This section describes how to control access to the configuration file and privileged EXEC commands. It contains this configuration information:

Default Password and Privilege Level Configuration

Table 5-1 shows the default password and privilege level configuration.

Table 5-1 Default Password and Privilege Levels

Feature	Default Setting
Username and password	Default username is *Cisco* and the default password is *Cisco*.
Enable password and privilege level	Default password is *Cisco*. The default is level 15 (privileged EXEC level). The password is encrypted in the configuration file.
Enable secret password and privilege level	The default enable password is *Cisco*. The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file.
Line password	Default password is *Cisco*. The password is encrypted in the configuration file.

Setting or Changing a Static Enable Password

The enable password controls access to the privileged EXEC mode.

Note The **no enable password** global configuration command removes the enable password, but you should use extreme care when using this command. If you remove the enable password, you are locked out of the EXEC mode.

Beginning in privileged EXEC mode, follow these steps to set or change a static enable password:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**enable password** *password*	Define a new password or change an existing password for access to privileged EXEC mode. The default password is *Cisco*. For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. It can contain the question mark (?) character if you precede the question mark with the key combination Crtl-V when you create the password; for example, to create the password abc?123, do this: 1. Enter **abc**. 2. Enter **Crtl-V**. 3. Enter **?123**. When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-V; you can simply enter abc?123 at the password prompt. **Note** Characters TAB, ?, $, +, and [are invalid characters for passwords.

	Command	Purpose
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file. The enable password is not encrypted and can be read in the wireless device configuration file.

This example shows how to change the enable password to *l1u2c3k4y5*. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
AP(config)# enable password l1u2c3k4y5
```

Protecting Enable and Enable Secret Passwords with Encryption

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a Trivial File Transfer Protocol (TFTP) server, you can use either the **enable password** or **enable secret** global configuration commands. Both commands accomplish the same thing; that is, you can establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify.

We recommend that you use the **enable secret** command because it uses an improved encryption algorithm.

If you configure the **enable secret** command, it takes precedence over the **enable password** command; the two commands cannot be in effect simultaneously.

Beginning in privileged EXEC mode, follow these steps to configure encryption for enable and enable secret passwords:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.

Step 2	**enable password** [**level** *level*] {*password* | *encryption-type encrypted-password*}
	or
	enable secret [**level** *level*] {*password* | *encryption-type encrypted-password*}
		Define a new password or change an existing password for access to privileged EXEC mode.
		or
		Define a secret password, which is saved using a nonreversible encryption method.
		• (Optional) For *level*, the range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges).
		• For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.
		• (Optional) For *encryption-type*, both type 0 and type 7 are available. Encryption type 0 is for providing an unencrypted password. Encryption type 7 is for providing an encrypted password. Both types are taken and the password string is converted into an encryption type 5, a Cisco proprietary encryption algorithm. .
		Note If you specify an encryption type and then enter a clear text password, you can not re-enter privileged EXEC mode. You cannot recover a lost encrypted password by any method.

Step 3	**service password-encryption**	(Optional) Encrypt the password when the password is defined or when the configuration is written. Encryption prevents the password from being readable in the configuration file.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

If both the enable and enable secret passwords are defined, users must enter the enable secret password.

Use the **level** keyword to define a password for a specific privilege level. After you specify the level and set a password, give the password only to users who need to have access at this level. Use the **privilege level** global configuration command to specify commands accessible at various levels. For more information, see the "Configuring Multiple Privilege Levels" section on page 5-8.

If you enable password encryption, it applies to all passwords including username passwords, authentication key passwords, the privileged command password, and console and virtual terminal line passwords.

To remove a password and level, use the **no enable password** [**level** *level*] or **no enable secret** [**level** *level*] global configuration command. To disable password encryption, use the **no service password-encryption** global configuration command.

This example shows how to configure the encrypted password *$1$FaD0$Xyti5Rkls3LoyxzS8* for privilege level 2:

```
AP(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

Configuring Username and Password Pairs

You can configure username and password pairs, which are locally stored on the wireless device. These pairs are assigned to lines or interfaces and authenticate each user before that user can access the wireless device. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

Beginning in privileged EXEC mode, follow these steps to establish a username-based authentication system that requests a login username and a password:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**login local**	Enable local password checking at login time. Authentication is based on the username specified in Step 2.
Step 3	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	Enter the username, privilege level, and password for each user. • For *name*, specify the user ID as one word. Spaces and quotation marks are not allowed. • (Optional) For *level*, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 1 gives user EXEC mode access. • For *encryption-type*, enter 0 to specify that an unencrypted password will follow. Enter 7 to specify that a hidden password will follow. • For *password*, specify the password the user must enter to gain access to the wireless device. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable username authentication for a specific user, use the **no username** *name* global configuration command.

To disable password checking and allow connections without a password, use the **no login** line configuration command.

Note You must have at least one username configured and you must have login local set to open a Telnet session to the wireless device. If you enter the only username for the **no username** command, you can be locked out of the wireless device.

Alternatively, you can disable username verification for telnet with the line configuration command **no login**. You can then login to the AP with user verification, and then you will need the **enable password** (or **enable secret**) commands to gain privilege exec level. You can also grant this level by default to the telnet line with the command **privilege level 15**.

Note If you use both the no login and privilege level 15 commands, any telnet client connecting to the AP will have full privilege access to the AP.

```
ap(config)# line vty 0 4
ap(config-line)# no login
ap(config-line)# privilege level 15
```

Configuring Multiple Privilege Levels

By default, Cisco IOS software has two modes of password security: user EXEC and privileged EXEC. You can configure up to 16 hierarchical levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands.

For example, if you want many users to have access to the **clear line** command, you can assign it level 2 security and distribute the level 2 password fairly widely. But if you want more restricted access to the **configure** command, you can assign it level 3 security and distribute that password to a more restricted group of users.

This section includes this configuration information:

- Setting the Privilege Level for a Command, page 5-9
- Logging Into and Exiting a Privilege Level, page 5-9

Setting the Privilege Level for a Command

Beginning in privileged EXEC mode, follow these steps to set the privilege level for a command mode:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**privilege** *mode* **level** *level command*	Set the privilege level for a command. • For *mode*, enter **configure** for global configuration mode, **exec** for EXEC mode, **interface** for interface configuration mode, or **line** for line configuration mode. • For *level*, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the **enable** password. • For *command*, specify the command to which you want to restrict access.
Step 3	**enable password level** *level password*	Specify the enable password for the privilege level. • For *level*, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. • For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined. **Note** Characters TAB, ?, $, +, and [are invalid characters for passwords.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config** or **show privilege**	Verify your entries. The first command displays the password and access level configuration. The second command displays the privilege level configuration.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

When you set a command to a privilege level, all commands whose syntax is a subset of that command are also set to that level. For example, if you set the **show ip route** command to level 15, the **show** commands and **show ip** commands are automatically set to privilege level 15 unless you set them individually to different levels.

To return to the default privilege for a given command, use the **no privilege** *mode* **level** *level command* global configuration command.

This example shows how to set the **configure** command to privilege level 14 and define *SecretPswd14* as the password users must enter to use level 14 commands:

```
AP(config)# privilege exec level 14 configure
AP(config)# enable password level 14 SecretPswd14
```

Logging Into and Exiting a Privilege Level

Beginning in privileged EXEC mode, follow these steps to log in to a specified privilege level and to exit to a specified privilege level:

	Command	Purpose
Step 1	**enable** *level*	Log in to a specified privilege level. For *level*, the range is 0 to 15.
Step 2	**disable** *level*	Exit to a specified privilege level. For *level*, the range is 0 to 15.

Configuring Easy Setup

You can now configure a network and radio in a single screen using the Easy Setup.

Network Configuration

To configure an access point using the network configuration, enter the values for the following fields:

- Hostname
- Server protocol (DHCP / Static)
- IP Address
- IP Subnet
- Default Gateway
- IPv6 Protocol (DHCP / Autoconfig / Static IP)
- IPV6 address
- Username
- Password
- SNMP Community
- Current SSID list (list SSIDs configured to the access point)

Radio Configuration

To configure an access point using Radio Configuration, configure the following fields:

- SSID—a 32 byte string.
- Broadcast SSID in beacon
- Security
- Role in Radio Network
  - Access point—Root device. This setting can be applied to any access point.
  - Repeater—Nonroot device. This setting also can be applied to any access point.
  - Root Bridge—This setting can be applied to any access point.
  - Non-Root Bridge—This setting can be applied to any access point.
  - Workgroup Bridge—This setting can be applied to any access point.
  - Universal Workgroup Bridge
  - Scanner—Access point functions as a network monitoring device. It continuously scans and reports wireless traffic that it detects from other wireless devices on the wireless LAN in this mode. All access points can be configured as a scanner.

  - Spectrum—See Configuring Spectrum Expert Mode.
- Optimize Radio Network—You can either select preconfigured settings or customize the settings for the wireless device radio.
- Aironet Extensions—You can enable this setting only if there are Cisco Aironet wireless devices on your wireless LAN.
- Channel
- Power

Click **Factory Reset** to reset the access point to the factory settings. To reload the access point image, click **Reboot AP**.

Configuring Spectrum Expert Mode

The Spectrum Expert mode is supported in all CleanAir-enabled access points such as the AP3500, AP3600, AP2600, and AP1550 series. When configured as a dedicated Spectrum Sensor, a Spectrum Expert Connect autonomous access point can be connected to the Cisco Spectrum Expert. Spectrum Expert Mode is a separate mode and is not a subset of the Monitor Mode.

To enable the Spectrum Expert Mode, follow these steps:

Step 1 Click the **Spectrum Expert** icon.

Step 2 Choose **Network > Network Interface.**

Step 3 Click **Radio0-802.11n 2G.Hz** or **Radio0-802.11n 5G.Hz**

Step 4 Click **Enable**.

Step 5 Click the **Spectrum** radio button.

Step 6 Click **Apply**.

The Spectrum Expert mode is supported in all CleanAir-enabled access points such as the AP3500, AP3600, AP2600, and AP1550 series.

Configuring Spectrum Expert Connection

To configure the access point as a Spectrum Expert, use the following commands:

- AP(config)#**interface dot11Radio 0**
- AP(config-if)#**station-role spectrum**
- AP(config-if)# **no shutdown**
- AP# **show spectrum status**

Spectrum Expert is supported only on Internet Explorer. Before launching Spectrum Expert, change the following settings:

Step 1 Choose **Tools > Internet options > Security > custom level > ActiveX Controls & plug-ins > Initialize and script ActiveX controls not marked as safe for scripting**.

Step 2 Click the **Enable** radio button.

You can ignore the following popup message:

```
Your current security settings put computer at risk.
```

Controlling Access Point Access with RADIUS

This section describes how to control administrator access to the wireless device using Remote Authentication Dial-In User Service (RADIUS). For complete instructions on configuring the wireless device to support RADIUS, see Chapter 13, "Configuring RADIUS and TACACS+ Servers."

RADIUS provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS is facilitated through AAA and can be enabled only through AAA commands.

Note For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Security Command Reference for Release 12.3*.

These sections describe RADIUS configuration:

- Default RADIUS Configuration, page 5-12
- Configuring RADIUS Login Authentication, page 5-12 (required)
- Defining AAA Server Groups, page 5-14 (optional)
- Configuring RADIUS Authorization for User Privileged Access and Network Services, page 5-16 (optional)
- Displaying the RADIUS Configuration, page 5-17

Default RADIUS Configuration

RADIUS and AAA are disabled by default.

To prevent a lapse in security, you cannot configure RADIUS through a network management application. When enabled, RADIUS can authenticate users accessing the wireless device through the CLI.

Configuring RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.
Step 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	Create a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. • For *list-name*, specify a character string to name the list you are creating. • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: • **local**—Use the local username database for authentication. You must enter username information in the database. Use the **username** *password* global configuration command. • **radius**—Use RADIUS authentication. You must configure the RADIUS server before you can use this authentication method. For more information, see the "Identifying the RADIUS Server Host" section on page 13-5.
Step 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	**login authentication** {**default** | *list-name*}	Apply the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] global configuration command. To either disable RADIUS authentication for logins or to return to the default value, use the **no login authentication** {**default** | *list-name*} line configuration command.

Defining AAA Server Groups

You can configure the wireless device to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service (such as accounting), the second configured host entry acts as a fail-over backup to the first one.

You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.

	Command	Purpose
Step 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	Specify the IP address or host name of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout** *seconds*, specify the time interval that the wireless device waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting. If no timeout is set with the **radius-server host** command, the setting of the **radius-server timeout** command is used. • (Optional) For **retransmit** *retries*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the **radius-server host** command, the setting of the **radius-server retransmit** global configuration command is used. • (Optional) For **key** *string*, specify the authentication and encryption key used between the wireless device and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the wireless device to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The wireless device software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.
Step 4	**aaa group server radius** *group-name*	Define the AAA server-group with a group name. This command puts the wireless device in a server group configuration mode.
Step 5	**server** *ip-address*	Associate a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined in Step 2.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.
Step 9		Enable RADIUS login authentication. See the "Configuring RADIUS Login Authentication" section on page 5-12.

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* global configuration command. To remove a server group from the configuration list, use the **no aaa group server radius** *group-name* global configuration command. To remove the IP address of a RADIUS server, use the **no server** *ip-address* server group configuration command.

In this example, the wireless device is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over backup to the first entry.

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1812 acct-port 1813
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
AP(config)# aaa group server radius group1
AP(config-sg-radius)# server 172.20.0.1 auth-port 1812 acct-port 1813
AP(config-sg-radius)# exit
AP(config)# aaa group server radius group2
AP(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
AP(config-sg-radius)# exit
```

Configuring RADIUS Authorization for User Privileged Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the wireless device uses information retrieved from the user profile, which is in the local user database or on the security server, to configure the user session. The user is granted access to a requested service only if the information in the user profile allows it.

You can use the **aaa authorization** global configuration command with the **radius** keyword to set parameters that restrict a user network access to privileged EXEC mode.

The **aaa authorization exec group radius local** command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.

Note Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify RADIUS authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa authorization network group radius**	Configure the wireless device for user RADIUS authorization for all network-related service requests.
Step 3	**aaa authorization exec group radius**	Configure the wireless device for user RADIUS authorization to determine if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 4	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Displaying the RADIUS Configuration

To display the RADIUS configuration, use the **show running-config** privileged EXEC command.

Controlling Access Point Access with TACACS+

This section describes how to control administrator access to the wireless device using Terminal Access Controller Access Control System Plus (TACACS+). For complete instructions on configuring the wireless device to support TACACS+, see Chapter 13, "Configuring RADIUS and TACACS+ Servers."

TACACS+ provides detailed accounting information and flexible administrative control over authentication and authorization processes. TACACS+ is facilitated through AAA and can be enabled only through AAA commands.

Note For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Security Command Reference*.

These sections describe TACACS+ configuration:

- Default TACACS+ Configuration, page 5-17
- Configuring TACACS+ Login Authentication, page 5-17
- Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, page 5-19
- Displaying the TACACS+ Configuration, page 5-19

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application.When enabled, TACACS+ can authenticate administrators accessing the wireless device through the CLI.

Configuring TACACS+ Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.
Step 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	Create a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. • For *list-name*, specify a character string to name the list you are creating. • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: • **local**—Use the local username database for authentication. You must enter username information into the database. Use the **username** *password* global configuration command. • **tacacs+**—Use TACACS+ authentication. You must configure the TACACS+ server before you can use this authentication method.
Step 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	**login authentication** {**default** | *list-name*}	Apply the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] global configuration command. To either disable TACACS+ authentication for logins or to return to the default value, use the **no login authentication** {**default** | *list-name*} line configuration command.

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the wireless device uses information retrieved from the user profile, which is located either in the local user database or on the security server, to configure the user session. The user is granted access to a requested service only if the information in the user profile allows it.

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict a user network access to privileged EXEC mode.

The **aaa authorization exec group tacacs+ local** command sets these authorization parameters:

- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.

Note Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa authorization network group tacacs+**	Configure the wireless device for user TACACS+ authorization for all network-related service requests.
Step 3	**aaa authorization exec group tacacs+**	Configure the wireless device for user TACACS+ authorization to determine if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Displaying the TACACS+ Configuration

To display TACACS+ server statistics, use the **show tacacs** privileged EXEC command.

Configuring Ethernet Speed and Duplex Settings

You can assign the wireless device Ethernet port speed and duplex settings. We recommend that you use **auto**, the default setting, for both the speed and duplex settings on the wireless device Ethernet port. When the wireless device receives inline power from a switch, any change in the speed or duplex settings that resets the Ethernet link reboots the wireless device. If the switch port to which the wireless device is connected is not set to **auto**, you can change the wireless device port to **half** or **full** to correct a duplex mismatch and the Ethernet link is not reset. However, if you change from **half** or **full** back to **auto**, the link is reset and, if the wireless device receives inline power from a switch, the wireless device reboots.

Note The speed and duplex settings on the wireless device Ethernet port must match the Ethernet settings on the port to which the wireless device is connected. If you change the settings on the port to which the wireless device is connected, change the settings on the wireless device Ethernet port to match.

The Ethernet speed and duplex are set to **auto** by default. Beginning in privileged EXEC mode, follow these steps to configure Ethernet speed and duplex:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface gigabitethernet0**	Enter configuration interface mode.
Step 3	**speed** {**10** | **100** | **1000** | **auto**}	Configure the Ethernet speed. We recommend that you use **auto**, the default setting.
Step 4	**duplex** {**auto** | **full** | **half**}	Configure the duplex setting. We recommend that you use **auto**, the default setting.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configuring the Access Point for Wireless Network Management

You can enable the wireless device for wireless network management. The wireless network manager (WNM) manages the devices on your wireless LAN.

Enter this command to configure the wireless device to interact with the WNM:

```
AP(config)# wlccp wnm ip address ip-address
```

Enter this command to check the authentication status between the WDS access point and the WNM:

```
AP# show wlccp wnm status
```

Possible statuses are *not authenticated*, *authentication in progress*, *authentication fail*, *authenticated*, and *security keys setup*.

Configuring the Access Point for Local Authentication and Authorization

You can configure AAA to operate without a server by configuring the wireless device to implement AAA in local mode. The wireless device then handles authentication and authorization. No accounting is available in this configuration.

Note You can configure the wireless device as a local authenticator for 802.1x-enabled client devices to provide a backup for your main server or to provide authentication service on a network without a RADIUS server. See Chapter 9, "Configuring an Access Point as a Local Authenticator," for detailed instructions on configuring the wireless device as a local authenticator.

Beginning in privileged EXEC mode, follow these steps to configure the wireless device for local AAA:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.
Step 3	**aaa authentication login default local**	Set the login authentication to use the local username database. The **default** keyword applies the local user database authentication to all interfaces.
Step 4	**aaa authorization exec default local**	Configure user AAA authorization to determine if the user is allowed to run an EXEC shell by checking the local database.
Step 5	**aaa authorization network default local**	Configure user AAA authorization for all network-related service requests.
Step 6	**username** *name* [**privilege** *level*] {**password** *encryption-type password*}	Enter the local database, and establish a username-based authentication system. Repeat this command for each user. • For *name*, specify the user ID as one word. Spaces and quotation marks are not allowed. • (Optional) For *level*, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access. • For *encryption-type*, enter **0** to specify that an unencrypted password follows. Enter **7** to specify that a hidden password follows. • For *password*, specify the password the user must enter to gain access to the wireless device. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command. **Note** Characters TAB, ?, $, +, and [are invalid characters for passwords.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show running-config**	Verify your entries.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Configuring the Authentication Cache and Profile

The authentication cache and profile feature allows the access point to cache the authentication/authorization responses for a user so that subsequent authentication/authorization requests do not need to be sent to the AAA server.

Note On the access point, this feature is only supported for Admin authentication.

The following commands that support this feature are included in Cisco IOS Release 12.3(7):

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```

Note See the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for information about these commands.

The following is a configuration example from an access point configured for Admin authentication using TACACS+ with the auth cache enabled. While this example is based on a TACACS server, the access point could be configured for Admin authentication using RADIUS:

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
!
username Cisco password 7 123A0C041104
username admin privilege 15 password 7 01030717481C091D25
ip subnet-zero
!
!
aaa new-model
!
!
aaa group server radius rad_eap
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_acct
server 192.168.134.229 auth-port 1645 acct-port 1646
!
aaa group server radius rad_admin
server 192.168.134.229 auth-port 1645 acct-port 1646
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
```

```
!
aaa group server tacacs+ tac_admin
server 192.168.133.231
cache expiry 1
cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default local cache tac_admin group tac_admin
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local cache tac_admin group tac_admin
aaa accounting network acct_methods start-stop group rad_acct
aaa cache profile admin_cache
all
!
aaa session-id common
!
!
!
bridge irb
!
!
interface Dot11Radio0
no ip address
no ip route-cache
shutdown
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio1
no ip address
no ip route-cache
shutdown
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
station-role root
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface BVI1
ip address 192.168.133.207 255.255.255.0
no ip route-cache
```

```
!
ip http server
ip http authentication aaa
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
tacacs-server host 192.168.133.231 key 7 105E080A16001D1908
tacacs-server directed-request
radius-server attribute 32 include-in-access-req format %h
radius-server host 192.168.134.229 auth-port 1645 acct-port 1646 key 7 111918160405041E00
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
transport preferred all
transport output all
line vty 0 4
transport preferred all
transport input all
transport output all
line vty 5 15
transport preferred all
transport input all
transport output all
!
end
```

Configuring the Access Point to Provide DHCP Service

These sections describe how to configure the wireless device to act as a DHCP server:

- Setting up the DHCP Server, page 5-24
- Monitoring and Maintaining the DHCP Server Access Point, page 5-26

Setting up the DHCP Server

By default, access points are configured to receive IP settings from a DHCP server on your network. You can also configure an access point to act as a DHCP server to assign IP settings to devices on both your wired and wireless LANs.

Note When you configure the access point as a DHCP server, it assigns IP addresses to devices on its subnet. The devices communicate with other devices on the subnet but not beyond it. If data needs to be passed beyond the subnet, you must assign a default router. The IP address of the default router should be on the same subnet as the access point configured as the DHCP server.

For detailed information on DHCP-related commands and options, refer to the Configuring DHCP chapter in the *Cisco IOS IP Configuration Guide, Release 12.3*. Click this URL to browse to the "Configuring DHCP" chapter:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm

Beginning in privileged EXEC mode, follow these steps to configure an access point to provide DHCP service and specify a default router:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip dhcp excluded-address** *low_address* [*high_address*]	Exclude the wireless device IP address from the range of addresses the wireless device assigns. Enter the IP address in four groups of characters, such as 10.91.6.158. the wireless device assumes that all IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients. You must specify the IP addresses that the DHCP Server should not assign to clients. (Optional) To enter a range of excluded addresses, enter the address at the low end of the range followed by the address at the high end of the range.
Step 3	**ip dhcp pool** *pool_name*	Create a name for the pool of IP addresses that the wireless device assigns in response to DHCP requests, and enter DHCP configuration mode.
Step 4	**network** *subnet_number* [*mask* | *prefix-length*]	Assign the subnet number for the address pool. The wireless device assigns IP addresses within this subnet. (Optional) Assign a subnet mask for the address pool, or specify the number of bits that comprise the address prefix. The prefix is an alternative way of assigning the network mask. The prefix length must be preceded by a forward slash (/).
Step 5	**lease** { *days* [*hours*] [*minutes*] | **infinite** }	Configure the duration of the lease for IP addresses assigned by the wireless device. • days—configure the lease duration in number of days • (optional) hours—configure the lease duration in number of hours • (optional) minutes—configure the lease duration in number of minutes • infinite—set the lease duration to infinite
Step 6	**default-router** *address* [*address2 ... address 8*]	Specify the IP address of the default router for DHCP clients on the subnet. One IP address is required; however, you can specify up to eight addresses in one command line.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show running-config**	Verify your entries.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of these commands to return to default settings.

This example shows how to configure the wireless device as a DHCP server, exclude a range of IP address, and assign a default router:

```
AP# configure terminal
AP(config)# ip dhcp excluded-address 172.16.1.1 172.16.1.20
AP(config)# ip dhcp pool wishbone
AP(dhcp-config)# network 172.16.1.0 255.255.255.0
AP(dhcp-config)# lease 10
AP(dhcp-config)# default-router 172.16.1.1
AP(dhcp-config)# end
```

Monitoring and Maintaining the DHCP Server Access Point

These sections describe commands you can use to monitor and maintain the DHCP server access point:

- Show Commands, page 5-26
- Clear Commands, page 5-26
- Debug Command, page 5-27

Show Commands

In Exec mode, enter the commands in Table 5-2 to display information about the wireless device as DHCP server.

Table 5-2 Show Commands for DHCP Server

Command	Purpose
show ip dhcp conflict [*address*]	Displays a list of all address conflicts recorded by a specific DHCP Server. Enter the wireless device IP address to show conflicts recorded by the wireless device.
show ip dhcp database [*url*]	Displays recent activity on the DHCP database. **Note** Use this command in privileged EXEC mode.
show ip dhcp server statistics	Displays count information about server statistics and messages sent and received.

Clear Commands

In privileged Exec mode, use the commands in Table 5-3 to clear DHCP server variables.

Table 5-3 Clear Commands for DHCP Server

Command	Purpose
clear ip dhcp binding { *address* | * }	Deletes an automatic address binding from the DHCP database. Specifying the address argument clears the automatic binding for a specific (client) IP address. Specifying an asterisk (*) clears all automatic bindings.
clear ip dhcp conflict { *address* | * }	Clears an address conflict from the DHCP database. Specifying the address argument clears the conflict for a specific IP address. Specifying an asterisk (*) clears conflicts for all addresses.
clear ip dhcp server statistics	Resets all DHCP Server counters to 0.

Debug Command

To enable DHCP server debugging, use this command in privileged EXEC mode:

debug ip dhcp server { **events** | **packets** | **linkage** }

Use the **no** form of the command to disable debugging for the wireless device DHCP server.

Configuring the Access Point for Secure Shell

This section describes how to configure the Secure Shell (SSH) feature.

Note For complete syntax and usage information for the commands used in this section, refer to the "Secure Shell Commands" section in the *Cisco IOS Security Command Reference for Release 12.3*.

Understanding SSH

SSH is a protocol that provides a secure, remote connection to a Layer 2 or a Layer 3 device. There are two versions of SSH: SSH Version 1 and SSH Version 2. This software release supports both SSH versions. If you do not specify the version number, the access point defaults to Version 2.

SSH provides more security for remote connections than Telnet by providing strong encryption when a device is authenticated. The SSH feature has an SSH server and an SSH integrated client. The client supports these user authentication methods:

- RADIUS (for more information, see the "Controlling Access Point Access with RADIUS" section on page 5-12)
- Local authentication and authorization (for more information, see the "Configuring the Access Point for Local Authentication and Authorization" section on page 5-21)

For more information about SSH, see the *Secure Shell Configuration Guide* at the following URL:
http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/12-4t/secuser-12-4t-library.html

Note The SSH feature in this software release does not support IP Security (IPsec).

Configuring SSH

Before configuring SSH, download the crypto software image from Cisco.com. For more information, refer to the release notes for this release.

For information about configuring SSH and displaying SSH settings, see the *Secure Shell Configuration Guide* at the following URL:
http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/12-4t/secuser-12-4t-library.html

Support for Secure Copy Protocol

The Secure Copy Protocol (SCP) supports file transfers between hosts on a network using Secure Shell (SSH) for security. Cisco IOS Release 15.2(2)JB supports SCP file transfers to and from an access point while you are logged into the access point itself.

AAA authentication is used to restrict the transfer of data. SCP enables AAA authorization to ascertain your username and password to ensure the authenticity and confidentiality of the data in transit.

To configure SSH, use the following commands:

- **ip hostname**
- **ip domain-name**
- **crypto key generate rsa (512, 1024,2048)**
- **ip SSH version**
- **aaa new-model**
- **aaa authentication login default local**
- **aaa authorization exec default local**
- **username cisco privilege 15 password 0 cisco**

To perform SCP, use the **copy run scp://url** command.

Configuring Client ARP Caching

You can configure the wireless device to maintain an ARP cache for associated client devices. Maintaining an ARP cache on the wireless device reduces the traffic load on your wireless LAN. ARP caching is disabled by default.

This section contains this information:

- Understanding Client ARP Caching, page 5-28
- Configuring ARP Caching, page 5-29

Understanding Client ARP Caching

ARP caching on the wireless device reduces the traffic on your wireless LAN by stopping ARP requests for client devices at the wireless device. Instead of forwarding ARP requests to client devices, the wireless device responds to requests on behalf of associated client devices.

When ARP caching is disabled, the wireless device forwards all ARP requests through the radio port to associated clients, and the client to which the ARP request is directed responds. When ARP caching is enabled, the wireless device responds to ARP requests for associated clients and does not forward requests to clients. When the wireless device receives an ARP request for an IP address not in the cache, the wireless device drops the request and does not forward it. In its beacon, the wireless device includes an information element to alert client devices that they can safely ignore broadcast messages to increase battery life.

Optional ARP Caching

When a non-Cisco client device is associated to an access point and is not passing data, the wireless device might not know the client IP address. If this situation occurs frequently on your wireless LAN, you can enable optional ARP caching. When ARP caching is optional, the wireless device responds on behalf of clients with IP addresses known to the wireless device but forwards out its radio port any ARP requests addressed to unknown clients. When the wireless device learns the IP addresses for all associated clients, it drops ARP requests not directed to its associated clients.

Configuring ARP Caching

Beginning in privileged EXEC mode, follow these steps to configure the wireless device to maintain an ARP cache for associated clients:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 arp-cache** [**optional**]	Enable ARP caching on the wireless device. • (Optional) Use the **optional** keyword to enable ARP caching only for the client devices whose IP addresses are known to the wireless device.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure ARP caching on an access point:

```
AP# configure terminal
AP(config)# dot11 arp-cache
AP(config)# end
```

Managing the System Time and Date

You can manage the system time and date on the wireless device automatically, using the Simple Network Time Protocol (SNTP), or manually, by setting the time and date on the wireless device.

Note For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.3*.

This section contains this configuration information:

- Understanding Simple Network Time Protocol, page 5-30
- Configuring SNTP, page 5-30
- Configuring Time and Date Manually, page 5-30

Understanding Simple Network Time Protocol

Simple Network Time Protocol (SNTP) is a simplified, client-only version of NTP. SNTP can only receive the time from NTP servers; it cannot be used to provide time services to other systems. SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP.

You can configure SNTP to request and accept packets from configured servers or to accept NTP broadcast packets from any source. When multiple sources are sending NTP packets, the server with the best stratum is selected. Click this URL for more information on NTP and strata:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800ca66f.html#1001131

If multiple servers are at the same stratum, a configured server is preferred over a broadcast server. If multiple servers pass both tests, the first one to send a time packet is selected. SNTP will only choose a new server if it stops receiving packets from the currently selected server, or if a better server (according to the above criteria) is discovered.

Configuring SNTP

SNTP is disabled by default. To enable SNTP on the access point, use one or both the commands listed in Table 5-4 in the global configuration mode.

Table 5-4 SNTP Commands

Command	Purpose
sntp server {*address* | *hostname*} [**version** *number*]	Configures SNTP to request NTP packets from an NTP server.
sntp broadcast client	Configures SNTP to accept NTP packets from any NTP broadcast server.

Enter the **sntp server** command once for each NTP server. The NTP servers must be configured to respond to the SNTP messages from the access point.

If you enter both the **sntp server** command and the **sntp broadcast client** command, the access point will accept time from a broadcast server but prefers time from a configured server, assuming the strata are equal. To display information about SNTP, use the **show sntp** EXEC command.

Configuring Time and Date Manually

If no other source of time is available, you can manually configure the time and date after the system is restarted. The time remains accurate until the next system restart. We recommend that you use manual configuration only as a last resort. If you have an outside source to which the wireless device can synchronize, you do not need to manually set the system clock.

This section contains this configuration information:

- Setting the System Clock, page 5-31
- Displaying the Time and Date Configuration, page 5-32

- Configuring the Time Zone, page 5-32
- Configuring Summer Time (Daylight Saving Time), page 5-33

Setting the System Clock

If you have an outside source on the network that provides time services, such as an NTP server, you do not need to manually set the system clock.

Beginning in privileged EXEC mode, follow these steps to set the system clock:

	Command	Purpose
Step 1	**clock set** *hh***:***mm***:***ss day month year* or **clock set** *hh***:***mm***:***ss month day year*	Manually set the system clock using one of these formats: • For *hh***:***mm***:***ss*, specify the time in hours (24-hour format), minutes, and seconds. The time specified is relative to the configured time zone. • For *day*, specify the day by date in the month. • For *month*, specify the month by name. • For *year*, specify the year (no abbreviation).
Step 2	**show running-config**	Verify your entries.
Step 3	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to manually set the system clock to 1:32 p.m. on July 23, 2001:

```
AP# clock set 13:32:00 23 July 2001
```

Displaying the Time and Date Configuration

To display the time and date configuration, use the **show clock** [**detail**] privileged EXEC command.

The system clock keeps an *authoritative* flag that shows whether the time is authoritative (believed to be accurate). If the system clock has been set by a timing source such as NTP, the flag is set. If the time is not authoritative, it is used only for display purposes. Until the clock is authoritative and the *authoritative* flag is set, the flag prevents peers from synchronizing to the clock when the peers' time is invalid.

The symbol that precedes the **show clock** display has this meaning:

- *—Time is not authoritative.
- (blank)—Time is authoritative.
- .—Time is authoritative, but NTP is not synchronized.

Configuring the Time Zone

Beginning in privileged EXEC mode, follow these steps to manually configure the time zone:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**clock timezone** *zone hours-offset* [*minutes-offset*]	Set the time zone. the wireless device keeps internal time in universal time coordinated (UTC), so this command is used only for display purposes and when the time is manually set. • For *zone*, enter the name of the time zone to be displayed when standard time is in effect. The default is UTC. • For *hours-offset*, enter the hours offset from UTC. • (Optional) For *minutes-offset*, enter the minutes offset from UTC.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The *minutes-offset* variable in the **clock timezone** global configuration command is available for those cases where a local time zone is a percentage of an hour different from UTC. For example, the time zone for some sections of Atlantic Canada (AST) is UTC-3.5, where the 3 means 3 hours and .5 means 50 percent. In this case, the necessary command is **clock timezone AST -3 30**.

To set the time to UTC, use the **no clock timezone** global configuration command.

Configuring Summer Time (Daylight Saving Time)

Beginning in privileged EXEC mode, follow these steps to configure summer time (daylight saving time) in areas where it starts and ends on a particular day of the week each year:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**clock summer-time** *zone* **recurring** [*week day month hh***:***mm week day month hh***:***mm* [*offset*]]	Configure summer time to start and end on the specified days every year. Summer time is disabled by default. If you specify **clock summer-time** *zone* **recurring** without parameters, the summer time rules default to the United States rules. • For *zone*, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect. • (Optional) For *week*, specify the week of the month (1 to 5 or **last**). • (Optional) For *day*, specify the day of the week (Sunday, Monday...). • (Optional) For *month*, specify the month (January, February...). • (Optional) For *hh***:***mm*, specify the time (24-hour format) in hours and minutes. • (Optional) For *offset*, specify the number of minutes to add during summer time. The default is 60.
Step 3	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The first part of the **clock summer-time** global configuration command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

This example shows how to specify that summer time starts on the first Sunday in April at 02:00 and ends on the last Sunday in October at 02:00:

```
AP(config)# clock summer-time PDT recurring 1 Sunday April 2:00 last Sunday October 2:00
```

Beginning in privileged EXEC mode, follow these steps if summer time in your area does not follow a recurring pattern (configure the exact date and time of the next summer time events):

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**clock summer-time** *zone* **date** [*month date year hh***:***mm month date year hh***:***mm* [*offset*]] or **clock summer-time** *zone* **date** [*date month year hh***:***mm date month year hh***:***mm* [*offset*]]	Configure summer time to start on the first date and end on the second date. Summer time is disabled by default. • For *zone*, specify the name of the time zone (for example, PDT) to be displayed when summer time is in effect. • (Optional) For *week*, specify the week of the month (1 to 5 or **last**). • (Optional) For *day*, specify the day of the week (Sunday, Monday...). • (Optional) For *month*, specify the month (January, February...). • (Optional) For *hh***:***mm*, specify the time (24-hour format) in hours and minutes. • (Optional) For *offset*, specify the number of minutes to add during summer time. The default is 60.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The first part of the **clock summer-time** global configuration command specifies when summer time begins, and the second part specifies when it ends. All times are relative to the local time zone. The start time is relative to standard time. The end time is relative to summer time. If the starting month is after the ending month, the system assumes that you are in the southern hemisphere.

To disable summer time, use the **no clock summer-time** global configuration command.

This example shows how to set summer time to start on October 12, 2013, at 02:00, and end on April 26, 2014, at 02:00:

```
AP(config)# clock summer-time pdt date 12 October 2013 2:00 26 April 2014 2:00
```

Defining HTTP Access

By default, 80 is used for HTTP access, and port 443 is used for HTTPS access. These values can be customized by the user. Follow these steps to define the HTTP access via the GUI.

Step 1 From the access point GUI, click **Services > HTTP**. The Service: HTTP-Web server window appears.

Step 2 On this window, enter the desired HTTP and HTTPS port number. If not values are entered in the port number fields, the default values are used.

Step 3 Click **Apply**.

Follow these steps to define the HTTP access via the CLI.

Step 1 AP(config)# **conf t**

Step 2 AP(config)# **ip http port** *value*

Step 3 AP(config)# **ip http secure-port** *value*

Configuring a System Name and Prompt

You configure the system name on the wireless device to identify it. By default, the system name and prompt are *ap*.

If you have not configured a system prompt, the first 20 characters of the system name are used as the system prompt. A greater-than symbol (>) is appended. The prompt is updated whenever the system name changes, unless you manually configure the prompt by using the **prompt** global configuration command.

Note For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Configuration Fundamentals Command Reference* and the *Cisco IOS IP and IP Routing Command Reference* guides.

This section contains this configuration information:

- Default System Name and Prompt Configuration, page 5-35
- Configuring a System Name, page 5-36
- Understanding DNS, page 5-36

Default System Name and Prompt Configuration

The default access point system name and prompt is *ap*.

Configuring a System Name

Beginning in privileged EXEC mode, follow these steps to manually configure a system name:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**hostname** *name*	Manually configure a system name. The default setting is *ap*. **Note** When you change the system name, the wireless device radios reset, and associated client devices disassociate and quickly reassociate. **Note** You can enter up to 63 characters for the system name. However, when the wireless device identifies itself to client devices, it uses only the first 15 characters in the system name. If it is important for client users to distinguish between access points, make sure a unique portion of the system name appears in the first 15 characters.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

When you set the system name, it is also used as the system prompt.

To return to the default host name, use the **no hostname** global configuration command.

Understanding DNS

The DNS protocol controls the Domain Name System (DNS), a distributed database with which you can map host names to IP addresses. When you configure DNS on the wireless device, you can substitute the host name for the IP address with all IP commands, such as **ping**, **telnet**, **connect**, and related Telnet support operations.

IP defines a hierarchical naming scheme that allows a device to be identified by its location or domain. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco Systems is a commercial organization that IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, such as the File Transfer Protocol (FTP) system, is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a domain name server, which holds a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the host names, specify the name server that is present on your network, and enable the DNS.

This section contains this configuration information:

- Default DNS Configuration, page 5-37
- Setting Up DNS, page 5-37
- Displaying the DNS Configuration, page 5-38

Default DNS Configuration

Table 5-5 shows the default DNS configuration.

Table 5-5 Default DNS Configuration

Feature	Default Setting
DNS enable state	Disabled.
DNS default domain name	None configured.
DNS servers	No name server addresses are configured.

Setting Up DNS

Beginning in privileged EXEC mode, follow these steps to set up the wireless device to use the DNS:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip domain-name** *name*	Define a default domain name that the software uses to complete unqualified host names (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. At boot time, no domain name is configured; however, if the wireless device configuration comes from a BOOTP or Dynamic Host Configuration Protocol (DHCP) server, then the default domain name might be set by the BOOTP or DHCP server (if the servers were configured with this information).
Step 3	**ip name-server** *server-address1* [*server-address2 ... server-address6*]	Specify the address of one or more name servers to use for name and address resolution. You can specify up to six name servers. Separate each server address with a space. The first server specified is the primary server. The wireless device sends DNS queries to the primary server first. If that query fails, the backup servers are queried.
Step 4	**ip domain-lookup**	(Optional) Enable DNS-based host name-to-address translation on the wireless device. This feature is enabled by default. If your network devices require connectivity with devices in networks for which you do not control name assignment, you can dynamically assign device names that uniquely identify your devices by using the global Internet naming scheme (DNS).
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

If you use the wireless device IP address as its host name, the IP address is used and no DNS query occurs. If you configure a host name that contains no periods (.), a period followed by the default domain name is appended to the host name before the DNS query is made to map the name to an IP address. The default domain name is the value set by the **ip domain-name** global configuration command. If there is a period (.) in the host name, Cisco IOS software looks up the IP address without appending any default domain name to the host name.

To remove a domain name, use the **no ip domain-name** *name* global configuration command. To remove a name server address, use the **no ip name-server** *server-address* global configuration command. To disable DNS on the wireless device, use the **no ip domain-lookup** global configuration command.

Displaying the DNS Configuration

To display the DNS configuration information, use the **show running-config** privileged EXEC command.

Note When DNS is configured on the wireless device, the **show running-config** command sometimes displays a server IP address instead of its name.

Creating a Banner

You can configure a message-of-the-day (MOTD) and a login banner. The MOTD banner appears on all connected terminals at login and is useful for sending messages that affect all network users (such as impending system shutdowns).

The login banner also appears on all connected terminals. It appears after the MOTD banner and before the login prompts.

Note For complete syntax and usage information for the commands used in this section, refer to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.3*.

This section contains this configuration information:

- Default Banner Configuration, page 5-38
- Configuring a Message-of-the-Day Login Banner, page 5-38
- Configuring a Login Banner, page 5-40

Default Banner Configuration

The MOTD and login banners are not configured.

Configuring a Message-of-the-Day Login Banner

You can create a single or multiline message banner that appears on the screen when someone logs into the wireless device.

Beginning in privileged EXEC mode, follow these steps to configure a MOTD login banner:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**banner motd** *c message c*	Specify the message of the day. For *c*, enter the delimiting character of your choice, such as a pound sign (#), and press the **Return** key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded. For *message*, enter a banner message up to 255 characters. You cannot use the delimiting character in the message.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To delete the MOTD banner, use the **no banner motd** global configuration command.

This example shows how to configure a MOTD banner for the wireless device using the pound sign (#) symbol as the beginning and ending delimiter:

```
AP(config)# banner motd #
This is a secure site. Only authorized users are allowed.
For access, contact technical support.
#
AP(config)#
```

This example shows the banner displayed from the previous configuration:

```
Unix> telnet 172.2.5.4
Trying 172.2.5.4...
Connected to 172.2.5.4.
Escape character is '^]'.

This is a secure site. Only authorized users are allowed.
For access, contact technical support.

User Access Verification

Password:
```

Configuring a Login Banner

You can configure a login banner to appear on all connected terminals. This banner appears after the MOTD banner and before the login prompt.

Beginning in privileged EXEC mode, follow these steps to configure a login banner:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**banner login** *c message c*	Specify the login message. For *c*, enter the delimiting character of your choice, such as a pound sign (#), and press the **Return** key. The delimiting character signifies the beginning and end of the banner text. Characters after the ending delimiter are discarded. For *message*, enter a login message up to 255 characters. You cannot use the delimiting character in the message.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To delete the login banner, use the **no banner login** global configuration command.

This example shows how to configure a login banner for the wireless device using the dollar sign ($) symbol as the beginning and ending delimiter:

```
AP(config)# banner login $
Access for authorized users only. Please enter your username and password.
$
AP(config)#
```

Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode

Note For information on only upgrading the Cisco IOS image on an autonomous access point through the GUI or CLI, go to the following URL: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00809f0e94.shtml.

You can run a utility to upgrade autonomous Cisco Aironet access points to the lightweight mode so that they can communicate with wireless LAN controllers on your network. For more information about using the upgrade utility, see the *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* at the following URL:

http://www.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html

To convert autonomous access points to lightweight mode, telnet to the access point and run this command:

```
archive download-sw {/overwrite | /reload} tftp: //location/image-name
```

CHAPTER 6

Configuring Radio Settings

This chapter describes how to configure radio settings for the wireless device.

Enabling the Radio Interface

The wireless device radios are disabled by default.

Note Beginning with Cisco IOS Release 12.3(8)JA there is no SSID. You must create an SSID before you can enable the radio interface.

Beginning in privileged EXEC mode, follow these steps to enable the access point radio:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ssid** *ssid*	Enter the SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.
Step 3	**interface dot11radio** {**0** | **1***slot***/***port*}	Enter interface configuration mode for the radio interface. The 2.4-GHz and the 802.11n 2.4-GHz radio is radio 0 The 5-GHz and the 802.11n 5-GHz radio is radio 1.
Step 4	**ssid** *ssid*	Assign the SSID you created in Step 2 to the appropriate radio interface.
Step 5	**no shutdown**	Enable the radio port.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **shutdown** command to disable the radio port.

Configuring the Role in Radio Network

Table 6-1 shows the role in the radio network for each device.

Table 6-1 Device Role in Radio Network Configuration

Role in Radio Network	AP 1040	AP 1140	AP 1260	AP 1530	AP 1550	AP 1600	AP 1700	AP 2600	AP 3500	AP 3600	AP 3700	AP 700	AP 2700
Access point	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Access point (fallback to radio shutdown)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Access point (fallback to repeater)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Repeater	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Root bridge	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Non-root bridge	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Root bridge with wireless clients	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Non-root bridge with wireless clients	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Workgroup bridge	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Universal workgroup bridge[1]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Scanner	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Spectrum	–	–	–	–	Yes	–	Yes	Yes	Yes	Yes	Yes	–	Yes
Install [automatic | non-root | root]	–	–	–	Yes	–	–	–	–	–	–	–	–	–

[1] When configuring a universal workgroup bridge using AES-CCM TKIP, the non-root device should use only TKIP or AES-CCM TKIP as ciphers in order to associate to the root device. The non-root device will not associate with the root if it is configured only AES-CCM. This configuration results in a mismatch in the multicast cipher between the root and non-root devices.

You can configure the role of an access point or bridge in a radio network. You can also configure a fallback role for root access points. The wireless device automatically assumes the fallback role when its Ethernet port is disabled or disconnected from the wired LAN. There are two possible fallback roles:

- **Repeater**—When the Ethernet port is disabled, the wireless device becomes a repeater and associates to a nearby root access point. You do not have to specify a root access point to which the fallback repeater associates; the repeater automatically associates to the root access point that provides the best radio connectivity.
- **Shutdown**—the wireless device shuts down its radio and disassociates all client devices.

Note When configuring a universal workgroup bridge using AES-CCM TKIP, the non-root device should use only TKIP or AES-CCM TKIP as ciphers in order to associate to the root device. The non-root device will not associate with the root if it is configured only AES-CCM. This configuration results in a mismatch in the multicast cipher between the root and non-root devices.

Beginning in privileged EXEC mode, follow these steps to set the wireless device radio network role and fallback role:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface: 2.4-GHz radio and the 802.11n 2.4-Ghz radio is interface 0. 5-GHz radio and the 802.11n 5-GHz radio is interface 1.

	Command	Purpose

Step 3	**station-role**
	non-root {bridge | wireless-clients}
	repeater
	root {access-point | ap-only | bridge [wireless-clients] |fallback [repeater | shutdown]}
	scanner
	workgroup-bridge {**multicast | mode** <*client | infrastructure*>| **universal** <*Ethernet client MAC address*>}
		Set the wireless device role.
		• Set the role to non-root bridge with or without wireless clients, repeater access point, root access point or bridge, scanner, or workgroup bridge.
		• When in bridge mode, they are interoperable with outdoor access point/bridge only on supported bridge features.
		• The bridge mode radio supports point-to-point and point-to-multipoint configuration.
		• An outdoor access point/bridge operating as a non-root bridge can associate with another non-root bridge as long as the station role for the non-root bridge is set to **non-root wireless clients**.
		• The Ethernet port is shut down when any one of the radios is configured as a repeater. Only one radio per access point may be configured as a workgroup bridge or repeater.
		• The **dot11radio 0|1 antenna-alignment** command is available when the access point is configured as a repeater.
		• A workgroup bridge can have a maximum of 254 clients, presuming that no other wireless clients are associated to the root bridge or access point.
		• A universal workgroup bridge configures the access point in workgroup bridge mode and able to interoperate with non-Cisco access points. You must enter the Ethernet client MAC address. The workgroup bridge associates with the configured MAC address only if it is present in the bridge table and it should not be a static entry. If validation fails, the workgroup bridge associates with its BVI MAC address. Also, the universal workgroup bridge role supports only one wired client.
		• Spanning Tree Protocol (STP) is configurable on access points in bridge modes.
		• (Optional) Select the root access point fallback role. If the wireless device Ethernet port is disabled or disconnected from the wired LAN, the wireless device can either shut down its radio port or become a repeater access point associated to any nearby root access point.

Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note When you enable the role in the radio network as a non root bridge or a workgroup bridge and enable the interface using the **no shut** command, the physical status and the software status of the interface will be up only if the device on the other end access point or bridge is up. Otherwise, only the physical status of the device will be up. The software status of the device comes up only when the device on the other end is configured and up.

Universal Workgroup Bridge Mode

When configuring the universal workgroup bridge role, you must include the client MAC address. The workgroup bridge will associate with this MAC address only if it is present in the bridge table and is not a static entry. If validation fails, the workgroup bridge associates with its BVI MAC address. In universal workgroup bridge mode, the workgroup bridge uses the Ethernet client MAC address to associate with Cisco or non-Cisco root devices. The universal workgroup bridge is transparent and is not managed.

Note The universal workgroup bridge role supports only one wired client.

You can enable a recovery mechanism and make the workgroup bridge manageable again by disabling the Ethernet client, causing the universal workgroup bridge to associate with an access point using its own BVI address.

The roaming keyword has been added to the interface command **world-mode dot11d country-code** *country* [**indoor** | **outdoor** | **both**] to support the “airline flying between different countries” scenario. The keyword causes the workgroup bridge to do passive scanning once it is deathenticated from a root access point. See the “Enabling and Disabling World Mode” section on page 6-22 for more information on this command.

Point-to-point and Multi Point bridging support for 802.11n platforms

The point-to-point and point-to-multipoint bridging is supported on all 802.11n access points. The 5 GHz bands support 20- and 40-MHz and the 2.4-GHz bands support 20 MHz.

The following are supported on all 802.11n access points:

- MIMO, short-range bridging (on campus or inter-building bridge deployments), with dipole and MIMO antennas (line of sight and short range) under 1 Km.
- 20-MHz and 40-MHz 802.11n support.
- Workgroup bridge (WGB) short-range support.
- SISO (single-in, single-out), MCS 0-7 and legacy bridge rates (802.11 a/b/g and 802.11n) using one outdoor antenna.

Note The aforementioned support is only for short range links and is not a replacement for the AP 1400 or other Bridge products.

The following are not supported by AP models with internal antennas, in their bridging modes:

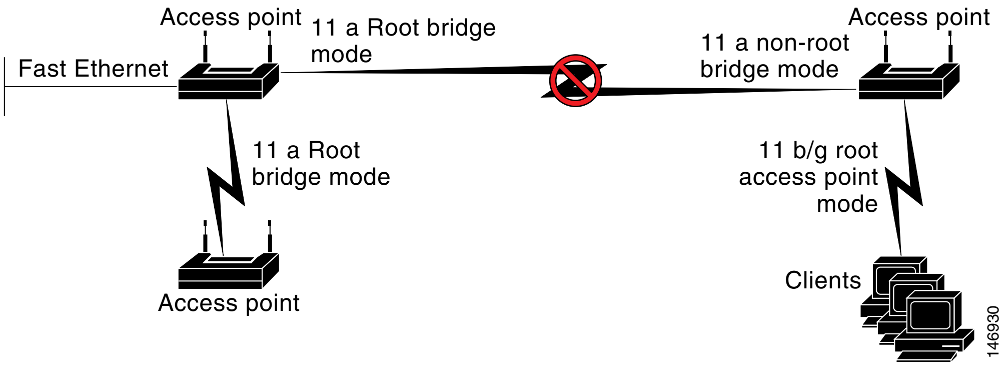
- The **distance** command. The **distance** command is supported only on access points that are approved for outdoor use.
- Outdoor MIMO bridging using external antennas.

Note In point-to-multipoint bridging, WGB is not recommended with the root bridge. WGB should be associated to the root AP in point-to-multipoint bridging setup.

Configuring Dual-Radio Fallback

The dual-radio fallback features allows you to configure access points so that if the non-root bridge link connecting the access point to the network infrastructure goes down, the root access point link through which a client connects to the access point shut down. Shutting down the root access point link causes the client to roam to another access point. Without this feature, the client remains connected to the access point, but will not be able to send or receive data from the network.

Figure 6-1 Dual-Radio Fallback



Note This feature is supported by all dual-radio access points.
This feature does not affect the fallback feature for single-radio access points.

You can configure dual-radio fallback in three ways:

- Radio tracking
- Fast Ethernet tracking
- MAC-address tracking

Radio Tracking

You can configure the access point to track or monitor the status of one of its radios. It the tracked radio goes down or is disabled, the access point shuts down the other radio. If the tracked radio comes up, the access point enables the other radio.

- To track radio 0, enter the following command on radio 1:

  ```
  # station-role root access-point fallback track d0 shutdown
  ```

- To track radio 1, enter the following command on radio 0:

  ```
  # station-role root access-point fallback track d1 shutdown
  ```

Fast Ethernet Tracking

You can configure the access point for fallback when its Ethernet port is disabled or disconnected from the wired LAN. You configure the access point for fast Ethernet tracking as described in the "Configuring the Role in Radio Network" section on page 6-3.

Note Fast Ethernet tracking does not support the Repeater mode.

- To configure non-802.11n access points for Fast Ethernet tracking, in the radio interfaces configuration mode enter the following command:

  ```
  # station-role root access-point fallback track fa 0
  ```

- To configure 802.11n access points for Gigabit Ethernet tracking, in the radio interfaces configuration mode enter the following command:

  ```
  # station-role root fallback shutdown
  ```

MAC-Address Tracking

You can configure the radio whose role is root access point to go up or down by tracking a non-root bridge or workgroup bridge, using its MAC address, on another radio. If the client disassociates from the access point, the root access point radio goes down. If the client reassociates to the access point, the root access point radio comes back up.

MAC-address tracking is most useful when the client is a non-root bridge access point connected to an upstream wired network.

For example, to track a a non-root bridge or workgroup bridge, having a MAC address 12:12:12:12:12:12, enter the following command:

```
# station-role root access-point fallback track mac-address 12:12:12:12:12:12 shutdown
```

Limiting Clients per Radio

You can set the number of clients allowed for association with an interface, using the command **max-client** *1-255*, under the dot11 radio interface configuration. This setting is disabled by default. The minimum number of clients allowed is 1 and the maximum is 255.

```
ap(config-if)# max-client 1-255
```

For setting this via the GUI:

Step 1 Go to **Network > Network Interfaces**.

Step 2 On the side menu, click Dot11 Radio 2.4 GHz or Dot11 Radio 5 GHZ depending on which radio interface you want to limit the clients.

Step 3 On the radio interface's settings page, you can either enable or disable the **Max-Client** option.

Step 4 If you enable the Max-Client option, then in the text box provided alongside the Max-Client option, specify the number of clients allowed for association with the interface.

Step 5 Click **Apply**.

Configuring Radio Data Rates

You use the data rate settings to choose the data rates the wireless device uses for data transmission. The rates are expressed in megabits per second. The wireless device attempts to transmit at the highest data rate set on the CLI or GUI interfaces. If there are obstacles or interference, the wireless device steps down to the next lower rate that allows data transmission. You can set each data rate to one of three states:

- Basic (the GUI labels Basic rates as Required)—Allows transmission at this rate for all packets, both unicast and multicast. At least one of the wireless device's data rates must be set to Basic.
- Enabled—The wireless device transmits only unicast packets at this rate; multicast packets are sent at one of the data rates set to Basic.
- Disabled—The wireless device does not transmit data at this rate.

Note At least one data rate must be set to **basic**.

You can use the Data Rate settings to set an access point to serve client devices operating at specific data rates. To set the 2.4-GHz, 802.11g radio to serve only 802.11g client devices, set any Orthogonal Frequency Division Multiplexing (OFDM) data rate (6, 9, 12, 18, 24, 36, 48, 54) to **Basic**.

You can configure the wireless device to set the data rates automatically to optimize either the range or the throughput. When you enter **range** for the data rate setting, the wireless device sets the 1 Mbps rate to basic and the other rates to **enabled**. The range setting allows the access point to extend the coverage area by compromising on the data rate. Therefore, if you have a client that is not able to connect to the access point while other clients can, one reason may be because the client is not within the coverage area of the access point. In such a case using the range option will help in extending the coverage area and the client may be able to connect to the access point. Typically the trade-off is between throughput and range. When the signal degrades (possibly due to distance from the access point,) the rates will renegotiate down in order to maintain the link (but at a lower data rate). Contrast that against a link configured for a higher throughput that will simply drop when the signal degrades enough to no longer sustain a configured high data rate, or roam to another access point with sufficient coverage, if one is available. The balance between the two (throughput vs. range) is one of those design decisions that has to be made based on resources available to the wireless project, type of traffic the users will be passing, service level desired, and as always, the quality of the RF environment.When you enter **throughput** for the data rate setting, the wireless device sets all data rates to **basic (**i.e. 12 rates for 2.4 Ghz and 8 rates for 5 GHz).

Note When a wireless network has a mixed environment of 802.11b clients and 802.11g clients, make sure that data rates 1, 2, 5.5, and 11 Mbps are set to required (**basic**) and that all other data rates are set to **enable**. The 802.11b adapters do not recognize the 802.11g rates and do not operate if data rates higher than 11Mbps are set to require on the connecting access point.

Access Points Send Multicast and Management Frames at Highest Basic Rate

Access points running recent Cisco IOS versions are transmitting multicast and management frames at the highest configured basic rate, and is a situation that could causes reliability problems.

Access points running LWAPP or autonomous IOS should transmit multicast and management frames at the lowest configured basic rate. This is necessary in order to provide for good coverage at the cell's edge, especially for unacknowledged multicast transmissions where multicast wireless transmissions may fail to be received.

Since multicast frames are not retransmitted at the MAC layer, stations at the edge of the cell may fail to receive them successfully. If reliable reception is a goal, then multicasts should be transmitted at a low data rate. If support for high data rate multicasts is required, then it may be useful to shrink the cell size and to disable all lower data rates.

Depending on your specific requirements, you can take the following action:

- If you need to transmit the multicast data with the greatest reliability and if there is no need for great multicast bandwidth, then configure a single basic rate, one that is low enough to reach the edges of the wireless cells.
- If you need to transmit the multicast data at a certain data rate in order to achieve a certain throughput, then configure that rate as the highest basic rate. You can also set a lower basic rate for coverage of non-multicast clients.

Beginning in privileged EXEC mode, follow these steps to configure the radio data rates:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1***slot*/*port*}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and 2.4-GHz N radio is radio 0, and the 5-GHz radio and 5-GHz N radios radio 1.

	Command	Purpose
Step 3	**speed** 802.11g, 2.4-GHz radio: {[**1.0**] [**2.0**] [**5.5**] [**6.0**] [**9.0**] [**11.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**basic-1.0**] [**basic-2.0**] [**basic-5.5**] [**basic-6.0**] [**basic-9.0**] [**basic-11.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] | **range** | **throughput** [**ofdm**] | **default** } 802.11a 5-GHz radio: {[**6.0**] [**9.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**basic-6.0**] [**basic-9.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] | **range** | **throughput** | **ofdm-throughput** | **default**} 802.11n 2.4-GHz radio: {[**1.0**] [**11.0**] [**12.0**] [**18.0**] [**2.0**] [**24.0**] [**36.0**] [**48.0**] [**5.5**] [**54.0**] [**6.0**] [**9.0**] [**basic-1.0**] [**basic-11.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-5.5**] [**basic-54.0**] [**basic-6.0**] [**basic-9.0**] [**default**] [**m0-7**] [**m0.**] [**m1.**] [**m10.**] [**m11.**] [**m12.**] [**m13.**] [**m14.**] [**m15.**] [**m2.**] [**m3.**] [**m4.**] [**m5.**] [**m6.**] [**m7.**] [**m8-15**] [**m8.**] [**m9.**] [**ofdm**] [**only-ofdm**] | **range** | **throughput**} 802.11n 5-GHz radio: {[**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**6.0**] [**9.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] [**basic-6.0**] [**basic-9.0**] [**default**] [**m0-7**] [**m0.**] [**m1.**] [**m10.**] [**m11.**] [**m12.**] [**m13.**] [**m14.**] [**m15.**] [**m2.**] [**m3.**] [**m4.**] [**m5.**] [**m6.**] [**m7.**] [**m8-15**] [**m8.**] [**m9.**] | **range** | **throughput**}	Set each data rate to **basic** or **enabled**, or enter **range** to optimize range or **throughput** to optimize throughput. • (Optional) Enter **basic-1.0**, **basic-2.0**, **basic-5.5**, **basic-6.0**, **basic-9.0**, **basic-11.0**, **basic-12.0**, **basic-18.0**, **basic-24.0**, **basic-36.0**, **basic-48.0**, and **basic-54.0** to set these data rates to **basic** on the 802.11g, 2.4-GHz radio. **Note** The client must support the basic rate that you select or it cannot associate to the wireless device. If you select 12 Mbps or higher for the basic data rate on the 802.11g radio, 802.11b client devices cannot associate to the wireless device 802.11g radio. Enter **basic-6.0**, **basic-9.0**, **basic-12.0**, **basic-18.0**, **basic-24.0**, **basic-36.0**, **basic-48.0**, and **basic-54.0** to set these data rates to **basic** on the 5-GHz radio. (Optional) Alternatively, enter **range** or **throughput** or **ofdm-throughput** (no ERP protection) to automatically optimize radio range or throughput. When you enter **range**, the wireless device sets the lowest data rate to basic and the other rates to **enabled**. When you enter **throughput**, the wireless device sets all data rates to **basic**. (Optional) On the 802.11g radio, enter **speed throughput ofdm** to set all OFDM rates (6, 9, 12, 18, 24, 36, and 48) to basic (required) and set all the CCK rates (1, 2, 5.5, and 11) to disabled. This setting disables 802.11b protection mechanisms and provides maximum throughput for 802.11g clients. However, it prevents 802.11b clients from associating to the access point. • (Optional) Enter **default** to set the data rates to factory default settings (not supported on 802.11b radios). On the 802.11g radio, the **default** option sets rates 1, 2, 5.5, and 11 to basic, and rates 6, 9, 12, 18, 24, 36, 48, and 54 to enabled. These rate settings allow both 802.11b and 802.11g client devices to associate to the wireless device 802.11g radio. On the 5-GHz radio, the **default** option sets rates 6.0, 12.0, and 24.0 to basic, and rates 9.0, 18.0, 36.0, 48.0, and 54.0 to enabled.

	Command	Purpose
	speed (continued)	On the 802.11n 2.4-GHz radio, the **default** option sets rates 1.0, 2.0, 5.5, and 11.0 to enabled. On the 802.11n 5-GHz radio, the **default** option sets rates to 6.0, 12.0, and 24.0 to enabled. The default MCS rate setting for both 802.11n radios is 0–15.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the **speed** command to remove one or more data rates from the configuration. This example shows how to remove data rates basic-2.0 and basic-5.5 from the configuration:

```
ap# configure terminal
ap(config)# interface dot11radio 0
ap(config-if)# no speed basic-2.0 basic-5.5
ap(config-if)# end
```

Configuring MCS Rates

Modulation Coding Scheme (MCS) is a specification of PHY parameters consisting of modulation order (BPSK, QPSK, 16-QAM, 64-QAM) and FEC code rate (1/2, 2/3, 3/4, 5/6). MCS is used in 802.11n radios, which define 32 symmetrical settings (8 per spatial stream):

- MCS 0–7
- MCS 8–15
- MCS 16–23
- MCS 24–31

MCS is an important setting because it provides for potentially greater throughput. High throughput data rates are a function of *MCS*, *bandwidth*, and *guard interval*. 802.11 a, b, and g radios use 20-MHz channel widths.

Tip For the latest information on the Data Rates based on MCS Index, Guard Interval (GI), and channel width, for you access point, refer to its *Cisco Aironet (AP series name) Series Access Points Data Sheet* on the Cisco.com site.

MCS rates are configured using the **speed** command. The following example shows a **speed** setting for an 802.11n 5-GHz radio:

```
interface Dot11Radio0
    no ip address
    no ip route-cache
    !
    ssid 1260test
    !
    speed basic-1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0 m0. m1. m2. m3. m4.
    m8. m9. m10. m11. m12. m13. m14. m15.
```

Enabling 11ac MCS rates

MCS rates are configured using the **speed** command.

To enable 11ac rates, it is mandatory to have at least one basic rate and one 11n rate enabled.

The following example shows a **speed** setting for an 802.11ac 5-GHz radio:

```
interface Dot11Radio1
!
!
ssid 11ac
!
speed 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0 m0. m1. m2. m3. m4. m5. m6. m7. m8. m9. m10.
m11. m12. m13. m14. m15. m16. m17. m18. m19. m20. m21. m22. m23. a1ss9 a2ss9 a3ss9
Channel width 80
```

Configuring Radio Transmit Power

Radio transmit power is based on the type of radio or radios installed in your access point and the regulatory domain in which it operates. To determine what transmit power is available for your access point and which regulatory domain it operates in, refer to the hardware installation guide for that device. hardware installation guides are available at cisco.com. Follow these steps to view and download them:

Step 1 Browse to http://www.cisco.com.

Step 2 Click **Technical Support & Documentation**. A small window appears containing a list of technical support links.

Step 3 Click **Technical Support & Documentation**. The Technical Support and Documentation page appears.

Step 4 In the Documentation & Tools section, choose **Wireless**. The Wireless Support Resources page appears.

Step 5 In the Wireless LAN Access section, choose the device you are working with. An introduction page for the device appears.

Step 6 In the Install and Upgrade section, choose **Install and Upgrade Guides**. The Install and Upgrade Guides page for the device appears.

Step 7 Choose the hardware installation guide for the device. The home page for the guide appears.

Step 8 In the left frame, click **Channels and Antenna Settings**.

Table 6-2 shows the relationship between mW and dBm.

Table 6-2 Translation between mW and dBm

dBm	-1	2	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
mW	1	2	3	4	5	6	8	10	12	15	20	25	30	40	50	60	80	100	125	150	200	250

Beginning in privileged EXEC mode, follow these steps to set the transmit power on access point radios:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1***slot*/*port*}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1. The 2.4-GHz 802.11n radio is 0, and the 5-GHz 802.11n radio is 1
Step 3	**power local** These options are available for the 802.11a, 5-GHz radio (in dBm), and for the 2.4-GHz 802.11n radio (in dBM): **{22 | 19 | 16 | 13 | 10 | 7 | 4}**	Set the transmit power for the 802.11b, 2.4-GHz radio or the 5-GHz radio to one of the power levels allowed in your regulatory domain. **Note** See the hardware installation guide for your access point to determine the power settings for your regulatory domain.
Step 4	**power local** These options are available for the 802.11g, 2.4-GHz radio: **power local cck** settings: { **-1** | **2** | **5** | **8** | **11** | **14** | **17** | **20** | **maximum** } **power local ofdm** settings: { **-1** | **2** | **5** | **8** | **11** | **14** | **17** |**maximum** } **Note** These options are not available on 802.11n APs.	Set the transmit power for the 802.11g, 2.4-GHz radio to one of the power levels allowed in your regulatory domain. Settings are in dBm. On the 2.4-GHz, 802.11g radio, you can set Orthogonal Frequency Division Multiplexing (OFDM) power levels and Complementary Code Keying (CCK) power levels. CCK modulation is supported by 802.11b and 802.11g devices. OFDM modulation is supported by 802.11g and 802.11a devices. **Note** See the hardware installation guide for your access point to determine the power settings for your regulatory domain. **Note** The 802.11g radio maximum transmission power level depends the AP model. See the AP data sheet for the power levels.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the power command to return the power setting to **maximum**, the default setting.

Limiting the Power Level for Associated Client Devices

You can also limit the power level on client devices that associate to the wireless device. When a client device associates to the wireless device, the wireless device sends the maximum power level setting to the client.

Note Cisco AVVID documentation uses the term Dynamic Power Control (DTPC) to refer to limiting the power level on associated client devices.

Beginning in privileged EXEC mode, follow these steps to specify a maximum allowed power setting on all client devices that associate to the wireless device:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1***slot/port*}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1. The 2.4-GHz 802.11n radio is 0, and the 5-GHz 802.11n radio is 1.
Step 3	**power client** These options are available for both 802.11n 2.4-GHz and 5-GHz clients (in dBm): {*-127 to 127* | **local** | **maximum**}	Set the power level allowed on client devices that associate to the wireless device. You can: • Set any power level value in dBm from -127 to 127 • Set the power level to **local**, to set the client power level to that of the access point. • Set the power level to **maximum**, to set the client power to the allowed maximum. **Note** The settings allowed in your regulatory domain might differ from the settings listed here.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the client power command to disable the maximum power level for associated clients.

Note Aironet extensions must be enabled to limit the power level on associated client devices. Aironet extensions are enabled by default.

Configuring Radio Channel Settings

The default channel setting for the wireless device radios is least congested; at startup, the wireless device scans for and selects the least-congested channel. For the most consistent performance after a site survey, however, we recommend that you assign a static channel setting for each access point. The channel settings on the wireless device correspond to the frequencies available in your regulatory domain. See the access point hardware installation guide for the frequencies allowed in your domain.

Note In places where RF interference might be causing clients to occasionally get disconnected from the wireless network, setting the wireless interface to run on a different channel, such as channel 1 (2412), might avoid the interference.

Each 2.4-GHz channel covers 22 MHz. The channels 1, 6, and 11 do not overlap, so you can set up multiple access points in the same vicinity without causing interference. Both 802.11b and 802.11g 2.4-GHz radios use the same channels and frequencies.

The 5-GHz radio operates on 9 channels from 5180 to 55825 MHz on 802.11n APs, and on 8 channels from 5180 to 5805 on 1140 series APs. Each channel covers 20 MHz, and the bandwidth for the channels overlaps slightly. For best performance, use channels that are not adjacent (44 and 46, for example) for radios that are close to each other.

Note Too many access points in the same vicinity creates radio congestion that can reduce throughput. A careful site survey can determine the best placement of access points for maximum radio coverage and throughput.

Because they change frequently, channel settings are not included in this document. For up-to-date information on channel settings for your access point or bridge, see the *Channels and Maximum Power Settings for Cisco Aironet Autonomous Access Points and Bridges.* This document is available on cisco.com at the following URL:

http://cisco.com/en/US/products/ps6521/tsd_products_support_install_and_upgrade.html

Channel Widths for 802.11n

802.11n allows both 20-MHz and 40-Mhz channel widths consisting of 2 contiguous non-overlapping channels (for example, 5-GHz channels 36 and 40). 802.11n radios operate in the same band. However the channel widths can be independently configured.

One of the 20-MHz channels is called the *control channel*. Legacy clients and 20-MHz high throughput clients use the control channel. Beacons can only be sent on this channel. The second 20-MHz channel is called the *extension channel.* 40-MHz stations may use this channel and the control channel simultaneously.

A 40-MHz channel is specified as a channel and -1 as extension. So here, the control channel is channel 40-MHz and the extension channel is 36-Mhz below it.

Beginning in privileged EXEC mode, follow these steps to set the wireless device channel width:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1***slot/port*}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 802.11n 2.4-GHz is radio 0. The 5-GHz radio and the 802.11n 5-GHz is radio 1.

	Command	Purpose
Step 3	**channel** {*frequency* | **least-congested** | **width** [**20** | **40-above** | **40-below**] | **dfs**}	Set the default channel for the wireless device radio. To search for the least-congested channel on startup, enter **least-congested**. Use the **width** option to specify a bandwidth to use. This option is available on all 802.11n APs, but only for the d1 (5 GHz) radio. It has three settings: 20, 40-above, and 40-below. Choosing 20 sets the channel width to 20 MHz. Choosing 40-above sets the channel width to 40 Mhz with the extension channel above the control channel. Choosing 40-below sets the channel width to 40 MHz with the extension channel below the control channel. **Note** The **channel** command is disabled for 5-GHz radios that comply with European Union regulations on dynamic frequency selection (DFS). See the "Setting the 802.11n Guard Interval" section on page 6-21 for more information.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Dynamic Frequency Selection

Access points with 5-GHz radios configured at the factory for use in the United States, Europe, Singapore, Korea, Japan, Israel, and Taiwan now comply with regulations that require radio devices to use Dynamic Frequency Selection (DFS) to detect radar signals and avoid interfering with them. When an access points detects a radar on a certain channel, it avoids using that channel for 30 minutes. Radios configured for use in other regulatory domains do not use DFS.

When a DFS-enabled 5-GHz radio operates on one of the 15 channels listed in Table 6-3, the access point automatically uses DFS to set the operating frequency. When DFS is enabled, the access point monitors its operating frequency for radar signals. If it detects radar signals on the channel, the access point takes these steps:

- Blocks new transmissions on the channel.
- Flushes the power-save client queues.
- Broadcasts an 802.11h channel-switch announcement.
- Disassociates remaining client devices.
- If participating in WDS, sends a DFS notification to the active WDS device that it is leaving the frequency.
- Randomly selects a different 5-GHz channel.
- If the channel selected is one of the channels in Table 6-3, scans the new channel for radar signals for 60 seconds.
- If there are no radar signals on the new channel, enables beacons and accepts client associations.
- If participating in WDS, sends a DFS notification of its new operating frequency to the active WDS device.

Note You cannot manually select a channel for DFS-enabled 5-GHz radios in some regions, depending on the regulatory requirements. The access points randomly selects a channel in that case.

The full list of channels that require DFS is shown in Table 6-3.

Table 6-3 DFS Channel List

Channel	Frequency	Channel	Frequency	Channel	Frequency
52	5260 MHz	104	5500 MHz	124	5620 MHz
56	5280 MHz	108	5520 MHz	128	5640 MHz
60	5300 MHz	112	5560 MHz	132	5660 MHz
64	5320 MHz	116	5580 MHz	136	5680 MHz
100	5500 MHz	120	5600 MHz	140	5700 MHz

For autonomous operation, DFS requires random channel selection among the channels listed in Table 6-3. The channels not listed in Table 6-3 do not require random selection and may be manually configured.

Channels requiring Dynamic Frequency Selection (DFS) may be manually selected from the 5 GHz radio configuration menu. To know the DFS channels, use the **show controllers d1** command.

The GUI/CLI used to manually configure non-DFS channels can also be used to select DFS channels as well. The default channel selection is "DFS", which randomly selects a channel.

If radar is detected on a manually configured DFS channel, the channel will be changed automatically and will not return to the configured channel.

Prior to transmitting on any channels listed in Table 6-3, the access point radio performs a Channel Availability Check (CAC). The CAC is a 60 second scan for the presence of radar signals on the channel. The following sample messages are displayed on the access point console showing the beginning and end of the CAC scan:

```
*Mar 6 07:37:30.423: %DOT11-6-DFS_SCAN_START: DFS: Scanning frequency 5500 MHz for
60 seconds
```

```
*Mar 6 07:37:30.385: %DOT11-6-DFS_SCAN_COMPLETE: DFS scan complete on frequency
5500 MHz
```

When operating on any of the DFS channels listed in Table 6-3, having already performed the CAC, the access point constantly monitors the channel for radar. If radar is detected, the access point stops forwarding data packets within 200 ms and broadcasts five beacons that include an 802.11h channel switch announcement, indicating the channel number that the access point begins using. The following example message displays on the access point console when radar is detected:

```
*Mar 6 12:35:09.750: %DOT11-6-DFS_TRIGGERED: DFS: triggered on frequency 5500 MHz
```

When radar is detected on a channel, that channel may not be used for 30 minutes. The access point maintains a flag in non-volatile storage for each channel that it detects radar on in the last 30 minutes. After 30 minutes, the flag is cleared for the corresponding channel. If the access point is rebooted before a flag is cleared, the non-occupancy time is reset to 30 minutes when the channel initializes.

Note The maximum legal transmit power is greater for some 5-GHz channels than for others. When it randomly selects a 5-GHz channel on which power is restricted, the access point automatically reduces transmit power to comply with power limits for that channel.

Note We recommend that you use the **world-mode dot11d** *country-code* configuration interface command to configure a country code on DFS-enabled radios. The IEEE 802.11h protocol requires access points to include the country information element (IE) in beacons and probe responses. By default, however, the country code in the IE is blank. You use the **world-mode** command to populate the country code IE.

Radar Detection on a DFS Channel

If your AP is installed near a radar station, it may detect radar activity on multiple channels. By using the **peakdetect** command on interface dot11radio1, you can ensure that the AP will detect radar signals and avoid interfering with them using Dynamic Frequency Selection (DFS). By default this command is enabled.

However, in cases where you suspect that the APs are getting false DFS triggers due to in-band/off-channel weather radar signals that cannot be resolved using physical RF signal filters, you can set the AP to not detect radar signals. If you do not want the AP to detect radar signals, use the **no peakdetect** command on interface dot11radio1.

When an access point detects a radar on a DFS channel, the access point creates a file in its flash memory. The file is based on the 802.11a radio serial number and contains the channel numbers on which the radar is detected. This is an expected behavior and you should not remove this file.

CLI Commands

The following sections describe CLI commands that apply to DFS.

Confirming that DFS is Enabled

Use the **show controllers dot11radio1** command to confirm that DFS is enabled. The command also includes indications that uniform spreading is required and channels that are in the non-occupancy period due to radar detection.

This example shows a line from the output for the show controller command for a channel on which DFS is enabled. The indications listed in the previous paragraph are shown in **bold**:

```
ap#sh controllers dot11Radio 1
!
interface Dot11Radio1
Radio ElliotNess 5, Base Address f4ea.6710.6590, BBlock version 0.00, Software version
4.10.1
Serial number: FOC16145K24
Unused dynamic SQRAM memory: 0x00007CB4 (31 KB)
Unused dynamic SDRAM memory: 0x0008E490 (569 KB)
Spectrum FW version: 1.14.2
Number of supported simultaneous BSSID on Dot11Radio1: 16
Carrier Set: Americas (OFDM) (US) (-A)
Uniform Spreading Required: Yes
Configured Frequency: 0 MHz  Channel 0
Allowed Frequencies: * Dynamic Frequency Selection (DFS) only
         5180( 36)  5200( 40)  5220( 44)  5240( 48) *5260( 52) *5280( 56) *5300( 60)
*5320( 64) *5500(100) *5520(104)
        *5540(108) *5560(112) *5580(116) *5660(132) *5680(136) *5700(140)  5745(149)
5765(153)  5785(157)  5805(161)
         5825(165)
```

```
Listen Frequencies:
         5180( 36)  5200( 40)  5220( 44)  5240( 48)  5260( 52)  5280( 56)  5300( 60)
5320( 64)  5500(100)  5520(104)
         5540(108)  5560(112)  5580(116)  5600(120)  5620(124)  5640(128)  5660(132)
5680(136)  5700(140)  5745(149)
         5765(153)  5785(157)  5805(161)  5825(165)

DFS Blocked Frequencies: none
Beacon Flags: 0, Interface Flags 20109, Interface Events 0, Mode 9; Beacons are disabled;
Probes are disabled
Configured TxPower:             14 dBm
Allowed Power Levels:           14 11  8  5  2  dBm
Allowed Client Power Levels:    14 11  8  5  2  dBm
Antenna:                        Rx[a b c d ]
                                Tx[a b c d  ofdm all]
                                External
                                Gain [Allowed 12, Reported 0, Configured 0, In Use 12]
(dBi x 2)
```

Configuring a Channel

Use the **channel** command to configure a channel. The command for the interface is modified to only allow you to select a specific channel number and to enable DFS.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio1 dfs**	Enter the configuration interface for the 802.11a radio
Step 3	**channel** {*number* | **dfs** |**band** <*1 - 4*>}	For *number*, enter a channel frequency from 36 to 5825. Enter **dfs** and one of the following frequency bands to use dynamic frequency selection on the selected channel: 1—5.150 to 5.250 GHz 2—5.250 to 5.350 Ghz 3—5.470 to 5.725 GHz 4—5.725 to 5.825 GHz If you attempt to configure a channel that may only be selected by dfs, the following message appears: `This channel number/frequency can only be used by Dynamic Frequency Selection (DFS)` **Note** The **channel dfs** command is not supported in -P and -Q regulatory domains.
Step 4	**end**	Return to the privileged EXEC mode.
Step 5	**show running-config**	Verify your entries
Step 6	**copy running-config startup-config**	(Optional) Save your entries to the configuration file.

The following example configures the 5 GHz radio to use DFS:

```
ap# configure terminal
ap(config)# interface dot11radio1
ap(config-if)# channel dfs
ap(config-if)# end
```

Blocking Channels from DFS Selection

If your regulatory domain limits the channels that you can use in specific locations--for example, indoors or outdoors--you can block groups of channels to prevent the access point from selecting them when DFS is enabled. Use this configuration interface command to block groups of channels from DFS selection:

[**no**] **dfs band** [**1**] [**2**] [**3**] [**4**] **block**

The 1, 2, 3, and 4 options designate blocks of channels:

- **1**—Specifies frequencies 5.150 to 5.250 GHz. This group of frequencies is also known as the UNII-1 band.
- **2**—Specifies frequencies 5.250 to 5.350 GHz. This group of frequencies is also known as the UNII-2 band.
- **3**—Specifies frequencies 5.470 to 5.725 GHz. This group of frequencies is also known as UNII-2 extended.
- **4**—Specifies frequencies 5.725 to 5.825 GHz. This group of frequencies is also known as the UNII-3 band.

This example shows how to prevent the access point from selecting frequencies 5.150 to 5.350 GHz during DFS:

```
ap(config-if)# dfs band 1 2 block
```

This example shows how to unblock frequencies 5.150 to 5.350 for DFS:

```
ap(config-if)# no dfs band 1 2 block
```

This example shows how to unblock all frequencies for DFS:

```
ap(config-if)# no dfs band block
```

Setting the 802.11n Guard Interval

The 802.11n guard interval is the period in nanoseconds between packets. Two settings are available: short (400ns) and long (800ns).

Beginning in privileged EXEC mode, follow these steps to set the 802.11n guard interval.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1**}	Enter interface configuration mode for the radio interface. The 802.11n 2.4-GHz radio is radio 0 The 802.11n 5-GHz radio is radio 1.
Step 3	**guard-interval** {**any** | **long**}	Enter a guard interval. • any—allows the AP to use 400 ns with clients supporting short GIs, and 800 ns with clients not supporting short GIs, i.e. either the short (400ns) or long (800ns) guard interval. • long—allows only the long (800ns) guard interval.

	Command	Purpose
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Enabling and Disabling World Mode

You can configure the wireless device to support 802.11d world mode, Cisco legacy world mode, or world mode roaming. When you enable world mode, the AP adds channel carrier set information to its beacon. Client devices with world mode enabled receive the carrier set information and adjust their settings automatically. For example, a client device used primarily in Japan could rely on world mode to adjust its channel and power settings automatically when it travels to Italy and joins a network there.

World mode is disabled by default.

Beginning in privileged EXEC mode, follow these steps to enable world mode:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0***slot/port* | **1**}	Enter interface configuration mode for the radio interface.
Step 3	**world-mode** **dot11d country_code** *code* { **both** | **indoor** | **outdoor** } **world-mode roaming** | **legacy**	Enable world mode. • Enter the **dot11d** option to enable 802.11d world mode. – When you enter the **dot11d** option, you must enter a two-character ISO country code (for example, the ISO country code for the United States is **US**). You can find a list of ISO country codes at the ISO website. – After the country code, you must enter **indoor**, **outdoor**, or **both** to indicate the placement of the wireless device. • Enter the **legacy** option to enable Cisco legacy world mode. • Enter the **world-mode roaming** to place the access point in a continuous world mode configuration. **Note** Aironet extensions must be enabled for legacy world mode operation, but Aironet extensions are not required for 802.11d world mode. Aironet extensions are enabled by default.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to disable world mode.

Disabling and Enabling Short Radio Preambles

The radio preamble is a section of data at the head of a frame that helps the APs and clients to synchronize their communication. You can set the radio preamble to long or short:

- Short—A short preamble improves throughput performance. Cisco Aironet Wireless LAN Client Adapters support short preambles. Any 802.11b or 802.11g certified device supports short preambles. However, some client devices still require long preambles, even when they are 802.11b/g certified.
- Long—Long preambles are used by legacy 802.11 only devices, and some 802.11b/g devices that expect long preambles for optimal operations. If these client devices do not associate to the wireless devices, you should use short preambles.

You cannot configure short or long radio preambles on the 5-GHz radio.

Beginning in privileged EXEC mode, follow these steps to disable short radio preambles:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio { 0*slot*/*port* }**	Enter interface configuration mode for the 2.4-GHz radio interface.
Step 3	**no preamble-short**	Disable short preambles and enable long preambles.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Short preambles are enabled by default. Use the **preamble-short** command to enable short preambles if they are disabled.

Configuring Transmit and Receive Antennas

You can select the antenna the wireless device uses to receive and transmit data. There are three options for both the receive and the transmit antenna:

- Gain—Sets the resultant antenna gain in dB.
- Diversity—This default setting tells the wireless device to use the antenna that receives the best signal. If the wireless device has two fixed (non-removable) antennas, you should use this setting for both receive and transmit. If the device has three removable antennas, you can use this setting to have all of them operate in diversity mode
- Right—If the wireless device has removable antennas and you install a high-gain antenna on the wireless device's right connector, you should use this setting for both receive and transmit. When you look at the wireless device's back panel, the right antenna is on the right.
- Middle—If the wireless device has removable antennas and you install a high-gain antenna on the wireless device middle connector, you should use this setting for receiving only. The antennas available for transmitting in a three-antenna configuration are the right and left antennas.

- Left—If the wireless device has removable antennas and you install a high-gain antenna on the wireless device's left connector, you should use this setting for both receive and transmit. When you look at the wireless device's back panel, the left antenna is on the left.
  This does not apply for dual antenna APs such as the 1600, 2600, and 3600 series. Please check the respective hardware guides for further information.

Beginning in privileged EXEC mode, follow these steps to select the antennas the wireless device uses to receive and transmit data:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1*slot/port***}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1. The 802.11n 2.4-GHz radio is radio 0 The 802.11n 5-GHz radio is radio 1.
Step 3	**antenna again** *dB*	Specifies the resultant gain of the antenna attached to the device. Enter a value from –128 to 128 dB. **Note** This setting does not affect the behavior of the wireless device; it only informs the management platform on your network of the device antenna gain.

Step 4	**antenna receive** {**diversity** | **left** | **middle** | **right**}
	On the 2600 and the 3600 series, this command is:
	antenna receive **{a-antenna** | **ab-antenna** | **abc-antenna** | **abcd-antenna**}
		Set the receive antenna to diversity, left, middle, right, or all.
		Note For best performance with two antennas, leave the receive antenna setting at the default setting, **diversity**. For one antenna, attach the antenna on the right and set the antenna for **right**.
		On the 2600 and the 3600 series APs:
		• a-antenna—to use antenna A
		• ab-antenna—to use antennas A and B
		• abc-antenna—to use antennas A, B, and C
		• abcd-antenna—to use antennas A, B, C, and D

Step 5	**antenna transmit** {**diversity** | **left** | **right**}
	On the 2600 and the 3600 series, this command is:
	antenna transmit **{a-antenna** | **ab-antenna** | **abc-antenna** | **abcd-antenna**}
		Set the transmit antenna to diversity, left, or right.
		Note For best performance with two antennas, leave the receive antenna setting at the default setting, **diversity**. For one antenna, attach the antenna on the right and set the antenna for **right**.
		On the 2600 and the 3600 series APs:
		• a-antenna—to use antenna A
		• ab-antenna—to use antennas A and B
		• abc-antenna—to use antennas A, B, and C
		• abcd-antenna—to use antennas A, B, C, and D

Step 6	**end**	Return to privileged EXEC mode.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Enabling and Disabling Gratuitous Probe Response

Gratuitous Probe Response (GPR) aids in conserving battery power in dual mode phones that support cellular and WLAN modes of operation. GPR is available on 5-Ghz radios and is disabled by default. You can configure two GPR settings:

- Period—This setting determines the time between GPR transmissions in Kusec (or milliseconds) intervals from 10 to 255 (similar to the beacon period)
- Speed—The speed is the data rate used to transmit the GPR

Selecting a longer period reduces the amount of RF bandwidth consumed by the GPR with the possibility of shorter battery life. Selecting higher transmission speeds also reduces the amount of bandwidth consumed but at the expense of a smaller cell size.

Beginning in privileged EXEC mode, follow these steps to enable GPR and set its parameters:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio {1}***slot/port*	Enter interface configuration mode for the 5-GHz radio interface.
Step 3	**probe-response gratuitous** {**period** | **speed**}	Enable the Gratuitous Probe Response feature using default period (10 Kusec) and speed (6.0 Mbps).
Step 4	**period** *Kusec*	(Optional) Enter a value from 10 to 255. The default value is 10
Step 5	**speed** {[**6.0**] [**9.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] }	(Optional) Sets the response speed in Mbps. The default value is 6.0.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The optional parameters can be configured independently or combined when you do not want to use the defaults, as shown in the following examples:

```
(config-if)# probe-response gratuitous period 30
(config-if)# probe-response gratuitous speed 12.0
(config-if)# probe-response gratuitous period 30 speed 12.0
```

Use the **no** form of the command to disable the GPR feature.

Disabling and Enabling Aironet Extensions

By default, the wireless device uses Cisco Aironet 802.11 extensions to detect the capabilities of Cisco Aironet client devices and to support features that require specific interaction between the wireless device and associated client devices. Aironet extensions must be enabled to support these features:

- Load balancing—The wireless device uses Aironet extensions to direct client devices to an access point that provides the best connection to the network based on factors such as number of users, bit error rates, and signal strength.
- Message Integrity Check (MIC)—MIC is an additional WEP security feature that prevents attacks on encrypted packets called bit-flip attacks. The MIC, implemented on both the wireless device and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof.

- Cisco Key Integrity Protocol (CKIP)—Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group. The standards-based algorithm, TKIP, does not require Aironet extensions to be enabled.
- Repeater mode—Aironet extensions must be enabled on repeater access points and on the root access points to which they associate.
- World mode (legacy only)—Client devices with legacy world mode enabled receive carrier set information from the wireless device and adjust their settings automatically. Aironet extensions are not required for 802.11d world mode operation.
- Limiting the power level on associated client devices—When a client device associates to the wireless device, the wireless device sends the maximum allowed power level setting to the client.

Disabling Aironet extensions disables the features listed above, but it sometimes improves the ability of non-Cisco client devices to associate to the wireless device.

Aironet extensions are enabled by default. Beginning in privileged EXEC mode, follow these steps to disable Aironet extensions:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1***slot/port* }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1. The 802.11n 2.4-GHz radio is radio 0 The 802.11n 5-GHz radio is radio 1.
Step 3	**no dot11 extension aironet**	Disable Aironet extensions.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **dot11 extension aironet** command to enable Aironet extensions if they are disabled.

Configuring the Ethernet Encapsulation Transformation Method

Frames contain a field that specifies the upper Layer protocol that should be used (such as IP, IPX, ARP, etc). This field is necessary at the receiver level to direct the frame properly in the receiver network stack.

There are two main techniques for protocol indication:

- EtherType—A 16 bit value that indicates the protocol carried in the frame. EtherType is used in Ethernet 2.0/DIX networks.
- LLC/SNAP—A 6 byte header that allows for an 802.2 link layer protocol indication. LLC/SNAP is used in 802.3 and 802.11 networks.

When the access point receives from the wired network frames that use EtherType information, it needs a mechanism to convert this EtherType information to SNAP/LLC information. There are two transformation methods:

- 802.1H—This method provides good performance for Cisco Aironet wireless products.
- RFC 1042—Use this setting to ensure good interoperability with non-Cisco Aironet wireless equipment. RFC 1042 is used by other manufacturers of wireless equipment and is the default setting. This is the default setting.

Beginning in privileged EXEC mode, follow these steps to configure the encapsulation transformation method:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1***slot/port*}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1. The 802.11n 2.4-GHz radio is radio 0 The 802.11n 5-GHz radio is radio 1.
Step 3	**payload-encapsulation** **rfc1042** | **dot1h**	Set the encapsulation transformation method to RFC 1042 (**rfc1042**, the default setting) or 802.1h (**dot1h**).
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Enabling and Disabling Reliable Multicast to Workgroup Bridges

The *Reliable multicast messages from the access point to workgroup bridges* setting limits reliable delivery of multicast messages to up to 20 Cisco Aironet Workgroup Bridges that are associated to the AP. The default setting, **disabled**, reduces the reliability of multicast delivery but allows more workgroup bridges to associate to the wireless device.

Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. Treating a workgroup bridge as an infrastructure device means that the wireless device reliably delivers multicast packets and some broadcast packets, including Address Resolution Protocol (ARP) packets, to the workgroup bridge.

The AP sends multicast frames to a multicast address, and then again sends the multicast frames to the workgroup bridge, encapsulated in a unicast frame, that is acknowledged by the workgroup bridge. This verification mechanism creates wireless overhead, and reduces the throughput on the access point.

The performance cost of reliable multicast delivery—duplication of each multicast packet sent to each workgroup bridge—limits the number of infrastructure devices, including workgroup bridges, that can associate to the wireless device. To increase beyond 20 the number of workgroup bridges that can maintain a radio link to the wireless device, the wireless device must reduce the delivery reliability of multicast packets to workgroup bridges. With reduced reliability, the wireless device cannot confirm whether multicast packets reach the intended workgroup bridge, so workgroup bridges at the edge of the wireless device's coverage area might lose IP connectivity. When you treat workgroup bridges as client devices, you increase performance but reduce reliability.

Note This feature is best suited for use with stationary workgroup bridges. Mobile workgroup bridges might encounter spots in the wireless device's coverage area where they do not receive multicast packets and lose communication with the wireless device even though they are still associated to it.

A Cisco Aironet Workgroup Bridge provides a wireless LAN connection for up to eight Ethernet-enabled devices.

Beginning in privileged EXEC mode, follow these steps to configure the encapsulation transformation method:

Note To configure reliable multicast forwarding, this configuration should be done on the AP, and not on the workgroup bridge.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio {0 | 1}**	Enter interface configuration mode for the 2.4-GHz radio interface.
Step 3	**infrastructure-client**	Enable reliable multicast messages to workgroup bridges.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to disable reliable multicast messages to workgroup bridges.

The workgroup bridge will start receiving the multicast frame and then the unicast copy of the same frame, which results in duplication of frames at the receiver level and is therefore inefficient.

To configure the workgroup bridge to consider only the multicast frame or the unicast copy at the workgroup bridge radio level, use the following commands:

Command	Purpose
station-role workgroup-bridge multicast mode {**client** | **infrastructure**}	You can set either one of the following: • Client—Client-mode accepts only 3-MAC address header mulitcast packets • Infrastructure—Infrastructure-mode accepts only 4-MAC address header multicast packets If you set reliable multicast on the AP, then you are recommended to use infrastructure at workgroup bridge level. If you do not set reliable multicast at the AP, use client at the workgroup bridge level.

For example, the following command uses infrastructure at the workgroup bridge level:

```
WGB(config-if)# station-role workgroup-bridge multicast mode infrastructure
```

Enabling and Disabling Public Secure Packet Forwarding

Public Secure Packet Forwarding (PSPF) prevents client devices associated to an access point from inadvertently sharing files or communicating with other client devices associated to the access point. It provides Internet access to client devices without providing other capabilities of a LAN. This feature is useful for public wireless networks like those installed in airports or on college campuses.

Note To prevent communication between clients associated to different access points, you must set up protected ports on the switch to which the wireless devices are connected. See the "Configuring Protected Ports" section on page 6-30 for instructions on setting up protected ports.

To enable and disable PSPF using CLI commands on the wireless device, you use bridge groups. You can find a detailed explanation of bridge groups and instructions for implementing them in this document:

- *Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*. Click this link to browse to the Configuring Transparent Bridging chapter: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcfpart1/bcftb.htm

You can also enable and disable PSPF using the web-browser interface. The PSPF setting is on the Radio Settings pages.

PSPF is disabled by default. Beginning in privileged EXEC mode, follow these steps to enable PSPF:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1***slot/port*}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1. The 802.11n 2.4-GHz radio is radio 0 The 802.11n 5-GHz radio is radio 1.
Step 3	**bridge-group** *group* **port-protected**	Enable PSPF.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to disable PSPF.

Configuring Protected Ports

To prevent communication between client devices associated with different access points on your wireless LAN, you can set up protected ports on the switch to which the wireless devices are connected. Alternatively, you should isolate ports on the same switch that leads to APs between which you do not want communication to occur.

Beginning in privileged EXEC mode, follow these steps to define a port on your switch as a protected port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and enter the type and number of the switchport interface to configure, such as **gigabitethernet0/1**.
Step 3	**switchport protected**	Configure the interface to be a protected port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interfaces** *interface-id* **switchport**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable protected port, use the **no switchport protected** interface configuration command. This command is only valid at an individual switch level. It does not isolate APs connected to different switches. You can use this command on ports to all APs on a given switch among which you do not want communication to occur. Alternatively, you can use private VLAN configuration for the AP.

Note When using wireless domain services (WDS), make sure not to block communication between the APs and their WDS.

For detailed information on configuring private VLANs and on protected ports and port blocking, see the *Catalyst 3750 Software Configuration Guide*, at the following URL:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750.html

Configuring the Beacon Period and the DTIM

The beacon period is the amount of time between access point beacons in Kilomicroseconds. One Kµsec equals 1,024 microseconds. The Data Beacon Rate, always a multiple of the beacon period, determines how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them.

For example, if the beacon period is set at 100, its default setting, and the DTIM is set at 2, its default setting, then the AP sends a beacon containing a DTIM every 2 beacons, or every 200 Kµsec, or every 200 ms. One Kµsec equals 1,024 microseconds.

The default beacon period is 100, and the default DTIM is 2. Beginning in privileged EXEC mode, follow these steps to configure the beacon period and the DTIM:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1***slot/port*}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 802.11n 2.4-GHz radio is 0. The 5-GHz radio and the 802.11n 5-GHz radio is 1.
Step 3	**beacon period** *value*	Set the beacon period in the range 20 to 4000. Enter a value in Kilomicroseconds.
Step 4	**beacon dtim-period** *value*	Set the DTIM in the range 1 to 100. Enter a value in Kilomicroseconds.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configure RTS Threshold and Retries

The RTS threshold determines the packet size at which the wireless device issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the wireless device, or in areas where the clients are far apart and can detect only the wireless device and not each other. You can enter a setting ranging from 0 to 23472347 bytes.

Maximum RTS retries is the maximum number of times the wireless device issues an RTS before stopping the attempt to send the packet over the radio. Enter a value from 1 to 128.

The default RTS threshold is 2347 for all access points and bridges, and the default maximum RTS retries setting is 3264. Beginning in privileged EXEC mode, follow these steps to configure the RTS threshold and maximum RTS retries:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1***slot/port*}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.

	Command	Purpose
Step 3	**rts threshold** *value*	Set the RTS threshold. Enter an RTS threshold from 0 to 23472347.
Step 4	**rts retries** *value*	Set the maximum RTS retries. Enter a setting from 1 to 128.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the RTS settings to defaults.

Configuring the Maximum Data Packet Retries

The maximum data retries setting determines the number of attempts the wireless device makes to send a packet before giving up and dropping the packet.

The default setting is 32. Beginning in privileged EXEC mode, follow these steps to configure the maximum data retries:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1***slot/port*}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	**packet retries** *value* [**drop-packet**]	Set the maximum data retries. Enter a setting from 1 to 128. If the drop-packet option is used, the device stops trying to send the current packet, and moves on to try sending the next packet in the queue, without disconnecting. When the drop-packet option is not used, the wireless device determines that the link is not usable anymore, stops trying to send the current packet and terminates the connection.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the setting to defaults.

Configuring the Fragmentation Threshold

The fragmentation threshold determines the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.

The default setting is 23382346 bytes. Beginning in privileged EXEC mode, follow these steps to configure the fragmentation threshold:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1***slot/port*}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	**fragment-threshold** *value*	Set the fragmentation threshold. Enter a setting from 256 to 2346 bytes for the 2.4-GHz radio. Enter a setting from 256 to 2346 bytes for the 5-GHz radio.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the setting to defaults.

Enabling Short Slot Time for 802.11g Radios

You can increase throughput on the 802.11g, 2.4-GHz radio by enabling short slot time. Reducing the slot time from the standard 20 microseconds to the 9-microsecond short slot time decreases the overall backoff, which increases throughput. Backoff, which is a multiple of the slot time, is the random length of time that a station waits before sending a packet on the LAN.

Many 802.11g radios support short slot time, but some do not. When you enable short slot time, the wireless device uses the short slot time only when all clients associated to the 802.11g, 2.4-GHz radio support short slot time.

Short slot time is supported only on the 802.11g, 2.4-GHz radio. Short-slot time is not supported by 802.11b clients. If you enable short slot time, 802.11b clients will not be able to join or communicate with the AP radio. Short slot time is disabled by default.

In radio interface mode, enter this command to enable short slot time:

```
ap(config-if)# short-slot-time
```

Enter **no short-slot-time** to disable short slot time.

Performing a Carrier Busy Test

You can perform a carrier busy test to check the radio activity on wireless channels. During the carrier busy test, the wireless device drops all associations with wireless networking devices for 4 seconds while it conducts the carrier test and then displays the test results.

In privileged EXEC mode, enter this command to perform a carrier busy test:

```
dot11 interface-number carrier busy
```

For *interface-number*, enter **dot11radio 0** to run the test on the 2.4-GHz radio, or enter **dot11radio 1** to run the test on the 5-GHz radio.

Note The interface must be enabled for the carrier busy test to be performed.

Use the **show dot11 carrier busy** command to re-display the carrier busy test results.

```
ap#dot11 dot11Radio 1 carrier busy
ap#show dot11 carrier busy
Frequency  Carrier Busy %
---------  --------------
   5180         2
   5200         0
   5220         2
   5240         1
   5260         1
   5280         0
   5300         1
   5320         0
   5500         0
   5520         0
   5540         0
   5560         0
   5580         0
   5660         0
   5680         0
   5700         0
   5745         0
   5765         0
   5785         0
   5805         0
   5825         0
```

Configuring VoIP Packet Handling

You can improve the quality of VoIP packet handling per radio on access points by enhancing 802.11 MAC behavior for lower latency for Wireless class of service 5 (Video) and wireless class of service 6 (Voice).

Follow these steps to configure VoIP packet handling on an access point:

Step 1 Using a browser, log in to the access point.

Step 2 Click **Services** in the task menu at the top of the web-browser interface.

Step 3 In the left menu, click **Stream**.

The Stream page appears.

Step 4 Click the tab for the radio to configure.

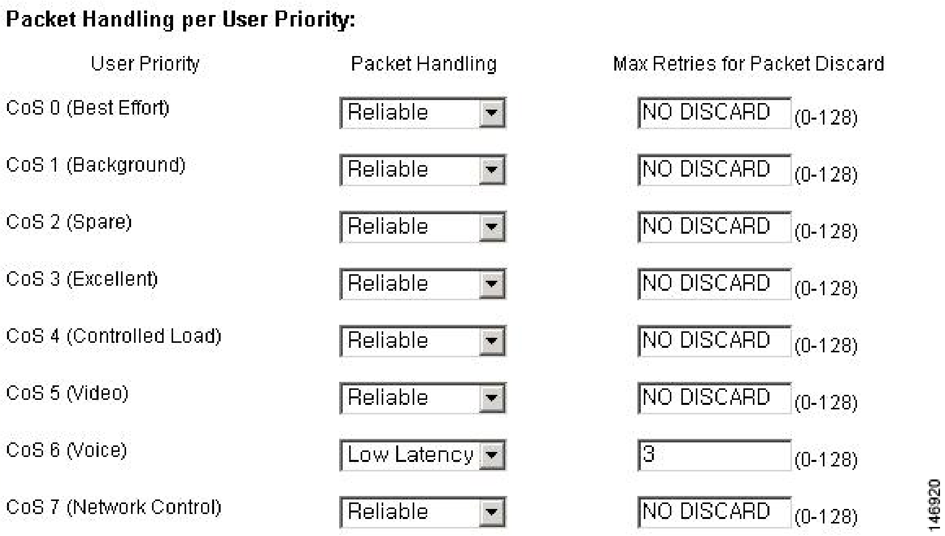
Step 5 For both CoS 5 (Video) and CoS 6 (Voice) user priorities, choose Low Latency from the Packet Handling drop-down list and enter a value for maximum retries for packet discard in the corresponding field. Packets in other queues are dequeued, giving delay-sensitive data preferential treatment over other traffic.

The default value for maximum retries is 3 for the Low Latency setting (Figure 6-2). This value indicates how many times the access point will try to resend a lost packet before discarding it.

Note You may also configure the CoS 4 (Controlled Load) user priority and its maximum retries value.

Step 6 Click **Apply**.

Figure 6-2 Packet Handling Configuration



Packet Handling per User Priority:

User Priority	Packet Handling	Max Retries for Packet Discard
CoS 0 (Best Effort)	Reliable	NO DISCARD (0-128)
CoS 1 (Background)	Reliable	NO DISCARD (0-128)
CoS 2 (Spare)	Reliable	NO DISCARD (0-128)
CoS 3 (Excellent)	Reliable	NO DISCARD (0-128)
CoS 4 (Controlled Load)	Reliable	NO DISCARD (0-128)
CoS 5 (Video)	Reliable	NO DISCARD (0-128)
CoS 6 (Voice)	Low Latency	3 (0-128)
CoS 7 (Network Control)	Reliable	NO DISCARD (0-128)

You can also configure VoIP packet handling using the CLI. For a list of Cisco IOS commands for configuring VoIP packet handling using the CLI, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Once you have defined the retry level, you can also configure the speed at which those frames should be sent. This is done at the bottom of the page, in the **Low Latency Packet Rates** section. You can set each rate to:

- Nominal—The AP will try to use this rate to send the Low Latency Packets (using the faster rate first, and of course depending on the client signal level).
- Non-nominal—The AP will try not to use that rate, but will revert to it if no nominal rate is possible.
- Disabled—The AP will not try to use that rate.

From the CLI, use radio interface config commands as follows (The CLI commands offer more options than the GUI page):

packet max-retries *number 1 number 2* **fail-threshold** *number 3 number 4* **priority** *value* **drop-packet**

In the previous command:

- Number 1—Defines the number of times the AP should try to resend a packet that was not received properly (not acknowledged), for a given priority level. Once number 1 is reached, the AP drops the packet and tries to send the next one (to the same recipient).
- Number 3—Determines how many consecutive packets (sent to one recipient) can fail before the AP decides that its fail-rate exceeds an acceptable threshold.
- Number 2—Once the fail-threshold is exceeded, the AP may still resend failed packets, but with a different number of attempts than before the threshold is exceeded. This is number 2. For example, you can decide initially to resend each packet 3 times (number 1). Then, if your AP fails to send a certain number of consecutive packets (for example 100, as number 3), you can decide that conditions are degraded, and that your AP should only try to resend each following packet once (which is number 2).
- Number 4—Determines how many more consecutive packets the AP should try to resend with number 2 retries before de-associating the target client.

Example:

```
ap(config-if)# packet max-retries 3 0 fail-threshold 100 500 priority 6 drop-packet
```

In this example, the AP tries to resend each packet of priority level 6 three times (number one = 3). If more than 100 consecutive packets (number three = 100) fail to the same destination, the AP sends each consecutive packet to that destination only once (number two = 0). If 500 more packets (number four = 500) fail to that same destination, the AP disconnects that client.

When using the GUI, number one is defined manually (default is 3). Number 2 defaults to 0, number 3 defaults to 100 and number 4 defaults to 500. These numbers can then be changed from the CLI.

```
ap(config-if)#packet max-retries ?
  <0-128>  # packet retries before dropping pkt if first fail-threshold not
           reached


ap(config-if)#packet max-retries 3 ?
  <0-128>  # packet retries before dropping pkt if 2nd fail-threshold not
           reached

ap(config-if)#packet max-retries 3 0 ?
  fail-threshold  maximum # consecutive dropped packets thresholds

ap(config-if)#packet max-retries 3 0 fa
ap(config-if)#packet max-retries 3 0 fail-threshold ?
  <0-1000>  # consecutive dropped packets before switching max-retries
            thresholds

ap(config-if)#packet max-retries 3 0 fail-threshold 100 ?
  <0-1000>  number of consecutive dropped packets before disassociating client

ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 ?
  priority  qos user-priority

ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 p
ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority ?
  <0-7>  qos user-priority number

ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority 6 ?
  drop-packet  Don't retry pkts, just drop packets when max retries reached
```

```
ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority 6 d
ap(config-if)#packet max-retries 3 0 fail-threshold 100 500 priority 6 drop-packet
```

Low latency Packet rates can also be defined at the interface level, using the following command which defines the nominal rates and the allowed rates to use:

traffic-stream priority *value* **sta-rates {[***nominal rates***] | [***rates***]}**

```
ap(config-if)# traffic-stream priority 6 sta-rates ?
  12.0      Allow 12.0 Mb/s rate
  18.0      Allow 18.0 Mb/s rate
  24.0      Allow 24.0 Mb/s rate
  36.0      Allow 36.0 Mb/s rate
  48.0      Allow 48.0 Mb/s rate
  54.0      Allow 54.0 Mb/s rate
  6.0       Allow 6.0 Mb/s rate
  9.0       Allow 9.0 Mb/s rate
  nom-12.0  Allow Nominal 12.0 Mb/s rate
  nom-18.0  Allow Nominal 18.0 Mb/s rate
  nom-24.0  Allow Nominal 24.0 Mb/s rate
  nom-36.0  Allow Nominal 36.0 Mb/s rate
  nom-48.0  Allow Nominal 48.0 Mb/s rate
  nom-54.0  Allow Nominal 54.0 Mb/s rate
  nom-6.0   Allow Nominal 6.0 Mb/s rate
  nom-9.0   Allow Nominal 9.0 Mb/s rate
 <cr>
```

Example:

```
ap(config-if)# traffic-stream priority 6 sta-rates nom-5.5 nom-11.0 nom-6.0 9.0 nom-12.0
nom-24.0
```

For the voice queue (UP 6 specifically), you can also use the interface command packet speed to determine the rates allowed to use to send packets in the voice queue:

packet speed 5.5 11.0 6.0 9.0 12.0 24.0 priority 6

Notice that the packet speed command focuses on defining the allowed rates, while the command traffic-stream priority also defines the preferred rates among the allowed rates. If you use both commands for the voice queue, the rates defined as nominal in the traffic stream priority command are tried first, then non nominal rates and packet speed rates are attempted.

Configuring ClientLink

Cisco ClientLink (referred to as Beam Forming) is an intelligent beamforming technology that directs the RF signal to 802.11a/g devices to improve performance by 65%, improve coverage by up to 27% percent, and reduce coverage holes.

Cisco ClientLink helps extend the useful life of existing 802.11a/g devices in mixed-client networks and 802.11n clients supporting only one traffic stream. It is beneficial for organizations that move to 802.11n and want to ensure that all clients on the network, regardless of type, are guaranteed the bandwidth and throughput they need.

Note CLientLink Ver 1 supports 802.11 a/g devices and ClientLink Ver 2 supports 802.11 a/g devices and 802.11n devices with one spatial stream.

Note ClientLink is not supported on the 1040, 702 series access points.

Using the CLI to Configure ClientLink

To enable ClientLink, enter this CLI command in interface configuration mode on 802.11n radio interfaces:

```
beamform ofdm
```

Note Currently the ClientLink configuration option is not available through GUI.

To determine the threshold from which you start doing ClientLink, use the following command:

ap(config-if)# **beamform rssi** *30to128-rssi-threshold-in-dBm*

ClientLink is disabled by default. Additional details can be found on cisco.com at the following URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10092/white_paper_c11-516389.html

Debugging Radio Functions

Use the **debug dot11** privileged EXEC command to begin debugging of radio functions. Use the **no** form of this command to stop the debug operation. The command syntax is:

```
[no] debug dot11
{events | packets | forwarding | mgmt | network-map | syslog | virtual-interface}
```

The syntax is described in Table 6-4.

Table 6-4 Syntax for debug dot11 Command

Syntax	Description
events	Activates debugging of all radio related events
packets	Activates debugging of radio packets received and transmitted
forwarding	Activates debugging of radio forwarded packets
mgmt	Activates debugging of radio access point management activity
network-map	Activates debugging of radio association management network map
syslog	Activates debugging of radio system log
virtual interface	Activates debugging of radio virtual interfaces

This example shows how to begin debugging of all radio-related events:

```
AP# debug dot11 events
```

This example shows how to begin debugging of radio packets:

```
AP# debug dot11 packets
```

This example shows how to begin debugging of the radio system log:

```
AP# debug dot11 syslog
```

This example shows how to stop debugging of all radio related events:

```
AP# no debug dot11 events
```

Note Debugging not enabled is the default of the command.

802.11r Configuration

802.11r enables fast roaming across access point in the same subnet using Wireless Domain Service. When you enable 802.11r, a Mobility Domain Information Element (MDIE) is advertised in the AP beacons. The same MDIE is announced by all APs associated to the same WDS. The last 2 bytes of the WDS BVI IP address (IPv4 or Ipv6) is used as MDIE. 802.11r compatible clients use this MDIE to identify APs belonging to the same domain and between which fast roaming is possible.

For a client to move from its current AP to a target AP utilizing the FT protocols, the message exchanges are performed using one of two methods:

- Over-the-Air—The client communicates directly with the target AP using IEEE 802.11 authentication with the FT authentication algorithm. To set this, use the command: ap(config-if)#**dot11 dot11r pre-authentication over-air**
- Over-the-DS—The client communicates with the target AP via the current AP. The communication between the client and the target AP is carried in FT action frames between the client and the current AP, and is then sent through the WDS to the target AP. To set this, use the command: ap(config-if)#**dot11 dot11r pre-authentication over-ds**

On an AP radio, you can enable 802.11r support, and decide if roaming dialog should occur over the air (default) or over the DS, and also configure the maximum time allowed for a client to complete the roaming transaction. The maximum time allowed for a client to complete the roaming transaction is called Re-association Timer. This timer allows you to add security to your network by preventing attackers from opening many 802.11r transactions without completing any of them, which can overload the AP. You can set this timer using the following command:

ap(config-if)#**dot11 dot11r reassociation-time value** *20to1200-timeout-value-in-milli-seconds*

Example:Enable 802.11r, with authentication over the DS, and re-association time value of 200 ms.

```
aap(config-if)#dot11 dot11r pre-authentication over-ds
ap(config-if)#dot11 dot11r reassociation-time value 200
```

Note Test 802.11r before implementing it into your network. Some non-802.11r clients do not support 802.11r MDIE and do not operate well in 802.11r environments.

Setting Traffic Rate Limits for an SSID and Radio Interface

To limit the bandwidth usage by wireless client devices, you can limit the traffic rate to and from wireless client devices. This rate limiting feature can be:

- Configured for each SSID and can be applied on one or both radio interfaces
- Applied only to TCP/UDP on IPv4. Not supported for IPv6 traffic.
- Applied to both input (ingress) and output (egress) traffic on a radio interface

The rate limiting feature is available for VLANs. If you have more than one SSID configured on the same interface, then you cannot configure rate limits without having VLANs.

For information on configuring multiple SSIDs, see Chapter 7, “Configuring Multiple SSIDs”.

For information on VLANs, see Chapter 14, “Configuring VLANs”.

As part of Quality of Service (QoS) feature, a rate limiting feature which limits the input or output transmission rate of a class of traffic based on user-defined criteria is present. See Chapter 15, “Configuring QoS”, for more information on that.

Configuring Rate Limits

To configure the rate limits, use the command **rate-limit {tcp | udp} {input | output} data-rate** *rate* **burst-size** *size*, where;

- Date-rate is the average rate of data transmission, specified in Kilobits/sec.
- Burst-size is the total data that can be transmitted before the traffic is throttled. It is specified in Kilobits.

These parameters are converted and limited to the nearest multiple of 8, whereby data-rate is converted to KiloBytes/sec and burst-size is converted to Bytes, and then are considered for rate limiting.

To understand how these parameters work, follow this example. Consider the average data rate as 10 Bytes/sec and the burst-size as 20 Bytes. Then the rate limit applied here is such that in a duration of 2 seconds (calculated as Burst-size/Average Rate) the total data transmission is not allowed to exceed 20 Bytes. This also allows for more data to be transmitted per second as long the average data-rate does not exceed 10 Bytes/sec.

To configure via the GUI, go to **Security > SSID Manager**. Under the **Rate Limit Parameters** section, you can limit input or output traffic for TCP or UDP, as required. You can also specify the rate and burst-size in each case.

Viewing the Rate Limit Statistics

To view the statistics of rate limits, for each ssid configured on a given interface, use the command **show interface dot11radio {0 | 1} qos-info**

To clear the statistics counters, use the command **clear counters dot11Radio {0 | 1}**

To view the rate limit statistics via the GUI, go to **Network > Network Interface > Radio0-802.11N 2.4GHz** or **Radio1-802.11N 5GHz**. To clear the statistics, click **Clear**.

CHAPTER 7

Configuring Multiple SSIDs

This chapter describes how to configure and manage multiple Service Set Identifiers (SSIDs) on the access point.

Understanding Multiple SSIDs

The SSID is an ASCII string that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. SSIDs are case sensitive and can contain up to 32 alphanumeric characters.

You can configure up to 16 SSIDs on your access point and assign different configuration settings to each SSID. All the SSIDs may be active at the same time; that is, client devices can associate to the access point using any of the SSIDs. These are the settings you can assign to each SSID:

- VLAN
- Client authentication settings

Note For detailed information on client authentication types, see Chapter 11, "Configuring Authentication Types."

- Client authenticated key management settings
- Insert AP authentication parameters (when using AP to AP links, such as bridges)
- Insert Management frame protection settings (802.11w and/or Cisco MFP)
- Maximum number of client associations using the SSID
- RADIUS accounting for traffic using the SSID
- Guest mode (defines if the SSID string should be broadcasted in the beacons
- Define legacy AP to AP authentication method, when using PSK or LEAP security in AP to AP links
- Redirection of packets received from client devices

If you want the access point SSID to be visible to all wireless clients, including clients not having a profile to that particular SSID, you can setup a guest SSID. The access point mentions the guest SSID in its beacon. If the guest mode is disabled, the AP will still send beacons for this SSID, but the SSID string will not be mentioned. If you do not want clients that do not have a preconfigured SSID, disable the guest SSID feature. Note that the SSID will still be available to clients specifically querying for that particular SSID string. Clients sending broadcast probe messages will not receive that SSID string in the AP answer, and will not see the SSID string in the AP beacons. For information on how to configure guest mode SSID and disable Guest mode SSID, see the "Creating an SSID Globally" section on page 7-3.

If your access point is intended to be a repeater or a non-root bridge, you can setup, on the repeater or non-root bridge side, credentials so that the root or primary AP can authenticate the repeater or non-root bridge. You can assign an authentication username and password to the repeater-mode SSID to allow the repeater to authenticate to your network like a client device.

If your network uses VLANs, you can assign each SSID to a VLAN, and client devices using the SSID are grouped in that VLAN.

Configuring Multiple SSIDs

These sections contain configuration information for multiple SSIDs:

- Creating an SSID Globally, page 7-3
- Using a RADIUS Server to Restrict SSIDs, page 7-5

Note You need to configure SSIDs globally and then apply them to a specific radio interface. Follow the instructions in the "Creating an SSID Globally" section on page 7-3 to configure SSIDs globally.

Creating an SSID Globally

In Cisco IOS Releases you use the **dot11 ssid** global configuration command to create an SSID, and you can use the **ssid** configuration interface command to assign the SSID to a specific interface.

When an SSID has been created in global configuration mode, the **ssid** configuration interface command attaches the SSID to the interface but does not enter ssid configuration mode. However, if the SSID has not been created in global configuration mode, the **ssid** command puts the CLI into SSID configuration mode for the new SSID. However, the parameters that you can configure from the radio interface SSID configuration mode are more limited than the parameters you can configure from the SSID global configuration mode.

Beginning in privileged EXEC mode, follow these steps to create an SSID globally. After you create an SSID, you can assign it to specific radio interfaces.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ssid** *ssid-string*	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. The SSID can consist of up to 32 alphanumeric, case-sensitive, characters. **Note** TAB and trailing spaces are invalid characters for SSIDs.
Step 3	**authentication client username** *username* **password** *password*	(Optional) Set an authentication username and password that the access point uses to authenticate to the network when in repeater mode or non-root bridge mode, and using a legacy authentication system, such as LEAP. Set the username and password on the SSID that the repeater access point uses to associate to a root access point, with another repeater or non-root bridge.
Step 4	**accounting** *list-name*	(Optional) Enable RADIUS accounting for this SSID. For *list-name*, specify the accounting method list. Click this link for more information on method lists: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacct.html

	Command	Purpose
Step 5	**vlan** *vlan-id*	(Optional) Assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. You can assign several SSIDs to the same VLAN, but you can assign each SSID to only one VLAN.
Step 6	**guest-mode**	(Optional) Designate the SSID as your access point guest-mode SSID. The access point includes the SSID in its beacon and is visible to client devices that do not specify an SSID in their probe requests.
Step 7	**infrastructure-ssid** [**optional**]	This command controls the SSID that access points and bridges use when associating with one another. A root access point only allows a repeater access point to associate using the infrastructure SSID. A root bridge only allows a non-root bridge to associate using the infrastructure SSID. Repeater access points and non-root bridges use this SSID to associate with root devices. The access point and bridge GUI requires the configuration of infrastructure-ssid for repeater, and non-root bridge roles. It is not mandatory to configure infrastructure SSID for workgroup bridge roles. In case you are using legacy IOS code, if you use the CLI to configure the device role, you do not have to configure an infrastructure SSID unless multiple SSIDs are configured on the radio. If multiple SSIDs are configured on the radio, you must use the infrastructure-ssid command to specify which SSID the non-root bridge uses to connect to the root bridge. However, from 12.4(21a)JA1 and 12.3(8)JEC release onwards, repeaters do not associate with bridges when infrastructure-ssid is not configured irrespective of the presence of single or multiple SSIDs.
Step 8	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface to which you want to assign the SSID. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 9	**ssid** *ssid-string*	Assign the global SSID that you created in Step 2 to the radio interface.
Step 10	**end**	Return to privileged EXEC mode.
Step 11	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note You use the **ssid** command authentication options to configure an authentication type for each SSID. See Chapter 9, “Configuring an Access Point as a Local Authenticator,” for instructions on configuring authentication types.

Note When you enable guest SSID mode for the 802.11g radio it applies to the 802.11b radio as well since 802.11b and 802.11g operate in the same 2.4Ghz band.

Use the **no** form of the command to disable the SSID or to disable SSID features.

This example shows how to:

- Name an SSID
- Configure the SSID for RADIUS accounting
- Set the maximum number of client devices that can associate using this SSID to 15
- Assign the SSID to a VLAN
- Assign the SSID to a radio interface

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config-ssid)# accounting accounting-method-list
AP(config-ssid)# max-associations 15
AP(config-ssid)# vlan 3762
AP(config-ssid)# exit
AP(config)# interface dot11radio 0
AP(config-if)# ssid batman
AP(config-if)#end
```

Viewing SSIDs Configured Globally

Use this command to view configuration details for SSIDs that are configured globally:

```
AP# show running-config ssid ssid-string
```

Using a RADIUS Server to Restrict SSIDs

To prevent client devices from associating to the access point using an unauthorized SSID, you can create a list of authorized SSIDs that clients must use on your RADIUS authentication server.

The SSID authorization process consists of these steps:

1. A client device associates to the access point using any SSID configured on the access point.
2. The client begins RADIUS authentication.
3. The RADIUS server returns a list of SSIDs that the client is allowed to use. The access point checks the list for a match of the SSID used by the client. There are three possible outcomes:
   a. If the SSID that the client used to associate to the access point matches an entry in the allowed list returned by the RADIUS server, the client is allowed network access after completing all authentication requirements.
   b. If the access point does not find a match for the client in the allowed list of SSIDs, the access point disassociates the client.
   c. If the RADIUS server does not return any SSIDs (no list) for the client, then the administrator has not configured the list, and the client is allowed to associate and attempt to authenticate.

The allowed list of SSIDs from the RADIUS server are in the form of Cisco VSAs. The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the access point and the RADIUS server by using the vendor-specific attribute

(attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. The Cisco vendor-ID is 9, and the supported option has vendor-type 1, which is named *cisco-avpair*. The Radius server is allowed to have zero or more SSID VSAs per client.

In this example, the following AV pair adds the SSID *batman* to the list of allowed SSIDs for a user:

```
cisco-avpair= "ssid=batman"
```

For instructions on configuring the access point to recognize and use VSAs, see the "Configuring the Access Point for Vendor-Proprietary RADIUS Server Communication" section on page 13-17".

Configuring Multiple Basic SSIDs

Access point 802.11a, 802.11g, 802.11n radios support up to 16 basic SSIDs (BSSIDs). The BSSID is the radio mac address associated to a given SSID (network name) string.

You use multiple SSIDs to assign a unique DTIM setting for each SSID to broadcast one beacon per SSID. A large DTIM value increases battery life for power-save client devices that use an SSID, and broadcasting multiple SSIDs makes your wireless LAN more accessible to guests.

Note Devices on your wireless LAN that are configured to associate to a specific access point based on the access point MAC address (for example, client devices, repeaters, hot standby units, or workgroup bridges) might lose their association when you add or delete a multiple BSSID. When you add or delete a multiple BSSID, check the association status of devices configured to associate to a specific access point. If necessary, reconfigure the disassociated device to use the new BSSID MAC address.

Requirements for Configuring Multiple BSSIDs

To configure multiple BSSIDs, your access points must meet these minimum requirements:

- VLANs must be configured
- Access points must run Cisco IOS Release 12.3(4)JA or later
- To determine the number of multiple basic SSIDs supported, enter the **show controllers** *radio_interface* command. The radio supports multiple basic SSIDs if the results include this line:

```
Number of supported simultaneous BSSID on radio_interface: 16
```

Guidelines for Using Multiple BSSIDs

Keep these guidelines in mind when configuring multiple BSSIDs:

- RADIUS-assigned VLANs are not supported when you enable multiple BSSIDs.
- When you enable BSSIDs, the access point automatically maps a BSSID to each SSID. You cannot manually map a BSSID to a specific SSID.
- When multiple BSSIDs are enabled on the access point, the optional SSIDL IE does not contain a list of SSIDs; it contains only extended capabilities.
- Any Wi-Fi certified client device can associate to an access point using multiple BSSIDs.

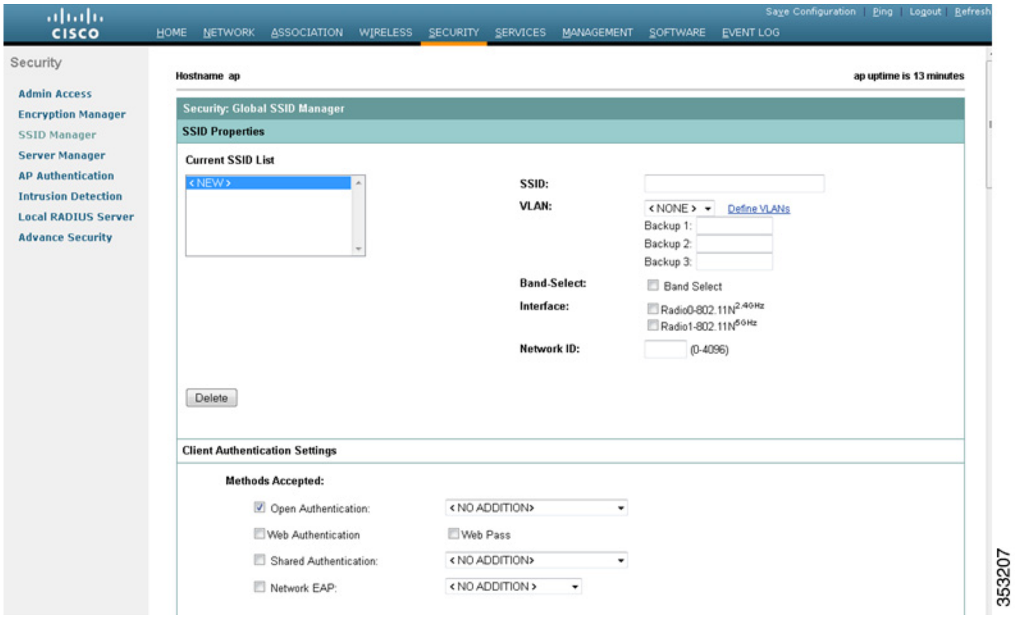
- You can enable multiple BSSIDs on access points that participate in WDS.

Configuring Multiple BSSIDs

Follow these steps to configure multiple BSSIDs (MBSSIDs):

Step 1 Browse to the Global SSID Manager page on the access point GUI. (If you use the CLI instead of the GUI, refer to the CLI commands listed in the CLI Configuration Example at the end of this section.) Figure 7-1 shows the top portion of the Global SSID Manager page.

Figure 7-1 Global SSID Manager Page



Hostname ap

ap uptime is 13 minutes

Security: Global SSID Manager

SSID Properties

Current SSID List

< NEW >

SSID:

VLAN: < NONE >

Backup 1:

Backup 2:

Backup 3:

Band-Select: □ Band Select

Interface: □ Radio0-802.11N$^{2.4GHz}$
□ Radio1-802.11N^{5GHz}

Network ID: (0-4096)

Client Authentication Settings

Methods Accepted:

☑ Open Authentication: < NO ADDITION>

□ Web Authentication □ Web Pass

□ Shared Authentication: < NO ADDITION>

□ Network EAP: < NO ADDITION >

Step 2 Enter the SSID name in the **SSID** field.

Step 3 Use the **VLAN** drop-down list to select the VLAN to which the SSID is assigned.

Step 4 Select the radio interfaces on which the SSID is enabled. The SSID remains inactive until you validate the SSID settings and enable the radio interface.

Step 5 (Optional) Enter a Network ID for the SSID in the **Network ID** field.

Step 6 Assign authentication, authenticated key management, and accounting settings to the SSID in the Authentication Settings, Authenticated Key Management, and Accounting Settings sections of the page. MBSSIDs support all the authentication types that are supported on SSIDs.

Step 7 (Optional) In the Multiple BSSID Beacon Settings section, select the **Set SSID as Guest Mode** check box to include the SSID in beacons.

Step 8 (Optional) To increase the battery life for power-save clients that use this SSID, select the **Set Data Beacon Rate (DTIM)** check box and enter a beacon rate for the SSID. The beacon rate determines how often the access point sends a beacon containing a Delivery Traffic Indicator Message (DTIM).

When client devices receive a beacon that contains a DTIM, they normally wake up to check for pending packets. Longer intervals between DTIMs let clients sleep longer and preserve power. Conversely, shorter DTIM periods reduce the delay in receiving packets but use more battery power because clients wake up more often.

The default beacon rate is 2, which means that every other beacon contains a DTIM. Enter a beacon rate between 1 and 100.

Note Increasing the DTIM period count delays the delivery of multicast packets. Because multicast packets are buffered, large DTIM period counts can cause a buffer overflow.

Step 9 In the Guest Mode/Infrastructure SSID Settings section, select **Multiple BSSID**.

Step 10 Click **Apply**.

CLI Configuration Example

This example shows the CLI commands that you use to enable multiple BSSIDs on a radio interface, create an SSID called *visitor*, designate the SSID as a BSSID, specify that the BSSID is included in beacons, set a DTIM period for the BSSID, and assign the SSID *visitor* to the radio interface:

```
ap(config)# interface do0
ap(config-if)# mbssid
ap(config-if)# exit
ap(config)# dot11 ssid visitor vlan20
ap(config-ssid)# mbssid guest-mode dtim-period 3
ap(config-ssid)# exit
ap(config)# interface do0
ap(config-if)# ssid visitor
```

You can also use the **dot11 mbssid** global configuration command to simultaneously enable multiple BSSIDs on all radio interfaces that support multiple BSSIDs.

Displaying Configured BSSIDs

Use the **show dot11 bssid** privileged EXEC command to display the relationship between SSIDs and BSSIDs or MAC addresses. This example shows the command output:

```
AP1230#show dot11 bssid
Interface     BSSID           Guest  SSID
Dot11Radio1   0011.2161.b7c0  Yes  atlantic
Dot11Radio0   0005.9a3e.7c0f  Yes  WPA2-TLS-g
```

Assigning IP Redirection for an SSID

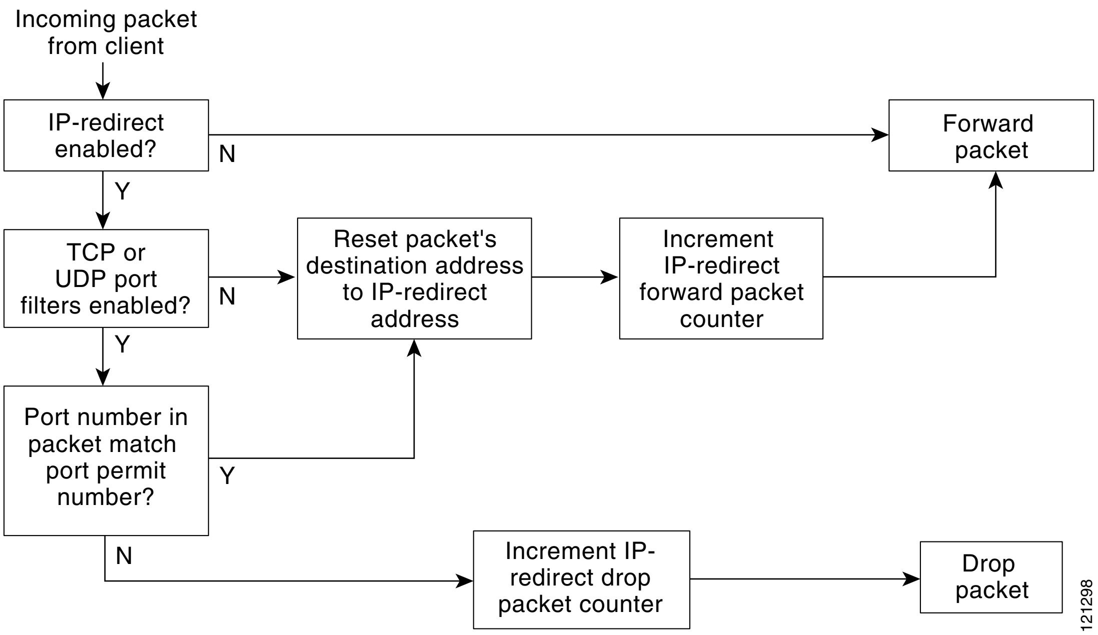
When you configure IP redirection for an SSID, the access point redirects all packets sent from client devices associated to that SSID to a specific IP address. IP redirection is used mainly on wireless LANs serving handheld devices that use a central software application and are statically configured to communicate with a specific IP address. For example, the wireless LAN administrator at a retail store or warehouse might configure IP redirection for its bar code scanners, which all use the same scanner application and all send data to the same IP address.

You can redirect all packets from client devices associated using an SSID or redirect only packets directed to specific TCP or UDP ports (as defined in an access control list). When you configure the access point to redirect only packets addressed to specific ports, the access point redirects those packets from clients using the SSID and drops all other packets from clients using the SSID.

Note When you perform a ping test from the access point to a client device that is associated using an IP-redirect SSID, the response packets from the client are redirected to the specified IP address and are not received by the access point.

Figure 7-2 shows the processing flow that occurs when the access point receives client packets from clients associated using an IP-redirect SSID.

Figure 7-2 Processing Flow for IP Redirection


Incoming packet from client
IP-redirect enabled?
N
Forward packet
Y
TCP or UDP port filters enabled?
N
Reset packet's destination address to IP-redirect address
Increment IP-redirect forward packet counter
Y
Port number in packet match port permit number?
Y
N
Increment IP-redirect drop packet counter
Drop packet
121298

Guidelines for Using IP Redirection

Keep these guidelines in mind when using IP redirection:

- The access point does not redirect broadcast, unicast, or multicast BOOTP/DHCP packets received from client devices.
- Existing ACL filters for incoming packets take precedence over IP redirection.

Configuring IP Redirection

Beginning in privileged EXEC mode, follow these steps to configure IP redirection for an SSID:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ssid** *ssid-string*	Enter configuration mode for a specific SSID.
Step 3	**ip redirection host** *ip-address*	Enter IP redirect configuration mode for the IP address. Enter the IP address with decimals, for example: 10.91.104.92 If you do not specify an access control list (ACL) which defines TCP or UDP ports for redirection, the access point redirects all packets that it receives from client devices.
Step 4	**ip redirection host** *ip-address* **access-group** *acl* **in**	(Optional) Specify an ACL to apply to the redirection of packets. Only packets sent to the specific UDP or TCP ports defined in the ACL are redirected. The access point discards all received packets that do not match the settings defined in the ACL. The **in** parameter specifies that the ACL is applied to the incoming interface for the access point.

Note ACL logging is not supported on the bridging interfaces of access point platforms. When applied on a bridging interface, it works as if the interface were configured without the log option, and logging does not take effect. However ACL logging does work for the BVI interfaces as long as a separate ACL is used for the BVI interface.

This example shows how to configure IP redirection for an SSID without applying an ACL. The access point redirects all packets that it receives from client devices associated to the SSID *batman*:

```
AP# configure terminal
AP(config)# dot11 ssid batman
AP(config-if-ssid)# ip redirection host 10.91.104.91
AP(config-if-ssid-redirect)# end
```

Including SSIDL IE in an SSID Beacon

The access point broadcasts one beacon per SSID. By default, only one of the SSID beacons will mention the relevant SSID name. The beacons for the other SSIDs on the same radio leave the SSID field empty, unless you use the MBSSID feature.

Note When multiple BSSIDs are enabled on the access point, the SSIDL IE does not contain a list of SSIDs; it contains only extended capabilities.

Beginning in privileged EXEC mode, follow these steps to include an SSIDL IE in an SSID beacon:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ssid** *ssid-string*	Enter configuration mode for a specific SSID. You are recommended to choose the SSID that is set to guest-mode (i.e. advertises its SSID string into its beacon)
Step 3	**information-element ssidl** [**advertisement**] [**wps**]	Include an SSIDL IE in the access point beacon that advertises the extended capabilities for the access point, such as 802.1x and support for Microsoft Wireless Provisioning Services (WPS). Use the **advertisement** option to include the SSID name and capabilities in the SSIDL IE. Use the **wps** option to set the WPS capability flag in the SSIDL IE.

Use the **no** form of the command to disable SSIDL IEs. By default SSIDL IEs are disabled.

NAC Support for MBSSID

Networks must be protected from security threats, such as viruses, worms, and spyware. These security threats disrupt business, causing downtime and continual patching. Endpoint visibility and control is needed to help ensure that all wired and wireless devices attempting to access a network meet corporate security policies. Infected or vulnerable endpoints need to be automatically detected, isolated, and cleaned.

NAC is designed specifically to help ensure that all wired and wireless endpoint devices (such as PCs, laptops, servers, and PDAs) accessing network resources are adequately protected from security threats. NAC allows organizations to analyze and control all devices coming into the network. By ensuring that every endpoint device complies with corporate security policy and is running the latest and most relevant security protections, organizations can significantly reduce or eliminate endpoint devices as a common source of infection or network compromise.

WLANs need to be protected from security threats such as viruses, worms, and spyware. Both the NAC Appliance and the NAC Framework provide security threat protection for WLANs by enforcing device security policy compliance when WLAN clients attempt to access the network. These solutions quarantine non-compliant WLAN clients and provide remediation services to help ensure compliance.

A client, based on its health (software version, virus version, and so on) is placed on a separate VLAN that is specified to download the required software to upgrade the client to the software versions required to access the network. Four VLANs are specified for NAC support, one of which is the normal VLAN where clients having the correct software version are placed. The other VLANs are reserved for specific quarantine action and all infected clients are placed on one of these VLANs until the client is upgraded.

Each SSID has up to 3 additional VLANs configured as “unhealthy” VLANs. Infected clients are placed on one of these VLANs, based on how the client is infected. When a client sends an association request, it includes its infected status in the request to the RADIUS server. The policy to place the client on a specific VLAN is provisioned on the RADIUS server.

When an infected client associates with an access point and sends its state to the RADIUS server, the RADIUS server puts it into one of the quarantine VLANs based on its health. This VLAN is sent in the RADIUS server Access Accept response during the dot1x client authentication process. If the client is healthy and NAC compliant, the RADIUS server returns a normal VLAN assignment for the SSID and the client is placed in the correct VLAN and BSSID.

Each SSID is assigned a normal VLAN, which is the VLAN on which healthy clients are placed. The SSID can also be configured to have up to 3 backup VLANs that correspond to the quarantine VLANs on which clients are placed based on their state of health. These VLANs for the SSID use the same BSSID as assigned by the MBSSID for the SSID.

The configured VLANs are different and no VLAN overlap within an SSID is allowed. Therefore, a VLAN can be specified once and cannot be part of 2 different SSIDs per interface.

Quarantine VLANs are automatically configured under the interface on which the normal VLAN is configured. A quarantine VLAN inherits the same encryption properties as that of the normal VLAN. VLANs have the same key/authentication type and the keys for the quarantine VLANs are derived automatically.

Dot11 sub-interfaces are generated and configured automatically along with the dot1q encapsulation VLAN (equal to the number of configured VLANs). The sub-interfaces on the wired side is also configured automatically along with the bridge-group configurations under the Gigabit Ethernet 0 sub-interface.

When a client associates and the RADIUS server determines that it is unhealthy, the server returns one of the quarantine NAC VLANs in its RADIUS authentication response for dot1x authentication. This VLAN should be one of the configured backup VLANs under the client SSID. If the VLAN is not one of the configured backup VLANs, the client is disassociated.

Data corresponding to the all the backup VLANs are sent and received using the BSSID that is assigned to the SSID. Therefore, all clients (healthy and unhealthy) listening to the BSSID corresponding the the SSID wake up. Based on the multicast key being used corresponding to the VLAN (healthy or unhealthy), packet decrypting takes place on the client. Wired side traffic is segregated because different VLANs are used, thereby ensuring that traffic from infected and uninfected clients do not mix.

A new keyword, **backup**, is added to the existing **vlan** <*name*> | <*id*> under **dot11 ssid** <*ssid*> as described below:

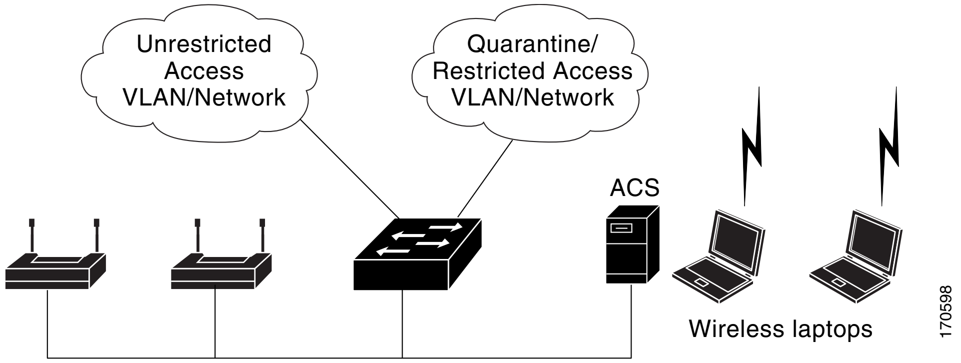
```
vlan <name>|<id> [backup <name>|<id>, <name>|<id>, <name>|<id>
```

Configuring NAC for MBSSID

Note This feature supports only Layer 2 mobility within VLANs. Layer 3 mobility using network ID is not supported in this feature.

Note Before you attempt to enable NAC for MBSSID on your access points, you should first have NAC working properly. Figure 7-3 shows a typical network setup.

Figure 7-3 Typical NAC Network Setup


Unrestricted Access VLAN/Network
Quarantine/ Restricted Access VLAN/Network
ACS
Wireless laptops
170598

For additional information, see the documentation for deploying NAC for Cisco wireless networks.

Follow these steps to configure NAC for MBSSID on your access point:

Step 1 Configure your network as shown in Figure 7-3.

Step 2 Configure standalone access points and NAC-enabled client-EAP authentication.

Step 3 Configure the local profiles on the ACS server for posture validation.

Step 4 Configure the client and access point to allow the client to successful authenticate using EAP-FAST.

Step 5 Ensure that the client posture is valid.

Step 6 Verify that the client associates to the access point and that the client is placed on the unrestricted VLAN after successful authentication and posture validation.

A sample configuration is shown below.

```
dot11 mbssid
dot11 vlan-name engg-normal vlan 100
dot11 vlan-name engg-infected vlan 102
dot11 vlan-name mktg-normal vlan 101
dot11 vlan-name mktg-infected1 vlan 103
dot11 vlan-name mktg-infected2 vlan 104
dot11 vlan-name mktg-infected3 vlan 105
!
dot11 ssid engg
    vlan engg-normal backup engg-infected
    authentication open
    authentication network-eap eap_methods
!
dot11 ssid mktg
    vlan mktg-normal backup mktg-infected1, mktg-infected2, mktg-infected3
    authentication open
    authentication network-eap eap_methods
!
interface Dot11Radio0
!
encryption vlan engg-normal key 1 size 40bit 7 482CC74122FD transmit-key
encryption vlan engg-normal mode ciphers wep40
!
encryption vlan mktg-normal key 1 size 40bit 7 9C3A6F2CBFBC transmit-key
encryption vlan mktg-normal mode ciphers wep40
!
ssid engg
!
ssid mktg
!
speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
station-role root
!
interface Dot11Radio0.100
encapsulation dot1Q 100 native
no ip route-cache
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio0.102
encapsulation dot1Q 102
no ip route-cache
bridge-group 102
bridge-group 102 subscriber-loop-control
bridge-group 102 block-unknown-source
no bridge-group 102 source-learning
no bridge-group 102 unicast-flooding
bridge-group 102 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface FastEthernet0.100
encapsulation dot1Q 100 native
no ip route-cache
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface FastEthernet0.102
encapsulation dot1Q 102
no ip route-cache
bridge-group 102
no bridge-group 102 source-learning
bridge-group 102 spanning-disabled
!
```

CHAPTER 8

Configuring Spanning Tree Protocol

This chapter descibes how to configure Spanning Tree Protocol (STP) on your access point/bridge.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference for Access Points and Bridges* of this release.

Note STP is available only when the access point is in bridge mode.

Understanding Spanning Tree Protocol

This section describes how spanning-tree features work. It includes this information:

STP Overview

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or to a LAN of multiple segments.

When you create fault-tolerant internetworks, you must have a loop-free path between all nodes in a network. The spanning-tree algorithm calculates the best loop-free path throughout a Layer 2 network. Infrastructure devices such as wireless access point/bridges and switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The devices do not forward these frames but use them to construct a loop-free path.

Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Infrastructure devices might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network.

STP defines a tree with a root bridge and a loop-free path from the root to all infrastructure devices in the Layer 2 network.

Note STP discussions use the term *root* to describe two concepts: the bridge on the network that serves as a central point in the spanning tree is called the *root bridge*, and the port on each bridge that provides the most efficient path to the root bridge is called the *root port*. These meanings are separate from the Role in radio network setting that includes root and non-root options. A bridge whose Role in radio network setting is Root Bridge does not necessarily become the root bridge in the spanning tree. In this chapter, the root bridge in the spanning tree is called the *spanning-tree root*.

STP forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path.

When two interfaces on a bridge are part of a loop, the spanning-tree port priority and path cost settings determine which interface is put in the forwarding state and which is put in the blocking state. The port priority value represents the location of an interface in the network topology and how well it is located to pass traffic. The path cost value represents media speed.

The access point/bridge supports both per-VLAN spanning tree (PVST) and a single 802.1q spanning tree without VLANs. The access point/bridge cannot run 802.1s MST or 802.1d Common Spanning Tree, which maps multiple VLANs into a one-instance spanning tree.

The access point/bridge maintains a separate spanning-tree instance for each active VLAN configured on it. A bridge ID, consisting of the bridge priority and the access point/bridge MAC address, is associated with each instance. For each VLAN, the access point/bridge with the lowest access point/bridge ID becomes the spanning-tree root for that VLAN.

Access Point/Bridge Protocol Data Units

The stable, active spanning-tree topology of your network is determined by these elements:

- The unique access point/bridge ID (wireless access point/bridge priority and MAC address) associated with each VLAN on each wireless access point/bridge
- The spanning-tree path cost to the spanning-tree root
- The port identifier (port priority and MAC address) associated with each Layer 2 interface

When the access point/bridges in a network are powered up, each access point/bridge functions as the STP root. The access point/bridges send configuration BPDUs through the Ethernet and radio ports. The BPDUs communicate and compute the spanning-tree topology. Each configuration BPDU contains this information:

- The unique access point/bridge ID of the wireless access point/bridge that the sending access point/bridge identifies as the spanning-tree root
- The spanning-tree path cost to the root
- The access point/bridge ID of the sending access point/bridge
- Message age
- The identifier of the sending interface
- Values for the hello, forward delay, and max-age protocol timers

When a access point/bridge receives a configuration BPDU that contains *superior* information (lower access point/bridge ID, lower path cost, and so forth), it stores the information for that port. If this BPDU is received on the root port of the access point/bridge, the access point/bridge also forwards it with an updated message to all attached LANs for which it is the designated access point/bridge.

If a access point/bridge receives a configuration BPDU that contains *inferior* information to that currently stored for that port, it discards the BPDU. If the access point/bridge is a designated access point/bridge for the LAN from which the inferior BPDU was received, it sends that LAN a BPDU containing the up-to-date information stored for that port. In this way, inferior information is discarded, and superior information is propagated on the network.

A BPDU exchange results in these actions:

- One access point/bridge is elected as the spanning-tree root.
- A root port is selected for each access point/bridge (except the spanning-tree root). This port provides the best path (lowest cost) when the access point/bridge forwards packets to the spanning-tree root.
- The shortest distance to the spanning-tree root is calculated for each access point/bridge based on the path cost.
- A designated access point/bridge for each LAN segment is selected. The designated access point/bridge incurs the lowest path cost when forwarding packets from that LAN to the spanning-tree root. The port through which the designated access point/bridge is attached to the LAN is called the *designated port*.

- Interfaces included in the spanning-tree instance are selected. Root ports and designated ports are put in the forwarding state.
- All interfaces not included in the spanning tree are blocked.

Election of the Spanning-Tree Root

All access point/bridges in the Layer 2 network participating in STP gather information about other access point/bridges in the network through an exchange of BPDU data messages. This exchange of messages results in these actions:

- The election of a unique spanning-tree root for each spanning-tree instance
- The election of a designated access point/bridge for every LAN segment
- The removal of loops in the network by blocking Layer 2 interfaces connected to redundant links

For each VLAN, the access point/bridge with the highest access point/bridge priority (the lowest numerical priority value) is elected as the spanning-tree root. If all access point/bridges are configured with the default priority (32768), the access point/bridge with the lowest MAC address in the VLAN becomes the spanning-tree root. The access point/bridge priority value occupies the most significant bits of the access point/bridge ID.

When you change the access point/bridge priority value, you change the probability that the access point/bridge will be elected as the root access point/bridge. Configuring a higher value decreases the probability; a lower value increases the probability.

The spanning-tree root is the logical center of the spanning-tree topology. All paths that are not needed to reach the spanning-tree root from anywhere in the network are placed in the spanning-tree blocking mode.

BPDUs contain information about the sending access point/bridge and its ports, including access point/bridge and MAC addresses, access point/bridge priority, port priority, and path cost. STP uses this information to elect the spanning-tree root and root port for the network and the root port and designated port for each LAN segment.

Spanning-Tree Timers

Table 8-1 describes the timers that affect the entire spanning-tree performance.

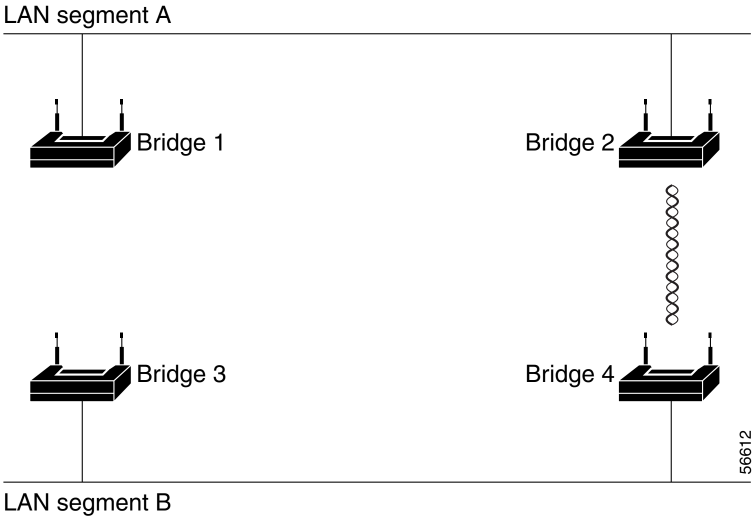
Table 8-1 Spanning-Tree Timers

Variable	Description
Hello timer	Determines how often the access point/bridge broadcasts hello messages to other access point/bridges.
Forward-delay timer	Determines how long each of the listening and learning states last before the interface begins forwarding.
Maximum-age timer	Determines the amount of time the access point/bridge stores protocol information received on an interface.

Creating the Spanning-Tree Topology

In Figure 8-1, bridge 4 is elected as the spanning-tree root because the priority of all the access point/bridges is set to the default (32768) and bridge 4 has the lowest MAC address. However, because of traffic patterns, number of forwarding interfaces, or link types, bridge 4 might not be the ideal spanning-tree root. By increasing the priority (lowering the numerical value) of the ideal bridge so that it becomes the spanning-tree root, you force a spanning-tree recalculation to form a new topology with the ideal bridge as the spanning-tree root.

Figure 8-1 Spanning-Tree Topology



Spanning-Tree Interface States

Propagation delays can occur when protocol information passes through a wireless LAN. As a result, topology changes can take place at different times and at different places in the network. When an interface transitions directly from nonparticipation in the spanning-tree topology to the forwarding state, it can create temporary data loops. Interfaces must wait for new topology information to propagate through the LAN before starting to forward frames. They must allow the frame lifetime to expire for forwarded frames that have used the old topology.

Each interface on a access point/bridge using spanning tree exists in one of these states:

- Blocking—The interface does not participate in frame forwarding.
- Listening—The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.
- Learning—The interface prepares to participate in frame forwarding.
- Forwarding—The interface forwards frames.
- Disabled—The interface is not participating in spanning tree because of a shutdown port, no link on the port, or no spanning-tree instance running on the port.

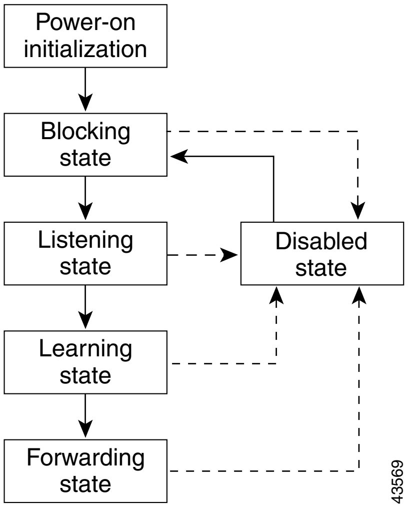
An interface moves through these states:

- From initialization to blocking

- From blocking to listening or to disabled
- From listening to learning or to disabled
- From learning to forwarding or to disabled
- From forwarding to disabled

Figure 8-2 illustrates how an interface moves through the states.

Figure 8-2 Spanning-Tree Interface States



When you enable STP on the access point/bridge, the Ethernet and radio interfaces go through the blocking state and the transitory states of listening and learning. Spanning tree stabilizes each interface at the forwarding or blocking state.

When the spanning-tree algorithm places a Layer 2 interface in the forwarding state, this process occurs:

1. The interface is in the listening state while spanning tree waits for protocol information to transition the interface to the blocking state.
2. While spanning tree waits the forward-delay timer to expire, it moves the interface to the learning state and resets the forward-delay timer.
3. In the learning state, the interface continues to block frame forwarding as the access point/bridge learns end-station location information for the forwarding database.
4. When the forward-delay timer expires, spanning tree moves the interface to the forwarding state, where both learning and frame forwarding are enabled.

Blocking State

An interface in the blocking state does not participate in frame forwarding. After initialization, a BPDU is sent to the access point/bridge's Ethernet and radio ports. A access point/bridge initially functions as the spanning-tree root until it exchanges BPDUs with other access point/bridges. This exchange establishes which access point/bridge in the network is the spanning-tree root. If there is only one access point/bridge in the network, no exchange occurs, the forward-delay timer expires, and the interfaces move to the listening state. An interface always enters the blocking state when you enable STP.

An interface in the blocking state performs as follows:

- Discards frames received on the port
- Does not learn addresses
- Receives BPDUs

Note If a access point/bridge port is blocked, some broadcast or multicast packets can reach a forwarding port on the access point/bridge and cause the bridging logic to switch the blocked port into listening state momentarily before the packets are dropped at the blocked port.

Listening State

The listening state is the first state an interface enters after the blocking state. The interface enters this state when STP determines that the interface should participate in frame forwarding.

An interface in the listening state performs as follows:

- Discards frames received on the port
- Does not learn addresses
- Receives BPDUs

Learning State

An interface in the learning state prepares to participate in frame forwarding. The interface enters the learning state from the listening state.

An interface in the learning state performs as follows:

- Discards frames received on the port
- Learns addresses
- Receives BPDUs

Forwarding State

An interface in the forwarding state forwards frames. The interface enters the forwarding state from the learning state.

An interface in the forwarding state performs as follows:

- Receives and forwards frames received on the port
- Learns addresses
- Receives BPDUs

Disabled State

An interface in the disabled state does not participate in frame forwarding or in the spanning tree. An interface in the disabled state is nonoperational.

A disabled interface performs as follows:

- Discards frames received on the port
- Does not learn addresses

- Does not receive BPDUs

Configuring STP Features

You complete three major steps to configure STP on the access point/bridge:

1. If necessary, assign interfaces and sub-interfaces to bridge groups
2. Enable STP for each bridge group
3. Set the STP priority for each bridge group

These sections include spanning-tree configuration information:

- Default STP Configuration, page 8-8
- Configuring STP Settings, page 8-9
- STP Configuration Examples, page 8-10

Default STP Configuration

STP is disabled by default. Table 8-2 lists the default STP settings when you enable STP.

Table 8-2 Default STP Values When STP is Enabled

Setting	Default Value
Bridge priority	32768
Bridge max age	20
Bridge hello time	2
Bridge forward delay	15
Ethernet port path cost	19
Ethernet port priority	128
Radio port path cost	33
Radio port priority	128

The radio and Ethernet interfaces and the native VLAN on the access point/bridge are assigned to bridge group 1 by default. When you enable STP and assign a priority on bridge group 1, STP is enabled on the radio and Ethernet interfaces and on the primary VLAN, and those interfaces adopt the priority assigned to bridge group 1. You can create bridge groups for sub-interfaces and assign different STP settings to those bridge groups.

Configuring STP Settings

Beginning in privileged EXEC mode, follow these steps to configure STP on the access point/bridge:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface { dot11radio** *number* | **fastethernet** *number* | GigabitEthernet *number*}	Enter interface configuration mode for radio or Ethernet interfaces or sub-interfaces. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1. The fast Ethernet interface is 0.
Step 3	**bridge-group** *number*	Assign the interface to a bridge group. You can number your bridge groups from 1 to 255.
Step 4	**no bridge-group** *number* **spanning-disabled**	Counteract the command that automatically disables STP for a bridge group. STP is enabled on the interface when you enter the **bridge** *n* **protocol ieee** command.
Step 5	**exit**	Return to global configuration mode.
Step 6	**bridge** *number* **protocol ieee**	Enable STP for the bridge group. You must enable STP on each bridge group that you create with **bridge-group** commands.
Step 7	**bridge** *number* **priority** *priority*	(Optional) Assign a priority to a bridge group. The lower the priority, the more likely it is that the bridge becomes the spanning-tree root.
Step 8	**end**	Return to privileged EXEC mode.
Step 9	**show spanning-tree bridge**	Verify your entries.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

STP Configuration Examples

These configuration examples show how to enable STP on root and non-root access point/bridges with and without VLANs:

- Root Bridge Without VLANs, page 8-10
- Non-Root Bridge Without VLANs, page 8-11
- Root Bridge with VLANs, page 8-12
- Non-Root Bridge with VLANs, page 8-14

Root Bridge Without VLANs

This example shows the configuration of a root bridge with no VLANs configured and with STP enabled:

```
hostname master-bridge-south
!
dot11 syslog
!
dot11 ssid visitor
!
dot11 ssid visitor2
!
dot11 guest
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid visitor
 !
 antenna gain 0
 stbc
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 ssid visitor2
 !
 antenna gain 0
 peakdetect
 dfs band 3 block
 stbc
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
```

```
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 priority 9000
bridge 1 protocol ieee
bridge 1 route ip
!
line con 0
line vty 0 4
 login local
 transport input all
!
end
```

Non-Root Bridge Without VLANs

This example shows the configuration of a non-root bridge with no VLANs configured with STP enabled:

```
hostname client-bridge-north
!
dot11 syslog
!
dot11 ssid visitor
!
dot11 ssid visitor2
!
dot11 guest
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid visitor
 !
 antenna gain 0
 stbc
 station-role non-root
 bridge-group 1
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
 ssid visitor2
 !
 antenna gain 0
 peakdetect
 stbc
 station-role non-root
 bridge-group 1
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 path-cost 40
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 priority 10000
bridge 1 protocol ieee
bridge 1 route ip
!
line con 0
line vty 0 4
 login local
 transport input all
!
End
```

Root Bridge with VLANs

This example shows the configuration of a root bridge with VLANs configured with STP enabled:

```
hostname master-bridge-hq
!
dot11 syslog
!
dot11 ssid vlan1
   vlan 1
   authentication open
!
dot11 guest
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid vlan1
 !
 antenna gain 0
 stbc
 station-role root
!
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
!
interface Dot11Radio0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 path-cost 500
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 antenna gain 0
 peakdetect
 dfs band 3 block
 channel dfs
 station-role root
!
interface Dot11Radio1.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
!
interface Dot11Radio1.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 subscriber-loop-control
 bridge-group 3 path-cost 500
 bridge-group 3 block-unknown-source
 no bridge-group 3 source-learning
 no bridge-group 3 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
!
interface GigabitEthernet0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
!
interface GigabitEthernet0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
 no bridge-group 2 source-learning
!
interface GigabitEthernet0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 no bridge-group 3 source-learning
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 priority 9000
bridge 1 protocol ieee
bridge 1 route ip
bridge 2 priority 10000
bridge 2 protocol ieee
bridge 3 priority 3100
bridge 3 protocol ieee
!
line con 0
line vty 0 4
 login local
 transport input all
!
end
```

Non-Root Bridge with VLANs

This example shows the configuration of a non-root bridge with VLANs configured with STP enabled:

```
hostname client-bridge-remote
!
dot11 syslog
!
dot11 ssid vlan1
   vlan 1
   authentication open
!
dot11 guest
!
bridge irb
!
interface Dot11Radio0
```

```
 no ip address
 no ip route-cache
 !
 ssid vlan1
 !
 antenna gain 0
 stbc
 station-role non-root
!
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
!
interface Dot11Radio0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
!
interface Dot11Radio0.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 antenna gain 0
 peakdetect
 station-role non-root
!
interface Dot11Radio1.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
!
interface Dot11Radio1.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
!
interface Dot11Radio1.3
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 path-cost 500
!
interface GigabitEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
!
interface GigabitEthernet0.1
 encapsulation dot1Q 1 native
 no ip route-cache
 bridge-group 1
!
interface GigabitEthernet0.2
 encapsulation dot1Q 2
 no ip route-cache
 bridge-group 2
!
interface GigabitEthernet0.3
```

```
 encapsulation dot1Q 3
 no ip route-cache
 bridge-group 3
 bridge-group 3 path-cost 400
!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
bridge 1 priority 10000
bridge 1 protocol ieee
bridge 1 route ip
bridge 2 priority 12000
bridge 2 protocol ieee
bridge 3 priority 2900
bridge 3 protocol ieee
!
line con 0
line vty 0 4
 login local
 transport input all
!
end
```

Displaying Spanning-Tree Status

To display the spanning-tree status, use one or more of the privileged EXEC commands in Table 8-3.

Table 8-3 Commands for Displaying Spanning-Tree Status

Command	Purpose
show spanning-tree	Displays information on your network's spanning tree.
show spanning-tree blocked-ports	Displays a list of blocked ports on this bridge.
show spanning-tree bridge	Displays status and configuration of this bridge.
show spanning-tree active	Displays spanning-tree information on active interfaces only.
show spanning-tree root	Displays a detailed summary of information on the spanning-tree root.
show spanning-tree interface *interface-id*	Displays spanning-tree information for the specified interface.
show spanning-tree summary [**totals**]	Displays a summary of port states or displays the total lines of the STP state section.

For information about other keywords for the **show spanning-tree** privileged EXEC command, refer to the *Cisco Aironet IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release.

CHAPTER 9

Configuring an Access Point as a Local Authenticator

This chapter describes how to configure the access point as a local authenticator to serve as a stand-alone authenticator for a small wireless LAN or to provide backup authentication service. As a local authenticator, the access point performs LEAP, EAP-FAST, and MAC-based authentication for up to 50 client devices.

Understanding Local Authentication

Many small wireless LANs that could be made more secure with 802.1x authentication do not have access to a RADIUS server. On many wireless LANs that use 802.1x authentication, access points rely on RADIUS servers housed in a distant location to authenticate client devices, and the authentication traffic must cross a WAN link. If the WAN link fails, or if the access points cannot access the RADIUS servers for any reason, client devices cannot access the wireless network even if the work they wish to do is entirely local.

To provide local authentication service or backup authentication service in case of a WAN link or a server failure, you can configure an access point to act as a local authentication server. The access point can authenticate up to 50 wireless client devices using LEAP, EAP-FAST, or MAC-based authentication. The access point performs up to 5 authentications per second.

You configure the local authenticator access point manually with client usernames and passwords because it does not synchronize its database with the main RADIUS servers. You can also specify a VLAN and a list of SSIDs that a client is allowed to use.

Note If your wireless LAN contains only one access point, you can configure the access point as both the 802.1x authenticator and the local authenticator. However, users associated to the local authenticator access point might notice a drop in performance when the access point authenticates client devices.

You can configure your access points to use the local authenticator when they cannot reach the main servers, or you can configure your access points to use the local authenticator or as the main authenticator if you do not have a RADIUS server. When you configure the local authenticator as a backup to your main servers, the access points periodically check the link to the main servers and stop using the local authenticator automatically when the link to the main servers is restored.

Caution The access point you use as an authenticator contains detailed authentication information for your wireless LAN, so you should secure it physically to protect its configuration.

Configuring a Local Authenticator

This section provides instructions for setting up an access point as a local authenticator and includes these sections:

- Guidelines for Local Authenticators, page 9-3
- Configuration Overview, page 9-3
- Configuring the Local Authenticator Access Point, page 9-3
- Configuring Other Access Points to Use the Local Authenticator, page 9-6
- Configuring EAP-FAST Settings, page 9-7
- Unblocking Locked Usernames, page 9-9
- Viewing Local Authenticator Statistics, page 9-9
- Using Debug Messages, page 9-10

Guidelines for Local Authenticators

Follow these guidelines when configuring an access point as a local authenticator:

- Use an access point that does not serve a large number of client devices. When the access point acts as an authenticator, performance might degrade for associated client devices.
- Secure the access point physically to protect its configuration.

Configuration Overview

You complete four major steps when you set up a local authenticator:

1. On the local authenticator, create a list of access points authorized to use the authenticator to authenticate client devices. Each access point that uses the local authenticator is a network access server (NAS).

   Note If your local authenticator access point also serves client devices, you must enter the local authenticator access point as a NAS. When a client associates to the local authenticator access point, the access point uses itself to authenticate the client.

2. On the local authenticator, create user groups and configure parameters to be applied to each group (optional).
3. On the local authenticator, create a list of up to 50 LEAP users, EAP-FAST users, or MAC addresses that the local authenticator is authorized to authenticate.

   Note You do not have to specify which type of authentication that you want the local authenticator to perform. It automatically performs LEAP, EAP-FAST, or MAC-address authentication for the users in its user database.

4. On the access points that use the local authenticator, enter the local authenticator as a RADIUS server.

   Note If your local authenticator access point also serves client devices, you must enter the local authenticator as a RADIUS server in the local authenticator's configuration. When a client associates to the local authenticator access point, the access point uses itself to authenticate the client.

Configuring the Local Authenticator Access Point

Beginning in Privileged Exec mode, follow these steps to configure the access point as a local authenticator:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable NEW access control commands and functions.

	Command	Purpose
Step 3	**radius-server local**	Enable the access point as a local authenticator and enter configuration mode for the authenticator.
Step 4	**nas** *ip-address* **key** *shared-key*	Add an access point to the list of units that use the local authenticator. Enter the access point's IP address and the shared key used to authenticate communication between the local authenticator and other access points. You must enter this shared key on the access points that use the local authenticator. If your local authenticator also serves client devices, you must enter the local authenticator access point as a NAS. **Note** Leading spaces in the key string are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. Repeat this step to add each access point that uses the local authenticator.
Step 5	**group** *group-name*	(Optional) Enter user group configuration mode and configure a user group to which you can assign shared settings.
Step 6	**vlan** *vlan*	(Optional) Specify a VLAN to be used by members of the user group. The access point moves group members into that VLAN, overriding other VLAN assignments. You can assign only one VLAN to the group.
Step 7	**ssid** *ssid*	(Optional) Enter up to 16 SSIDs to limit members of the user group to those SSIDs. The access point checks that the SSID that the client used to associate matches one of the SSIDs in the list. If the SSID does not match, the client is disassociated.
Step 8	**reauthentication time** *seconds*	(Optional) Enter the number of seconds after which access points should reauthenticate members of the group. The reauthentication provides users with a new encryption key. The default setting is 0, which means that group members are never required to reauthenticate.
Step 9	**block count** *count* **time** { *seconds* | **infinite** }	(Optional) To help protect against password guessing attacks, you can lock out members of a user group for a length of time after a set number of incorrect passwords. • count—The number of failed passwords that triggers a lockout of the username. • time—The number of seconds the lockout should last. If you enter **infinite**, an administrator must manually unblock the locked username. See the "Unblocking Locked Usernames" section on page 9-9 for instructions on unblocking client devices.
Step 10	**exit**	Exit group configuration mode and return to authenticator configuration mode.

	Command	Purpose
Step 11	**user** *username* { **password** | **nthash** } *password* [**group** *group-name*] [**mac-auth-only**]	Enter the LEAP and EAP-FAST users allowed to authenticate using the local authenticator. You must enter a username and password for each user. If you only know the NT value of the password, which you can often find in the authentication server database, you can enter the NT hash as a string of hexadecimal digits. To add a client device for MAC-based authentication, enter the client's MAC address as both the username and password. Enter 12 hexadecimal digits without a dot or dash between the numbers as the username and the password. For example, for the MAC address 0009.5125.d02b, enter *00095125d02b* as both the username and the password. To limit the user to MAC authentication only, enter **mac-auth-only**. To add the user to a user group, enter the group name. If you do not specify a group, the user is not assigned to a specific VLAN and is never forced to reauthenticate.
Step 12	**end**	Return to privileged EXEC mode.
Step 13	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to set up a local authenticator used by three access points with three user groups and several users:

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# radius-server local
AP(config-radsrv)# nas 10.91.6.159 key 110337
AP(config-radsrv)# nas 10.91.6.162 key 110337
AP(config-radsrv)# nas 10.91.6.181 key 110337
AP(config-radsrv)# group clerks
AP(config-radsrv-group)# vlan 87
AP(config-radsrv-group)# ssid batman
AP(config-radsrv-group)# ssid robin
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group cashiers
AP(config-radsrv-group)# vlan 97
AP(config-radsrv-group)# ssid deer
AP(config-radsrv-group)# ssid antelope
AP(config-radsrv-group)# ssid elk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# group managers
AP(config-radsrv-group)# vlan 77
AP(config-radsrv-group)# ssid mouse
AP(config-radsrv-group)# ssid chipmunk
AP(config-radsrv-group)# reauthentication time 1800
AP(config-radsrv-group)# block count 2 time 600
AP(config-radsrv-group)# exit
AP(config-radsrv)# user jsmith password twain74 group clerks
AP(config-radsrv)# user stpatrick password snake100 group clerks
AP(config-radsrv)# user nick password uptown group clerks
AP(config-radsrv)# user 00095125d02b password 00095125d02b group clerks mac-auth-only
AP(config-radsrv)# user 00095125d02b password 00095125d02b group cashiers
AP(config-radsrv)# user 00079431f04a password 00079431f04a group cashiers
AP(config-radsrv)# user carl password 272165 group managers
AP(config-radsrv)# user vic password lid178 group managers
AP(config-radsrv)# end
```

Configuring Other Access Points to Use the Local Authenticator

You add the local authenticator to the list of servers on the access point the same way that you add other servers. For detailed instructions on setting up RADIUS servers on your access points, see Chapter 13, "Configuring RADIUS and TACACS+ Servers."

Note If your local authenticator access point also serves client devices, you must configure the local authenticator to use itself to authenticate client devices.

On the access points that use the local authenticator, use the **radius-server host** command to enter the local authenticator as a RADIUS server. The order in which the access point attempts to use the servers matches the order in which you enter the servers in the access point configuration. If you are configuring the access point to use RADIUS for the first time, enter the main RADIUS servers first, and enter the local authenticator last.

Note You must enter **1812** or **1645** as the authentication port and **1813** or **1646** as the accounting port. The local authenticator listens on UDP port 1813 for RADIUS accounting packets. It discards the accounting packets but sends acknowledge packets back to RADIUS clients to prevent clients from assuming that the server is down.

Use the **radius-server deadtime** command to set an interval during which the access point does not attempt to use servers that do not respond, thus avoiding the wait for a request to time out before trying the next configured server. A server marked as dead is skipped by additional requests for the duration of minutes that you specify, up to 1440 (24 hours).

This example shows how to set up two main servers and a local authenticator with a server deadtime of 10 minutes:

```
AP(config)# aaa new-model
AP(config)# radius server radserv
AP(config-radius-server)# address ipv4 172.10.0.1 auth-port 1000 acct-port 1001
AP(config-radius-server)# key 77654
AP(config)# radius-server deadtime 10
```

In this example, if the WAN link to the main servers fails, the access point completes these steps when a LEAP-enabled client device associates:

1. It tries the first server, times out multiple times, and marks the first server as dead.
2. It tries the second server, times out multiple times, and marks the second server as dead.
3. It tries and succeeds using the local authenticator.

If another client device needs to authenticate during the 10-minute dead-time interval, the access point skips the first two servers and tries the local authenticator first. After the dead-time interval, the access point tries to use the main servers for authentication. When setting a dead time, you must balance the need to skip dead servers with the need to check the WAN link and begin using the main servers again as soon as possible.

Each time the access point tries to use the main servers while they are down, the client device trying to authenticate might report an authentication timeout. The client device retries and succeeds when the main servers time out and the access point tries the local authenticator. You can extend the timeout value on Cisco client devices to accommodate expected server timeouts.

To remove the local authenticator from the access point configuration, use the **no radius server** ***radserv*** global configuration command.

Configuring EAP-FAST Settings

The default settings for EAP-FAST authentication are suitable for most wireless LANs. However, you can customize the credential timeout values, authority ID, and server keys to match your network requirements.

Configuring PAC Settings

This section describes how to configure Protected Access Credential (PAC) settings. The first time that an EAP-FAST client device attempts to authenticate to the local authenticator, the local authenticator generates a PAC for the client. You can also generate PACs manually and import PAC files manually on the client.

PAC Expiration Times

You can limit the number of days for which PACs are valid, and a grace period during which PACs are valid after they have expired. By default, PACs are valid for 2 days (one day default period plus one day grace period). You can also apply the expiration of time and the grace period settings to a group of users.

Use this command to configure the expiration time and grace period for PACs:

```
AP(config-radsrv-group)# [no] eapfast pac expiry days [grace days]
```

Enter a number of days from 2 to 4095. Enter the **no** form of the command to reset the expiration time or grace period to infinite days.

In this example, PACs for the user group expire in 100 days with a grace period of two days:

```
AP(config-radsrv-group)# eapfast pac expiry 100 grace 2
```

Generating PACs Manually

The local authenticator automatically generates PACs for EAP-FAST clients that request them. However, you might need to generate a PAC manually for some client devices. When you enter the command, the local authenticator generates a PAC file and writes it to the network location that you specify. The user imports the PAC file into the client profile.

Use this command to generate a PAC manually:

AP# **radius local-server pac-generate** *username filename* [**password** *password*] [**expiry** *days*]

When you enter the PAC filename, enter the full path to which the local authenticator writes the PAC file (such as tftp://172.1.1.1/test/user.pac). The password is optional and, if not specified, a default password understood by the CCX client is used. Expiry is also optional and, if not specified, the default period is 1 day.

In this example, the local authenticator generates a PAC for the username *joe*, password-protects the file with the password *bingo*, sets the PAC to expire in 10 days, and writes the PAC file to the TFTP server at 10.0.0.5:

```
AP# radius local-server pac-generate tftp://10.0.0.5 joe password bingo expiry 10
```

Configuring an Authority ID

All EAP-FAST authenticators are identified by an authority identity (AID). The local authenticator sends its AID to an authenticating client, and the client checks its database for a matching AID. If the client does not recognize the AID, it requests a new PAC.

Use these commands to assign an AID to the local authenticator:

```
AP(config-radserv)# [no] eapfast authority id identifier

AP(config-radserv)# [no] eapfast authority info identifier
```

The *identifier* can consist of up to 32 hexadecimal digits. The **eapfast authority id** command assigns an AID that the client device uses during authentication.

Configuring Server Keys

The local authenticator uses server keys to encrypt PACs that it generates and to decrypt PACs when authenticating clients. The server maintains two keys, a primary key and a secondary key, and uses the primary key to encrypt PACs. By default, the server uses a default value as the primary key but does not use a secondary key unless you configure one.

When the local authenticator receives a client PAC, it attempts to decrypt the PAC with the primary key. If decryption fails with the primary, the authenticator attempts to decrypt the PAC with the secondary key if one is configured. If decryption fails, the authenticator rejects the PAC as invalid.

Use these commands to configure server keys:

```
AP(config-radsrv)# [no] eapfast server-key primary {[auto-generate] | [ [0 | 7] key]}

AP(config-radsrv)# [no] eapfast server-key secondary [0 | 7] key
```

Keys can contain up to 32 hexadecimal digits. Enter **0** before the key to enter an unencrypted key. Enter **7** before the key to enter an encrypted key. Use the **no** form of the commands to reset the local authenticator to the default setting, which is to use a default value as a primary key.

Possible PAC Failures Caused by Access Point Clock

The local authenticator uses the access point clock to both generate PACs and to determine whether PACs are valid. However, relying on the access point clock can lead to PAC failures.

If your local authenticator access point receives its time setting from an NTP server, there is an interval between boot up and synchronization with the NTP server during which the access point uses its default time setting. If the local authenticator generates a PAC during that interval, the PAC might be expired when the access point receives a new time setting from the NTP server. If an EAP-FAST client attempts to authenticate during the interval between boot and NTP-synch, the local authenticator might reject the client's PAC as invalid.

If your local authenticator does not receive its time setting from an NTP server and it reboots frequently, PACs generated by the local authenticator might not expire when they should. The access point clock is reset when the access point reboots, so the elapsed time on the clock would not reach the PAC expiration time.

Limiting the Local Authenticator to One Authentication Type

By default, a local authenticator access point performs LEAP, EAP-FAST, and MAC-based authentication for client devices. However, you can limit the local authenticator to perform only one or two authentication types. Use the **no** form of the authentication command to restrict the authenticator to an authentication type:

```
AP(config-radsrv)# [no] authentication [eapfast] [leap] [mac]
```

Because all authentication types are enabled by default, you enter the **no** form of the command to disable authentication types. For example, if you want the authenticator to perform only LEAP authentication, you enter these commands:

```
AP(config-radsrv)# no authentication eapfast
AP(config-radsrv)# no authentication mac
```

Unblocking Locked Usernames

You can unblock usernames before the lockout time expires, or when the lockout time is set to infinite. In Privileged Exec mode on the local authenticator, enter this command to unblock a locked username:

```
AP# clear radius local-server user username
```

Viewing Local Authenticator Statistics

In privileged exec mode, enter this command to view statistics collected by the local authenticator:

```
AP# show radius local-server statistics
```

This example shows local authenticator statistics:

```
Successes              : 0          Unknown usernames      : 0
Client blocks          : 0          Invalid passwords      : 0
Unknown NAS            : 0          Invalid packet from NAS: 0

NAS : 10.91.6.158
Successes              : 0          Unknown usernames      : 0
Client blocks          : 0          Invalid passwords      : 0
Corrupted packet       : 0          Unknown RADIUS message : 0
No username attribute  : 0          Missing auth attribute : 0
Shared key mismatch    : 0          Invalid state attribute: 0
Unknown EAP message    : 0          Unknown EAP auth type  : 0
Auto provision success : 0          Auto provision failure : 0
PAC refresh            : 0          Invalid PAC received   : 0

Username                  Successes  Failures  Blocks
nicky                             0         0       0
jones                             0         0       0
jsmith                            0         0       0
```

The first section of statistics lists cumulative statistics from the local authenticator.

The second section lists stats for each access point (NAS) authorized to use the local authenticator. The EAP-FAST statistics in this section include these stats:

- Auto provision success—the number of PACs generated automatically
- Auto provision failure—the number of PACs not generated because of an invalid handshake packet or invalid username or password
- PAC refresh—the number of PACs renewed by clients
- Invalid PAC received—the number of PACs received that were expired, that the authenticator could not decrypt, or that were assigned to a client username not in the authenticator's database

The third section lists stats for individual users. If a user is blocked and the lockout time is set to infinite, *blocked* appears at the end of the stat line for that user. If the lockout time is not infinite, *Unblocked in x seconds* appears at the end of the stat line for that user.

Use this privileged exec mode command to reset local authenticator statistics to zero:

```
AP# clear radius local-server statistics
```

Using Debug Messages

In privileged exec mode, enter this command to control the display of debug messages for the local authenticator:

```
AP# debug radius local-server { client | eapfast | error | packets}
```

Use the command options to display this debug information:

- Use the **client** option to display error messages related to failed client authentications.
- Use the **eapfast** option to display error messages related to EAP-FAST authentication. Use the sub-options to select specific debugging information:
  - **encryption** —displays information on the encryption and decryption of received and transmitted packets
  - **events**—displays information on all EAP-FAST events
  - **pac**—displays information on events related to PACs, such as PAC generation and verification
  - **pkts**—displays packets sent to and received from EAP-FAST clients
- Use the **error** option to display error messages related to the local authenticator.
- Use the **packets** option to turn on display of the content of RADIUS packets sent and received.

CHAPTER 10

Configuring WLAN Authentication and Encryption

This chapter describes how to configure authentication and encryption schemes to protect your WLANs.

Encryption can be achieved using shared keys or individual client keys. Individual client keys are more robust, but need to be managed. Key management can be achieved using cipher suites with Wi-Fi Protected Access (WPA) version 1 or version 2 and Cisco Centralized Key Management (CCKM) authenticated key management.

Encryption robustness can be achieved using Wired Equivalent Privacy (WEP), WEP features including AES, Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC), and broadcast key rotation. Authentication can be achieved using shared keys (with WEP), pre-shared keys (with WPA v1 or WPAv2) or individual client authentication with 802.1x/EAP.

Understanding Authentication and Encryption Mechanisms

Just as anyone within range of a radio station can tune to the station's frequency and listen to the signal, any wireless networking device within range of an access point can receive the access point's, and any wireless client's, radio transmissions. Also, the access point typically connects to the wired infrastructure. As the access point's radio signal can expand beyond the walls of the facility where the access point is deployed, external users may be provided access to the wired infrastructure through the access point. Therefore WLAN security relies on two major pillars:

- Authenticating the users, to make sure that only valid users are allowed to communicate through the access point.
- Encrypting wireless communications, to make sure that eavesdroppers cannot deciphers signals captured from the access point and clients communications.

On Cisco Aironet access points, SSIDs are mapped directly to the access point radio, or to VLANs configured on the AP radio interface. Encryption is configured at the radio level (if no VLAN is defined on the radio interface), or at the VLAN level (as soon as one or more VLANs are defined on the radio interface). This means that if you enable several SSIDs on a given radio interface or a given VLAN, all these SSIDs must share a common encryption scheme.

Authentication is configured at the SSID level. Each SSID can have a different authentication mechanism. However, as the SSID is mapped to a VLAN (or a radio interface), you need to make sure that the authentication mechanism defined at the SSID level is compatible with the encryption mechanism defined at the VLAN (or the radio) level for that SSID.

Encryption, defined at the radio (or the VLAN) level, can use one of the following schemes:

- No encryption
- Optional Static WEP (with a 40 bit or a 128 bit long key) encryption, both clients supporting WEP and those not supporting encryption are allowed to join the SSID
- Mandatory Static WEP (with a 40 bit or a 128 bit long key) encryption, clients must support static WEP encryption to be allowed to join the SSID
- Cipher 40 bit or 128 bit WEP encryption with key management, allowing for unicast WEP key rotation (if your authentication mechanism is compatible with individual client key determination) and/or broadcast key rotation (if your authentication mechanism is compatible with individual client key determination)
- Cipher TKIP, CKIP, CMIC,CKIP-CMIC, or AES (if your authentication mechanism is compatible with individual client key determination)
- A combination of two or three ciphers.
  This type of combination is used when you want to elevate the security level of your SSID, but still support clients that only support a weaker encryption scheme. In that case, clients will use the strongest encryption mechanism allowed by the SSID. Broadcast keys will use the encryption mechanism supported by all clients.
  Among all supported encryption schemes, AES-CCMP is the strongest, followed by TKIP. WEP is considered a weak encryption mechanism and is deprecated by the IEEE 802.11 standard.
  For example, suppose you define an AES+TKIP+WEP encryption. Clients supporting AES will use AES for their unicast key encryption. Clients not supporting AES but supporting TKIP will be allowed to join the cell, and will use TKIP for their unicast key encryption. Clients only supporting WEP will also be allowed to join the cell, and will use WEP for their unicast key encryption. When the cell contains AES, TKIP and WEP clients, the broadcast key will use WEP encryption (because WEP is the only common encryption scheme supported by all clients). When the cell contains AES and TKIP clients, but no WEP client, the broadcast key will use TKIP (the broadcast key encryption

will change to WEP if a WEP client joins the cell). When the cell contains only AES clients, the broadcast key uses AES (and will change to TKIP if TKIP clients join the cell, and to WEP if WEP clients join the cell).

Note Encryption mechanism support is incremental. A client supporting WEP may or may not support TKIP or AES. However, a client supporting TKIP necessarily supports WEP. Similarly, an AES client necessarily supports TKIP and WEP.

You can find more details about each encryption mechanism in the Understanding Encryption Modes section of this chapter.

Encryption is configured at the radio or the VLAN level. Authentication is configured at the SSID level. Authentication can use one or a combination of the following mechanisms:

- Open—No authentication is required to associate to the Access Point.
- Shared key—For using static WEP authentication.
- Network EAP—For using LEAP

Note Both Open and Shared key modes can be combined with other modes, such as EAP/802.1x, where authentication occurs after association to the access point, or with MAC authentication, where authentication occurs during the final phase of the association to the access point.

You can find more details about each authentication mechanism in the "Understanding Authentication Mechanisms" section of this chapter.

Combination of different authentication and encryption mechanisms result in different security schemes for your SSID. The following table summarizes the supported combinations:

SSID Authentication	Interface encryption	Supported security
Open	WEP optional	The AP announces the SSID as Open/Open, without broadcasting explicit support for WEP. However, the AP also accepts client association when client configuration is set to WEP encryption and/or WEP authentication. You must define a WEP key if you want to use this mode with clients using WEP.
Open	WEP mandatory	The AP announces the SSID as supporting WEP. The AP accepts client association when client configuration is set to Open/None, WEP encryption and/or WEP authentication. After the association phase, WEP support is mandatory in order to forward traffic through the access point. You must define a WEP key if you want to use this mode with clients using WEP.
Open with MAC	Any mode supported with Open authentication	Client MAC authentication is added to the final phase of the client association to the AP (see the MAC Address Authentication to the Network, page 11-5 section for more details)

SSID Authentication	Interface encryption	Supported security
Open with EAP	Any cipher (WEP 40, WEP 128, TKIP, CKIP, CMIC, CKIP-CMIC, TKIP + WEP 40, TKIP+WEP 128, AES-CCMP, AES-CCMP+TKIP, AES-CCMP + TKIP + WEP 40, AES-CCMP + TKIP + WEP 128)	Client association to the AP is followed with 802.1x/EAP authentication (supported EAP modes are LEAP,EAP-FAST, PEAP/GTC, MSPEAP, EAP-TLS, and EAP-FAST). During this process individual client keys are generated. When several ciphers are allowed, the key will be generated using the strongest cipher supported by the client. A broadcast key will be forwarded to all clients, using a cipher supported by all clients.
Open with MAC and EAP	Any cipher (WEP 40, WEP 128, TKIP, CKIP, CMIC, CKIP-CMIC, TKIP + WEP 40, TKIP+WEP 128, AES-CCMP, AES-CCMP+TKIP, AES-CCMP + TKIP + WEP 40, AES-CCMP + TKIP + WEP 128)	Client MAC authentication is added to the final phase of the client association to the AP. Client association to the AP is followed with 802.1x/EAP authentication. During this process individual client keys are generated. When several ciphers are allowed, the key will be generated using the strongest cipher supported by the client. A broadcast key will be forwarded to all clients, using a cipher supported by all clients.
Open with Optional EAP	Any cipher (WEP 40, WEP 128, TKIP, CKIP, CMIC, CKIP-CMIC, TKIP + WEP 40, TKIP+WEP 128, AES-CCMP, AES-CCMP+TKIP, AES-CCMP + TKIP + WEP 40, AES-CCMP + TKIP + WEP 128)	Clients configured for EAP will use individual authentication and encryption with individual keys. Clients with no security configuration can also associate to the AP. This mode is designed as a transition mechanism to stronger security. Broadcast key uses the common security mechanism supported by all clients. When both EAP and Open clients are associated, the broadcast key is not encrypted.
Shared Authentication	WEP Optional	The AP announces the SSID as supporting WEP. The AP only accepts clients configured with WEP authentication. WEP encryption after association is supported, but optional.
Shared Authentication	WEP Mandatory	The AP announces the SSID as supporting WEP. The AP only accepts clients configured with WEP authentication. WEP encryption after association is mandatory.
Shared Authentication with MAC	Any mode supported with Shared authentication	WEP authentication is followed, during the final phase of the association phase, with MAC authentication.
Shared Authentication with EAP	Any mode supported with Shared authentication	WEP authentication is followed with open association to the AP. Association is followed with individual client EAP authentication and individual key generation.

SSID Authentication	Interface encryption	Supported security
Shared Authentication with EAP and MAC	Any mode supported with Shared authentication	WEP authentication is followed, during the final phase of the association phase, with MAC authentication. Association is followed with individual client EAP authentication and individual key generation.
Network EAP	Any cipher (WEP 40, WEP 128, TKIP, CKIP, CMIC, CKIP-CMIC, TKIP + WEP 40, TKIP+WEP 128, AES-CCMP, AES-CCMP+TKIP, AES-CCMP + TKIP + WEP 40, AES-CCMP + TKIP + WEP 128)	Client association to the AP is followed with Cisco LEAP authentication. During this process individual client keys are generated. When several ciphers are allowed, the key will be generated using the strongest cipher supported by the client. A broadcast key will be forwarded to all clients, using a cipher supported by all clients.
Network EAP with MAC	Any cipher (WEP 40, WEP 128, TKIP, CKIP, CMIC, CKIP-CMIC, TKIP + WEP 40, TKIP+WEP 128, AES-CCMP, AES-CCMP+TKIP, AES-CCMP + TKIP + WEP 40, AES-CCMP + TKIP + WEP 128)	Client MAC authentication is added to the final phase of the client association to the AP. Client association to the AP is followed with 802.1x/EAP authentication using LEAP. During this process individual client keys are generated. When several ciphers are allowed, the key will be generated using the strongest cipher supported by the client. A broadcast key will be forwarded to all clients, using a cipher supported by all clients.
Web Authentication	Any	Web authentication can be used independently (with no other SSID authentication or encryption), or in combination with any other authentication and encryption scheme.

You can enable Network EAP authentication in combination with Open (with EAP or not, and any combination of MAC, namely Network EAP with or without MAC, with Open with or without EAP, with or without MAC, or with or without EAP and MAC). Network EAP uses LEAP, but requires support for LEAP formatting in the AP announcements. Clients that do not support this specific announcement formatting can use the Open mode (with LEAP or another EAP mechanism). The client will always try to use the most secure authentication mechanism supported through the access point, and the strongest encryption mechanism. However, client access points (in bridge or workgroup bridge mode) will use Network EAP by default, unless you configure the client side specifically to use a stronger authentication mechanism.

When configuring the SSID, using a cipher allows you to manage each client individual key. When configuring the SSID, you can define how this key should be managed. If you configure the interface to use a Cipher, you must also enable key management when configuring the SSID. Key management can be set to none (when using no security or shared key security), mandatory (when using a cipher), or Optional (when using Open with optional EAP or Shared key with optional EAP authentications). Please refer to the Key management sections of this chapter for more details on the different key management modes.

Understanding Encryption Modes

As encryption is defined at the interface (VLAN or radio) level of the access point, and can be common to several SSIDs, encryption is usually configured before the SSID and its authentication mechanism.

Just as anyone within range of a radio station can tune to the station's frequency and listen to the signal, any wireless networking device within range of an access point can receive the access point's radio transmissions. Because encrypted communication is the first line of defense against attackers, Cisco recommends that you use full encryption on your wireless network.

The original encryption mechanism described by the 802.11 standard is WEP (Wired Equivalent Privacy). WEP encryption scrambles the communication between the access point and client devices to keep the communication private. The 802.11 standard describes what Cisco and some other vendors describe as static WEP. In this mode, WEP keys are defined statically on the client and the AP. Both the access point and client devices use the same WEP key to encrypt and unencrypt radio signals. WEP keys encrypt both unicast and multicast messages. Unicast messages are addressed to just one device on the network. Multicast messages are addressed to multiple devices on the network.

WEP is a legacy protocol deprecated by the 802.11 standard. Cisco recommends using a stronger protocol, such as AES/CCMP, whenever possible.

When your SSID authentication mechanism uses Extensible Authentication Protocol (EAP) with 802.1x authentication (and without WPA v1 or WPA v2 support), dynamic WEP keys can be generated for each wireless user. Dynamic WEP keys are more secure than static, or unchanging, WEP keys. If an intruder passively receives enough packets encrypted by the same WEP key, the intruder can perform a calculation to learn the key and use it to join your network. Because they change frequently, dynamic WEP keys prevent intruders from performing the calculation and learning the key. See Chapter 11, "Configuring Authentication Types," for detailed information on EAP and other authentication types.

Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN. You must use a cipher suite when using WPA, WPA2 or CCKM. When using WEP encryption, you have the choice to set WEP using the WEP encryption command, or the cipher command. When using the WEP encryption command, you can use a static WEP key for authentication and / or encryption. However, you cannot use per user secure authentication (using 802.1x) in this mode. Because cipher suites can provide WEP encryption while also allowing use of individual user authentication and key management, Cisco recommends that you enable WEP by using the encryption mode cipher command in the CLI or by using the cipher drop-down list in the web-browser interface, instead of the WEP encryption command. However, WEP is a protocol deprecated by the IEEE, and Cisco recommends using WEP only when client drivers do not support any stronger security mechanism. The recommended security is AES-CCMP.

These security features protect the data traffic on your wireless LAN:

- AES-CCMP—Based on the Advanced Encryption Standard (AES) defined in the National Institute of Standards and Technology's *FIPS Publication 197*, AES-CCMP is a symmetric block cipher that can encrypt and decrypt data using keys of 128, 192, and 256 bits. AES-CCMP is superior to WEP encryption and is defined in the IEEE 802.11i standard.

Note The 802.11n amendment relies on implementation of either No encryption or AES-CCMP encryption. Therefore, 802.11n radios require that either no encryption or AES-CCMP be configured to provide 802.11n rates support.

- WEP (Wired Equivalent Privacy)—WEP is an 802.11 standard encryption algorithm originally designed to provide your wireless LAN with the same level of privacy available on a wired LAN. However, the basic WEP construction is flawed, and an attacker can compromise the privacy with reasonable effort.
- TKIP (Temporal Key Integrity Protocol)—TKIP is a suite of algorithms surrounding WEP that is designed to achieve the best possible security on legacy hardware built to run WEP. TKIP adds four enhancements to WEP:
  - A per-packet key mixing function to defeat weak-key attacks
  - A new IV sequencing discipline to detect replay attacks
  - A cryptographic message integrity check (MIC), called *Michael*, to detect forgeries such as bit flipping and altering packet source and destination
  - An extension of IV space, to virtually eliminate the need for re-keying
- CKIP (Cisco Key Integrity Protocol)—Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group. WPA TKIP replaced most CKIP implementations.
- CMIC (Cisco Message Integrity Check)—Like TKIP's *Michael*, Cisco's message integrity check mechanism is designed to detect forgery attacks. Cisco CKIP is required to use CMIC.
- Broadcast key rotation (also known as Group Key Update)—Broadcast key rotation allows the access point to generate the best possible random group key and update all key-management capable clients periodically. Wi-Fi Protected Access (WPA) also provides additional options for group key updates. See the "Using WPA Key Management" section on page 11-7 for details on WPA.

Note Client devices using static WEP cannot use the access point when you enable broadcast key rotation. Broadcast key rotation is supported only when using key management (such as dynamic WEP (802.1x), WPA with EAP, or pre-shared key).

Note Encryption is configured at the interface or the VLAN level, and authentication is configured for each SSDI to be supported on the relevant VLAN or interface. Therefore, encryption and authentication combine. See Chapter 11, "Configuring Authentication Types,"for details on how encryption and authentication combinations.

Configuring Encryption Modes

Encryption is configured at the VLAN or radio interface level. Ensure that the encryption mechanism you enable is compatible with the authentication mechanism you plan on using for the SSID, that is mapped to the relevant VLAN or radio interface. For more details on encryption and authentication schemes compatibility, see the Understanding Authentication and Encryption Mechanisms section.

Note WEP, TKIP, MIC and broadcast key rotation are disabled by default.

Creating Static WEP Keys

Note You need to configure static WEP keys only if your access point needs to support client devices that use static WEP. If all the client devices that associate to the access point use key management (WPA, CCKM, or 802.1x authentication) you do not need to configure static WEP keys.

Beginning in privileged EXEC mode, follow these steps to create a WEP key and set the key properties:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	**encryption** [**vlan** *vlan-id*] **key** *1-4* **size** { **40** | **128** } *encryption-key* [**0** | **7**] [**transmit-key**]	Create a WEP key and set up its properties. • (Optional) Select the VLAN for which you want to create a key. • Name the key slot in which this WEP key resides. You can assign up to 4 WEP keys for each VLAN. • Enter the key and set the size of the key, either 40-bit or 128-bit. 40-bit keys contain 10 hexadecimal digits; 128-bit keys contain 26 hexadecimal digits. • (Optional) Specify whether the key string you enter in this command is an encrypted string or the plain text key. The plain text key will be encrypted when you press the Enter key. • (Optional) Set this key as the transmit key. The key in slot 1 is the transmit key by default. **Note** If you configure static WEP with MIC (key hash), the access point and associated client devices must use the same WEP key as the transmit key, and the key must be in the same key slot on the access point and the clients. **Note** Configuration of static WEP with CMIC is not supported. **Note** Using security features such as authenticated key management can limit WEP key configurations. See the "WEP Key Restrictions" section on page 10-9 for a list of features that impact WEP keys.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to create a 128-bit WEP key in slot 3 for VLAN 22 and sets the key as the transmit key:

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# encryption vlan 22 key 3 size 128 12345678901234567890123456
transmit-key
ap1200(config-if)# end
```

WEP Key Restrictions

Table 10-1 lists WEP key restrictions based on your security configuration.

Table 10-1 WEP Key Restrictions

Security Configuration	WEP Key Restriction
CCKM or WPA authenticated key management	Cannot configure a WEP key in key slot 1
LEAP or EAP authentication	Cannot configure a WEP key in key slot 4
Cipher suite with 40-bit WEP	Cannot configure a 128-bit key
Cipher suite with 128-bit WEP	Cannot configure a 40-bit key
Cipher suite with TKIP	Cannot configure any WEP keys
Cipher suite with TKIP and 40-bit WEP or 128-bit WEP	Cannot configure a WEP key in key slot 1 and 4
Static WEP with MIC	Access point and client devices must use the same WEP key as the transmit key, and the key must be in the same key slot on both access point and clients.
Broadcast key rotation	Keys in slots 2 and 3 are overwritten by rotating broadcast keys **Note** Client devices using static WEP cannot use the access point when you enable broadcast key rotation. Broadcast key rotation is supported only when using key management (such as dynamic WEP (802.1x), WPA with EAP, or pre-shared key).

Example WEP Key Setup

Table 10-2 shows an example WEP key setup that would work for the access point and an associated device.

Table 10-2 WEP Key Setup Example

Key Slot	Access Point		Associated Device	
	Transmit?	Key Contents	Transmit?	Key Contents
1	x	12345678901234567890abcdef	—	12345678901234567890abcdef
2	—	09876543210987654321fedcba	x	09876543210987654321fedcba

Table 10-2 WEP Key Setup Example (continued)

Key Slot	Access Point		Associated Device	
	Transmit?	**Key Contents**	**Transmit?**	**Key Contents**
3	—	not set	—	not set
4	—	not set	—	FEDCBA09876543211234567890

Because the access point's WEP key 1 is selected as the transmit key, WEP key 1 on the other device must have the same contents. WEP key 4 on the other device is set, but because it is not selected as the transmit key, WEP key 4 on the access point does not need to be set at all.

Note If you enable MIC but you use static WEP (you do not enable any type of EAP authentication), both the access point and any devices with which it communicates must use the same WEP key for transmitting data. For example, if the MIC-enabled access point uses the key in slot 1 as the transmit key, a client device associated to the access point must use the same key in its slot 1, and the key in the client's slot 1 must be selected as the transmit key.

Enabling Cipher Suites

Beginning in privileged EXEC mode, follow these steps to enable a cipher suite:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.

	Command	Purpose
Step 3	**encryption [vlan** *vlan-id*] **mode ciphers {aes-ccm | ckip | ckip-cmic | cmic | tkip | wep128 | wep40}**	Enable a cipher suite containing the protection you need. Table 10-3 lists guidelines for selecting a cipher suite that matches the type of authenticated key management you configure. • (Optional) Select the VLAN for which you want to enable a cipher type. • Select the cipher options you need. You can select more than one cipher. **Note** If you enable a cipher suite with 2 or 3 elements, each client will use the highest encryption mechanism enabled on the interface and supported by the client. The broadcast key will use the element supported by all clients. See the Understanding Authentication and Encryption Mechanisms section for more details. **Note** If you configure **ckip** you must also enable Aironet extensions. The command to enable Aironet extensions is **dot11 extension aironet**. **Note** You can also use the **encryption mode wep** command to set up static WEP. However, you should use **encryption mode wep** only if no clients that associate to the access point are capable of key management. See the *Cisco IOS Command Reference for Cisco Access Points and Bridges* for a detailed description of the **encryption mode wep** command. **Note** When you configure the cipher TKIP (not **TKIP + WEP 128** or **TKIP + WEP 40**) for an SSID, the SSID must use WPA or CCKM key management. Client authentication fails on an SSID that uses the cipher TKIP without enabling WPA or CCKM key management. **Note** You must configure WPA key management as optional in order to configure cipher modes **TKIP + WEP 128** or **TKIP + WEP 40**.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the encryption command to disable a cipher suite.

Matching Cipher Suites with WPA or CCKM

If you configure your access point to use WPA or CCKM authenticated key management, you must select a cipher suite compatible with the authenticated key management type. Table 10-3 lists the cipher suites that are compatible with WPA and CCKM.

Table 10-3 Cipher Suites Compatible with WPA and CCKM

Authenticated Key Management Types	Compatible Cipher Suites
CCKM	• encryption mode ciphers wep128 • encryption mode ciphers wep40 • encryption mode ciphers ckip • encryption mode ciphers cmic • encryption mode ciphers ckip-cmic • encryption mode ciphers tkip • encryption mode aes
WPA	• encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40 • encryption mode ciphers eas **Note** Encryption mode ciphers tkip wep128 and tkip wep-40 can only be used is WPA is configured as optional.

Note If using WPA and CCKM as key management, only tkip and aes ciphers are supported. If using only CCKM as key management, ckip, cmic, ckip-cmic, tkip, wep, and aes ciphers are supported.

Note When you configure the cipher TKIP (not **TKIP + WEP 128** or **TKIP + WEP 40**) for an SSID, the SSID must use WPA or CCKM key management. Client authentication fails on an SSID that uses the cipher TKIP without enabling WPA or CCKM key management.

For a complete description of WPA and instructions for configuring authenticated key management, see the "Using WPA Key Management" section on page 11-7.

Note Wi-Fi certified access points no longer support WPA/TKIP configuration. TKIP is only allowed in combination with WPA2/AES for backward compatibility to allow older TKIP-only devices to associate. WPA version 1 option has been removed from the authentication key-management wpa cli and configuring TKIP only under this interface is not supported.

Enabling and Disabling Broadcast Key Rotation

Broadcast key rotation is disabled by default.

Note Client devices using static WEP cannot use the access point when you enable broadcast key rotation. Broadcast key rotation is supported only when using key management (such as dynamic WEP (802.1x), WPA with EAP, or pre-shared key).

Beginning in privileged EXEC mode, follow these steps to enable broadcast key rotation:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	**broadcast-key** **change** *seconds* [**vlan** *vlan-id*] [**membership-termination**] [**capability-change**]	Enable broadcast key rotation. • Enter the number of seconds between each rotation of the broadcast key. • (Optional) Enter a VLAN for which you want to enable broadcast key rotation. • (Optional) If you enable WPA authenticated key management, you can enable additional circumstances under which the access point changes and distributes the WPA group key. – Membership termination—the access point generates and distributes a new group key when any authenticated client device disassociates from the access point. This feature protects the privacy of the group key for associated clients. However, it might generate some overhead if clients on your network roam frequently. – Capability change—the access point generates and distributes a dynamic group key when the last non-key management (static WEP) client disassociates, and it distributes the statically configured WEP key when the first non-key management (static WEP) client authenticates. In WPA migration mode, this feature significantly improves the security of key-management capable clients when there are no static-WEP clients associated to the access point. See Chapter 11, "Configuring Authentication Types," for detailed instructions on enabling authenticated key management.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the encryption command to disable broadcast key rotation.

This example enables broadcast key rotation on VLAN 22 and sets the rotation interval to 300 seconds:

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# broadcast-key vlan 22 change 300
ap1200(config-if)# end
```

CHAPTER 11

Configuring Authentication Types

This chapter describes how to configure authentication types on the access point.

Understanding Authentication Types

This section describes in detail the authentication types that you can configure on the access point. The authentication types are tied to the SSIDs that you configure for the access point. The SSID is then tied to a VLAN or a radio interface with a possible configured encryption mechanism. Hence, make sure that the authentication scheme you configure for the SSID is compatible with the encryption method configured for the associated VLAN or radio interface.

See Chapter 10, "Understanding Authentication and Encryption Mechanisms," section for more details. If you want to serve different types of client devices with the same access point, you can configure multiple SSIDs. See Chapter 7, "Configuring Multiple SSIDs." for complete instructions on configuring multiple SSIDs.

Before a wireless client device can communicate on your network through the access point, it must authenticate to the access point using open or shared-key authentication. For maximum security, client devices should also authenticate to your network using MAC-address or EAP authentication, both of which rely on an authentication server on your network.

The authentication server can be configured on the AP or on an external server. You can set the client authentication process to be as follows:

1. The client can authenticate to the access point (using open or shared key).
2. During the association phase, optionally the client can be authenticated using it's MAC address
3. After association to the AP, optionally the client can be authenticated against a RADIUS server,
4. Individual client key generation and management can be done using EAP/802.1x. EAP/802.1x mechanism.

Note By default, the access point sends re-authentication requests to the authentication server with the service-type attribute set to authenticate-only. However, some Microsoft IAS servers do not support the authenticate-only service-type attribute. Depending on the user requirements, set the service-type attribute to: **dot11 aaa authentication attributes service-type login-user** or **dot11 aaa authentication attributes service-type framed-user**. By default the service type "login" is sent in the access request.

The access point uses several authentication mechanisms or types and can use more than one at the same time. These sections explain each authentication type:

- Open Authentication to the Access Point, page 11-2
- WEP Shared Key Authentication to the Access Point, page 11-3
- EAP Authentication to the Network, page 11-4
- MAC Address Authentication to the Network, page 11-5
- Combining MAC-Based, EAP, and Open Authentication, page 11-6
- Using CCKM for Authenticated Clients, page 11-6
- Using WPA Key Management, page 11-7

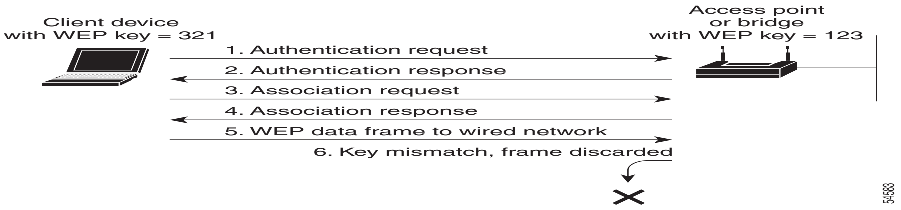
Open Authentication to the Access Point

Open authentication allows any device to authenticate and then attempt to communicate with the access point. Using open authentication, any wireless device can authenticate with the access point, Open authentication does not rely on a RADIUS server on your network.

In a scenario where you use Open authentication and WEP encryption, authentication will be successful even if the client and the AP WEP are mismatched. The client will not be able to send data (including DHCP requests) after Open authentication completes. However, with Open authentication and no encryption, the wireless client can transmit data as soon as the association phase is complete.

Figure 11-1 shows the authentication sequence between a device trying to authenticate and an access point using open authentication. In this example, the device's WEP key does not match the access point's key, so it can authenticate but not pass data.

Figure 11-1 Sequence for Open Authentication



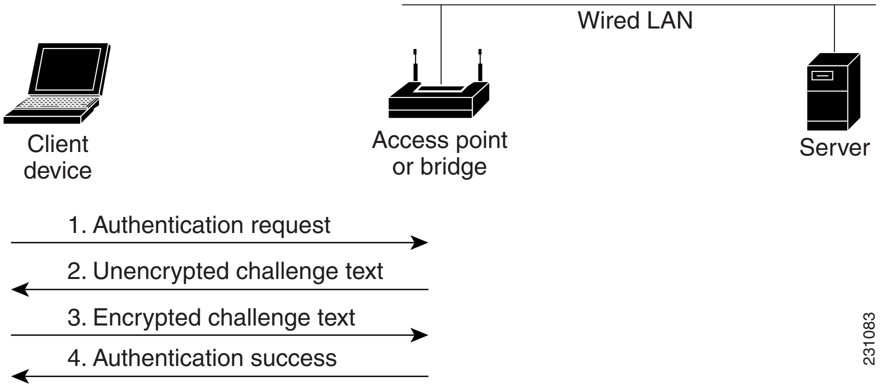
WEP Shared Key Authentication to the Access Point

Cisco provides shared key authentication to comply with WEP authentication described in the 802.11 standard. However, because of a shared key's security flaws WEP has been deprecated. The IEEE and Cisco recommend that you avoid using it.

During shared key authentication, the access point sends an unencrypted challenge text string to any device attempting to communicate with the access point. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. Both the unencrypted challenge and the encrypted challenge can be monitored, however, which leaves the access point open to attack from an intruder who calculates the WEP key by comparing the unencrypted and encrypted text strings. Because of this weakness, shared key authentication can be less secure than open authentication. Like open authentication, shared key authentication does not rely on a RADIUS server on your network.

Figure 11-2 shows the authentication sequence between a device trying to authenticate and an access point using shared key authentication. In this example the device's WEP key matches the access point's key, so it can authenticate and communicate.

Figure 11-2 Sequence for Shared Key Authentication


Wired LAN
Client
device
Access point
or bridge
Server
1. Authentication request
2. Unencrypted challenge text
3. Encrypted challenge text
4. Authentication success
231083

EAP Authentication to the Network

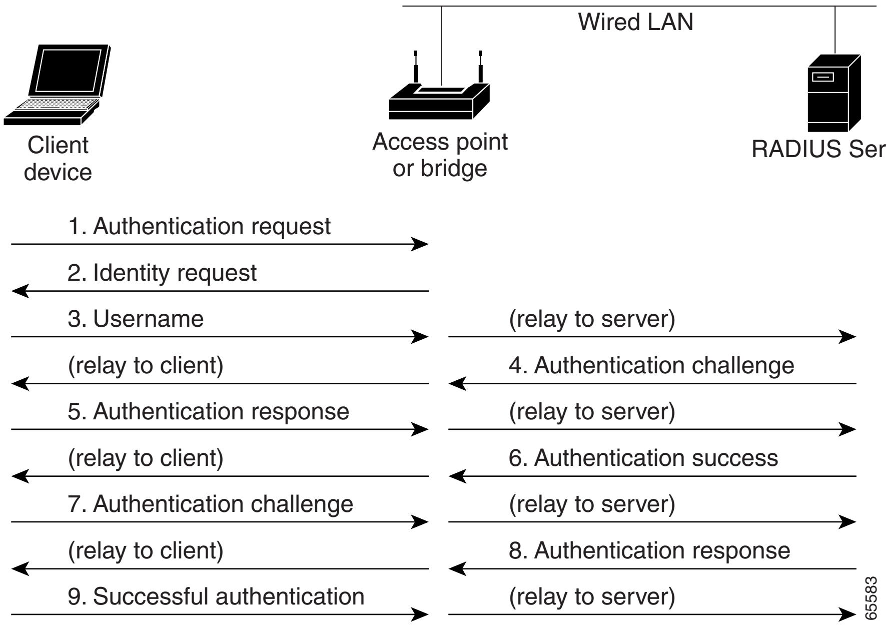
This authentication type provides the highest level of security for your wireless network. By using the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast key. The RADIUS server sends the key to the access point, which uses it for all unicast data signals that it sends to or receives from the client. The access point also encrypts its broadcast key with the client's unicast key and sends it to the client.

Depending on the underlying security framework (802.1X with dynamic WEP, WPA or WPA 2), the key is used:

- In the case of WEP – directly by the Access Point for all unicast data signals that it sends to or receives from the client,
- In the case of WPAv1/v2 – the key is used to derive unicast keys that are used for all unicast data signals that it sends to or receives from the client.

When you enable EAP on your access points and client devices, authentication to the network occurs in the sequence shown in Figure 11-3:

Figure 11-3 Sequence for EAP Authentication



In Steps 1 through 9 in Figure 11-3, a wireless client device and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the access point. The RADIUS server sends an authentication challenge to the client. The client uses a one-way encryption of the user-supplied or machine-supplied credentials to generate a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the client. When the RADIUS server authenticates the client, the process repeats in reverse, and the client authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the client determine a a WEP key or a Pairwise Master Key (WPAv1/v2) that is unique to the client and provides the client with the appropriate level of network access, thereby approximating the level of security in a wired switched segment to an individual desktop. The client loads this key and prepares to use it for the logon session.

During the logon session, the RADIUS server encrypts and sends the WEP key, or the WPAv1/v2 Pairwise Master Key, over the wired LAN to the access point. The AP uses this key to encrypt its broadcast key, and sends the encrypted broadcast key to the client, which uses its identical unicast key to decrypt it. The client and access point activate encryption and use the unicast and broadcast keys for all communications during the remainder of the session.

There is more than one type of EAP authentication, but the access point behaves the same way for each type: it relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device. See the "Assigning Authentication Types to an SSID" section on page 11-9 for instructions on setting up EAP on the access point.

Note If you use EAP authentication, you can select open or shared key authentication, but you do not have to. EAP authentication controls authentication both to your access point and to your network.

MAC Address Authentication to the Network

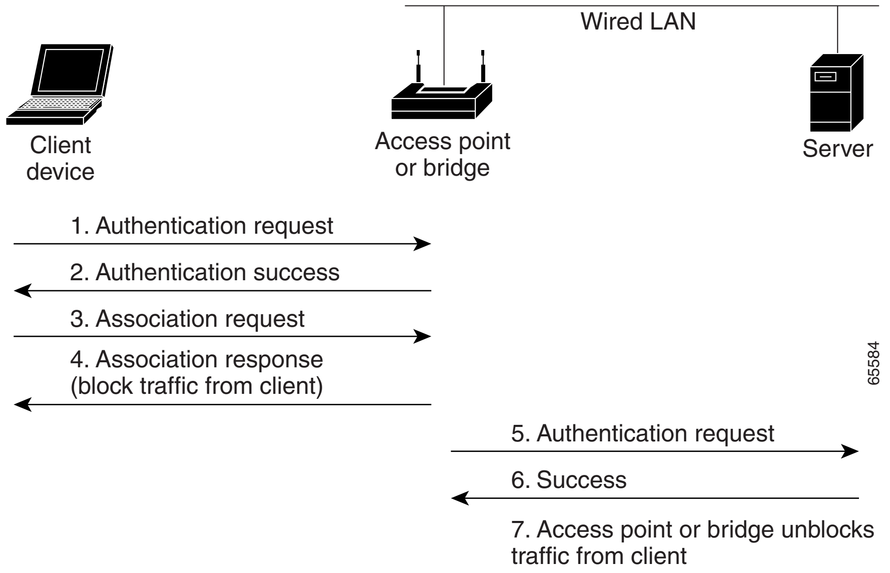
The access point relays the wireless client device's MAC address to a RADIUS server on your network, and the server checks the address against a list of allowed MAC addresses. Intruders can create counterfeit MAC addresses, so MAC-based authentication is less secure than EAP authentication. However, MAC-based authentication provides an alternate authentication method for client devices that do not have EAP capability. See the "Assigning Authentication Types to an SSID" section on page 11-9 for instructions on enabling MAC-based authentication.

Tip If you do not have a RADIUS server on your network, you can create a list of allowed MAC addresses on the access point's Advanced Security: MAC Address Authentication page. Devices with MAC addresses not on the list are not allowed to authenticate.

Tip If MAC-authenticated clients on your wireless LAN roam frequently, you can enable a MAC authentication cache on your access points. MAC authentication caching reduces overhead because the access point authenticates devices in its MAC-address cache without sending the request to your authentication server. See the "Configuring MAC Authentication Caching" section on page 11-15 for instructions on enabling this feature.

Figure 11-4 shows the authentication sequence for MAC-based authentication.

Figure 11-4 Sequence for MAC-Based Authentication


Wired LAN
Client device
Access point or bridge
Server
1. Authentication request
2. Authentication success
3. Association request
4. Association response (block traffic from client)
5. Authentication request
6. Success
7. Access point or bridge unblocks traffic from client
65584

Combining MAC-Based, EAP, and Open Authentication

You can set up the access point to authenticate client devices using a combination of MAC-based and EAP authentication. When you enable this feature, client devices that associate to the access point using 802.11 open authentication first attempt MAC authentication; if MAC authentication succeeds, the client device joins the network. If MAC authentication fails, EAP authentication takes place. See the "Assigning Authentication Types to an SSID" section on page 11-9 for instructions on setting up this combination of authentications.

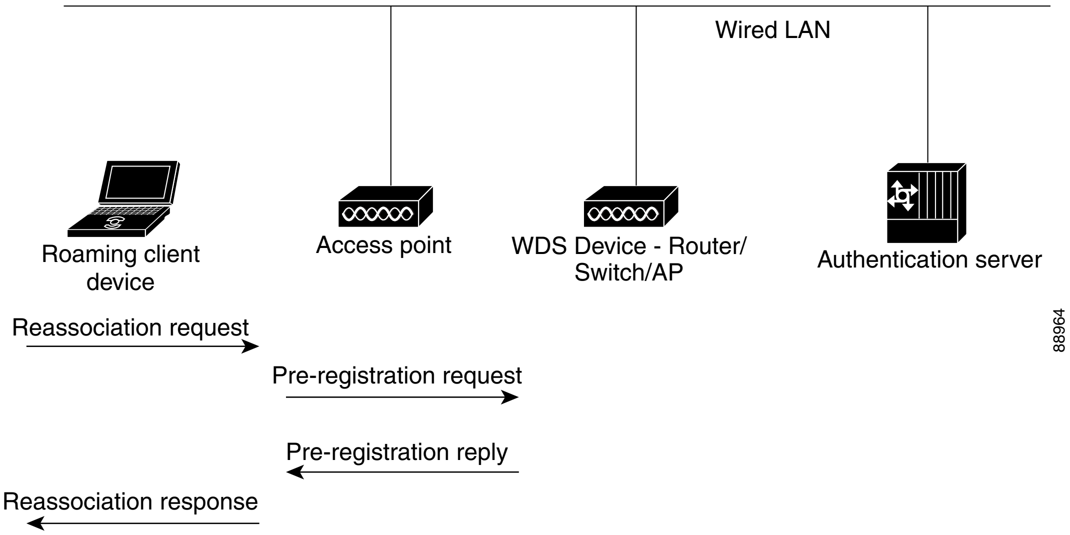
Using CCKM for Authenticated Clients

Using Cisco Centralized Key Management (CCKM), authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network provides Wireless Domain Services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point. When a client device roams, the WDS access point forwards the client's security credentials to the new access point, and the reassociation process is reduced to a two-packet exchange between the roaming client and the new access point. Roaming clients reassociate so quickly that there is no perceptible delay in voice or other time-sensitive applications. See the "Assigning Authentication Types to an SSID" section on page 11-9 for instructions on enabling CCKM on your access point. See the "Configuring Access Points as Potential WDS Devices" section on page 12-7 for detailed instructions on setting up a WDS access point on your wireless LAN.

Note The RADIUS-assigned VLAN feature is not supported for client devices that associate using SSIDs with CCKM enabled.

Figure 11-5 shows the reassociation process using CCKM.

Figure 11-5 Client Reassociation Using CCKM



Using WPA Key Management

WPAv1 is a Wi-Fi Alliance certification based on an early draft of the 802.11i amendment. WPAv1 leverages TKIP (Temporal Key Integrity Protocol) for data protection. WPAv2 is a Wi-Fi Alliance certification based on the final 802.11i amendment published in the year 2004. WPAv2 leverages AES (Advanced Encryption Standard) with the Counter-Mode Cipher Block Chaining (CBC) Message Authentication Code (MAC) Protocol. Both WPAv1 and WPAv2 allow authentication using pre-shared key (PSK) for home-type of deployment, and 802.1X for authenticated key management for enterprise-type of deployments.

Note WPA recommends the use of TKIP, and allows the use of AES. WPA2 recommends the use of AES-CCMP, and allows the use of TKIP for backward compatibility. Cisco and the Wi-Fi Alliance recommend that you do not use WPAv1 with AES, or WPAv2 with TKIP. The strongest level of security is achieved with WPAv2 and AES-CCMP. WPAv1 and TKIP can be used in networks where clients do not support WPAv2 with AES-CCMP.

Using WPA (WPAv1 or WPAv2) key management, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). Using WPA, the server generates the PMK dynamically and passes it to the access point. Using WPA-PSK, however, you configure a pre-shared key on both the client and the access point, and that pre-shared key is used as the PMK.

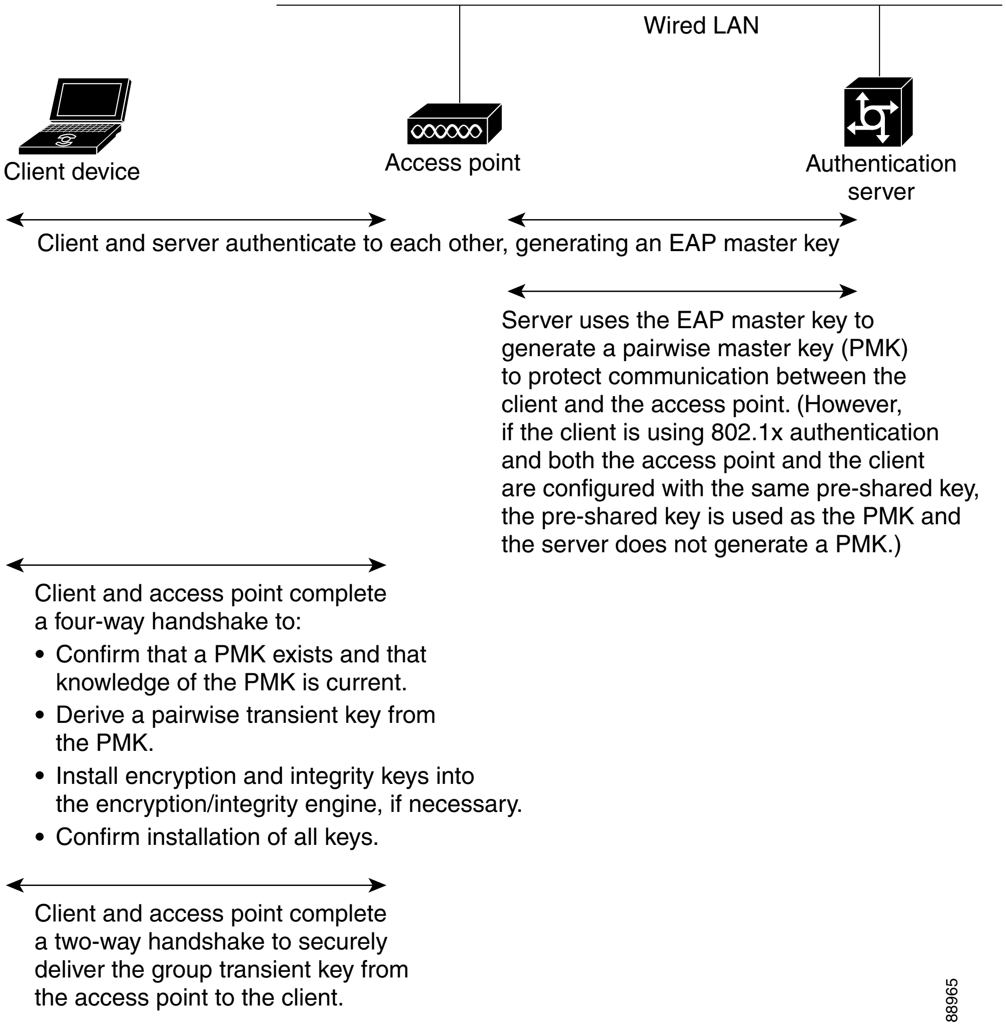
WPA key management supports two mutually exclusive management types: WPA and WPA-pre-shared key (WPA-PSK). Using WPA key management, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). Using WPA, the server generates the PMK dynamically and passes it to the access point. Using WPA-PSK, however, you configure a pre-shared key on both the client and the access point, and that pre-shared key is used as the PMK.

Note Unicast and multicast cipher suites advertised in WPA information element (and negotiated during 802.11 association) may potentially mismatch with the cipher suite supported in an explicitly assigned VLAN. If the RADIUS server assigns a new vlan ID which uses a different cipher suite from the previously negotiated cipher suite, there is no way for the access point and client to switch back to the new cipher suite. Currently, the WPA and CCKM protocols does not allow the cipher suite to be changed after the initial 802.11 cipher negotiation phase. In this scenario, the client device is disassociated from the wireless LAN.

See the "Assigning Authentication Types to an SSID" section on page 11-9 for instructions on configuring WPA key management on your access point.

Figure 11-6 shows the WPA key management process.

Figure 11-6 WPA Key Management Process



Client and server authenticate to each other, generating an EAP master key

Server uses the EAP master key to generate a pairwise master key (PMK) to protect communication between the client and the access point. (However, if the client is using 802.1x authentication and both the access point and the client are configured with the same pre-shared key, the pre-shared key is used as the PMK and the server does not generate a PMK.)

Client and access point complete a four-way handshake to:

- Confirm that a PMK exists and that knowledge of the PMK is current.
- Derive a pairwise transient key from the PMK.
- Install encryption and integrity keys into the encryption/integrity engine, if necessary.
- Confirm installation of all keys.

Client and access point complete a two-way handshake to securely deliver the group transient key from the access point to the client.

Configuring Authentication Types

This section describes how to configure authentication types. You attach configuration types to the access point's SSIDs. See the "Configuring Multiple SSIDs" section on page 7-3 for details on setting up multiple SSIDs. This section contains these topics:

- Assigning Authentication Types to an SSID, page 11-9
- Configuring Authentication Holdoffs, Timeouts, and Intervals, page 11-16
- Creating and Applying EAP Method Profiles for the 802.1X Supplicant, page 11-17

Assigning Authentication Types to an SSID

The SSID you configure will be mapped to a VLAN or a radio interface. Hence, make sure that the authentication type you define for the SSID is compatible with the encryption type defined for the associated VLAN or radio interface. See Chapter 10, "Understanding Authentication and Encryption Mechanisms," for more details.

Beginning in privileged EXEC mode, follow these steps to configure authentication types for SSIDs:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ssid** *ssid-string*	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. Some clients do not support special characters in the SSID string. Cisco recommends avoiding the following characters in the SSID string: !#;+\/"

	Command	Purpose
Step 3	**authentication open** [**mac-address** *list-name* [**alternate**]] [[**optional**] **eap** *list-name*]	(Optional) Set the authentication type to open for this SSID. Open authentication allows any device to authenticate and then attempt to communicate with the access point. • (Optional) Set the SSID's authentication type to open with MAC address authentication. The access point forces all client devices to perform MAC-address authentication before they are allowed to join the network. For *list-name*, specify the authentication method list. • Use the **alternate** keyword to allow client devices to join the network using either MAC or EAP authentication; clients that successfully complete either authentication are allowed to join the network. • (Optional) Set the SSID's authentication type to open with EAP authentication. The access point forces all client devices to perform EAP authentication before they are allowed to join the network. For *list-name*, specify the authentication method list. Use the **optional** keyword to allow client devices using either open or EAP authentication to associate and become authenticated. This setting is used mainly by service providers that require special client accessibility. **Note** An access point configured for EAP authentication forces all client devices that associate to perform EAP authentication. Client devices that do not use EAP cannot use the access point.
Step 4	**authentication shared** [**mac-address** *list-name*] [**eap** *list-name*]	(Optional) Set the authentication type for the SSID to shared key. **Note** Because of WEP shared key's security flaws, We recommend that you avoid using it. • (Optional) Set the SSID's authentication type to shared key with MAC address authentication. For list-name, specify the authentication method list. • (Optional) Set the SSID's authentication type to shared key with EAP authentication. For list-name, specify the authentication method list. This mode is designed for networks with phased migration to EAP. Clients supporting EAP will use individual client authentication and individual client key management, while clients supporting only static WEP will be allowed to associate using static WEP.

	Command	Purpose
Step 5	**authentication network-eap** *list-name* [**mac-address** *list-name*]	(Optional) set the authentication type for the SSID to Network-EAP. Using the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible RADIUS server supporting Cisco LEAP, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast key. • (Optional) Set the SSID’s authentication type to Network-EAP with MAC address authentication. All client devices that associate to the access point are required to perform MAC-address authentication. For list-name, specify the authentication method list.

	Command	Purpose
Step 6	**authentication key-management** { [**wpa** [**version** *versionnumber*]] | [**cckm**] } [**optional**]	(Optional) Set the authentication type for the SSID to WPA, CCKM, or both. If you use the **optional** keyword, client devices other than WPA (WPAv1 or WPAv2) and CCKM clients can use this SSID. If you do not use the **optional** keyword, only WPA (WPAv1 or WPAv2) or CCKM client devices are allowed to use the SSID. To enable CCKM for an SSID, you must also enable a form of EAP authentication (Open with EAP and/or Network EAP). When CCKM and EAP are enabled for an SSID, client devices using LEAP, EAP-FAST, PEAP/GTC, MSPEAP, EAP-TLS, and EAP-FAST authenticate using the SSID, and can benefit from fast roaming using CCKM. To enable WPA key management for an SSID (with WPAv1 or WPAv2), you must also enable Open authentication with EAP or Network-EAP or both (with or without additional MAC authentication). In that case, individual client authentication will occur using EAP, and individual client Pairwise Master Key will be defined. Alternatively, you can enable Open and define a WPA pre-shared key. In that case, the pre-shared key will be used as the Pairwise Master Key (PMK) by the AP and the wireless client. **Note** When you enable both WPA and CCKM for an SSID from the CLI, you must enter WPA first and CCKM second (but from the WebUI, simply check both options). Any WPA client can attempt to authenticate, but only CCKM voice clients can attempt to authenticate. **Note** Before you can enable CCKM or WPA, you must set the encryption mode for the SSID's VLAN to one of the cipher suite options. See the Chapter 10, "Configuring Encryption Modes," for instructions on configuring the VLAN encryption mode. **Note** If you enable WPA for an SSID without a pre-shared key, the key management type is WPA. If you enable WPA with a pre-shared key, the key management type is WPA-PSK. See the Configuring Additional WPA Settings for instructions on configuring a pre-shared key. See Chapter 12, "Configuring Other Services," for detailed instructions on setting up your wireless LAN to use CCKM and a subnet context manager. (Optional) When using WPA, you can specify which WPA version you want to support – WPAv1 or WPAv2.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the SSID commands to disable the SSID or to disable SSID features.

This example sets the authentication type for the SSID *batman* to Network-EAP with CCKM authenticated key management. Client devices using the batman SSID authenticate using the adam server list. After they are authenticated, CCKM-enabled clients can perform fast reassociations using CCKM.

```
ap1200# configure terminal
ap1200(config-if)# ssid batman
ap1200(config-ssid)# authentication network-eap adam
ap1200(config-ssid)# authentication key-management cckm optional
ap1200(config)# interface dot11radio 0
ap1200(config-if)# ssid batman
ap1200(config-ssid)# end
```

Configuring WPA Migration Mode for Legacy WEP SSIDs

WPA migration is a specific mode intended for SSIDs needing to support legacy WEP client types while still allowing for more secure authentication and encryption. This specific mode allows for the following client device types:

- WPA clients capable of TKIP and authenticated key management
- 802.1X-2001 clients (such as legacy LEAP clients and clients using TLS) capable of authenticated key management but not TKIP
- Static-WEP clients not capable of TKIP or authenticated key management

If all three client types associate using the same SSID, the multicast cipher suite for the SSID must be WEP. If only the first two types of clients use the same SSID the multicast key can be dynamic, but if the static-WEP clients use the SSID, the key must be static. The access point can switch automatically between a static and a dynamic group key to accommodate associated client devices. To support all three types of clients on the same SSID, you must configure the static key in key slots 2 or 3.

To set up an SSID for WPA migration mode, configure these settings:

- WPA optional
- A cipher suite containing TKIP and 40-bit or 128-bit WEP
- A static WEP key in key slot 2 or 3

This example sets the SSID migrate for WPA migration mode:

```
ap1200# configure terminal
ap1200(config-if)# ssid migrate
ap1200(config-if)# encryption mode cipher tkip wep128
ap1200(config-if)# encryption key 3 size 128 12345678901234567890123456 transmit-key
ap1200(config-ssid)# authentication open
ap1200(config-ssid)# authentication network-eap adam
ap1200(config-ssid)# authentication key-management wpa optional
ap1200(config-ssid)# wpa-psk ascii batmobile65
ap1200(config)# interface dot11radio 0
ap1200(config-if)# ssid migrate
ap1200(config-ssid)# end
```

Configuring Additional WPA Settings

Use two optional settings to configure a pre-shared key on the access point and adjust the frequency of group key updates.

Setting a pre-shared Key

To support WPA (WPAv1 or WPAv2) on a wireless LAN where 8021X/EAP-based authentication is not available, you must configure a pre-shared key on the access point. You can enter the pre-shared key as ASCII or hexadecimal characters. If you enter the key as ASCII characters, you enter between 8 and 63 characters, and the access point expands the key using the process described in the *Password-based Cryptography Standard* (RFC2898). If you enter the key as hexadecimal characters, you must enter 64 hexadecimal characters.

Configuring Group Key Updates

In the last step in the WPA process, the access point distributes a group key to the authenticated client device. You can use these optional settings to configure the access point to change and distribute the group key based on client association and disassociation:

- Membership termination—the access point generates and distributes a new group key when any authenticated device disassociates from the access point. This feature keeps the group key private for associated devices, but it might generate some overhead traffic if clients on your network roam frequently among access points.
- Capability change—the access point generates and distributes a dynamic group key when there is a change in the cell clients capability. For example, in a cell allowing AES, TKIP and WEP and currently containing only AES clients, the broadcast key uses AES. The access point generates a new broadcast key using TKIP when the first TKIP client joins the cell, and generates a new broadcast key when the first WEP client joins the cell. Symmetrically, the access point generates a new broadcast key when the last WEP client leaves the cell. If at that time all clients support AES, the new broadcast key will use AES. If some clients use TKIP and others use AES (AES clients also support TKIP), the new broadcast key will use TKIP. When the last TKIP client leaves the cell, with only AES clients left in the cell, the access point generates a new broadcast key using AES.

Beginning in privileged EXEC mode, follow these steps to configure a WPA pre-shared key and group key update options:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ssid** *ssid-string*	Enter SSID configuration mode for the SSID.
Step 3	**wpa-psk** { **hex** | **ascii** } [**0** | **7**] *encryption-key*	Enter a pre-shared key for client devices using WPA that also use static WEP keys. Enter a pre-shared key for client devices using WPAv1 or WPAv2 with PSK authentication. If you use hexadecimal, you must enter 64 hexadecimal characters to complete the 256-bit key. If you use ASCII, you must enter a minimum of 8 letters, numbers, or symbols, and the access point expands the key for you. You can enter a maximum of 63 ASCII characters.

	Command	Purpose
Step 4	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 5	**ssid** *ssid-string*	Enter the ssid defined in Step 2 to assign the ssid to the selected radio interface.
Step 6	**exit**	Return to privileged EXEC mode.
Step 7	**broadcast-key** [**vlan** *vlan-id*] { **change** *seconds* } [**membership-termination**] [**capability-change**]	Use the **broadcast key rotation** command to configure additional updates of the WPA group key.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure a pre-shared key for clients using WPA and static WEP, with group key update options:

```
ap# configure terminal
ap(config-if)# ssid batman
ap(config-ssid)# wpa-psk ascii batmobile65
ap(config)# interface dot11radio 0
ap(config-ssid)# ssid batman
ap(config-if)# exit
ap(config)# broadcast-key vlan 87 membership-termination capability-change
```

Configuring MAC Authentication Caching

If MAC-authenticated clients on your wireless LAN roam frequently, you can enable a MAC authentication cache on your access points. MAC authentication caching reduces overhead because the access point authenticates devices in its MAC-address cache without sending the request to your authentication server. When a client device completes MAC authentication to your authentication server, the access point adds the client's MAC address to the cache.

Beginning in privileged EXEC mode, follow these steps to enable MAC authentication caching:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 aaa authentication mac-authen filter-cache** [**timeout** *seconds*]	Enable MAC authentication caching on the access point. Use the **timeout** option to configure a timeout value for MAC addresses in the cache. Enter a value from 30 to 65555 seconds. The default value is 1800 (30 minutes). When you enter a timeout value, MAC-authentication caching is enabled automatically.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show dot11 aaa authentication mac-authen filter-cache** [*address*]	Show entries in the MAC-authentication cache. Include client MAC addresses to show entries for specific clients.
Step 5	**clear dot11 aaa authentication mac-authen filter-cache** [*address*]	Clear all entries in the cache. Include client MAC addresses to clear specific clients from the cache.

	Command	Purpose
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to enable MAC authentication caching with a one-hour timeout:

```
ap# configure terminal
ap(config)# dot11 aaa authentication mac-authen filter-cache timeout 3600
ap(config)# end
```

Use the **no** form of the **dot11 aaa authentication mac-authen filter-cache** command to disable MAC authentication caching. For example:

```
no dot11 aaa authentication mac-authen filter-cache
```

or

```
no wlccp wds aaa authentication mac-authen filter-cache
```

Configuring Authentication Holdoffs, Timeouts, and Intervals

Beginning in privileged EXEC mode, follow these steps to configure holdoff times, reauthentication periods, and authentication timeouts for client devices authenticating through your access point:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 holdoff-time** *seconds*	Enter the number of seconds a client device must wait before it can reattempt to authenticate following a failed authentication. The holdoff time is invoked when a client fails three login attempts or fails to respond to three authentication requests from the access point. Enter a value from 1 to 65555 seconds.
Step 3	**dot1x timeout supp-response** *seconds* [local]	Enter the number of seconds the access point should wait for a client to reply to an EAP/dot1x message before the authentication fails. Enter a value from 1 to 120 seconds. The RADIUS server can be configured to send a different timeout value which overrides the one that is configured. Enter the **local** keyword to configure the access point to ignore the RADIUS server value and use the configured value. The optional **no** keyword resets the timeout to its default state, 30 seconds.
Step 4	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.

	Command	Purpose
Step 5	**dot1x reauth-period** { *seconds* | **server** }	Enter the interval in seconds that the access point waits before forcing an authenticated client to reauthenticate. Enter the **server** keyword to configure the access point to use the reauthentication period specified by the authentication server. If you use this option, configure your authentication server with RADIUS attribute 27, Session-Timeout. This attribute sets the maximum number of seconds of service to be provided to the client before termination of the session or prompt. The server sends this attribute to the access point when a client device performs EAP authentication. **Note** If you configure both MAC address authentication and EAP authentication for an SSID, the server sends the Session-Timeout attribute for both MAC and EAP authentications for a client device. The access point uses the Session-Timeout attribute for the last authentication that the client performs. For example, if a client performs MAC address authentication and then performs EAP authentication, the access point uses the server's Session-Timeout value for the EAP authentication. To avoid confusion on which Session-Timeout attribute is used, configure the same Session-Timeout value on your authentication server for both MAC and EAP authentication.
Step 6	**countermeasure tkip hold-time** *seconds*	Configure a TKIP MIC failure holdtime. You can specify a hold-time in the range 0 to 65535 seconds. The default is 60 seconds. If the access point detects two MIC failures within, for example 60 seconds, it blocks all the TKIP clients on that interface for the holdtime period.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of these commands to reset the values to default settings.

Creating and Applying EAP Method Profiles for the 802.1X Supplicant

This section describes the optional configuration of an EAP method list for the 802.1X supplicant. Configuring EAP method profiles enables the supplicant not to acknowledge some EAP methods, even though they are available on the supplicant. For example, if a RADIUS server supports EAP-FAST and LEAP, under certain configurations, the server might initially employ LEAP instead of a more secure method. If no preferred EAP method list is defined, the supplicant supports LEAP, but it may be advantageous to force the supplicant to force a more secure method such as EAP-FAST.

See Creating a Credentials Profile, page 4-25 for additional information about the 802.1X supplicant.

Creating an EAP Method Profile

Beginning in privileged exec mode, follow these steps to define a new EAP profile:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**eap profile** *profile name*	Enter a name for the profile
Step 3	**description**	(Optional)—Enter a description for the EAP profile
Step 4	**method** {**fast** | **gtc** | **leap** | **md5** | **mschapv2** | **peap** | **tls**}	Enter an allowed EAP method or methods. **Note** Although they appear as sub-parameters, EAP-GTC, EAP-MD5, and EAP-MSCHAPV2 are intended as inner methods for tunneled EAP authentication and should not be used as the primary authentication method.
Step 5	**end**	Return to the privileged EXEC mode.
Step 6	**copy running config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** command to negate a command or set its defaults.

Use the **show eap registrations method** command to view the currently available (registered) EAP methods.

```
ap#show eap registrations method
Registered EAP Methods:
  Method  Type           Name
    4     Auth and Peer   MD5
    6     Auth and Peer   GTC
    13    Auth and Peer   TLS
    17    Auth and Peer   LEAP
    25    Auth and Peer   PEAP
    26    Auth and Peer   MSCHAPV2
    43    Auth and Peer   FAST
```

Use the **show eap sessions** command to view existing EAP sessions.

Applying an EAP Profile to the Fast Ethernet Interface

This operation normally applies to access points that need to be authenticated against a RADIUS server, when they are connected to a switch port that is configured to perform 802.1x authentication of connected devices. The AP will act as a 802.1x client, and will need to provide credentials to be authenticated.

Beginning in privileged exec mode, follow these steps to apply an EAP profile to the Fast Ethernet interface:

	Command	Purpose
Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**interface gigabitethernet 0**	Enter the interface configuration mode for the access point's Fast Ethernet port. You can also use **interface g0** to enter the fast Ethernet configuration mode.
Step 3	**dot1x eap profile** *profile*	Enter the profile preconfigured profile name.
Step 4	**end**	Exit the interface configuration mode.

Applying an EAP Profile to an Uplink SSID

This operation typically applies to repeater access points, non-root bridges and workgroup bridges needing to authenticate over their radio link to a root-AP or root bridge. Beginning in the privileged exec mode, follow these steps to apply an EAP profile to the uplink SSID.

	Command	Purpose
Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**interface dot11radio** {**0** | **1**}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	**ssid** *ssid*	Assign the uplink SSID to the radio interface.
Step 4	**dot1x** {**credentials** | **default** | **eap**}	You can specify one of the following: • credentials—Credentials profile configuration • default—Configure Dot1x with default values for this SSID • eap—Configure EAP specific parameters
Step 5	**dot1x eap profile** *profilename*	Enter the profile preconfigured profile name.
Step 6	**end**	Return to the privileged EXEC mode.
Step 7	**copy running config startup-config**	(Optional) Save your entries in the configuration file.

Matching Access Point and Client Device Authentication Types

To use the authentication types described in this section, the access point authentication settings must match the authentication settings on the client adapters that associate to the access point. Refer to Configuring Encryption Modes, page 10-7 for instructions on configuring cipher suites and WEP on the access point.

Table 11-1 lists the client and access point settings required for each authentication type.

Note Some non-Cisco Aironet client adapters do not perform 802.1X authentication to the access point unless you configure **Open authentication with EAP**. To allow both Cisco Aironet clients using LEAP and non-Cisco Aironet clients using LEAP to associate using the same SSID, you might need to configure the SSID for both **Network EAP** authentication and **Open authentication with EAP**.

Table 11-1 Client and Access Point Security Settings

Security Feature	Client Setting	Access Point Setting
Static WEP with open authentication	Create a WEP key and enable Use Static WEP Keys and Open Authentication	Set up and enable WEP and enable Open Authentication for the SSID
Static WEP with shared key authentication	Create a WEP key and enable Use Static WEP Keys and Shared Key Authentication	Set up and enable WEP and enable Shared Key Authentication for the SSID
LEAP authentication	Enable LEAP	Set up and enable WEP and enable Network-EAP for the SSID[1]
EAP-FAST authentication	Enable EAP-FAST and enable automatic provisioning or import a PAC file	Set up and enable WEP and enable Network-EAP for the SSID[1] If radio clients are configured to authenticate using EAP-FAST, open authentication with EAP should also be configured. If you do not configure open authentication with EAP, the following GUI warning message appears: WARNING: Network EAP is used for LEAP authentication only. If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured. If you are using the CLI, this warning message appears: SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.
EAP-FAST authentication with WPA	Enable EAP-FAST and Wi-Fi Protected Access (WPA) and enable automatic provisioning or import a PAC file. To allow the client to associate to both WPA and non-WPA access points, enable Allow Association to both WPA and non-WPA authenticators.	Select a cipher suite that includes TKIP, set up and enable WEP, and enable Network-EAP and WPA for the SSID. **Note** To allow both WPA and non-WPA clients to use the SSID, enable optional WPA.

Table 11-1 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
802.1X authentication and CCKM	Enable LEAP	Select a cipher suite and enable Open with EAP and/or Network EAP, and CCKM for the SSID. **Note** To allow both 802.1X clients and non-802.1X clients to use the SSID, enable optional CCKM.
802.1X authentication and WPA	Enable any 802.1X authentication method	Select a cipher suite and enable Open with EAP and WPA for the SSID (you can also enable Network-EAP authentication in addition to or instead of Open with EAP) **Note** To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA.
802.1X authentication and WPA-PSK	Enable any 802.1X authentication method	Select a cipher suite and enable Open authentication with Optional EAP and WPA for the SSID (you can also enable Network-EAP authentication in addition to or instead of Open authentication with Optional EAP). Enter a WPA pre-shared key. Clients using 802.1x/EAP will generate individual WPA PMKs. Clients using WPA-PSK will use the PSK as a PMK. **Note** To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA.
EAP-TLS authentication with dynamic WEP encryption		
If using Windows to configure card	Select Enable network access control using IEEE 802.1X and Smart Card or other Certificate as the EAP Type	Set up and enable WEP and enable EAP and Open with EAP for the SSID
EAP-MD5 authentication with dynamic WEP encryption		
If using Windows XP to configure card	Select Enable network access control using IEEE 802.1X and MD5-Challenge as the EAP Type	Set up and enable WEP and enable EAP and Open Authentication for the SSID

Table 11-1 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
PEAP authentication with dynamic WEP encryption		
If using Windows to configure card	Select Enable network access control using IEEE 802.1X and PEAP as the EAP Type	Set up and enable WEP and enable Require EAP and Open with EAP for the SSID
EAP-SIM authentication with dynamic WEP encryption		
If using Windows to configure card	Select Enable network access control using IEEE 802.1X and SIM Authentication as the EAP Type	Set up and enable WEP with full encryption and enable Require EAP and Open with EAP for the SSID

[1] Some non-Cisco Aironet client adapters do not perform 802.1X authentication to the access point unless you configure **Open authentication with EAP**. To allow both Cisco Aironet clients using LEAP and non-Cisco Aironet clients using LEAP to associate using the same SSID, you might need to configure the SSID for both **Network EAP** authentication and **Open authentication with EAP**.

Guest Access Management

Guest Access allows a guest to gain access to the Internet, and the guest's own enterprise without compromising the security of the host enterprise.

Guest access is allowed through these methods:

- Web Authentication (secured)
- Web Pass-through

Web Authentication (secured)

Web authentication is a Layer 3 security feature that enables the Autonomous AP to block IP traffic (except DHCP & DNS-related packets) until the guest provides a valid username and password.

In web authentication, a separate username and password must be defined for each guest. Using the username and password, the guest is authenticated either by the local radius server or an external RADIUS server.

Perform these steps to enable web authentication:

Step 1 Browse to the Security page on the access point GUI.

Step 2 Select SSID Manager.

Step 3 Check the **Web Authentication** check box.

Beginning in privileged EXEC mode, use these commands to enable web authentication:

- The network security type is set to none by default, because the authentication will occur at Layer 3 through the web interface, and therefore does not need to occur at Layer 2. However, you can combine Layer 3 security with any Layer 2 security. Web authentication is supported only with Open authentication. No encryption is allowed.
  - ap(config)# **dot11 ssid guestssid**
  - ap(config-ssid)# **web-auth**

- ap(config-ssid)# **authentication open**
- ap(config-ssid)# **exit**

- To enable web authentication:
  - ap(config)# **ip admission name Web_auth proxy http**
  - ap(config)# **interface dot11Radio 0**
  - ap(config-if)# **ip admission Web_auth**

Web Pass-through

Web Pass-through is similar to Web Authentication. However, the guest is not required to provide authentication details.

In Web Pass-through, guests are redirected to the usage policy page when they use the Internet for the first time. When the policy is accepted, access is granted. The access point redirects the guest to the policy page.

Perform these steps to enable web authentication:

Step 1 Browse to the Security page on the access point GUI.

Step 2 Select SSID Manager.

Step 3 Check the **Web Pass** check box.

Beginning in privileged EXEC mode, use these commands to enable Web Pass-through:

- ap(config)# **ip admission name Web_passthrough consent**
- ap(config)# **interface dot11Radio 0**
- ap(config-if)# **ip admission Web_passthrough**

Note Web Authentication or Web Pass-through works in an interface only when there is no VLAN. The IP admission Web_auth or IP admission Web_passthrough must be configured in the VLAN when the SSID is mapped to the VLAN.

Guest Account Creation

Perform these steps to create new guest accounts:

Step 1 Browse to **Management > Guest Management Services** page on the access point in the GUI.

Step 2 Select **New** to create a new guest account.

The Webauth page is displayed.

Step 3 Enter these values:

- Username
- Password
- Confirm Password
- Lifetime

Step 4 To let the system automatically generate a random string as a password, check the **Generate Password** check box. Alternatively, you can manually enter the password value.

Step 5 Click **Apply.**

Perform these steps to delete an existing user:

Step 1 Browse to the Guest Management Services page on the access point GUI.

Step 2 Select the username to be deleted.

Step 3 Click **Delete**.

A confirmation message appears.

Step 4 Click **Ok** to delete the user or **Cancel** to cancel the changes.

Beginning in privileged EXEC mode, use these commands to create guest accounts using CLI commands:

- ap(config)# **dot11 guest**
- ap(config-guest-mode)# **username Gues-1 lifetime 40 password t_ksdgon**
- ap(config-guest-mode)# **username Gues-2 lifetime 35 password gp2**
- ap(config)# **exit**

Guest access is allowed for a maximum of twenty-four days (35791 minutes) and a minimum of five minutes.

Beginning in privileged EXEC mode, use this command to delete a guest user:

```
ap# clear dot11 guest-user Gues-1
```

Beginning in privileged EXEC mode, use this command to display guest users:

```
ap# show dot11 guest-users
```

Customized Guest Access Pages

The Webauth Login guest access pages can be customized to display a custom logo or other images. You can customize the Login page, Success page, Failure page, or the Expired page. To customize a page, follow these steps:

Step 1 Save the image to be displayed in the customized page, on a web server and set the web server's IP address as allowed in the ACL in/out lists.

Step 2 Get the default HTML code of the page to be customized.

Step 3 Edit the source code of the page to insert the images, by specifying the full path of the image files on the web-server. For example: <Body background="http://40.40.5.10/image.jpg" width="600" height="600">, where the image.jpg file resides on the web server with IP address 40.40.5.10.

Note When editing the HTML code of the default page, do not make any changes to the code for the submit function and for the fields of Username and Password.

Step 4 Save the customized pages to the web server.

Step 5 In the access point GUI, browse to the **Management > Guest Management Services** page.

Step 6 Select **Webauth Login.**

Step 7 Browse and upload these pages from the web server:

- Login Page
- Success Page
- Failure Page
- Expired page

Note It is mandatory to load the Login page, Success page, Failure page, and Expired page when you customize the guess access login.

Step 8 Select the file transfer method: FTP or TFTP.

Step 9 Enter the **Username**.

Step 10 Enter the **Password**.

Step 11 Enter the **Allowed-In ACL Name** and the **Allowed-Out ACL Name**.

Step 12 Click **Close Window** to save your changes.

Alternatively, you can use the following CLI commands to configure a customized guest access page. Copy all edited files to the flash memory. Then, beginning in privileged EXEC mode, use these commands to load all the edited files from flash:

- ap(config)# **ip auth-proxy proxy http login page file flash:web_login.html**
- ap(config)# **ip auth-proxy proxy http success page file flash:web_success.html**
- ap(config)# **ip auth-proxy proxy http failure page file flash:web_fail.html**
- ap(config)# **ip auth-proxy proxy http login expired page file flash:web_logout.html**

To configure the IP address of the web server (IP address here is 40.40.5.10) in the ACL, the following commands are also required. Beginning in privileged EXEC mode, use these ACL commands:

- ap(config)# **dot11 webauth allowed incoming webauth_acl_in outgoing webaut_acl_out**
- ap(config)# **ip access-list extended webauth_acl_in**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq www**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq 443**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq 443**
- ap(config-ext-nacl)# **exit**
- ap(config)# **ip access-list extended webauth_acl_out**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq www**
- ap(config-ext-nacl)# **permit tcp any host 40.40.5.10 eq 443**
- ap(config-ext-nacl)# **exit**

Note In the previous commands acl-in and acl-out are the names of the Access-list. These ACLs allow you to download the image file from the machine, where it is stored and use it for the customization of web page.

The default page displays only the username, password, OK page.

Guest access does not support these:

- IPv6
- SNMP
- Roaming

CHAPTER 12

Configuring Other Services

This chapter describes how to configure your access points for wireless domain services (WDS), fast, secure roaming of client devices, radio management, wireless intrusion detection services (WIDS), and other services.

Understanding WDS

When you configure Wireless Domain Services on your network, access points on your wireless LAN use the WDS device (either an access point, an Integrated Services Router configured as the WDS device) to provide fast, secure roaming for client devices in a given subnet and to participate in radio management. An access point configured as the WDS device supports up to 60 participating access points, an Integrated Services Router (ISR) configured as the WDS devices supports up to 100 participating access points.

Note A single access point supports up to 16 mobility groups.

Fast, secure roaming provides rapid reauthentication when a client device roams from one access point to another in the same subnet, preventing delays in voice and other time-sensitive applications.

Access points participating in radio management forward information about the radio environment (such as possible rogue access points and client associations and disassociations) to the WDS device.

Role of the WDS Device

The WDS device performs several tasks on your wireless LAN:

- Advertises its WDS capability and participates in electing the best WDS device for your wireless LAN. When you configure your wireless LAN for WDS, you set up one device as the main WDS candidate and one or more additional devices as backup WDS candidates. If the main WDS device goes off line, one of the backup WDS devices takes its place.
- Authenticates all access points in the subnet and establishes a secure communication channel with each of them, over the wired interface.
- Acts as a pass-through for all 802.1x-authenticated client devices associated to participating access points.
- Registers all client devices in the subnet that use dynamic keying, establishes session keys for them, and caches their security credentials. When a client roams to another access point registered to the WDS device, the WDS device forwards the client's security credentials to the new access point.

Table 12-1 lists the number of participating access points supported by the platforms that can be configured as a WDS device: an access point, an ISR.

Table 12-1 Participating Access Points Supported by WDS Devices

Unit Configured as WDS Device	Participating Access Points Supported
Access point that also serves client devices	30
Access point with radio interfaces disabled	60
Integrated Services Router (ISR)	100 (depending on ISR platform)

Role of Access Points Using the WDS Device

The access points on your wireless LAN interact with the WDS device in these activities:

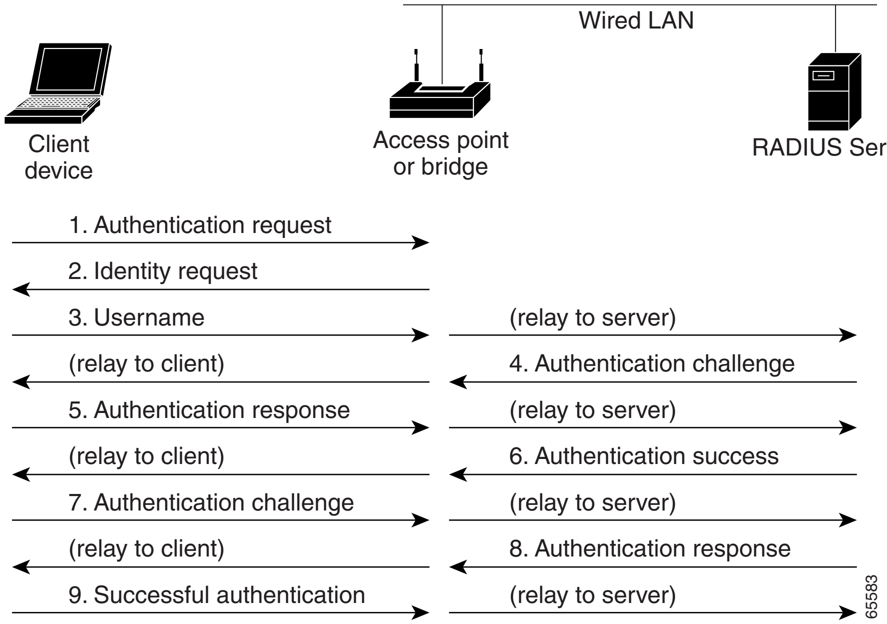
- Discover and track the current WDS device and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS device and establish a secure communication channel to the WDS device.
- Register associated client devices with the WDS device.
- Report radio data to the WDS device.

Understanding Fast Secure Roaming

Access points in many wireless LANs serve mobile client devices that roam from access point to access point throughout the installation. Some applications running on client devices require fast reassociation when they roam to a different access point. Voice applications, for example, require seamless roaming to prevent delays and gaps in conversation.

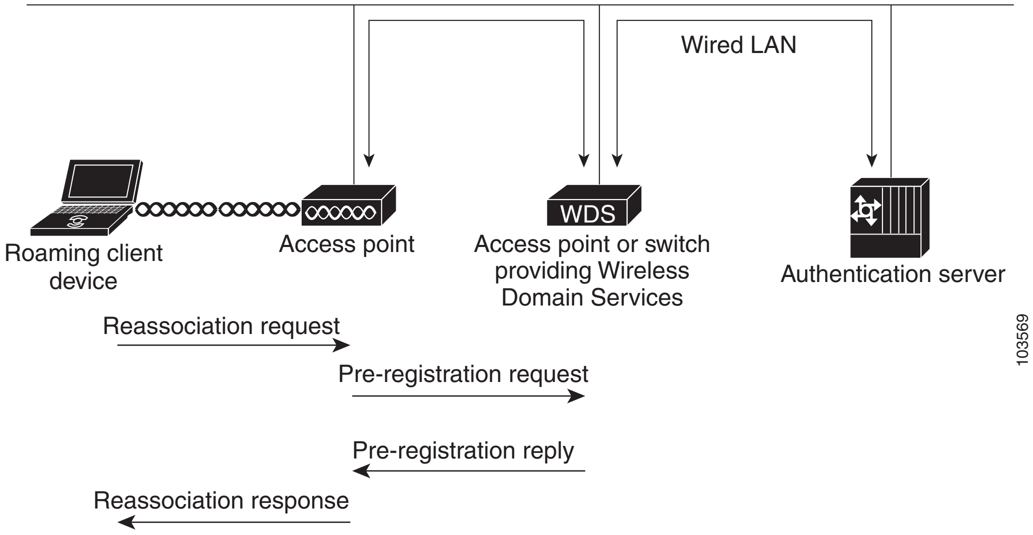
During normal operation, EAP/802.1x-enabled client devices mutually authenticate with a new access point by performing a complete EAP/802.1x authentication, including communication with the main RADIUS server, as in Figure 12-1.

Figure 12-1 Example of Client Authentication Exchange using a RADIUS Server (LEAP case)



When you configure your wireless LAN for fast, secure roaming, however, EAP/802.1x-enabled client devices roam from one access point to another without involving the main RADIUS server. Using Cisco Centralized Key Management (CCKM), a device configured to provide Wireless Domain Services (WDS) takes the place of the RADIUS server and authenticates the client so quickly that there is no perceptible delay in voice or other time-sensitive applications. Figure 12-2 shows client authentication using CCKM.

Figure 12-2 Client Reassociation Using CCKM and a WDS Access Point



The WDS device maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the client sends a reassociation request to the new access point, and the new access point relays the request to the WDS device. The WDS device forwards the client's credentials to the new access point, and the new access point sends the reassociation response to the client. Only two packets pass between the client and the new access point, greatly shortening the reassociation time. The client also uses the reassociation response to generate the unicast key. Refer to the "Configuring Fast Secure Roaming" section on page 12-17 for instructions on configuring access points to support fast, secure roaming.

Note This mechanism also requires the client to accept the credentials that are being passed from one AP to the other. Make sure that you enable CCKM on the access points, and also make sure that your wireless client supports CCKM for the authentication mechanism (with CCX) used in your network. Without CCKM support, the client may refuse the fast roaming mechanism and force a re-authentication through the RADIUS server.
To know the CCX versions needed for each authentication mechanism, go to the following URL:
http://www.cisco.com/web/partners/pr46/pr147/program_additional_information_new_release_features.html
To know the CCX version supported by each client type, go to the following URL:
http://www.cisco.com/web/partners/pr46/pr147/partners_pgm_partners_0900aecd800a7907.html

Understanding Wireless Intrusion Detection Services

When you implement Wireless Intrusion Detection Services (WIDS) on your wireless LAN, your access points, and an optional (non-Cisco) WIDS engine work together to detect and prevent attacks on your wireless LAN infrastructure and associated client devices.

Working with the (non-Cisco) WIDS engine, access points can detect intrusions and take action to defend the wireless LAN.

WIDS consists of these features:

- Switch port tracing and rogue suppression—Switch port tracing and suppression uses an RF detection method that produces the radio MAC address of an unknown radio (a potential rogue device). The (non-Cisco) WIDS engine derives a wired-side MAC address from the wireless MAC address and uses it to search the switch's BRIDGE MIB.
- Excessive management frame detection—Excessive management frames indicate an attack on your wireless LAN. An attacker might carry out a denial-of-service attack by injecting excessive management frames over the radio to overwhelm access points which have to process the frames. As part of the WIDS feature set, access points in scanning mode and root access points monitor radio signals and detect excessive management frames. When they detect excessive management frames, the access points generate a fault and send it through the WDS to the non-Cisco) WIDS engine.
- Authentication/protection failure detection—Authentication/protection failure detection looks for attackers who are either trying to overcome the initial authentication phase on a wireless LAN or to compromise the ongoing link protection. These detection mechanisms address specific authentication attacks:
  - EAPOL flood detection
  - MIC/encryption failures detection
  - MAC spoofing detection
- Frame capture mode—In frame capture mode, a scanner access point collects 802.11 frames and forwards them to the address of a WIDS engine on your network.

Note See the "Configuring Access Points to Participate in WIDS" section on page 12-26 for instructions on configuring the access point to participate in WIDS and Configuring Management Frame Protection, page 12-21 for instructions on configuring the access point for MFP.

- 802.11 Management Frame Protection (MFP)—Wireless is an inherently broadcast medium enabling any device to eavesdrop and participate either as a legitimate or rogue device. Since control and management frames are used by client stations to select and initiate a session with an AP, these frames must be open. While management frames cannot be encrypted, they must be protected from forgery. MFP is a means by which the 802.11 management frames can be integrity protected.

Configuring WDS

This section describes how to configure WDS on your network. This section contains these sections:

Guidelines for WDS

Follow these guidelines when configuring WDS:

- A WDS access point that also serves client devices supports up to 30 participating access points, but a WDS access point with radios disabled supports up to 60 participating access points.

  In WDS only mode, the WDS supports up to 60 infrastructure access points and 1200 clients.
- Repeater access points do not support WDS. Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to return (fall back) to repeater mode in case of Ethernet failure.

Requirements for WDS

To configure WDS, you must have these items on your wireless LAN:

- At least one access point, Integrated Services Router (ISR)
- An authentication server (or an access point or ISR configured as a local authenticator)

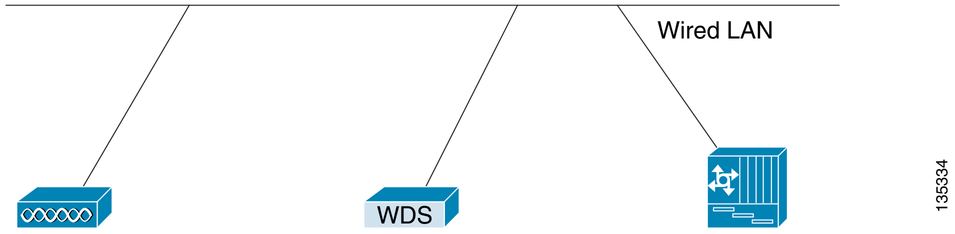
Configuration Overview

You must complete three major steps to set up WDS and fast, secure roaming:

1. Configure access points, ISRs, or switches as potential WDS devices. This chapter provides instructions for configuring an access point as a WDS device.
2. Configure the rest of your access points to use the WDS device.
3. Configure the authentication server on your network to authenticate the WDS device and the access points that use the WDS device.

Figure 12-3 shows the required configuration for each device that participates in WDS.

Figure 12-3 Configurations on Devices Participating in WDS



Access point:

- Wireless Services enabled
- Username and password for authentication to the server

WDS device:

- Configured as a WDS candidate
- If an access point serving client devices, username and password for authentication to the server

Authentication server

- WDS access point entered as an infrastructure device
- Access points that use the WDS entered on the server as client devices with usernames and passwords that match those configured on the access points

Configuring Access Points as Potential WDS Devices

Note For the main WDS candidate, configure an access point that does not serve a large number of client devices. If client devices associate to the WDS access point when it starts up, the clients might wait several minutes to be authenticated.

Note Repeater access points do not support WDS. Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to fall back to repeater mode in case of Ethernet failure.

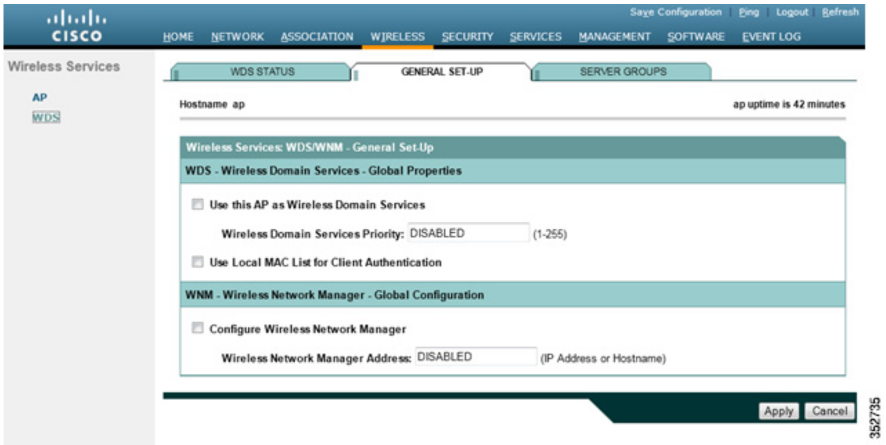
Note When WDS is enabled, the WDS access point performs and tracks all authentications. Therefore, you must configure EAP security settings on the WDS access point. See Chapter 11, "Configuring Authentication Types," for instructions on configuring EAP on the access point.

On the access point that you want to configure as your primary WDS access point, follow these steps to configure the access point as the main WDS candidate:

Step 1 Choose **Wireless** > **WDS**.

Step 2 Click **General Set-Up** tab.

Figure 12-4 General Setup Hostname ap page


Save Configuration | Ping | Logout | Refresh
CISCO
HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
Wireless Services
AP
WDS
WDS STATUS
GENERAL SET-UP
SERVER GROUPS
Apply
Cancel
352735

Hostname ap

ap uptime is 42 minutes

Wireless Services: WDS/WNM - General Set-Up

WDS - Wireless Domain Services - Global Properties

□ Use this AP as Wireless Domain Services

Wireless Domain Services Priority: DISABLED (1-255)

□ Use Local MAC List for Client Authentication

WNM - Wireless Network Manager - Global Configuration

□ Configure Wireless Network Manager

Wireless Network Manager Address: DISABLED (IP Address or Hostname)

Step 3 Check the ***Use this AP as Wireless Domain Services*** check box.

Step 4 In the Wireless Domain Services Priority field, enter a priority number from 1 to 255 to set the priority of this WDS candidate.

The WDS access point candidate with the highest number in the priority field becomes the acting WDS access point. For example, if one WDS candidate is assigned priority 255 and one candidate is assigned priority 100, the candidate with priority 255 becomes the acting WDS access point.

Step 5 (Only for WDS clients) Check the **Use Local MAC List for Client Authentication** check box to authenticate client AP devices using MAC addresses in the local list of addresses configured on the WDS device.

If you do not check this check box, the WDS device uses the server specified for MAC-address authentication on the Server Groups page to authenticate clients based on MAC addresses.

Note Checking the **Use Local MAC List for Client Authentication** check box does not force client devices to perform MAC-based authentication. It provides a local alternative to server-based MAC-address authentication.

Step 6 Click **Apply**.

Step 7 Click **Server Groups** tab to go to the WDS Server Groups page.

Step 8 Create a group of servers to be used for 802.1x authentication for the infrastructure devices (access points) that use the WDS access point. Enter a group name in the Server Group Name field.

Step 9 Select the primary server from the Priority 1 drop-down list. (If a server that you need to add to the group does not appear in the Priority drop-down lists, click **Define Servers** to browse to the Server Manager page. Configure the server there, and then return to the WDS Server Groups page.)

Note If you do not have an authentication server on your network, you can configure an access point or an ISR as a local authentication server. See Chapter 9, "Configuring an Access Point as a Local Authenticator," for configuration instructions.

Step 10 (Optional) Select backup servers from the Priority 2 and 3 drop-down lists.

Step 11 Click **Apply**.

Step 12 Configure the list of servers to be used for 802.1x authentication for wireless client devices. You can specify a separate list for clients using a certain type of authentication, such as EAP, LEAP, other EAP types, or MAC-based, or specify a list for client devices using any type of authentication. Enter a group name for the server or servers in the Server Group Name field.

The LEAP Authentication check box is present specifically for the Cisco clients identified below:

- Cisco 7920, 7921, and 7925 phones using LEAP
- Autonomous APs configured as wireless clients (workgroup bridge or non-root bridge) and using LEAP authentication

Unchecking the LEAP authentication check box prevents these client devices from authenticating to the wireless network using LEAP and the WDS service. The clients can connect using any other form of EAP authentication if the EAP option is selected. However, this does not prevent other client cards or supplicant combinations from connecting, because these clients use the 802.1X standard for all form of EAP authentications, including LEAP. This information does not apply to non-Cisco clients.

Step 13 Select the primary server from the Priority 1 drop-down list. (If a server that you need to add to the group does not appear in the Priority drop-down lists, click **Define Servers** to browse to the Server Manager page. Configure the server there, and then return to the WDS Server Groups page.)

Step 14 (Optional) Select backup servers from the Priority 2 and 3 drop-down lists.

Step 15 (Optional) Select **Restrict SSIDs** to limit use of the server group to client devices using specific SSIDs. Enter an SSID in the SSID field and click **Add**. To remove an SSID, highlight it in the SSID list and click **Remove**.

Step 16 Click **Apply**.

Step 17 Configure the WDS access point for EAP authentication. See Chapter 11, "Configuring Authentication Types," for instructions on configuring EAP.

Note This authentication uses LEAP by default. Infrastructure access points using the WDS service need to be authenticated through the WDS device. If your WDS access point serves client devices, follow the instructions in the "Configuring Access Points to use the WDS Device" section on page 12-10 to configure the WDS access point to use the WDS.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Configuring Access Points as Potential WDS Devices" section on page 12-7:

```
AP# configure terminal
AP(config)# aaa new-model
AP(config)# wlccp wds priority 200 interface bvi1
AP(config)# wlccp authentication-server infrastructure infra_devices
AP(config)# wlccp authentication-server client any client_devices
AP(config-wlccp-auth)# ssid fred
AP(config-wlccp-auth)# ssid ginger
AP(config)# end
```

In this example, infrastructure devices are authenticated using server group *infra_devices*; client devices using SSIDs *fred* or *ginger* are authenticated using server group *client_devices*. If you do not specify the SSID list, all SSIDs are included.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

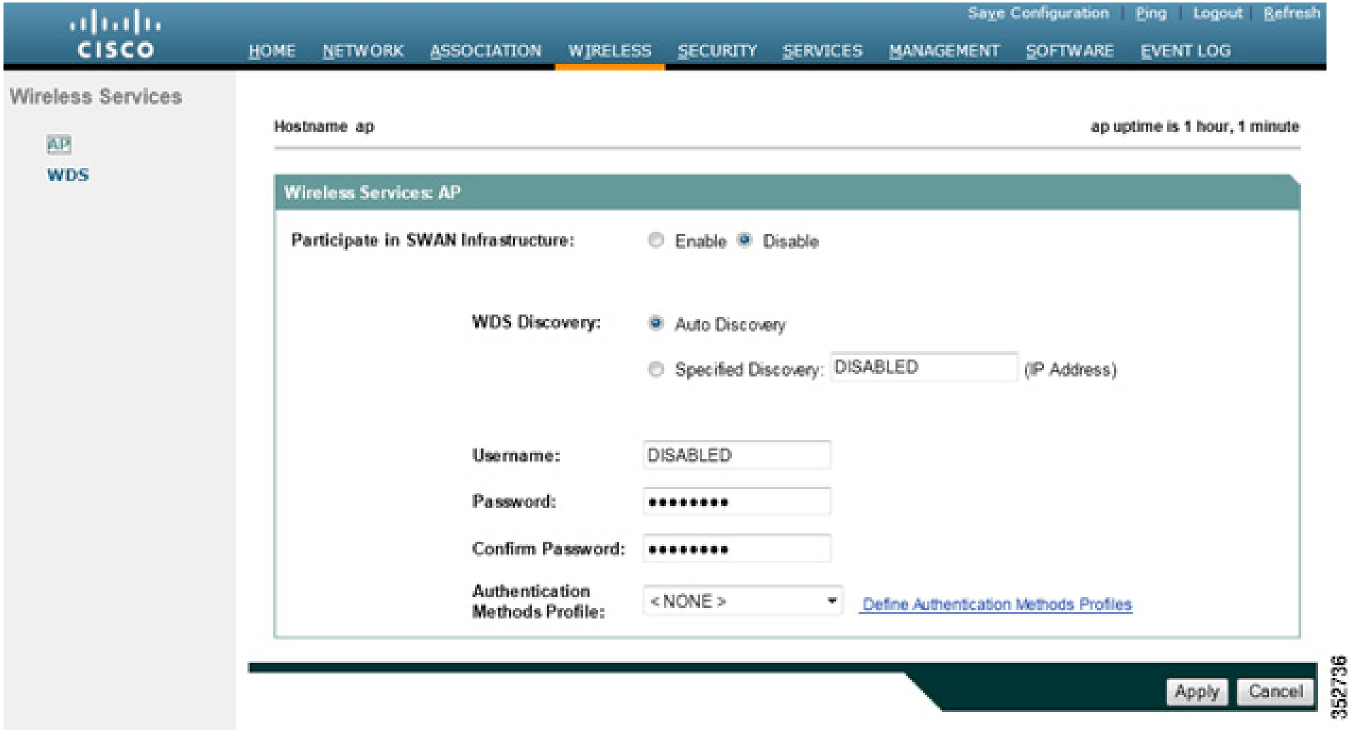
Configuring Access Points to use the WDS Device

Follow these steps to configure an access point to authenticate through the WDS device and participate in WDS:

Note To participate in WDS, infrastructure access points should run the same version of IOS as the one that WDS runs.

Step 1 Choose **Wireless > AP**. The Wireless Services AP page appears.

Figure 12-5 Wireless Services AP page



Hostname ap

ap uptime is 1 hour, 1 minute

Wireless Services: AP

Participate in SWAN Infrastructure: ○ Enable ● Disable

WDS Discovery: ● Auto Discovery

○ Specified Discovery: DISABLED (IP Address)

Username: DISABLED

Password: ••••••••

Confirm Password: ••••••••

Authentication Methods Profile: < NONE >

Step 2 Click **Enable** for the *Participate in SWAN Infrastructure* setting, to enable the AP to use the WDS service for client authentication.

Step 3 (Optional) Select **Specified Discovery** and enter the IP address of the WDS in the entry field. When you enable Specified Discovery, the access point immediately authenticates with the WDS device instead of waiting for WDS advertisements. If the WDS device that you specify does not respond, the access point waits for WDS advertisements.

Step 4 In the Username field, enter a username for the access point. This username must match the username that you create for the access point on your authentication server.

Step 5 In the Password field, enter a password for the access point, and enter the password again in the Confirm Password field. This password must match the password that you create for the access point on your authentication server. When configuring the username and password in this page, the AP uses LEAP to authenticate through the WDS server.

Step 6 (Optional) If you do not want your infrastructure AP to be authenticated through the WDS using LEAP, but want to use another EAP authentication method (for example EAP-FAST), select another authentication method profile from the Authentication Methods Profile drop down list. If you have not defined Authentication Method Profiles yet, click the **Define Authentication Method Profiles** link, configure a profile, then return to the Wireless Services AP configuration page to select the profile. See the Creating and Applying EAP Method Profiles for the 802.1X Supplicant, page 11-17 for more details on how to create a new profile.

Step 7 Click **Apply**.

The access points that you configure to interact with the WDS automatically perform these steps:

- Discover and track the current WDS device and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS device and establish a secure communication channel to the WDS device.
- Register associated client devices with the WDS device.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Configuring Access Points to use the WDS Device" section on page 12-10:

```
AP# configure terminal
AP(config)# wlccp ap username APWestWing password 0 wes7win8
AP(config)# wlccp ap eap profile Myfast
AP(config)# end
```

In this example, the access point is enabled to interact with the WDS device, and it authenticates to your authentication server using *APWestWing* as its username and *wes7win8* as its password.

An optional Myfast EAP profile is called to authenticate using another method than LEAP. In this example, the profile uses EAP-FAST, and is configured as follows:

```
ap(config)# eap profile myfast
ap(config-eap-profile)# method fast
ap(config-eap-profile)# end
```

You must configure the same username and password pair when you set up the access point as a client on your authentication server.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Configuring the Authentication Server to Support WDS

The WDS device and all access points participating in WDS must authenticate to your authentication server. On your server, you must configure usernames and passwords for the access points and a username and password for the WDS device.

If your server runs Cisco ACS, follow these steps to configure the access points on your server:

Step 1 Log into Cisco Identity Services Engine (ISE).

Step 2 Choose **Administration > Network Resources > Network devices**.
The Network Devices page appears.
Here you can add the WDS as a AAA client.

Figure 12-6 Cisco ISE Network Devices Page

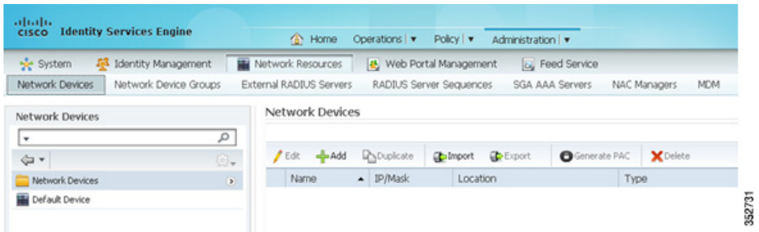
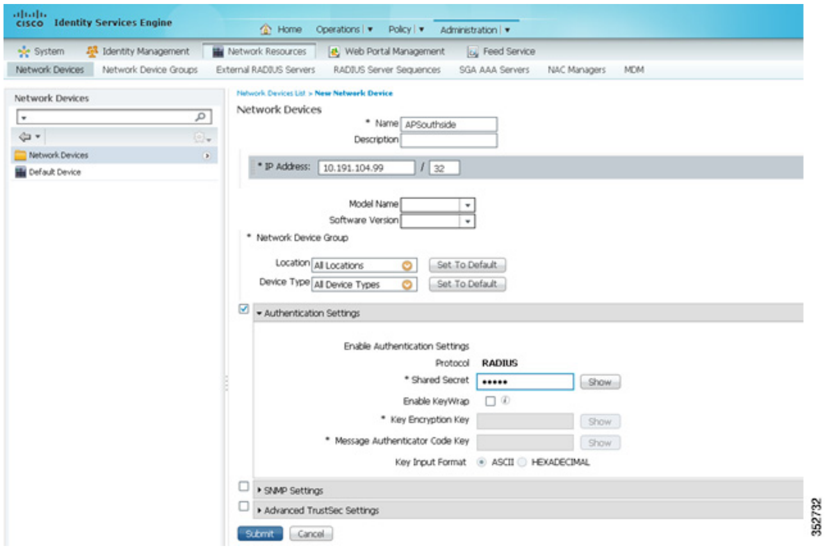


Figure 12-7 Cisco ISE Network Devices Page Detailed



* Name: APSouthside
Description:
* IP Address: 10.191.104.99 / 32
Model Name:
Software Version:
* Network Device Group
Location: All Locations
Device Type: All Device Types
☑ Authentication Settings
Enable Authentication Settings
Protocol: RADIUS
* Shared Secret: •••••
Enable KeyWrap: □
* Key Encryption Key:
* Message Authenticator Code Key:
Key Input Format: ● ASCII ○ HEXADECIMAL
□ SNMP Settings
□ Advanced TrustSec Settings

Step 3 Click **Add** to add the WDS as a new AAA client.

Step 4 In the Name field, enter the WDS device name. This name is significant only locally.
Optionally, enter a description for the WDS device.

Step 5 In the IP address field, enter the IP address of the WDS device.
Optionally, specify the device location and device type, but only if these categories have been configured on the ISE.

Step 6 Check the **Authentication Settings** check box. The fields in the Authentication Settings area get enabled.

Step 7 For the RADIUS protocol, in the Shared Secret field, enter a shared secret value. This value will be entered identically on the WDS device when configuring the ISE as a RADIUS server.

Step 8 Click **Submit** to validate your entries.

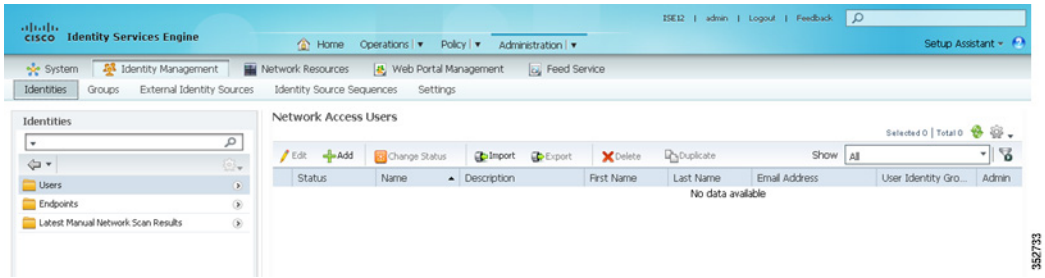
Step 9 Repeat Step 3 to Step 8 for each WDS device candidate.

Step 10 Choose **Administration > Identities Management > Identities**.
The Network Access Users page appears.

Note This procedure shows configuration of users in the ISE internal database. ISE can also use an external database. Please see the ISE guide for more details.

Step 11 Click **Add** to add a new user.

Figure 12-8 Network Access Users page



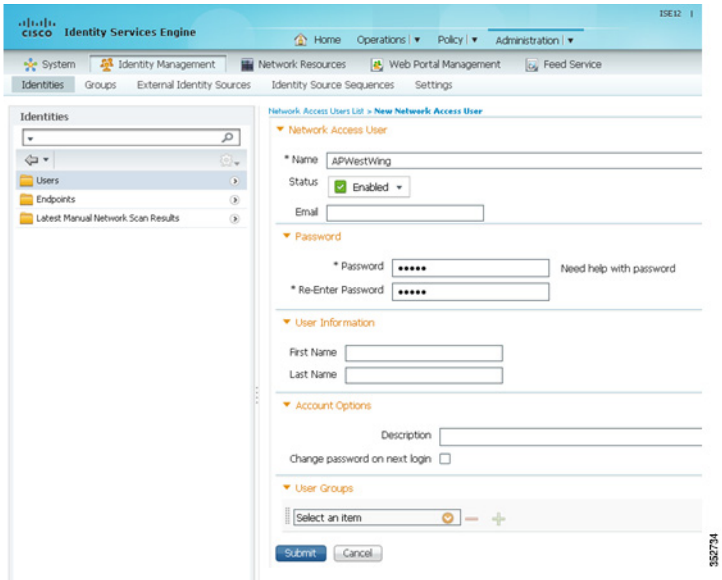
Step 12 In the Name field, enter the username configured for the access point client to the WDS.

Step 13 In the Password and Confirm Password fields, enter the exact same password that you entered on the access point on the Wireless Services AP page.

Step 14 Click **Submit**.

Step 15 Repeat Step 11 to Step 14 for each access point that uses the WDS device.

Figure 12-9 Cisco ISE Network Access Users page detailed



Network Access User

* Name APWestWing

Status Enabled

Email

Password

* Password •••••

* Re-Enter Password •••••

User Information

First Name

Last Name

Account Options

Description

Change password on next login □

User Groups

Select an item

Configuring WDS Only Mode

WDS access points can operate in WDS only mode using the **wlccp wds mode wds-only** command. After issuing this command and reloading, the access point starts working in the WDS only mode. In WDS only mode, the dot11 subsystems are not initialized and the dot11 interface related commands cannot be configured. In WDS only mode, the WDS supports up to 60 infrastructure access points and up to 1200 clients. Use the **no** form of this command to turn off WDS only mode. Use the **show wlccp wds** command to display the working mode of the WDS access point.

To set the WDS access point to operate in both AP and WDS modes, use the **no wlccp wds mode wds-only** command and use the **write erase** command to reload the access point immediately. After the access point reloads, the dot11 radio subsystems initialize. The access point and WDS associate directly to wireless clients. In this mode, the WDS supports 30 infrastructure access points and 600 clients in addition to 20 direct wireless client associations.

Viewing WDS Information

On the web-browser interface, browse to the Wireless Services Summary page to view a summary of WDS status.

On the CLI in privileged exec mode, use these commands to view information about the current WDS device and other access points participating in CCKM:

Command	Description
show wlccp ap	Use this command on access points participating in CCKM to display the WDS device's MAC address, the WDS device's IP address, the access point's state (authenticating, authenticated, or registered), the IP address of the infrastructure authenticator, and the IP address of the client device (MN) authenticator.
show wlccp wds ap [**cdp-neighbor** | **mac-address** *mac-address* | **order ip**]	On the WDS device only, use this command to display cached information about access points participating in CCKM. • cdp-neighbor—displays the CDP neighbors reported by each AP authenticated through the WDS. • mac-address *mac-address*—displays information only on the AP specified byt the entered MAC address. • order ip—changes the order used to display the AP, from ascending using the AP MAC address, to ascending using the AP IP address.
show wlccp wds mn [**detail**] [**mac-addr** *mac-address*]	Use this command to display cached information about client devices, also called mobile nodes. The command displays each client's MAC address, IP address, the access point to which the client is associated (cur-AP), and state (authenticating, authenticated, or registered). Use the detail option to display the client's lifetime (seconds remaining before the client must reauthenticate), SSID, and VLAN ID. Use the **mac-address** option to display information about a specific client device.
show wlccp wds	Use this command to display the access point's IP address, MAC address, priority, and interface state (administratively standalone, active, backup, candidate, or WDS-only). If the state is backup, the command also displays the current WDS device's IP address, MAC address, and priority.
show wlccp wds nm	Use this command to display the list of all configure network management platforms, along with statistics (transmitted and received messages, retransmissions, and dropped messages).

Command	Description
show wlccp wds statistics	Use this command to display statistics about the WDS. This includes Current AP count, Current client count on connected APs, AAA Authentication Attempt count, AAA Authentication Success count, AAA Authentication Failure count, MAC Spoofing Block count, Roaming without AAA Authentication count (Pre-shared key and Open networks), Roaming with full AAA Authentication count (for non-CCX devices not supporting fast secure roaming), Fast Secured Roaming count, MSC Failure count, KSC Failure count, MIC Failure count (to detect WPA/WPA2 replay attacks), and RN Mismatch count (to detect WPA2 mismatches)
show wlccp wds aggregator statistics	Use this command to display statistics about Radio Measurement information collected from participating APs (received and forwarded updates)

Using Debug Messages

In privileged exec mode, use these debug commands to control the display of debug messages for devices interacting with the WDS device:

Command	Description
debug wlccp ap {**mn** | **nm** | **wds-discovery** | **state**}	Use this command to turn on display of debug messages related to client devices (**mn**), configured management platforms (**nm**), the WDS discovery process, and access point authentication to the WDS device (**state**).
debug wlccp dump	Use this command to perform a dump of WLCCP packets received and sent in binary format.
debug wlccp packet	Use this command to turn on display of packets to and from the WDS device.
debug wlccp rmlib { errors | packets }	Use this command to debug radio measurement messages exchanged between the AP and the WDS, and between the WDS and the Network management platform, when applicable.

Command	Description
debug wlccp wds [aggregator | all | ap | authenticator | mn | nm | recovery | state | statistics]	Use this command and its options to turn on display of WDS debug messages. Use the **ap** option for debugging WDS events for all APs. You can optionally specify a mac-address also to debug the events of that specific AP. Use the **all** option to debug all WDS events. Use the **nm** option to debug messages exchanged with the network management platform when applicable Use the **recovery** option to debug the WDS failover (graceful recovery) process. Use the **statistics** option to turn on display of failure statistics.
debug wlccp wds authenticator {**all** | **dispatcher** | **mac-authen** | **process** | **rxdata** | **state-machine** | **txdata**}	Use this command and its options to turn on display of WDS debug messages related to authentication.

Configuring Fast Secure Roaming

After you configure WDS, access points configured for CCKM can provide fast, secure roaming for associated client devices. This section describes how to configure fast, secure roaming on your wireless LAN. This section contains these sections:

- Requirements for Fast Secure Roaming
- Configuring Access Points to Support Fast Secure Roaming

Requirements for Fast Secure Roaming

To configure fast secure roaming, you must have these items on your wireless LAN:

- At least one access point, ISR configured as the WDS device
- Access points configured to participate in WDS
- Access points configured for fast, secure roaming
- An authentication server (or an access point, ISR configured as a local authenticator)
- Cisco Aironet client devices, or Cisco-compatible client devices that comply with Cisco Compatible Extensions (CCX) Version 2 or later

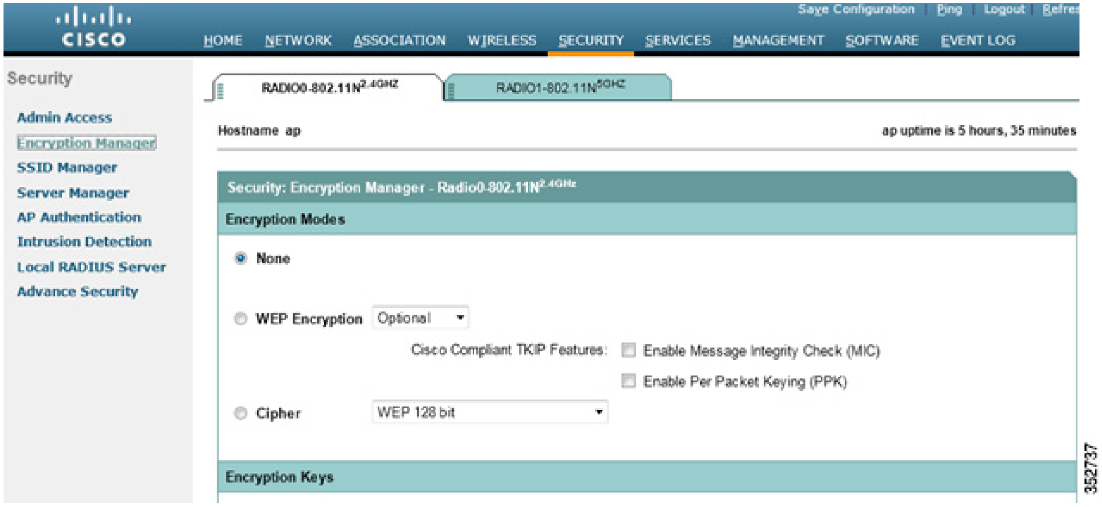
For instructions on configuring WDS, refer to the "Configuring WDS" section on page 12-5.

Configuring Access Points to Support Fast Secure Roaming

To support fast, secure roaming, the access points on your wireless LAN must be configured to participate in WDS and they must allow CCKM authenticated key management for the target SSIDs. Follow these steps to configure CCKM for an SSID:

Step 1 Browse to the Encryption Manager page on the access point GUI. Figure 12-10 shows the top section of the Encryption Manager page.

Figure 12-10 Encryption Manager Page



Hostname ap

ap uptime is 5 hours, 35 minutes

Security: Encryption Manager - Radio0-802.11N2.4GHz

Encryption Modes

● None

○ WEP Encryption Optional

Cisco Compliant TKIP Features: □ Enable Message Integrity Check (MIC)

□ Enable Per Packet Keying (PPK)

○ Cipher WEP 128 bit

Encryption Keys

Step 2 Click the **Cipher** button.

Step 3 Configure the encryption mechanism of your choice. Cisco recommends using WPA2 (except if you need to support legacy clients not supporting WPA2). To set the encryption mechanism to WPA2, choose AES CCMP from the Cipher drop-down list.

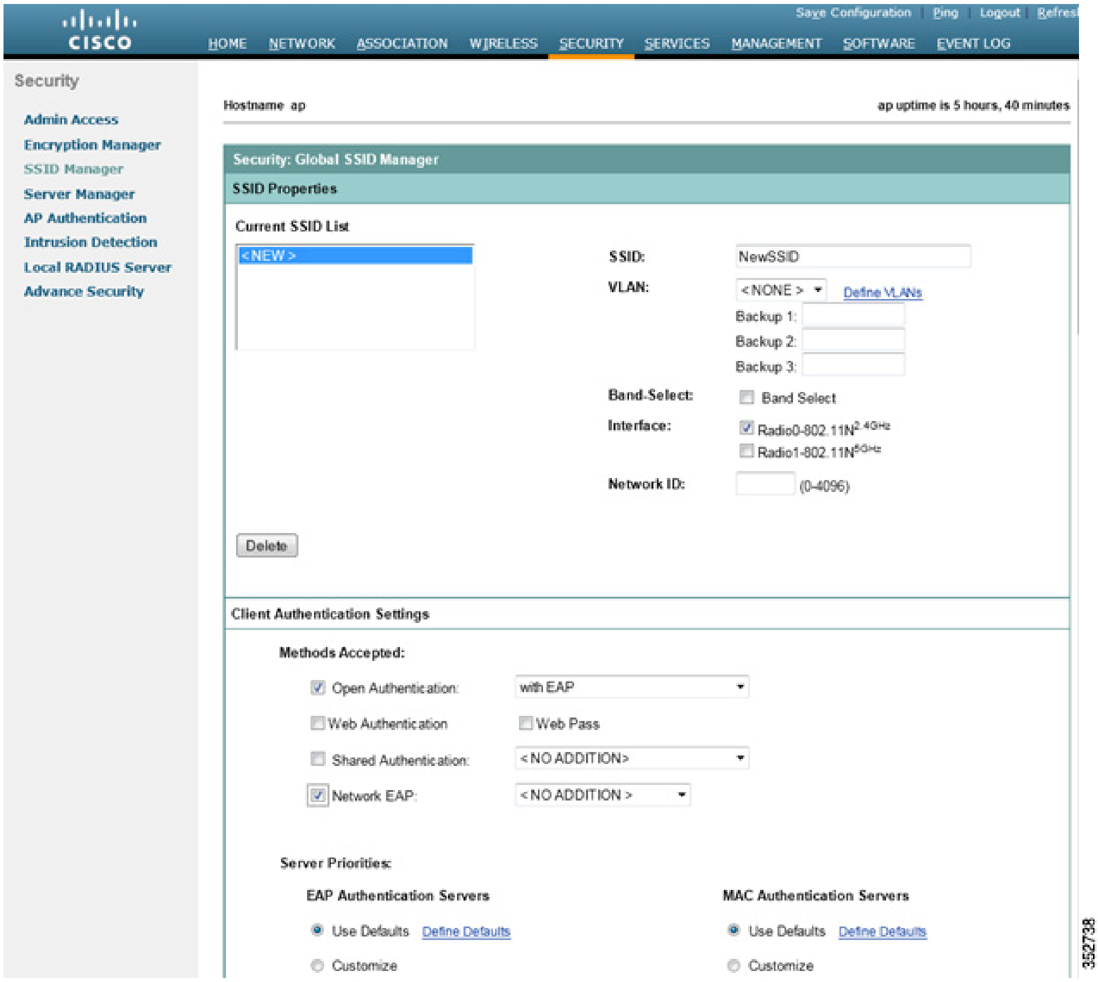
Note Cisco does not recommend configuring mixed modes (AES CCMP with TKIP and or WEP), as these modes are being deprecated and lower the security of your network.

Step 4 Select **CKIP + CMIC** from the Cipher drop-down list.

Step 5 Click **Apply**.

Step 6 Browse to the Global SSID Manager page. Figure 12-11 shows the top sections of the Global SSID Manager page.

Figure 12-11 Global SSID Manager Page



Hostname ap

ap uptime is 5 hours, 40 minutes

Security: Global SSID Manager

SSID Properties

Current SSID List

<NEW>

SSID: NewSSID

VLAN: < NONE > Define VLANs

Backup 1:

Backup 2:

Backup 3:

Band-Select: □ Band Select

Interface: ☑ Radio0-802.11N$^{2.4GHz}$

□ Radio1-802.11N^{5GHz}

Network ID: (0-4096)

Delete

Client Authentication Settings

Methods Accepted:

☑ Open Authentication: with EAP

□ Web Authentication □ Web Pass

□ Shared Authentication: < NO ADDITION>

☑ Network EAP: < NO ADDITION >

Server Priorities:

EAP Authentication Servers

● Use Defaults Define Defaults

○ Customize

MAC Authentication Servers

● Use Defaults Define Defaults

○ Customize

Step 7 On the target SSID where CCKM (fast secure roaming) needs to be supported, select these settings:

- **a.** If your access point contains multiple radio interfaces, select the interfaces on which the SSID applies.
- **b.** Under network settings, choose the 802.1X/EAP methods to be supported. **Network EAP** should be selected for LAP support with Cisco IP phones 7920, 7921, 7925 and 7926, and for client access points. **Open Authentication with EAP** should be selected for any other EAP type (e.g. PEAP, EAP-FAST, or EAP-TLS), and for all EAP types (including LEAP) for all other clients.
- **c.** Under Client Authenticated Key Management area, in the Key Management drop-down list choose **Mandatory** or **Optional** as required. If you select **Mandatory**, only clients that support CCKM can associate using the SSID. If you select Optional, both CCKM clients and clients that do not support CCKM can associate using the SSID.
- **d.** Check the **CCKM** check box.
- **e.** If you have selected the AES CCMP Cipher, check the Enable WPA check box, and choose the **WPAv2 option** from the drop-down list

Step 8 Click **Apply**.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Configuring Access Points to Support Fast Secure Roaming" section on page 12-18:

```
AP# configure terminal
AP(config)# dot11 ssid NewSSID
AP(config-ssid)# authentication open eap eap_methods
AP(config-ssid)# authentication key-management wpa version 2 cckm
AP(config-ssid)# exit
AP(config)# interface dot11radio0
AP(config-if)# encryption mode ciphers aes-ccm
AP(config-if)# ssid NewSSID
AP(config-if)# exit
AP(config)# end
```

In this example, the SSID *NewSSID* is configured to support EAP with CCKM, the AES CCMP cipher suite is enabled on the 2.4-GHz radio interface, and the SSID *NewSSID* is enabled on the 2.4-GHz radio interface.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Support for 802.11r

Support for 802.11r is provided in Autonomous access points. WGB, Non-root bridge, and repeaters are not supported in 802.11r. It supports only clients.

These types of roaming are supported over the wireless domain services:

- Fast transition over Distributed System (DS)
- Fast transition over Air

802.11r differs from Cisco Centralized Key Management (CCKM) and Pairwise Master Key Identifier (PMKID) roaming in these ways:

- Initial authentication occurs before roaming
- Authentication with the target AP over the Air, or through the DS uses the existing access point's communication channel

Enabling 802.11r

To enable 802.11r, perform these steps:

Step 1 Choose **Network > Network interface**.

Step 2 Click the **Settings** tab.

Step 3 Choose **Radio0-802.11n 2G.Hz** or **Radio0-802.11n 5G.Hz**.

Step 4 Click the **enable** radio button for 11r Configuration.

Step 5 Click the **over-air** or **over-ds** radio button.

Step 6 Enter the reassociation time.

The values range from 20 to 1200.

Step 7 Click **Apply**.

Beginning in privileged EXEC mode, perform these steps to configure 802.11r using the access point CLI:

	Command	Purpose
Step 1	**configure terminal**	Enters the global configuration mode.
Step 2	**dot11 ssid** <*ssid*>	Configures the SSID.
Step 3	**authentication key-management wpa version 2 dot11r**	Configures 802.11r on an access point.
Step 4	**interface dot11radio** {*0* | *1*}	Enters interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 5	**dot11 dot11r pre-authentication {over-air | over-ds}**	Enables or disables the over-air or over-ds transition.
Step 6	**dot11 dot11r re-association timer** <*value*>	Configures the reassociation timer.

Configuring Management Frame Protection

Management Frame Protection operation requires a WDS. You can configure MFP on an access point and WDS manually.

Note Without a management platform, MFP cannot report detected intrusions and so has limited effectiveness.

For complete protection, you should also configure an MFP access point for Simple Network Transfer Protocol (SNTP).

Management Frame Protection

Management Frame Protection provides security features for the management messages passed between Access Point and Client stations. MFP consists of two functional components: Infrastructure MFP and Client MFP.

Infrastructure MFP provides Infrastructure support. Infrastructure MFP utilizes a message integrity check (MIC) across broadcast and directed management frames which can assist in detection of rogue devices and denial of service attacks. Client MFP provides client support. Client MFP protects authenticated clients from spoofed frames, by preventing many of the common attacks against WLANs from becoming effective.

Client MFP Overview

Client MFP encrypts class 3 management frames sent between access points and CCXv5-capable client stations, so that both AP and client can take preventative action by dropping spoofed class 3 management frames (i.e. management frames passed between an AP and a client station that is authenticated and associated). Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect class 3 Unicast management frames. The unicast cipher suite negotiated by the STA in the reassociation request's RSNIE is used to protect both unicast data and class 3 management frames. An access point in workgroup bridge, repeater, or non-root bridge mode must negotiate either TKIP or AES-CCMP to use Client MFP.

Unicast class 3 management frames are protected by applying either AES-CCMP or TKIP in a similar manner to that already used for data frames. Client MFP is enabled for autonomous access points only if the encryption is AES-CCMP or TKIP and key management WPA Version 2.

In order to prevent attacks using broadcast frames, access points supporting CCXv5 and configured for Client MFP, do not emit any broadcast class 3 management frames. An access point in workgroup bridge, repeater, or non-root bridge mode discards broadcast class 3 management frames if Client MFP is enabled.

Client MFP is enabled for autonomous access points only if the encryption is AES-CCMP or TKIP and key management WPA Version 2.

Note Cisco recommends using WPA2, and not implementing TKIP with WPA version 2, as this mode is being deprecated.

Client MFP For Access Points in Root mode

Autonomous access points in root mode support mixed mode clients. Clients capable of CCXv5 with negotiated cipher suite AES or TKIP with WPAv2 are Client MFP enabled. Client MFP is disabled for clients which are not CCXv5 capable. By default, Client MFP is optional for a particular SSID on the access point, and can be enabled or disabled using the CLI in SSID configuration mode.

Client MFP can be configured as either required or optional for a particular SSID. To configure Client MFP as required, you must configure the SSID with key management WPA Version 2 mandatory. If the key management is not WPAv2 mandatory, an error message is displayed and your CLI command is rejected. If you attempt to change the key management with Client MFP configured as required and key management WPAv2, an error message displays and rejects your CLI command. When configured as optional, Client MFP is enabled if the SSID is capable of WPAv2, otherwise Client MFP is disabled.

Configuring Client MFP

Command	Description
ids mfp client required	This SSID configuration command enables Client MFP as required on a particular SSID. The Dot11Radio interface is reset when the command is executed if the SSID is bound to the Dot11Radio interface. The command also expects that the SSID is configured with WPA Version 2 mandatory. If the SSID is not configured with WPAv2 mandatory, an error message displays and the command is rejected. The **no** form of this command disables Client MFP on a particular SSID. The Dot11Radio interface is reset when the command is executed if the SSID is bound to the Dot11Radio interface.
ids mfp client optional	This ssid configuration command enables Client MFP as optional on a particular SSID. The Dot11Radio interface is reset when the command is executed if the SSID is bound to the Dot11Radio interface. Client MFP is enabled for this particular SSID if the SSID is WPAv2 capable, otherwise Client MFP is disabled.
authentication key management wpa version {1|2}	Use this command to explicitly specify which WPA Version to use for WPA key management for a particular SSID.
dot11 ids mfp {generator | detector}	Configures the access point as an MFP generator. When enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame will invalidate the MIC, causing any receiving access point that is configured to detect (validate) MFP frames to report the discrepancy. The access point must be a member of a WDS. Configures the access point as an MFP detector. When enabled, the access point validates management frames it receives from other access points. If it receives any frame that does not contain a valid, and expected, MIC IE, it will report the discrepancy to the WDS. The access point must be a member of a WDS.
sntp server *server IP address*	Enter the name or ip address of the SNTP server.
dot11 ids mfp distributor	Beginning in global configuration mode, use this command to configure the WDS as an MFP distributor. When enabled, the WDS manages signature keys, used to create the MIC IEs, and securely transfers them between generators and detectors.

The following CLI commands can be used to display and clear Client MFP statistics on the access point console for a Dot11Radio interface.

Command	Description
show dot11 ids mfp client statistics	Use this command to display Client MFP statistics on the access point console for a Dot11Radio interface.
clear dot11 ids mfp client statistics	Use this command to clear the Client MFP statistics.

Protection of Management Frames with 802.11w

The current 802.11 standard defines frame types for use in the management and control of wireless links. The management frames, included in the 802.11 protocol, are neither authenticated nor encrypted, even when the highest level of WLAN security are used. 802.11w is the Protected Management Frames standard for the IEEE 802.11 family of standards.

802.11w increases the security of the management frames by offering three new security pieces:

- Data Origin Authenticity
- Replay Detection
- Robust Management Frame Protection.

The Management frames that can be protected are:

- Disassociation
- Deauthentication
- Robust Action frames excluding Public Action frames

802.11w is also used to prevent association request replay attack. The protection offered by 802.11w is somewhat comparable to the protection offered by Cisco Client MFP. However, 802.11w does not offer a mechanism comparable to Cisco Infrastructure MFP.

To enable Cisco Client MFP, you need to make sure that the clients to be protected support CCXv5. To enable 802.11w, you need to make sure that the clients to be protected support 802.11w.

Both Cisco Infrastructure MFP and 802.11w can be enabled on the same SSID. However, you should not enable Cisco Client MFP and 802.11w on both the same SSID and the same radio.

Perform these steps to enable 802.11w:

Step 1 Browse to the Security page on the access point GUI.

Step 2 Select SSID Manager.

Step 3 From the Client Authenticated Key Management page, you can:

- Click the **11w Configuration Required** radio button, to allow only clients that support 802.11w to join the SSID.
- Click the **11w Configuration Optional** radio button, to allow both clients supporting 802.11w and clients not supporting 802.11w to join the SSID.

Step 4 Enter the **11w Association-comeback** time.

Step 5 Enter the **11w Saquery-retry** time.

This CLI command is used to enable 802.11w on the access point:

```
ap(config-ssid)# 11w-pmf client required/optional
```

This CLI command is used to configure the association time out and saquery retry time interval:

```
ap(config-ssid)# 11w-pmf association-comeback 1000-20000ms
ap(config-ssid)# 11w-pmf saquery-retry 100-500ms
```

These commands are optional. Default time intervals are configured if these commands are not used. To configuring 802.11w on an access point, mfp client should be disable

Note WPAv2/AES is mandatory for 802.11w.

Note After 802.11r is enabled, the CCKM, 11r fast roaming, DLS, Radio Measurement and Protected Dual of Public Action frames are not supported.

Configuring Radio Management

When you configure access points on your wireless LAN to use WDS, the access points automatically play a role in radio management when they interact with the WDS device. To complete the radio management configuration, you configure the WDS device to interact with the management platform on your network.

Follow these steps to enable radio management on an access point configured as a WDS device:

Step 1 Browse to the Wireless Services Summary page.

Step 2 Click **WDS** to browse to the General Setup page.

Step 3 Check the ***Configure Wireless Network Manager*** check box.

Step 4 In the ***Wireless Network Manager IP Address*** field, enter the IP address of the management platform on your network.

Step 5 Click **Apply**. The WDS access point is configured to interact with your management platform.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Configuring Radio Management" section on page 12-25:

```
AP# configure terminal
AP(config)# wlccp wnm ip address 192.250.0.5
AP(config)# end
```

In this example, the WDS access point is enabled to interact with a management platform with the IP address 192.250.0.5.

For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Configuring Access Points to Participate in WIDS

To participate in WIDS, access points must be configured to participate in WDS and in radio management. Follow the steps in the "Configuring Access Points to use the WDS Device" section on page 12-10 and in the "Configuring Radio Management" section on page 12-25 to configure the access point to participate in WDS and in radio management.

Configuring the Access Point for Scanner Mode

In scanner mode, the access point scans all of its channels for radio activity and reports the activity to the WDS device on your network. A scanner access point does not accept client associations.

Beginning in privileged EXEC mode, follow these steps to set the access point radio network role to scanner:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	**station role scanner**	Set the access point role to scanner.
Step 4	**end**	Return to privileged EXEC mode.

Configuring the Access Point for Monitor Mode

When an access point is configured as a scanner it can also capture frames in monitor mode. In monitor mode, the access point captures 802.11 frames and forwards them to the WIDS engine on your network. The access point adds a 28-byte capture header to every 802.11 frame that it forwards, and the WIDS engine on your network uses the header information for analysis. The access point uses UDP packets to forward captured frames. Multiple captured frames can be combined into one UDP packet to conserve network bandwidth.

In scanner mode the access point scans all channels for radio activity. However, in monitor mode the access point monitors only the channel for which the access point radio is configured.

Note If your access point contains two radios, both radios must be configured for scanner mode before you can configure monitor mode on the interfaces.

Beginning in privileged EXEC mode, follow these steps to configure the access point to capture and forward 802.11 frames:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1**}	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	**monitor frames endpoint ip address** *IP-address* **port** *UDP-port* [**truncate** *truncation-length*]	Configure the radio for monitor mode. Enter the IP address and the UDP port on the WIDS engine on your network. • (Optional) Configure a maximum length in bytes for each forwarded frame. The access point truncates frames longer than this value. The default length is 128 bytes.
Step 4	**end**	Return to privileged EXEC mode.

Displaying Monitor Mode Statistics

Use the **show wlccp ap rm monitor statistics** global configuration command to display statistics on captured frames.

This example shows output from the command:

```
ap# show wlccp ap rm monitor statistics

Dot11Radio 0
====================
WLAN Monitoring           : Enabled
Endpoint IP address       : 10.91.107.19
Endpoint port             : 2000
Frame Truncation Length   : 535 bytes

Dot11Radio 1
====================
WLAN Monitoring           : Disabled

WLAN Monitor Statistics
==========================
Total No. of frames rx by DOT11 driver      : 58475
Total No. of Dot11 no buffers               : 361
Total No. of Frames Q Failed                : 0
Current No. of frames in SCAN Q             : 0

Total No. of frames captured                : 0
Total No. of data frames captured           : 425
Total No. of control frames captured        : 1957
Total No. of Mgmt frames captured           : 20287
Total No. of CRC errored frames captured: 0

Total No. of captured frames forwarded      : 23179
Total No. of captured frames forward failed : 0
```

Use the **clear wlccp ap rm statistics** command to clear the monitor mode statistics.

Configuring Monitor Mode Limits

You can configure threshold values that the access point uses in monitor mode. When a threshold value is exceeded, the access point logs the information or sends an alert.

Configuring an Authentication Failure Limit

Setting an authentication failure limit protects your network against a denial-of-service attack called *EAPOL flooding*. The 802.1X authentication that takes place between a client and the access point triggers a series of messages between the access point, the authenticator, and an authentication server using EAPOL messaging. The authentication server, typically a RADIUS server, can quickly become overwhelmed if there are too many authentication attempts. If not regulated, a single client can trigger enough authentication requests to impact your network.

In monitor mode the access point tracks the rate at which 802.1X clients attempt to authenticate through the access point. If your network is attacked through excessive authentication attempts, the access point generates an alert when the authentication threshold has been exceeded.

You can configure these limits on the access point:

- Number of 802.1X attempts through the access point
- EAPOL flood duration in seconds on the access point

When the access point detects excessive authentication attempts it sets MIB variables to indicate this information:

- An EAPOL flood was detected
- Number of authentication attempts
- MAC address of the client with the most authentication attempts

Beginning in privileged EXEC mode, follow these steps to set authentication limits that trigger a fault on the access point:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ids eap attempts** *number* **period** *seconds*	Configure the number of authentication attempts and the number of seconds of EAPOL flooding that trigger a fault on the access point.
Step 3	**end**	Return to privileged EXEC mode.

Configuring 802.11u Hotspot and Hotspot 2.0

The 802.11u Hotspot feature enables IEEE 802.11 devices to interwork with external networks. It is used in hotspots or other public networks irrespective of whether the service is subscription based or free.

The feature aids network discovery and selection, enabling information transfer from external networks. It provides information to the stations about the networks prior to association. Interworking not only helps users within the home, enterprise, and public access, but also assists manufacturers and operators to provide common components and services for IEEE 802.11 customers.

Before configuring an 802.11u Hotspot, ensure that you have:

- WPA key management
- Multiple Basic SSIDs

Follow these steps to configure an 802.11u Hotspot and Hotspot 2.0:

Step 1 Enter the ap(config-ssid)# mode.

Step 2 Enter the following commands to enable and configure 802.11u Hotspot:

a. hotspot dot11u enable

b. hotspot dot11u domain *index domain_name*

c. hotspot dot11u network-type *network_type internet_availabily_status(0 or 1)*

d. hotspot dot11u auth-type *auth_type*

e. hotspot dot11u ipaddr-type *ipv4type ipv6type*

f. hotspot dot11u hessid *h.h.h*

g. hotspot dot11u nai-realm *index* realm-name *name_string*

h. hotspot dot11u nai-realm *index* eap-method *eap-index eap_method*

i. hotspot dot11u nai-realm *index* auth-method *eap-index auth-index auth_type auth_subtype*

j. hotspot dot11u roam-oi *index hex-string isbeacon*

k. hotspot dot11u 3gpp-info *index mobile_country_code mobile_network_code*

Example:Enabling 802.11u Hotspot

```
ap(config-ssid)# hotspot dot11u enable
ap(config-ssid)# hotspot dot11u domain 1 cisco
ap(config-ssid)# hotspot dot11u network-type  2   1
ap(config-ssid)# hotspot dot11u auth-type  1
ap(config-ssid)# hotspot dot11u ipaddr-type 2 2
ap(config-ssid)# hotspot dot11u hessid 1234.5678.1234
ap(config-ssid)# hotspot dot11u nai-realm 1 realm-name cisco
ap(config-ssid)# hotspot dot11u nai-realm 1 eap-method 1 17
ap(config-ssid)# hotspot dot11u nai-realm 1 auth-method  1 1 1 2
ap(config-ssid)# hotspot dot11u roam-oi 1 004096 1
ap(config-ssid)# hotspot dot11u 3gpp-info 1 123 123
```

Step 3 Enter the following commands to enable and configure 802.11u Hotspot 2.0 :

a. hotspot hs2 enable

b. hotspot hs2 operator-name *index language_code operator_name*

c. hotspot hs2 wan-metrics *link_status symmetric_link_status uplink_speed downlink_speed*

d. hotspot hs2 port-config *ip_protocol port_number port_status*

Example:Enabling 802.11u Hotspot 2.0

```
ap(config-ssid)# hotspot hs2 enable
ap(config-ssid)# hotspot hs2 operator-name 1 eng cisco
ap(config-ssid)# hotspot hs2 wan-metrics 1 1 2345 3434
ap(config-ssid)# hotspot hs2 port-config 1 23 34 2
```

Step 4 Enter the following global configuration commands:

a. dot11 dot11u ap-venue name *name_string*

b. dot11 dot11u ap-venue type *venue_group venue_type*

Example:Global configuration commands:

```
ap(config)# dot11 dot11u ap-venue name cisco_odc
ap(config)# dot11 dot11u ap-venue type 2 2
```

To debug the 802.11u Hotspot and Hotspot 2.0 configuration, use the command **debug dot11 dot11u**.

To enable and configure 802.11u Hotspot and Hotspot 2.0 via the GUI, go to
Security > Dot11u Manager.

CHAPTER 13

Configuring RADIUS and TACACS+ Servers

This chapter describes how to enable and configure the Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+), that provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS and TACACS+ are facilitated through AAA and can be enabled only through AAA commands.

Note You can configure your access point as a local authenticator to provide a backup for your main server or to provide authentication service on a network without a RADIUS server. See Chapter 11, "Configuring Authentication Types," for detailed instructions on configuring your access point as a local authenticator.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Security Command Reference for Release 12.2*.

Configuring and Enabling RADIUS

This section describes how to configure and enable RADIUS. These sections describe RADIUS configuration:

- Understanding RADIUS, page 13-1
- RADIUS Operation, page 13-2
- Configuring RADIUS, page 13-4
- Displaying the RADIUS Configuration, page 13-19
- RADIUS Attributes Sent by the Access Point, page 13-20

Understanding RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco devices and send authentication requests to a central RADIUS server, which contains all user authentication and network service access information. The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (Cisco Identity Services Engine), FreeRADIUS, Microsoft, or another software provider. For more information, refer to the RADIUS server documentation.

Use RADIUS in these network environments, which require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors' access servers, dial-in users are authenticated through a RADIUS server that is customized to work with the Kerberos security system.
- Turnkey network security environments in which applications support the RADIUS protocol, such as an access environment that uses a *smart card* access control system.
- Networks already using RADIUS. You can add a Cisco access point containing a RADIUS client to the network.
- Networks that require resource accounting. You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, showing the amount of resources (such as time, packets, bytes, and so forth) used during the session. An Internet service provider might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

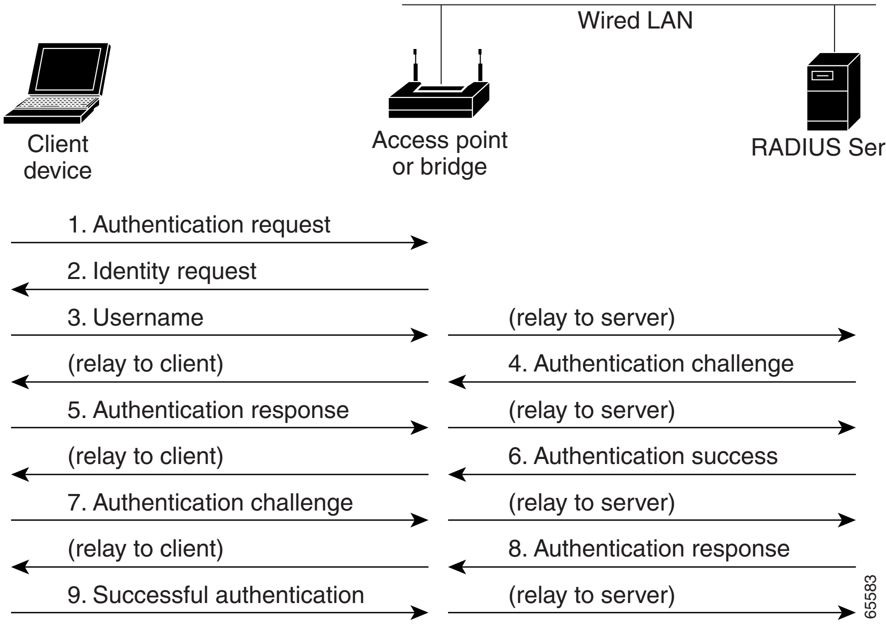
RADIUS is not suitable in these network security situations:

- Multiprotocol access environments– RADIUS does not support, for example, AppleTalk Remote Access (ARA), NetBIOS Frame Control Protocol (NBFCP), NetWare Asynchronous Services Interface (NASI), or X.25 PAD connections.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

RADIUS Operation

When a wireless user attempts to log in and authenticate to an access point whose access is controlled by a RADIUS server, authentication to the network occurs in the steps shown in Figure 13-1:

Figure 13-1 Sequence for EAP Authentication



As shown in Figure 13-1, at the start, a wireless client device and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the access point. The initial phase is an 802.11 open authentication and association. The EAP process then starts.

The AP communicates with the client over the wireless link using EAP/802.1x, and relays the client messages to the RADIUS server using RADIUS encapsulation. Once the client and the authentication server agrees on an EAP method, the RADIUS server sends an authentication challenge to the client.

Some EAP methods also require the client to authenticate the RADIUS server before accepting a challenge from the server. In all cases, the credential exchange is encrypted and cannot be read by eavesdroppers.

When (one way or mutual) authentication is complete, and when WPA/WPA2 is in use, the RADIUS server and the client derive an initial key called Pairwise Master Key (PMK). The the client and the RADIUS server use the same method to derive the PKM, and therefore derive the same PMK. However, the PMK is not exchanged over the wireless link.

The RADIUS server sends a copy of the PMK to the AP. The AP and the client will then use this PMK to derive unicast encryption keys that will be used to encrypt the exchanges between the client and the AP during the client session. The AP will also use the unicast encryption key to communicate to the client the broadcast key, or the key used to encrypt traffic broadcasted to all clients in the cell.

There is more than one type of EAP authentication, but the access point behaves the same way for each type. The AP relays authentication messages from the wireless client device to the RADIUS server and from the RADIUS server to the wireless client device. See the "Assigning Authentication Types to an SSID" section on page 11-9 for instructions on setting up client authentication using a RADIUS server.

Configuring RADIUS

This section describes how to configure your access point to support RADIUS. At the minimum, you must identify the host(s) that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting.

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a user. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on users; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

You should have access to and should configure a RADIUS server before configuring RADIUS features on your access point.

This section contains this configuration information:

- Default RADIUS Configuration, page 13-4
- Identifying the RADIUS Server Host, page 13-5 (required)
- Configuring RADIUS Login Authentication, page 13-7 (required)
- Defining AAA Server Groups, page 13-9 (optional)
- Configuring RADIUS Authorization for User Privileged Access and Network Services, page 13-11 (optional)
- Configuring Packet of Disconnect, page 13-12 (optional)
- Starting RADIUS Accounting, page 13-14 (optional)
- Configuring Settings for All RADIUS Servers, page 13-15 (optional)
- Configuring Settings for All RADIUS Servers, page 13-15 (optional)
- Configuring the Access Point to Use Vendor-Specific RADIUS Attributes, page 13-16 (optional)
- Configuring the Access Point for Vendor-Proprietary RADIUS Server Communication, page 13-17 (optional)
- Configuring WISPr RADIUS Attributes, page 13-18 (optional)

Note The RADIUS server CLI commands are disabled until you enter the **aaa new-model** command.

Default RADIUS Configuration

RADIUS and AAA are disabled by default.

To prevent a lapse in security, you cannot configure RADIUS through a network management application. When enabled, RADIUS can authenticate users accessing the access point through the CLI.

Identifying the RADIUS Server Host

Access point-to-RADIUS-server communication involves several components:

- Host name or IP address
- Authentication destination port
- Accounting destination port
- Key string
- Timeout period
- Retransmission value

You identify RADIUS security servers by their host name or IP address, host name and specific UDP port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

Note For Cisco IOS Releases 12.2(8)JA and later, the access point uses a randomly chosen UDP source port number in the range of 21645 to 21844 for communication with RADIUS servers.

If two different host entries on the same RADIUS server are configured for the same service—such as accounting—the second host entry configured acts as a fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the access point tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

A RADIUS server and the access point use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the access point.

The timeout, retransmission, and encryption key values can be configured globally per server for all RADIUS servers or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the access point, use the three unique global configuration commands: **radius-server timeout**, **radius-server retransmit**, and **radius-server key**. To apply these values on a specific RADIUS server, use the **radius-server host** global configuration command.

Note If you configure both global and per-server functions (timeout, retransmission, and key commands) on the access point, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands. For information on configuring these setting on all RADIUS servers, see the "Configuring Settings for All RADIUS Servers" section on page 13-15.

You can configure the access point to use AAA server groups to group existing server hosts for authentication. For more information, see the "Defining AAA Server Groups" section on page 13-9.

Beginning in privileged EXEC mode, follow these steps to configure per-server RADIUS server communication. This procedure is required.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.
Step 3	**radius-server** {hostname | ip-address}[**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] **Note** This command was supported in the older releases. You are recommended to use the following new commands. **radius server** *name* **address** [**IP address** *ip-address*] [**auth-port** *port-number*] [**acct-port** *port-number*] **address** {**ipv4** *radius-server-IPv4-Address* | **ipv6** *radius-server-IPv6-Address*}	Specify the server name of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests.(Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout** *seconds*, specify the time interval that the access point waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting. If no timeout is set with the **radius-server host** command, the setting of the **radius-server timeout** command is used. • (Optional) For **retransmit** *retries*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the **radius-server host** command, the setting of the **radius-server retransmit** global configuration command is used. • (Optional) For **key** *string*, specify the authentication and encryption key used between the access point and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the access point to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The access point software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.
Step 4	**dot11 ssid** *ssid-string*	Enter SSID configuration mode for an SSID on which you need to enable accounting. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive.
Step 5	**accounting** *list-name*	Enable RADIUS accounting for this SSID. For *list-name*, specify the accounting method list. Click this URL for more information on method lists: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacct.html **Note** To enable accounting for an SSID, you must include the **accounting** command in the SSID configuration. Click this URL to browse to a detailed description of the SSID configuration mode **accounting** command.

	Command	Purpose
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* global configuration command.

This example shows how to configure one RADIUS server to be used for authentication and another to be used for accounting:

```
AP(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
AP(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

This example shows how to configure an SSID for RADIUS accounting:

```
AP(config)# dot11 ssid batman
AP(config-ssid)# accounting accounting-method-list
```

This example shows how to configure *host1* as the RADIUS server and to use the default ports for both authentication and accounting:

```
AP(config)# radius-server host host1
```

Note You also need to configure some settings on the RADIUS server. These settings include the IP address of the access point and the key string to be shared by both the server and the access point. For more information, refer to the RADIUS server documentation.

Configuring RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.

	Command	Purpose
Step 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	Create a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. For more information on list names, click this link: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfathen.html • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: • **line**—Use the line password for authentication. You must define a line password before you can use this authentication method. Use the **password** *password* line configuration command. • **local**—Use the local username database for authentication. You must enter username information in the database. Use the **username** *password* global configuration command. • **radius**—Use RADIUS authentication. You must configure the RADIUS server before you can use this authentication method. For more information, see the "Identifying the RADIUS Server Host" section on page 13-5.
Step 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	**login authentication** {**default** | *list-name*}	Apply the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.
Step 6	**radius-server attribute 32 include-in-access-req format {%h | %i | %d}**	(Optional) Configure the access point to send its system name in the NAS_ID attribute for authentication. • %i—IP address • %h—Hostname • %d—domain name
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show running-config**	Verify your entries.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] global configuration command. To either disable RADIUS authentication for logins or to return to the default value, use the **no login authentication** {**default** | *list-name*} line configuration command.

Defining AAA Server Groups

You can configure the access point to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service (such as accounting), the second configured host entry acts as a fail-over backup to the first one.

You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.

	Command	Purpose
Step 3	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]	Specify the IP address or host name of the remote RADIUS server host. • (Optional) For **auth-port** *port-number*, specify the UDP destination port for authentication requests. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. • (Optional) For **timeout** *seconds*, specify the time interval that the access point waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the **radius-server timeout** global configuration command setting. If no timeout is set with the **radius-server host** command, the setting of the **radius-server timeout** command is used. • (Optional) For **retransmit** *retries*, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the **radius-server host** command, the setting of the **radius-server retransmit** global configuration command is used. • (Optional) For **key** *string*, specify the authentication and encryption key used between the access point and the RADIUS daemon running on the RADIUS server. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. To configure the access point to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The access point software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.
Step 4	**aaa group server radius** *group-name*	Define the AAA server-group with a group name. This command puts the access point in a server group configuration mode.
Step 5	**server** *ip-address*	Associate a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined in Step 2.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.
Step 9		Enable RADIUS login authentication. See the "Configuring RADIUS Login Authentication" section on page 13-7.

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* global configuration command. To remove a server group from the configuration list, use the **no aaa group server radius** *group-name* global configuration command. To remove the IP address of a RADIUS server, use the **no server** *ip-address* server group configuration command.

In this example, the access point is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over backup to the first entry.

```
AP(config)# aaa new-model
AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
AP(config)# aaa group server radius group1
AP(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
AP(config-sg-radius)# exit
AP(config)# aaa group server radius group2
AP(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
AP(config-sg-radius)# exit
```

Note The ports defined for each RADIUS server host in a radius group override the ports defined individually for each radius server host entry created from global configuration mode.

Configuring RADIUS Authorization for User Privileged Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the access point uses information retrieved from the user's profile, which is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

Note This section describes setting up authorization for access point administrators, not for wireless client devices. For wireless client devices and wireless network access authorization, no specific authorization profile needs to be returned from the RADIUS server.

You can use the **aaa authorization** global configuration command with the **radius** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The **aaa authorization exec radius local** command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.

Note Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify RADIUS authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa authorization network radius**	Configure the access point for user RADIUS authorization for all network-related service requests.
Step 3	**aaa authorization exec radius**	Configure the access point for user RADIUS authorization to determine if the user has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

Configuring Packet of Disconnect

Packet of Disconnect (PoD) is also known as Disconnect Message. Additional information on PoD can be found in the Internet Engineering Task Force (IETF) Internet Standard RFC 3576

Packet of Disconnect consists of a method of terminating a session that has already been connected. The PoD is a RADIUS Disconnect_Request packet and is intended to be used in situations where the authenticating agent server wants to disconnect the user after the session has been accepted by the RADIUS access_accept packet.

When a session is terminated, the RADIUS server sends a disconnect message to the Network Access Server (NAS); an access point or WDS. For 802.11 sessions, the Calling-Station-ID [31] RADIUS attribute (the MAC address of the client) must be supplied in the Pod request. The access point or WDS attempts to disassociate the relevant session and then sends a disconnect response message back to the RADIUS server. The message types are as follows:

- 40—Disconnect-Request
- 41—Disconnect—ACK
- 42—Disconnect—NAK

Note Refer to your RADIUS server application documentation for instructions on how to configure PoD requests.

Note The access point does not block subsequent attempts by the client to reassociate. It is the responsibility of the security administrator to disable the client account before issuing a PoD request.

Note When WDS is configured, PoD requests should be directed to the WDS. The WDS forwards the disassociation request to the parent access point and then purges the session from its own internal tables.

Beginning in privileged EXEC mode, follow these steps to configure a PoD:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa pod server** [**port** *port number*] [**auth-type** {**any** | **all** | **session-key**}] [**clients** *client 1...*] [**ignore** {**server-key** *string...*| **session-key** }] | **server-key** *string...*]}	Enables user sessions to be disconnected by requests from a RADIUS server when specific session attributes are presented. **port** *port number*—(Optional) The UDP port on which the access point listens for PoD requests. The default value is 1700. **auth-type**—This parameter is not supported for 802.11 sessions. **clients** (Optional)—Up to four RADIUS servers may be nominated as clients. If this configuration is present and a PoD request originates from a device that is not on the list, it is rejected. **ignore** (Optional)—When set to *server_key*, the shared secret is not validated when a PoD request is received. **session-key**—Not supported for 802.11 sessions. **server-key**—Configures the shared-secret text string. *string*—The shared-secret text string that is shared between the network access server and the client workstation. This shared-secret must be the same on both systems. **Note** Any data entered after this parameter is treated as the shared secret string.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Selecting the CSID Format

You can select the format for MAC addresses in Called-Station-ID (CSID) and Calling-Station-ID attributes in RADIUS packets.

The Calling-Station-ID [31] RADIUS attribute is the MAC address of the wireless client, and may need to be communicated to the RADIUS server, for example, for accounting or for the PoD.

Use the **dot11 aaa csid** global configuration command to select the CSID format. Table 13-1 lists the format options with corresponding MAC address examples.

Table 13-1 CSID Format Options

Option	MAC Address Example
default	0007.85b3.5f4a

Table 13-1 CSID Format Options

Option	MAC Address Example
ietf	00-07-85-b3-5f-4a
unformatted	000785b35f4a

To return to the default CSID format, use the **no** form of the **dot11 aaa csid** command, or enter **dot11 aaa csid default**.

Note You can also use the **wlccp wds aaa csid** command to select the CSID format.

Starting RADIUS Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the access point reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing. See the "RADIUS Attributes Sent by the Access Point" section on page 13-20 for a complete list of attributes sent and honored by the access point.

Beginning in privileged EXEC mode, follow these steps to enable RADIUS accounting for each Cisco IOS privilege level and for network services:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa accounting network start-stop radius**	Enable RADIUS accounting for all network-related service requests.
Step 3	**ip radius source-interface bvi1**	Configure the access point to send its BVI IP address in the NAS_IP_ADDRESS attribute for accounting records.
Step 4	**aaa accounting update periodic** *minutes*	Enter an accounting update interval in minutes.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable accounting, use the **no aaa accounting** {**network** | **exec**} {**start-stop**} *method1...* global configuration command.

Configuring Settings for All RADIUS Servers

Beginning in privileged EXEC mode, follow these steps to configure global communication settings between the access point and all RADIUS servers:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**radius-server key** *string*	Specify the shared secret text string used between the access point and all RADIUS servers. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 3	**radius-server retransmit** *retries*	Specify the number of times the access point sends each RADIUS request to the server before giving up. The default is 3; the range 1 to 1000.
Step 4	**radius-server timeout** *seconds*	Specify the number of seconds an access point waits for a reply to a RADIUS request before resending the request. The default is 5 seconds; the range is 1 to 1000.
Step 5	**radius-server deadtime** *minutes*	Use this command to cause the Cisco IOS software to mark as "dead" any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as dead is skipped by additional requests for the duration of minutes that you specify, up to a maximum of 1440 (24 hours). **Note** This command is required configuration when multiple RADIUS servers are defined. If not configured, client authentication does not occur. When one RADIUS server is defined, this command is optional.
Step 6	**radius-server attribute 32 include-in-access-req format %h**	Configure the access point to send its system name in the NAS_ID attribute for authentication.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**show running-config**	Verify your settings.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to set up two main servers with a server deadtime of 10 minutes:

```
ap(config)# aaa new-model
ap(config)# radius server server1
ap(config-radius-server)# address ipv4 172.20.0.1 auth-port 1812 acct-port 1813
ap(config-radius-server)# key 0 cisco
ap(config-radius-server)# exit
ap(config)# radius server server2
ap(config-radius-server)# address ipv4 172.10.0.1 auth-port 1000 acct-port 1001
ap(config-radius-server)# key 0 cisco
ap(config-radius-server)# exit
ap(config)# radius-server deadtime 10
```

To return to the default setting for retransmit, timeout, and deadtime, use the **no** forms of these commands.

Configuring the Access Point to Use Vendor-Specific RADIUS Attributes

Note The following configuration is done on the RADIUS server.

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the access point and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco's vendor ID is 9, and the supported option has vendor type 1, which is named *cisco-avpair*. The value is a string with this format:

```
protocol : attribute sep value *
```

Protocol is a value of the Cisco protocol attribute for a particular type of authorization. *Attribute* and *value* are an appropriate AV pair defined in the Cisco TACACS+ specification, and *sep* is = for mandatory attributes and the asterisk (*) for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair activates Cisco's *multiple named ip address pools* feature during IP authorization (during PPP's IPCP address assignment):

```
cisco-avpair= ”ip:addr-pool=first‟
```

The following example shows how to provide a user logging in from an access point with immediate access to privileged EXEC commands:

```
cisco-avpair= ”shell:priv-lvl=15‟
```

Other vendors have their own unique vendor IDs, options, and associated VSAs. For more information about vendor IDs and VSAs, refer to RFC 2138, "Remote Authentication Dial-In User Service (RADIUS)."

Beginning in privileged EXEC mode, follow these steps to configure the access point to recognize and use VSAs:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**radius-server vsa send** [**accounting** | **authentication**]	Enable the access point to recognize and use VSAs as defined by RADIUS IETF attribute 26. • (Optional) Use the **accounting** keyword to limit the set of recognized vendor-specific attributes to only accounting attributes. • (Optional) Use the **authentication** keyword to limit the set of recognized vendor-specific attributes to only authentication attributes. If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your settings.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

For a complete list of RADIUS attributes or more information about VSA 26, see the RADIUS guides at the following URL:
http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/12-4t/secuser-12-4t-library.html

Configuring the Access Point for Vendor-Proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the access point and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the access point. You specify the RADIUS host and secret text string by using the **radius-server** global configuration commands.

Beginning in privileged EXEC mode, follow these steps to specify a vendor-proprietary RADIUS server host and a shared secret text string:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**radius-server host** {*hostname* | *ip-address*} **non-standard**	Specify the IP address or host name of the remote RADIUS server host and identify that it is using a vendor-proprietary implementation of RADIUS.

	Command	Purpose
Step 3	**radius-server key** *string*	Specify the shared secret text string used between the access point and the vendor-proprietary RADIUS server. The access point and the RADIUS server use this text string to encrypt passwords and exchange responses. **Note** The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your settings.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To delete the vendor-proprietary RADIUS host, use the **no radius-server host** {*hostname* | *ip-address*} **non-standard** global configuration command. To disable the key, use the **no radius-server key** global configuration command.

This example shows how to specify a vendor-proprietary RADIUS host and to use a secret key of *rad124* between the access point and the server:

```
AP(config)# radius server Myserver
AP(config-radius-server)# address ipv4 172.20.30.15
AP(config-radius-server)# key 0 rad1234
AP(config-radius-server)# non-standard
```

Configuring WISPr RADIUS Attributes

The Wi-Fi Alliance's *WISPr Best Current Practices for Wireless Internet Service Provider Roaming,* and its updated *Annex D* published in 2010 by the Wireless Broadband Alliance under the name *WISPv2* lists RADIUS attributes that access points must send with RADIUS accounting and authentication requests. The access point currently supports only the WISPr location-name and the ISO and International Telecommunications Union (ITU) country and area codes attributes. Use the **snmp-server location** and the **dot11 location isocc** commands to configure these attributes on the access point.

The *WISPr and WISPv2 Best Current Practices for Wireless Internet Service Provider Roaming (WISPr)* document also requires the access point to include a class attribute in RADIUS authentication replies and accounting requests. The access point includes the class attribute automatically and does not have to be configured to do so.

You can find a list of ISO and ITU country and area codes at the ISO and ITU websites. Cisco IOS software does not check the validity of the country and area codes that you configure on the access point.

Beginning in privileged EXEC mode, follow these steps to specify WISPr RADIUS attributes on the access point:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server location** *location*	Specify the WISPr location-name attribute. The *WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming* document recommends that you enter the location name in this format: *hotspot_operator_name***,***location*
Step 3	**dot11 location isocc** *ISO-country-code* **cc** *country-code* **ac** *area-code*	Specify ISO and ITU country and area codes that the access point includes in accounting and authentication requests. • **isocc** *ISO-country-code*—specifies the ISO country code that the access point includes in RADIUS authentication and accounting requests • **cc** *country-code*—specifies the ITU country code that the access point includes in RADIUS authentication and accounting requests • **ac** *area-code*—specifies the ITU area code that the access point includes in RADIUS authentication and accounting requests
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your settings.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure the WISPr location-name attribute:

```
ap# snmp-server location ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport
```

This example shows how to configure the ISO and ITU location codes on the access point:

```
ap# dot11 location isocc us cc 1 ac 408
```

This example shows how the access point adds the SSID used by the client device and formats the location-ID string:

```
isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport
```

Displaying the RADIUS Configuration

To display the RADIUS configuration, use the **show running-config** privileged EXEC command.

Note When DNS is configured on the access point, the **show running-config** command sometimes displays a server’s IP address instead of its name.

RADIUS Attributes Sent by the Access Point

Table 13-2 through Table 13-6 identify the attributes sent by an access point to a client in access-request, access-accept, and accounting-request packets.

Note You can configure the access point to include in its RADIUS accounting and authentication requests attributes recommended by the Wi-Fi Alliance's *WISPr and WISPv2 Best Current Practices for Wireless Internet Service Provider Roaming (WISPr)* document. Refer to the "Configuring WISPr RADIUS Attributes" section on page 13-18 for instructions.

Table 13-2 Attributes Sent in Access-Request Packets

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
12	Framed-MTU
30	Called-Station-ID (MAC address)
31	Calling-Station-ID (MAC address)
32	NAS-Identifier[1]
61	NAS-Port-Type
79	EAP-Message
80	Message-Authenticator

[1] The access point sends the NAS-Identifier if attribute 32 (include-in-access-req) is configured.

Table 13-3 Attributes Honored in Access-Accept Packets

Attribute ID	Description
25	Class
27	Session-Timeout
64	Tunnel-Type[1]
65	Tunnel-Medium-Type[1]
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID[1]
VSA (attribute 26)	LEAP session-key
VSA (attribute 26)	Auth-Algo-Type
VSA (attribute 26)	SSID

[1] RFC2868; defines a VLAN override number.

Table 13-4 Attributes Sent in Accounting-Request (start) Packets

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
44	Acct-Session-Id
61	NAS-Port-Type
VSA (attribute 26)	SSID
VSA (attribute 26)	NAS-Location
VSA (attribute 26)	Cisco-NAS-Port
VSA (attribute 26)	Interface

Table 13-5 Attributes Sent in Accounting-Request (update) Packets

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
61	NAS-Port-Type
VSA (attribute 26)	SSID
VSA (attribute 26)	NAS-Location
VSA (attribute 26)	VLAN-ID
VSA (attribute 26)	Connect-Progress
VSA (attribute 26)	Cisco-NAS-Port
VSA (attribute 26)	Interface

Table 13-6 Attributes Sent in Accounting-Request (stop) Packets

Attribute ID	Description
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
25	Class
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-Id
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
61	NAS-Port-Type
VSA (attribute 26)	SSID
VSA (attribute 26)	NAS-Location
VSA (attribute 26)	Disc-Cause-Ext
VSA (attribute 26)	VLAN-ID
VSA (attribute 26)	Connect-Progress
VSA (attribute 26)	Cisco-NAS-Port
VSA (attribute 26)	Interface
VSA (attribute 26)	Auth-Algo-Type

Note By default, the access point sends reauthentication requests to the authentication server with the service-type attribute set to authenticate-only. However, some Microsoft IAS servers do not support the authenticate-only service-type attribute. Depending on the user requirements, set the service-type attribute to: **dot11 aaa authentication attributes service-type login-user** or **dot11 aaa authentication attributes service-type framed-user**. By default the service type "login" is sent in the access request.

Configuring and Enabling TACACS+

This section contains this configuration information:

Understanding TACACS+

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your access point. Unlike RADIUS, TACACS+ does not authenticate wireless client devices accessing the network through your access point.

You should have access to and should configure a TACACS+ server before configuring TACACS+ features on your access point.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

TACACS+, administered through the AAA security services, can provide these services:

- Authentication—Provides complete control of authentication of administrators through login and password dialog, challenge and response, and messaging support.

  The authentication facility can conduct a dialog with the administrator (for example, after a username and password are provided, to challenge a user with several questions, such as home address, mother's maiden name, service type, and social security number). The TACACS+ authentication service can also send messages to administrator screens. For example, a message could notify administrators that their passwords must be changed because of the company's password aging policy.

- Authorization—Provides fine-grained control over administrator capabilities for the duration of the administrator's session, including but not limited to setting autocommands, access control, session duration, or protocol support. You can also enforce restrictions on the commands that an administrator can execute with the TACACS+ authorization feature.
- Accounting—Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track administrator activity for a security audit or to provide information for user billing. Accounting records include administrator identities, start and stop times, executed commands, number of packets, and number of bytes.

The TACACS+ protocol provides authentication between the access point and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between the access point and the TACACS+ daemon are encrypted.

You need a system running the TACACS+ daemon software to use TACACS+ on your access point.

TACACS+ Operation

When an administrator attempts a simple ASCII login by authenticating to an access point using TACACS+, this process occurs:

1. When the connection is established, the access point contacts the TACACS+ daemon to obtain a username prompt, which is then displayed to the administrator. The administrator enters a username, and the access point then contacts the TACACS+ daemon to obtain a password prompt. The access point displays the password prompt to the administrator, the administrator enters a password, and the password is then sent to the TACACS+ daemon.

   TACACS+ allows a conversation to be held between the daemon and the administrator until the daemon receives enough information to authenticate the administrator. The daemon prompts for a username and password combination, but can include other items, such as e.g. the user mother maiden name, or any other information configured on the TACACS as being mandatory to identify the user.

2. The access point eventually receives one of these responses from the TACACS+ daemon:
   - ACCEPT—The administrator is authenticated and service can begin. If the access point is configured to require authorization, authorization begins at this time.
   - REJECT—The administrator is not authenticated. The administrator can be denied access or is prompted to retry the login sequence, depending on the TACACS+ daemon.
   - ERROR—An error occurred at some time during authentication with the daemon or in the network connection between the daemon and the access point. If an ERROR response is received, the access point typically tries to use an alternative method for authenticating the administrator.
   - CONTINUE—The administrator is prompted for additional authentication information.

   After authentication, the administrator undergoes an additional authorization phase if authorization has been enabled on the access point. Administrators must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the TACACS+ daemon is again contacted, and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response contains data in the form of attributes that direct the EXEC or NETWORK session for that administrator, determining the services that the administrator can access:
   - Telnet, rlogin, or privileged EXEC services
   - Connection parameters, including the host or client IP address, access list, and administrator timeouts

Configuring TACACS+

This section describes how to configure your access point to support TACACS+. At a minimum, you must identify the host or hosts maintaining the TACACS+ daemon and define the method lists for TACACS+ authentication. You can optionally define method lists for TACACS+ authorization and accounting. A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on an administrator. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on administrators; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

This section contains this configuration information:

- Default TACACS+ Configuration, page 13-25
- Identifying the TACACS+ Server Host and Setting the Authentication Key, page 13-25
- Configuring TACACS+ Login Authentication, page 13-26
- Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, page 13-27
- Starting TACACS+ Accounting, page 13-28

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate administrators accessing the access point through the CLI and the web interface.

Identifying the TACACS+ Server Host and Setting the Authentication Key

You can configure the access point to use a single server or AAA server groups to group existing server hosts for authentication. You can group servers to select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list and contains the list of IP addresses of the selected server hosts.

Beginning in privileged EXEC mode, follow these steps to identify the IP host or host maintaining TACACS+ server and optionally set the encryption key:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**tacacs-server host** *hostname* [**port** *integer*] [**timeout** *integer*] [**key** *string*]	Identify the IP host or hosts maintaining a TACACS+ server. Enter this command multiple times to create a list of preferred hosts. The software searches for hosts in the order in which you specify them. • For *hostname*, specify the name or IP address of the host. • (Optional) For **port** *integer*, specify a server port number. The default is port 49. The range is 1 to 65535. • (Optional) For **timeout** *integer*, specify a time in seconds the access point waits for a response from the daemon before it times out and declares an error. The default is 5 seconds. The range is 1 to 1000 seconds. • (Optional) For **key** *string*, specify the encryption key for encrypting and decrypting all traffic between the access point and the TACACS+ daemon. You must configure the same key on the TACACS+ daemon for encryption to be successful.
Step 3	**aaa new-model**	Enable AAA.
Step 4	**aaa group server tacacs+** *group-name*	(Optional) Define the AAA server-group with a group name. This command puts the access point in a server group subconfiguration mode.

	Command	Purpose
Step 5	**server** *ip-address*	(Optional) Associate a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group. Each server in the group must be previously defined in Step 2.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show tacacs**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove the specified TACACS+ server name or address, use the **no tacacs-server host** *hostname* global configuration command. To remove a server group from the configuration list, use the **no aaa group server tacacs+** *group-name* global configuration command. To remove the IP address of a TACACS+ server, use the **no server ip-address** server group subconfiguration command.

Configuring TACACS+ Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list describes the sequence and authentication methods to be queried to authenticate an administrator. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the administrator access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa new-model**	Enable AAA.

	Command	Purpose
Step 3	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]	Create a login authentication method list. • To create a default list that is used when a named list is *not* specified in the **login authentication** command, use the **default** keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. • For *list-name*, specify a character string to name the list you are creating. • For *method1...*, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. Select one of these methods: • **line**—Use the line password for authentication. You must define a line password before you can use this authentication method. Use the **password** *password* line configuration command. • **local**—Use the local username database for authentication. You must enter username information into the database. Use the **username** *password* global configuration command. • **tacacs+**—Uses TACACS+ authentication. You must configure the TACACS+ server before you can use this authentication method.
Step 4	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]	Enter line configuration mode, and configure the lines to which you want to apply the authentication list.
Step 5	**login authentication** {**default** | *list-name*}	Apply the authentication list to a line or set of lines. • If you specify **default**, use the default list created with the **aaa authentication login** command. • For *list-name*, specify the list created with the **aaa authentication login** command.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] global configuration command. To either disable TACACS+ authentication for logins or to return to the default value, use the **no login authentication** {**default** | *list-name*} line configuration command.

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to an administrator. When AAA authorization is enabled, the access point uses information retrieved from the administrator's profile, which is located either in the local user database or on the security server, to configure the administrator's session. The administrator is granted access to a requested service only if the information in the administrator profile allows it.

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict an administrator's network access to privileged EXEC mode.

The **aaa authorization exec tacacs+ local** command sets these authorization parameters:

- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.

Note Authorization is bypassed for authenticated administrators who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa authorization network tacacs+**	Configure the access point for administrator TACACS+ authorization for all network-related service requests.
Step 3	**aaa authorization exec tacacs+**	Configure the access point for administrator TACACS+ authorization to determine if the administrator has privileged EXEC access. The **exec** keyword might return user profile information (such as **autocommand** information).
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable authorization, use the **no aaa authorization** {**network** | **exec**} *method1* global configuration command.

You also need to configure your TACACS server with user credentials, and also configure the TACACS server to return an authorization profile for the authenticated user. The profile can be as extensive as shell privilege level 15, with no restriction of commands; or be more specific and target only a set of commands or a lower privilege level.

Starting TACACS+ Accounting

The AAA accounting feature tracks the services that administrators are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the access point reports administrator activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Beginning in privileged EXEC mode, follow these steps to enable TACACS+ accounting for each Cisco IOS privilege level and for network services:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**aaa accounting network start-stop tacacs+**	Enable TACACS+ accounting for all network-related service requests.

	Command	Purpose
Step 3	**aaa accounting exec start-stop tacacs+**	Enable TACACS+ accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable accounting, use the **no aaa accounting** {**network** | **exec**} {**start-stop**} *method1*... global configuration command.

Displaying the TACACS+ Configuration

To display TACACS+ server statistics, use the **show tacacs** privileged EXEC command.

CHAPTER 14

Configuring VLANs

This chapter describes how to configure your access point to operate with the VLANs set up on your wired LAN.

Understanding VLANs

A VLAN is a switched network that is logically segmented, by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network or the fact that they might be intermingled with other teams. You use VLANs to reconfigure the network through software rather than physically unplugging and moving devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment such as LAN switches that operate bridging protocols between them with a separate group for each VLAN.

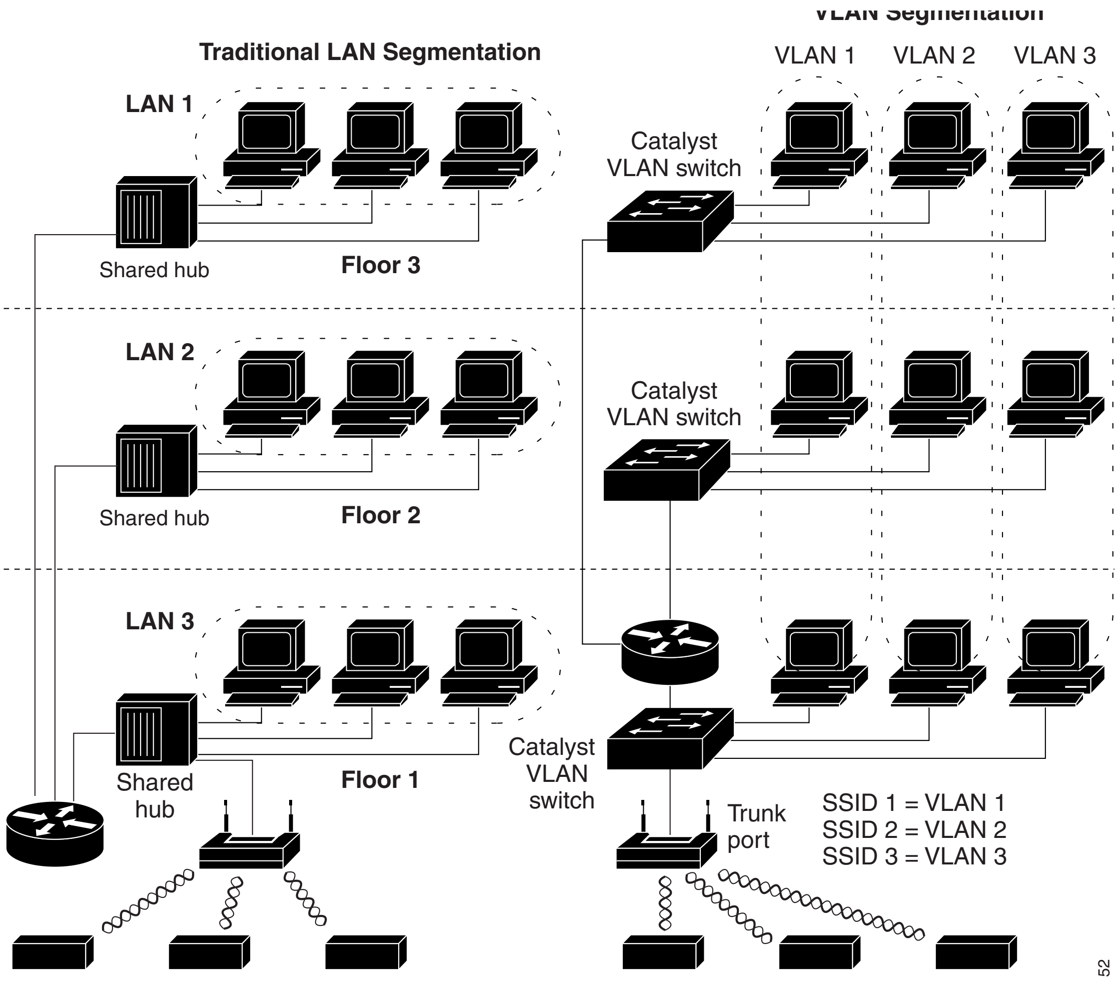
VLANs provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. You should consider several key issues when designing and building switched LAN networks:

- LAN segmentation
- Security
- Broadcast control
- Performance
- Network management
- Communication between VLANs

You extend VLANs into a wireless LAN by adding IEEE 802.1Q tag awareness to the access point. Frames destined for different VLANs are transmitted by the access point wirelessly on different SSIDs. Only the clients associated with that VLAN receive those packets. Conversely, packets coming from a client associated to an SSID mapped to a certain VLAN are 802.1Q tagged before they are forwarded onto the wired network.

Figure 14-1 shows the difference between traditional physical LAN segmentation and logical VLAN segmentation with wireless devices connected.

Figure 14-1 LAN and VLAN Segmentation with Wireless Devices



For more information on VLAN design and configuration, see the Cisco IOS Switching Services Configuration Guide at the following URL:
http://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/configuration/guide/fswtch_c.html

Incorporating Wireless Devices into VLANs

The basic wireless components of a VLAN consist of an access point and a client associated to it using wireless technology. The access point is physically connected through a trunk port to the network VLAN switch on which VLANs are configured. The physical connection to the VLAN switch is through the access point's Ethernet port.

In fundamental terms, the key to configuring an access point to connect to a specific VLAN is to configure its SSID to recognize that VLAN. Because VLANs are identified by a VLAN ID or name, it follows that if the SSID on an access point is configured to recognize a specific VLAN ID or name, a connection to the VLAN is established. When this connection is made, associated wireless client devices having the same SSID can access the VLAN through the access point. The VLAN processes data to and from the clients the same way that it processes data to and from wired connections. You can configure up to 16 SSIDs on your access point, so you can support up to 16 VLANs.

You can assign more than one SSID to a given VLAN. However, a given SSID can be mapped to only one VLAN. Also, the SSID to VLAN mapping must be unique per interface.

For example, you configure SSID1 and SSID2. If you assign SSID1 to VLANA on radio 0, then you cannot assign SSID2 to VLANA on the same radio 0. You can assign SSID2 to VLANA on radio 1. Alternatively, you can assign SSID2 to VLANB on radio 0 or on radio 1 or on both. If you assign SSID2 to VLANB on radio 0, you can assign SSID2 to radio 1, but it must also be assigned to VLANB. You cannot assign SSID2 (or SSID1) to VLANA on radio 0, and to VLANB on radio 1.

You can use the VLAN feature to deploy wireless devices with greater efficiency and flexibility. For example, one access point can now handle the specific requirements of multiple users having widely varied network access and permissions. Without VLAN capability, multiple access points would have to be employed to serve classes of users based on the access and permissions they were assigned.

These are two common strategies for deploying wireless VLANs:

- Segmentation by user groups: You can segment your wireless LAN user community and enforce a different security policy for each user group. For example, you can create three wired and wireless VLANs in an enterprise environment for full-time and part-time employees and also provide guest access.
- Segmentation by device types: You can segment your wireless LAN to allow different devices with different security capabilities to join the network. For example, some wireless users might have handheld devices that support only support only pre-shared key (PSK) security mechanisms, and some wireless users might have more sophisticated devices using 802.1x/EAP. You can group and isolate these devices into separate VLANs.

Repeaters cannot repeat SSIDs mapped to a VLAN. When configuring a root access point and a repeater, make sure that the SSID on the root AP and the same SSID on the repeater use the native VLAN. You can configure other SSIDs on the root AP and the repeater AP that would be mapped to a VLAN, but these tagged SSIDs cannot be repeated.

When configuring a bridge to non-root bridge link, the SSID used on the bridge must be untagged (use the native VLAN). You can also configure other SSIDs on both the root bridge AP and the non-root bridge AP that would be mapped to a VLAN. These SSIDs will be forwarded between the root bridge and the non-root bridge through the SSID associated to the native VLAN.

Configuring VLANs

These sections describe how to configure VLANs on your access point:

Configuring a VLAN

Configuring your access point to support VLANs is a three-step process:

1. Enable the VLAN on the radio and Ethernet ports.
   Enabling the VLAN on the radio and Ethernet ports also creates the VLANs in the access point configuration.
2. Create an SSID, and assign it to a VLAN.
3. Assign encryption settings to a VLAN on a given radio interface.

This section describes how to assign SSIDs to VLANs and how to enable a VLAN on the access point radio and Ethernet ports. For detailed instructions on assigning authentication types to SSIDs, see Chapter 11, "Configuring Authentication Types." For instructions on assigning other settings to SSIDs, see Chapter 7, "Configuring Multiple SSIDs."

You can configure up to 16 SSIDs on the access point, so you can support up to 16 VLANs that are configured on your LAN.

Step 1 - Enabling the VLAN on the radio and Ethernet ports

Beginning in privileged EXEC mode, follow these steps to assign an SSID to a VLAN and enable the VLAN on the access point radio and Ethernet ports.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio 0.x | 1.x**	Enter interface configuration mode for the radio VLAN sub interface.
Step 3	**encapsulation dot1q** *vlan-id* [**native**]	Enable a VLAN on the radio interface. (Optional) Designate the VLAN as the native VLAN. On many networks, the native VLAN is VLAN 1.
Step 4	**exit**	Return to global configuration mode.

Step 2 - Creating an SSID and assigning it to a VLAN

Beginning in privileged EXEC mode, follow these steps to assign an SSID to a VLAN.

	Command	Purpose
Step 1	**dot11 ssid** *ssid-string*	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters. SSIDs are case sensitive. The SSID can consist of up to 32 alphanumeric, case-sensitive, characters. **Note** You use the **ssid** command's authentication options to configure an authentication type for each SSID. See Chapter 11, "Configuring Authentication Types," for instructions on configuring authentication types.
Step 2	**vlan** *vlan-id*	(Optional) Assign the SSID to a VLAN on your network. Client devices that associate using the SSID are grouped into this VLAN. Enter a VLAN ID from 1 to 4095. You can assign only one VLAN to an SSID, but you can assign two SSIDs to a VLAN, as long as each SSID is sent to a different radio interface. However, you cannot assign two SSIDs to the same VLAN on the same interface. **Tip** If your network uses VLAN names, you can also assign names to the VLANs on your access point. See the "Assigning Names to VLANs" section on page 14-7 for instructions.
Step 3	**exit**	Return to interface configuration mode for the radio interface.

Step 3 - Assigning encryption settings to a VLAN on a given radio interface

Beginning in privileged EXEC mode, follow these steps to assign encryption settings to a VLAN on a given radio interface.

	Command	Purpose
Step 1	**interface dot11radio 0 | 1**	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 2	**ssid** *ssid-string*	Assigns the SSID to the interface.
Step 3	**encryption vlan** *vlan-id* **{mode | key}**	Configures the encryption method for the VLAN associated to this interface. For more details see Chapter 10, "Configuring WLAN Authentication and Encryption,"which describes in detail the possible methods and keys.

The following example shows how to:

- Enable a VLAN on the radio and ethernet ports as the native VLAN

- Assign an SSID to a VLAN
- Assign an AES-CCMP encryption method to a VLAN
- Assign an SSID to a radio interface

```
ap# configure terminal
ap(config)# interface dot11Radio 0.31
ap(config-subif)# encapsulation dot1Q 31 native
ap(config-subif)# exit
ap(config)# interface gigabitEthernet 0.31
ap(config-subif)# encapsulation dot1Q 31 native
ap(config-subif)# exit
ap(config)# dot11 ssid batman
ap(config-ssid)# vlan 31
ap(config-ssid)# exit
ap(config)# interface dot11Radio 0
ap(config-if)# encryption vlan 31 mode ciphers aes-ccm
ap(config-if)# ssid batman
ap(config-if)# end
```

Assigning Names to VLANs

You can assign a name to a VLAN in addition to its numerical ID. VLAN names can contain up to 32 ASCII characters. The access point stores each VLAN name and ID pair in a table.

Guidelines for Using VLAN Names

Keep these guidelines in mind when using VLAN names:

- The mapping of a VLAN name to a VLAN ID is local to each access point, so across your network, you can assign the same VLAN name to a different VLAN ID.

Note If clients on your wireless LAN require seamless roaming, We recommend that you assign the same VLAN name to the same VLAN ID across all access points, or that you use only VLAN IDs without names.

- Every VLAN configured on your access point must have an ID, but VLAN names are optional.
- VLAN names can contain up to 32 ASCII characters. However, a VLAN name cannot be a number between 1 and 4095. For example, *vlan4095* is a valid VLAN name, but *4095* is not. The access point reserves the numbers 1 through 4095 for VLAN IDs.

Creating a VLAN Name

Beginning in privileged EXEC mode, follow these steps to assign a name to a VLAN:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 vlan-name** *name* **vlan** *vlan-id*	Assign a VLAN name to a VLAN ID. The name can contain up to 32 ASCII characters.

	Command	Purpose
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to remove the name from the VLAN. Use the **show dot11 vlan-name** privileged EXEC command to list all the VLAN name and ID pairs configured on the access point.

Using a RADIUS Server to Assign Users to VLANs

You can configure your RADIUS authentication server to assign users or groups of users to a specific VLAN when they authenticate to the network.

Note Unicast and multicast cipher suites advertised in WPA or RSN Information Element information element (and negotiated during 802.11 association) may potentially mismatch with the cipher suite supported in an explicitly assigned VLAN. If the RADIUS server assigns a new vlan ID which uses a different cipher suite from the previously negotiated cipher suite, there is no way for the access point and client to switch back to the new cipher suite. Currently, WPA, WPA2 and CCKM protocols do not allow the cipher suite to be changed after the initial 802.11 cipher negotiation phase. In this scenario, the client device is disassociated from the wireless LAN.

The VLAN-mapping process consists of these steps:

1. A client device associates to the access point using any SSID configured on the access point.
2. The client begins RADIUS authentication.
3. When the client authenticates successfully, the RADIUS server maps the client to a specific VLAN, regardless of the VLAN mapping defined for the SSID the client is using on the access point. If the server does not return any VLAN attribute for the client, the client is assigned to the VLAN specified by the SSID mapped locally on the access point.

These are the RADIUS user attributes used for vlan-id assignment. Each attribute must have a common tag value between 1 and 31 to identify the grouped relationship.

- IETF 64 (Tunnel Type): Set this attribute to **VLAN**
- IETF 65 (Tunnel Medium Type): Set this attribute to **802**
- IETF 81 (Tunnel Private Group ID): Set this attribute to *vlan-id*

Viewing VLANs Configured on the Access Point

In privileged EXEC mode, use the **show vlan** command to view the VLANs that the access point supports. This is sample output from a **show vlan** command:

```
Virtual LAN ID:  1 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0
Dot11Radio1
GigabitEthernet0

   Protocols Configured:   Address:              Received:        Transmitted:
        Other                                           0                 995

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Other                                           0                 995

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Other                                           0                 995

   4330 packets, 363704 bytes input
   995 packets, 75675 bytes output

Virtual LAN ID:  31 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0.31
Dot11Radio1.31
GigabitEthernet0.31

 This is configured as native Vlan for the following interface(s) :
Dot11Radio0
Dot11Radio1
GigabitEthernet0

   Protocols Configured:   Address:              Received:        Transmitted:
        Bridging        Bridge Group 1                  0                5620

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Bridging        Bridge Group 1                  0                5620

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Bridging        Bridge Group 1                  0                5620

   0 packets, 0 bytes input
   5620 packets, 2737560 bytes output

Virtual LAN ID:  34 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0.34
GigabitEthernet0.34

   Protocols Configured:   Address:              Received:        Transmitted:
        Bridging        Bridge Group 34                 0                   0

   0 packets, 0 bytes input
   0 packets, 0 bytes output
        Bridging        Bridge Group 34                 0                   0

   0 packets, 0 bytes input
   0 packets, 0 bytes output

Virtual LAN ID:  35 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interface:   Dot11Radio0.35

   Protocols Configured:   Address:              Received:        Transmitted:

   0 packets, 0 bytes input
   0 packets, 0 bytes output
```

Configuring a Non-native VLAN as a Management VLAN

Usually, the native VLAN will always be the management VLAN.

Consider a case where you wish to change the VLAN bridge group to 1 for a non-native VLAN. In such a case you can use the **command dot11 management vlan** *vlanid* to configure the non-native VLAN as a management VLAN.

Conditions and Prerequisites

- You cannot have a native VLAN if you are using a non-native VLAN as a management VLAN.
- Workgroup Bridge is not supported for this feature.
- When changing the management VLAN, any sessions of telnet, GUI users which are in progress will be become unstable or get disrupted due to the change.

Configuration Steps (CLI)

Step 1 Use the command for setting the non-native VLAN as a management VLAN.

```
ap(config)# dot11 management vlan vlanid
```

Ensure that you do not have a native VLAN when using this command.

Step 2 Remove the bridge group 1 from main interface or native

```
ap(config)# interface d0
ap(config-if)# no bridge-group 1
```

Step 3 Configure the bridge group 1 to the non-native interface

```
ap(config-if)# interface 0.5
ap(config-if)# encapsulation dot1q vlanid
ap(config-if)# bridge-group 1
ap(config-if)# interface bvi1
```

Step 4 Setup DHCP

```
ap(config-if)# ip-address dhcp
```

Configuration Steps (GUI)

Step 1 Go to **Services > VLAN**

Step 2 Under the **Assigned VLANs** section, from the **Current VLAN List**, choose the VLAN to be set as management VLAN

Step 3 Check the **Management VLAN (If non-native)** check box.

Steps to Undo the Configuration (CLI)

Step 1 Use the command for removing the non-native VLAN as a management VLAN.

```
ap(config)# no dot11 management vlan vlanid
```

Step 2 Move the bridge group 1 to the main interface or to another native VLAN

Step 3 Configure another bridge group to the non-native interface

VLAN Configuration Example

This example shows how to use VLANs to manage wireless devices on a college campus. In this example, three levels of access are available through VLANs configured on the wired network:

- Management access—Highest level of access; users can access all internal drives and files, departmental databases, top-level financial information, and other sensitive information. Management users are required to authenticate using Cisco EAP-FAST.
- Faculty access—Medium level of access; users can access school's Intranet and Internet, access internal files, access student databases, and view internal information such as human resources, payroll, and other faculty-related material. Faculty users are required to authenticate using Cisco PEAP.
- Student access—Lowest level of access; users can access school's Intranet and the Internet, obtain class schedules, view grades, make appointments, and perform other student-related activities. Students are allowed to join the network using static WPA2 personal (Pre-shared key).

In this scenario, a minimum of three VLAN connections are required, one for each level of access. Because the access point can handle up to 16 SSIDs, you can use the basic design shown in Table 14-1.

Table 14-1 Access Level SSID and VLAN Assignment

Level of Access	SSID	VLAN ID
Management	manage (not boss)	01
Faculty	teach	02
Student	learn	03

Managers configure their wireless client adapters to use SSID manage, faculty members configure their clients to use SSID teach, and students configure their wireless client adapters to use SSID learn. When these clients associate to the access point, they automatically belong to the correct VLAN.

You would complete these steps to support the VLANs in this example:

1. Configure or confirm the configuration of these VLANs on one of the switches on your LAN.
2. On the access point, assign an SSID to each VLAN.
3. Assign authentication types to each SSID.
4. Configure VLAN 1, the Management VLAN, on both the Ethernet and dot11radio interfaces on the access point. You should make this VLAN the native VLAN.
5. Configure VLANs 2 and 3 on both the Ethernet and dot11radio interfaces on the access point.
6. Configure the client devices.

Table 14-2 shows the commands needed to configure the three VLANs in this example.

Table 14-2 Configuration Commands for VLAN Example

Configuring VLAN 1	Configuring VLAN 2	Configuring VLAN 3
ap# **configure terminal** ap(config)# **interface dot11radio 0** ap(config-if)# **ssid boss** ap(config-ssid)# **end**	ap# **configure terminal** ap(config)# **interface dot11radio 0** ap(config-if)# **ssid teach** ap(config-ssid)# **end**	ap# **configure terminal** ap(config)# **interface dot11radio 0** ap(config-if)# **ssid learn** ap(config-ssid)# **end**
ap **configure terminal** ap(config) **interface FastEthernet0.1** ap(config-subif) **encapsulation dot1Q 1 native** ap(config-subif) **exit**	ap(config) **interface FastEthernet0.2** ap(config-subif) **encapsulation dot1Q 2** ap(config-subif) **bridge-group 2** ap(config-subif) **exit**	ap(config) **interface FastEthernet0.3** ap(config-subif) **encapsulation dot1Q 3** ap(config-subif) **bridge-group 3** ap(config-subif) **exit**
ap(config)#dot11 ssid manage ap(config-ssid)#vlan 1 ap(config-ssid)#authentication open eap eap_methods ap(config-ssid)#exit ap(config)#interface dot11Radio 0 ap(config-if)#encryption vlan 1 mode ciphers aes-ccm	ap(config)#dot11 ssid teach ap(config-ssid)#vlan 2 ap(config-ssid)#authentication open eap eap_methods ap(config-ssid)#exit ap(config)#interface dot11Radio 0 ap(config-if)#encryption vlan 2 mode ciphers aes-ccm	ap(config)#dot11 ssid teach ap(config-ssid)#vlan 3 ap(config-ssid)#authentication open ap(config-ssid)#authentication key-management wpa version 2 ap(config-ssid)#wpa-psk ascii 0 Cisco123 ap(config-ssid)#exit ap(config)#interface dot11Radio 0 ap(config-if)#encryption vlan 3 mode ciphers aes-ccm

Table 14-3 shows the results of the configuration commands in Table 14-2. Use the **show running** command to display the running configuration on the access point.

Table 14-3 Results of Example Configuration Commands

VLAN 1 Interfaces	VLAN 2 Interfaces	VLAN 3 Interfaces
interface Dot11Radio**0**.1 encapsulation dot1Q 1 native no ip route-cache no cdp enable bridge-group 1 bridge-group 1 subscriber-loop-control bridge-group 1 block-unknown-source no bridge-group 1 source-learning no bridge-group 1 unicast-flooding bridge-group 1 spanning-disabled	interface Dot11Radio**0**.2 encapsulation dot1Q 2 no ip route-cache no cdp enable bridge-group 2 bridge-group 2 subscriber-loop-control bridge-group 2 block-unknown-source no bridge-group 2 source-learning no bridge-group 2 unicast-flooding bridge-group 2 spanning-disabled	interface Dot11Radio**0**.3 encapsulation dot1Q 3 no ip route-cache bridge-group 3 bridge-group 3 subscriber-loop-control bridge-group 3 block-unknown-source no bridge-group 3 source-learning no bridge-group 3 unicast-flooding bridge-group 3 spanning-disabled
interface gigabitethernet encapsulation dot1Q 1 native no ip route-cache bridge-group 1 no bridge-group 1 source-learning bridge-group 1 spanning-disabled	interface gigabitethernet encapsulation dot1Q 2 no ip route-cache bridge-group 2 no bridge-group 2 source-learning bridge-group 2 spanning-disabled	interface gigabitethernet encapsulation dot1Q 3 no ip route-cache bridge-group 3 no bridge-group 3 source-learning bridge-group 3 spanning-disabled

Notice that when you configure a bridge group on the radio interface, these commands are set automatically:

```
bridge-group 2 subscriber-loop-control
bridge-group 2 block-unknown-source
no bridge-group 2 source-learning
no bridge-group 2 unicast-flooding
bridge-group 2 spanning-disabled
```

When you configure a bridge group on the `gigabitethernet` interface, these commands are set automatically:

```
no bridge-group 2 source-learning
bridge-group 2 spanning-disabled
```

CHAPTER 15

Configuring QoS

This chapter describes how to configure quality of service (QoS) on your access point. With this feature, you can provide preferential treatment to certain traffic at the expense of others. Without QoS, the access point offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release.

Understanding QoS for Wireless LANs

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure QoS on the access point, you can select specific network traffic, prioritize it, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your wireless LAN makes network performance more predictable and bandwidth utilization more effective.

When you configure QoS, you create QoS policies and apply the policies to the VLANs configured on your access point. If you do not use VLANs on your network, you can apply your QoS policies to the access point's Ethernet and radio ports.

Note When you enable QoS, the access point uses Wi-Fi Multimedia (WMM) mode by default. See the "Using Wi-Fi Multimedia Mode" section on page 15-4 for information on WMM.

QoS for Wireless LANs Versus QoS on Wired LANs

The QoS implementation for wireless autonomous access points differs from QoS implementations on wired devices:

- They do not classify packets; they prioritize packets based on DSCP value, client type (such as a wireless phone), or the priority value in the 802.1q or 802.1p tag.
- They do not construct internal DSCP values; they only support mapping by assigning IP DSCP, Precedence, or Protocol values to Layer 2 COS values.
- They carry out WMM type of queuing on the radio egress ports.
- They do only FIFO queuing on the Ethernet egress port.
- They support only 802.1Q/P tagged packets. Access points do not support ISL.
- They support only MQC policy-map **set cos** action.
- They prioritize the traffic from voice clients (such as VoWLAN IP phones) over traffic from other clients when the QoS Element for Wireless Phones feature is enabled.
- They support Spectralink phones using the class-map IP protocol clause with the protocol value set to 119.

To contrast the wireless LAN QoS implementation with the QoS implementation on other Cisco network devices, see the *Cisco IOS Quality of Service Solutions Configuration Guide* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/index.htm

Impact of QoS on a Wireless LAN

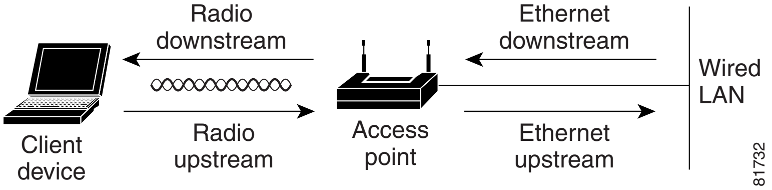
Wireless LAN QoS features are an implementation of the Wi-FI Alliance WMM certification, based on the IEEE 802.11e amendment. Any wireless client certified WMM can implement Wireless LAN QOS in the upstream direction (from the wireless client to the AP). Any client certified 802.11n or 802.11ac is also certified WMM.

Regardless of the client support (or lack of support) for WMM, Cisco access points support WMM and can be configured to provide wireless QoS in the downstream direction (from the AP toward the wireless clients), and in the upstream direction when forwarding wireless frames to the wired interface.

Just as in other media, you might not notice the effects of QoS on a lightly loaded wireless LAN. The benefits of QoS become more obvious as the load on the wireless LAN increases, keeping the latency, jitter, and loss for selected traffic types within an acceptable range.

QoS on the wireless LAN focuses on downstream prioritization from the access point. Figure 15-1 shows the upstream and downstream traffic flow.

Figure 15-1 Upstream and Downstream Traffic Flow



- The radio downstream flow is traffic transmitted out the access point radio to a wireless client device. This traffic is the main focus for QoS on a wireless LAN.
- The radio upstream flow is traffic transmitted out the wireless client device to the access point. Each client independently determines what prioritization mechanisms should be used for this traffic. The AP cannot force a prioritization mechanism for the client uplink traffic. However, the AP configuration determines if uplink prioritization is allowed (when WMM is enabled on the AP SSID) or disallowed (when WMM is disabled on the AP SSID).
- The Ethernet downstream flow is traffic sent from a switch or a router to the Ethernet port on the access point. If QoS is enabled on the switch or router, the switch or router might prioritize and rate-limit traffic to the access point.
- The Ethernet upstream flow is traffic sent from the access point Ethernet port to a switch or router on the wired LAN. The access point does not prioritize traffic that it sends to the wired LAN based on traffic classification. However, the AP maintains the traffic QoS marking.

Precedence of QoS Settings

When you enable QoS, the access point queues packets based on the Layer 2 class of service value for each packet. The access point applies QoS policies in this order:

1. Packets already classified—When the access point receives packets from a QoS-enabled switch or router that has already classified the packets with non-zero 802.1Q/P user_priority values, the access point uses that classification and does not apply other QoS policy rules to the packets. An existing classification takes precedence over all other policies on the access point.

Note Even if you have not configured a QoS policy, the access point always honors tagged 802.1P packets that it receives over the radio interface and uses the matching 802.11e user priority queue to send the packet over the air. You can use the Streams page to configure the rate at which each queue should be sent and the number of retries for unicast packets.

2. *QoS Element for Wireless Phones* setting—If you enable the *QoS Element for Wireless Phones* setting, dynamic voice classifiers are created for are created for RTP-based traffic, which allows the wireless phone traffic to be a higher priority than other clients' traffic. Additionally, the QoS Basic Service Set (QBSS) is enabled to advertise channel load information in the beacon and probe response frames. Some IP phones use QBSS elements to determine which access point to associate to, based on the traffic load.
   You can use the Cisco IOS command dot11 phone dot11e command to enable 802.11e/WMM QBSS Load IE. The 7920 phones with 1.05 firmware, and older, do not support the 802.11e QBSS IE.
   If your network wireless clients are primarily 7920 phones with firmware 1.05 or older, enable dot11 phone.
   If your network wireless clients are primarily 7920 with firmware 1.09 or later, or WMM compatible VoWLAN phones, enable the IEEE 802.11e compatible QBSS IE with the command dot11 phone dot11e.

   This example shows how to enable IEEE 802.11 phone support with the legacy QBSS Load element:

   ```
   AP(config)# dot11 phone
   ```

   This example shows how to enable IEEE 802.11 phone support with the standard IEEE 802.11e QBSS Load element:

   ```
   AP(config)# dot11 phone dot11e
   ```

   This example shows how to stop or disable the IEEE 802.11 phone support:

   ```
   AP(config)# no dot11 phone
   ```

3. Policies you create on the access point—QoS Policies that you create and apply to VLANs or to the access point interfaces are third in precedence after previously classified packets and the *QoS Element for Wireless Phones* setting.
4. Default classification for all packets on VLAN—If you set a default classification for all packets on a VLAN, that policy is fourth in the precedence list.

Using Wi-Fi Multimedia Mode

When you enable QoS, the access point uses Wi-Fi Multimedia (WMM) mode by default. WMM provides these enhancements over basic QoS mode:

- The access point adds each packet's class of service to the packet's 802.11 header to be passed to the receiving station.
- Each access class has its own 802.11 sequence number. The sequence number allows a high-priority packet to interrupt the retries of a lower-priority packet without overflowing the duplicate checking buffer on the receiving side.
- WPA/WPA2 replay detection is done per access class on the receiver. Like 802.11 sequence numbering, WPA/WPA2 replay detection allows high-priority packets to interrupt lower priority retries without signaling a replay on the receiving station.
- For access classes that are configured to allow it, transmitters that are qualified to transmit through the normal backoff procedure are allowed to send a set of pending packets during the configured transmit opportunity (a specific number of microseconds). Sending a set of pending packets improves throughput because each packet does not have to wait for a backoff to gain access; instead, the packets can be transmitted immediately one after the other.
- U-APSD Power Save is enabled.

The access point uses WMM enhancements in packets sent to client devices that support WMM. The access point applies basic QoS policies to packets sent to clients that do not support WMM.

Use the **no dot11 qos mode wmm** configuration interface command to disable WMM using the CLI. To disable WMM using the web-browser interface, unselect the check boxes for the radio interfaces on the QoS Advanced page. Figure 15-3 shows the QoS Advanced page.

Using Band Select

Band Select allows you to move dual-band capable wireless clients joining the cell, to the less congested 5 GHz radio, if your SSID is available on both radios. This feature improves the overall performance of the network.

When the Band Select feature is enabled, the access point delays the probe responses on the 2.4 GHz radio to all new clients, for all SSIDs that are Band Select-enabled. At the same time, the access point does not delay the probe responses on the 5 GHz radio. This mechanism allows dual-band clients to discover the SSID on the 5 GHz radio first, thus pushing these clients to associate to the SSID on the AP 5 GHz radio instead of the 2.4 Ghz radio. Only those clients that are 2.4 GHz-only will stay on the 2.4 GHz radio.

To enable Band Select, follow these steps:

Step 1 Choose **Security > SSID Manager.**

Step 2 Click **NEW** to create a new SSID.

or

Choose the required SSID from the **Current SSID.**

Step 3 Click the **Band Select** radio button.

Step 4 Click **Apply**.

Note The band select feature is useful only if the SSID is assigned to both radios.

When a client actively discovers a network, that client sends probe requests on one or several channels. A typical behavior is to send a burst of probe requests on a given channel, collect the replies from the responding APs, and then move to the next channel. For this reason, two consecutive probe requests received on a given channel does not necessarily indicate two attempts to discover APs on a channel, but may be part of the same scan cycle through a burst.

You can fine tune the Band Select behavior to determine information such as:

- How long a scan cycle is expected to last
- The number of cycles during which an AP will not respond to probe request from a client on a 2.4 GHz channel, along with client RSSI
- Timeout for the Band Select mechanism to be triggered.

To assign the parameters for Band Select, follow these steps:

Step 1 Choose **Services > Band Select.**

Step 2 Check the **Band Select** check box.

Step 3 Enter the values for the following:

- Client-Rssi—Minimum Receive Signal Strength Indicator (RSSI) required for the client to be eligible for band select. The range is from 20 to 90.
- Cycle-Count—Number of probe requests on the 2.4 GHz band that the access point ignores.
- Cycle-Threshold (ms)—Time in milliseconds that the access point can expect each probe request burst cycle from the client. The range is from 1 to 1000.
- Expire-Dual-Band (secs)—Time after which dual-band clients will be declared as new and may have their probe request frames delayed or ignored again. The range is from 10 to 300.
- Expire-Suppression (secs)—Time after which 2.4 GHz-only clients will be declared as new and may have their probe frames delayed or ignored again. The range is from 10 to 200.

Step 4 Click **Apply**.

Beginning in privileged EXEC mode, use these commands to configure BandSelect using the access point CLI:

```
- ap(config)# dot11 band-select parameters
- ap(config-bs-profile)# cycle-count?
- ap(config-bs-profile)# cycle-threshold?
- ap(config-bs-profile)# expire-suppression?
- ap(config-bs-profile)# expire-dual-band?
- ap(config-bs-profile)# client-rssi?
- ap (config)# dot11 ssid abcd
- ap(config-ssid)# band-select
```

Configuring QoS

QoS is disabled by default (however, the radio interface always honors tagged 802.1P packets even when you have not configured a QoS policy). This section describes how to configure QoS on your access point. It contains this configuration information:

- Configuration Guidelines, page 15-6
- Configuring QoS Using the Web-Browser Interface, page 15-7
- Adjusting Radio Access Categories, page 15-12
- AVVID Priority Mapping, page 15-11

Configuration Guidelines

Before configuring QoS on your access point, you should be aware of this information:

- The most important guideline in QoS deployment is to be familiar with the traffic on your wireless LAN. If you know the applications used by wireless client devices, the applications' sensitivity to delay, and the amount of traffic associated with the applications, you can configure QoS to improve performance.

- QoS does not create additional bandwidth for your wireless LAN; it helps control the allocation of bandwidth. If you have plenty of bandwidth on your wireless LAN, you might not need to configure QoS.
- The **ampdu** command is available for the 802.11n radio interfaces. Aggregate MAC protocol data unit (AMPDU) is a structure containing multiple MPDUs transported as a single PSDU by the physical layer. For additional information about this command, see the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges.*

Configuring QoS Using the Web-Browser Interface

This section describes configuring QoS using the web-browser interface.

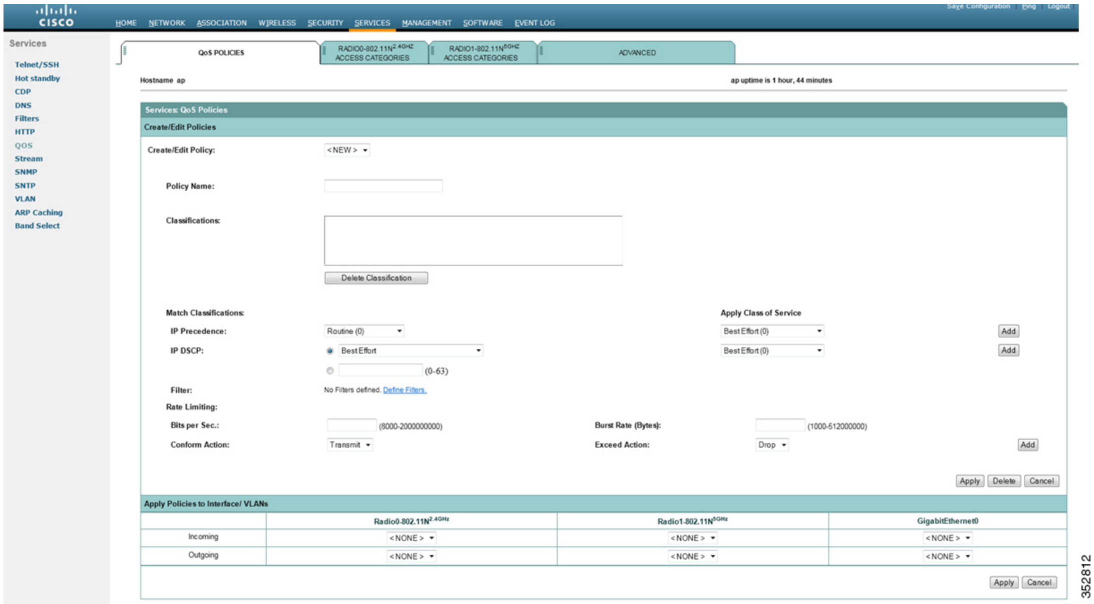
For a list of Cisco IOS commands for configuring QoS using the CLI, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Follow these steps to configure QoS:

Step 1 If you use VLANs on your wireless LAN, make sure the necessary VLANs are configured on your access point before configuring QoS.

Step 2 Click **Services** in the general menu bar at the top of any page in the web-browser interface. When the list of Services appears, click **QoS**. The QoS Policies page appears. Figure 15-2 shows the QoS Policies page.

Figure 15-2 QoS Policies Page



Hostname ap

ap uptime is 1 hour, 44 minutes

Services: QoS Policies

Create/Edit Policies

Create/Edit Policy: <NEW>

Policy Name:

Classifications:

Match Classifications:

Apply Class of Service

IP Precedence: Routine (0) Best Effort (0)

IP DSCP: ● Best Effort Best Effort (0)

○ (0-63)

Filter: No Filters defined. Define Filters.

Rate Limiting:

Bits per Sec.: (8000-2000000000) Burst Rate (Bytes): (1000-512000000)

Conform Action: Transmit Exceed Action: Drop

Apply Policies to Interface/ VLANs

	$Radio0\text{-}802.11N^{2.4GHz}$	$Radio1\text{-}802.11N^{5GHz}$	GigabitEthernet0
Incoming	<NONE>	<NONE>	<NONE>
Outgoing	<NONE>	<NONE>	<NONE>

Step 3 With **<NEW>** selected in the Create/Edit Policy field, type a name for the QoS policy in the Policy Name entry field. The name can contain up to 25 alphanumeric characters. Do not include spaces in the policy name.

Note You can also select two preconfigured QoS policies: WMM and Spectralink. When you select either of these, a set of default classifications are automatically populated in the Classification field.

Step 4 If the packets that you need to prioritize contain IP precedence information in the IP header TOS field, select an IP precedence classification from the IP Precedence drop-down list. Menu selections include:

- Routine (0)
- Priority (1)
- Immediate (2)
- Flash (3)
- Flash Override (4)
- Critic/CCP (5)
- Internet Control (6)
- Network Control (7)

Step 5 To select the 802.11e User Priority value that the access point will apply to the frames that will be sent to wireless clients, for packets of type that you selected from the IP Precedence menu. The access point matches your IP Precedence selection with your 802.11 user priority (class of service) selection. The Apply Class of Service (representing the 802.11e user priority value to apply) drop-down list contains:

- Best Effort (0)
- Background (1)
- Spare (2)
- Excellent (3)
- Control Lead (4)
- Video <100ms Latency (5)
- Voice <100ms Latency (6)
- Network Control (7)

Step 6 Click the **Add** button beside the Class of Service menu for IP Precedence. The classification appears in the Classifications field. To delete a classification, select it and click the **Delete** button beside the Classifications field.

Step 7 If the packets that you need to prioritize contain IP DSCP instead of IP precedence information in the IP header ToS field, select an IP DSCP classification from the IP DSCP drop-down list. Menu selections include:

- Best Effort
- Assured Forwarding — Class 1 Low
- Assured Forwarding — Class 1 Medium
- Assured Forwarding — Class 1 High
- Assured Forwarding — Class 2 Low
- Assured Forwarding — Class 2 Medium
- Assured Forwarding — Class 2 High
- Assured Forwarding — Class 3 Low

- Assured Forwarding — Class 3 Medium
- Assured Forwarding — Class 3 High
- Assured Forwarding — Class 4 Low
- Assured Forwarding — Class 4 Medium
- Assured Forwarding — Class 4 High
- Class Selector 1
- Class Selector 2
- Class Selector 3
- Class Selector 4
- Class Selector 5
- Class Selector 6
- Class Selector 7
- Expedited Forwarding

Step 8 Use the Apply Class of Service drop-down list to select the class of service (that is, the 802.11e user priority value) that the access point will apply to packets of the type that you selected from the IP DSCP menu. The access point matches your IP DSCP selection with your class of service selection.

Step 9 Click the **Add** button beside the Class of Service menu for IP DSCP. The classification appears in the Classifications field.

Step 10 If you need to prioritize the packets from Spectralink phones (IP Protocol 119) on your wireless LAN, use the Apply Class of Service drop-down list to select the class of service that the access point will apply to Spectralink phone packets. The access point matches Spectralink phone packets with your class of service selection.

Step 11 Click the **Add** button beside the Class of Service menu for IP Protocol 119. The classification appears in the Classifications field.

Step 12 If you need to assign a priority to filtered packets, use the Filter drop-down list to select a Filter to include in the policy. (If no filters are defined on the access point, a link to the Apply Filters page appears instead of the Filter drop-down list.) For example, you could assign a high priority to a MAC address filter that includes the MAC addresses of IP phones.

Note The access list you use in QoS only affects the prioritization of the target packets, not the AP (security) forwarding decisions.

Step 13 Use the Apply Class of Service drop-down list to select the class of service that the access point will apply to packets that match the filter that you selected from the Filter menu. The access point matches your filter selection with your class of service selection.

Step 14 Click the **Add** button beside the Class of Service menu for Filter. The classification appears in the Classifications field.

Step 15 When you finish adding classifications to the policy, click the **Apply** button under the Apply Class of Service drop-down lists. To cancel the policy and reset all fields to defaults, click the **Cancel** button under the Apply Class of Service drop-down lists. To delete the entire policy, click the **Delete** button under the Apply Class of Service drop-down lists.

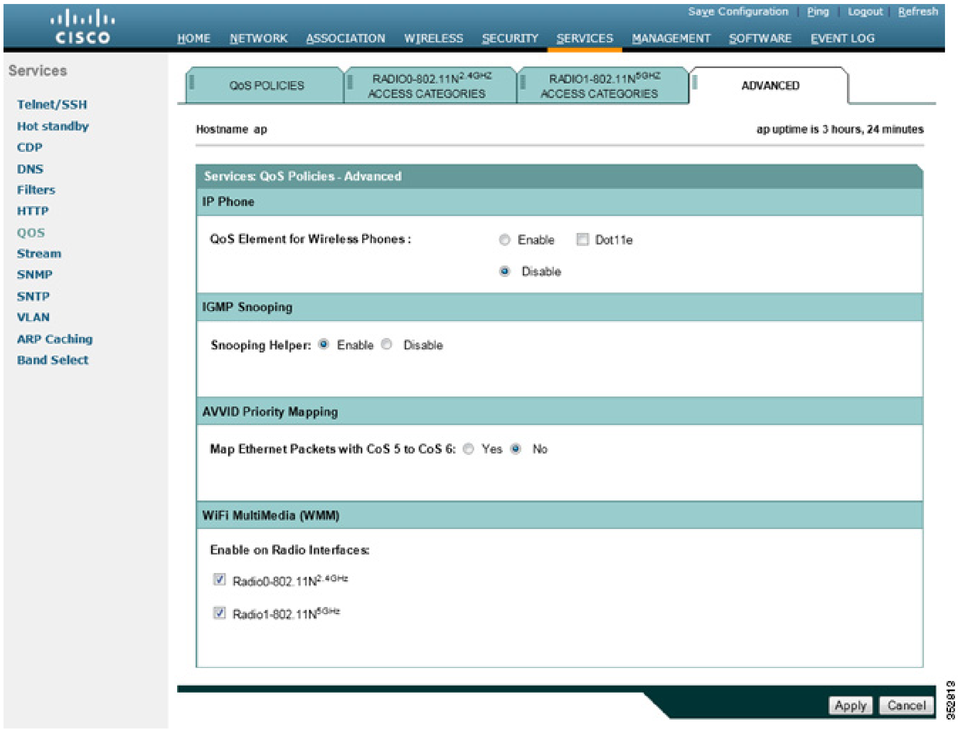
Step 16 Use the Apply Policies to Interface/VLANs drop-down lists to apply policies to the access point Ethernet and radio ports. If VLANs are configured on the access point, drop-down lists for each VLANs' virtual ports appear in this section. If VLANs are not configured on the access point, drop-down lists for each interface appear.

Step 17 Click the **Apply** button at the bottom of the page to apply the policies to the access point ports.

The QoS Policies Advanced Page

The QoS Policies Advanced page (Figure 15-3)

Figure 15-3 QoS Policies - Advanced Page



Hostname ap

ap uptime is 3 hours, 24 minutes

Services: QoS Policies - Advanced

IP Phone

QoS Element for Wireless Phones : ○ Enable □ Dot11e ● Disable

IGMP Snooping

Snooping Helper: ● Enable ○ Disable

AVVID Priority Mapping

Map Ethernet Packets with CoS 5 to CoS 6: ○ Yes ● No

WiFi MultiMedia (WMM)

Enable on Radio Interfaces:

☑ Radio0-802.11N$^{2.4GHz}$

☑ Radio1-802.11N^{5GHz}

Select **Enable the QoS Element for Wireless Phones** option and click Select Enable the QoS Element for Wireless Phones option and click Apply to give top priority to all voice packets.

QoS Element for Wireless Phones

When you enable the QoS Element for Wireless Phones, the access point gives top priority to voice packets even if you do not enable QoS. This setting operates independently from the QoS policies that you configure.

Select **dot11e** to use the WMM / 802.11e version of QBSS Load IE. If you leave this selection blank, the CCX pre-802.11e version of the QBSS Load IE is used. Use the pre-802.11e version if your wireless clients are primarily 7920 phones with firmware 1.05 or older. Use the 802.11e version if your clients are primarily WMM compatible clients.

IGMP Snooping

When Internet Group Membership Protocol (IGMP) snooping is enabled on a switch, the switch forwards multicast traffic only to those ports where the switch registers that multicast traffic as needed. As a consequence, when a wireless client roams from one access point to another access point connected to the same switch, the switch initially does not know whether or not the multicast traffic is needed on the port to the second access point. The result is that the clients' multicast session is interrupted. IGMP snooping on the access point helps mitigating this issue.

When the access points' IGMP snooping helper is enabled, and a client joins the access point cell, the access point immediately sends a general IGMP query to the wireless LAN, prompting the client to send in an IGMP membership report. The membership report is forwarded to the wired interface. When the network infrastructure receives the host's IGMP membership report, it ensures delivery of that host's multicast data stream to the access point port. The traffic is then relayed to the wireless interface. This way, the wireless client multicast flow is not interrupted while roaming.

When Internet Group Membership Protocol (IGMP) snooping is enabled on a switch and a client roams from one access point to another, the clients’ multicast session is dropped. When the access points’ IGMP snooping helper is enabled, the access point sends a general query to the wireless LAN, prompting the client to send in an IGMP membership report. When the network infrastructure receives the host’s IGMP membership report, it ensures delivery of that host’s multicast data stream.

The IGMP snooping helper is enabled by default. To disable it, browse to the QoS Policies - Advanced page, select **Disable**, and click **Apply**.

Note If there is no multicast router for processing IGMP query and response from the host, it is mandatory that **no igmp snooping** be configured on the access point. when IGMP snooping is enabled, all multicast group traffic must send IGMP query and response packets. If IGMP query or response packets are not detected, all multicast traffic for the group is dropped.

AVVID Priority Mapping

The 802.11e protocol assigns to voice packets a User Priority value of 6. Cisco wired networks follow the IETF recommendation to assign to voice packets a class of service value of 5. Enabling AVVID priority mapping maps the Ethernet packets tagged as class of service 5, to class of service 6 when these packets are exchanged between the wireless and the wired sides of the access point. This feature enables the access point to apply the correct priority to voice packets for compatibility with Cisco AVVID networks.

AVVID priority mapping is enabled by default. To disable it, browse to the QoS Policies - Advanced page, select **No** for Map Ethernet Packets with CoS 5 to CoS 6, and click **Apply**.

WiFi Multimedia (WMM)

Using the Admission Control check boxes, you can enable or disable WMM support on the access point's radio interfaces. Default is enabled. When WMM is enabled, both WMM and non-WMM clients are allowed to join the access point radio.

Note When you enable admission control (in RADIO1-802.11N2.4GHZ ACCESS CATEGORIES or RADIO1-802.11N5GHZ ACCESS CATEGORIES), clients associated to the access point must complete the WMM admission control procedure before they can use that access category.

Rate Limiting

Rate limiting provides control over the data traffic transmitted or received on an interface.The Class-Based Policing feature performs the following functions:

- Limits the input or output transmission rate of a class of traffic based on user-defined criteria.
- Marks packets by setting the IP precedence value, IP differentiated services code point (DSCP) value and Quality of Service (QoS) group.

This is used to rate-limit the upstream traffic originating from each of the non-roots to root bridge incase of P2MP setup. To do rate-limiting on downstream traffic , class-maps are applied at the root-side router/switch.

Note Rate-limiting can be applied to ethernet ingress only

Adjusting Radio Access Categories

The access point uses the radio access categories to calculate backoff times for each packet. As a rule, high-priority packets have short backoff times.

The default values in the Min and Max Contention Window fields and in the Slot Time fields are based on settings recommended in IEEE 802.11 amendment. For detailed information on these values, see the IEEE 802.11e amendment, 7.3.2.27 or 802.11-2012 standard, 8.4.2.31 (EDCA Parameter Set element).

Cisco strongly recommends that you use the default settings on the Radio Access Categories page. Changing these values can lead to unexpected blockages of traffic on your wireless LAN, and the blockages might be difficult to diagnose. If you change these values and find that you need to reset them to defaults, use the default settings listed in Table 15-1.

The values listed in Table 15-1 are to the power of 2. The access point computes Contention Window values with this equation:

CW = 2 ** X minus 1

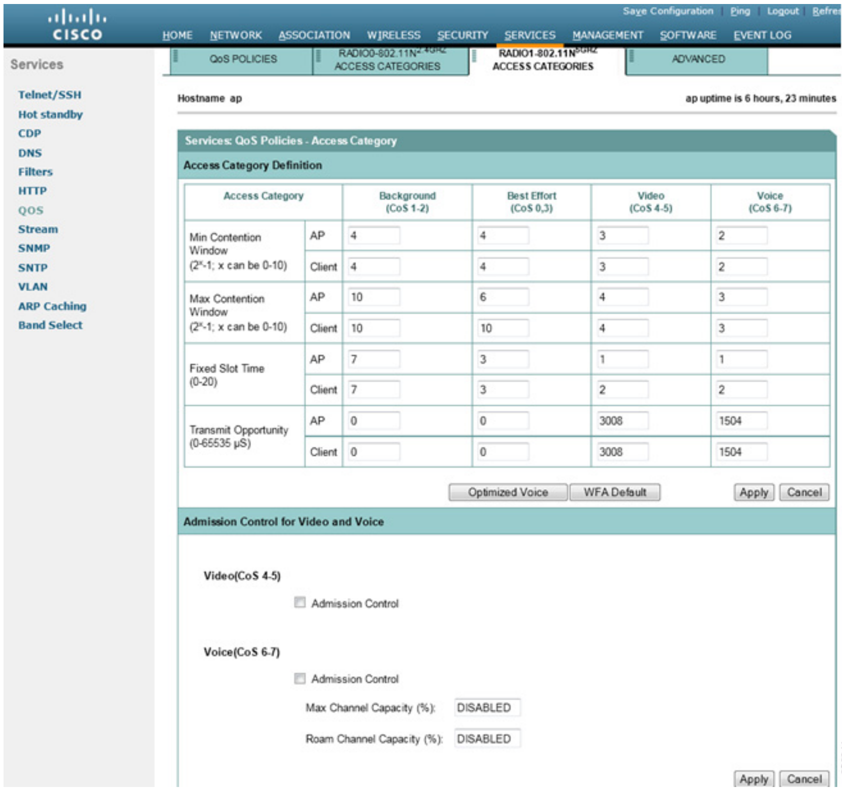
where X is the value from Table 15-1.

Table 15-1 Default QoS Radio Access Categories

Class of Service	Min Contention Window		Max Contention Window		Fixed Slot Time		Transmit Opportunity		Admission Control	
	Local	Cell	Local	Cell	Local	Cell	Local	Cell	Local	Cell
Background	4		10		6		0			
Best Effort	4		10		2		0			
Video <100ms Latency	3		2		1		3008			
Voice <100ms Latency	2		3		1		1504			

Figure 15-4 shows the Radio Access Categories page. Dual-radio access points have a Radio Access Categories page for each radio.

Figure 15-4 Radio Access Categories Page


Save Configuration | Ping | Logout | Refres
CISCO
HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES MANAGEMENT SOFTWARE EVENT LOG
QoS POLICIES
RADIO0-802.11N$^{2.4GHZ}$ ACCESS CATEGORIES
RADIO1-802.11N^{5GHZ} ACCESS CATEGORIES
ADVANCED
Services
Telnet/SSH
Hot standby
CDP
DNS
Filters
HTTP
QOS
Stream
SNMP
SNTP
VLAN
ARP Caching
Band Select
Optimized Voice
WFA Default
Apply
Cancel
Apply
Cancel
352814

Hostname ap

ap uptime is 6 hours, 23 minutes

Services: QoS Policies - Access Category

Access Category Definition

Access Category		Background (CoS 1-2)	Best Effort (CoS 0,3)	Video (CoS 4-5)	Voice (CoS 6-7)
Min Contention Window (2^x-1; x can be 0-10)	AP	4	4	3	2
	Client	4	4	3	2
Max Contention Window (2^x-1; x can be 0-10)	AP	10	6	4	3
	Client	10	10	4	3
Fixed Slot Time (0-20)	AP	7	3	1	1
	Client	7	3	2	2
Transmit Opportunity (0-65535 µS)	AP	0	0	3008	1504
	Client	0	0	3008	1504

Admission Control for Video and Voice

Video(CoS 4-5)

□ Admission Control

Voice(CoS 6-7)

□ Admission Control

Max Channel Capacity (%): DISABLED

Roam Channel Capacity (%): DISABLED

Wireless clients using TCLAS and TSPEC can request a class of service through an ADDTS (add Traffic Stream Request) sent to the access point before the client initiates the traffic stream. The ADDTS describes the intended traffic, along with the expected nominal rates for that traffic.

Configuring Nominal Rates

When an access point receives an ADDTS (add traffic stream) request from a WMM client, it checks the nominal rate or minimum PHY rate in the ADDTS request against the nominal rates defined by the CLI command **traffic-stream**. If they do not match, the access point rejects the ADDTS request.

If you choose Optimized Voice Settings (see Figure 15-4), the following nominal rates are configured:

- 5.5Mbps, 6.0Mbps, 11.0Mbps, 12.0Mbps, and 24.0Mbps

Information about the **traffic-stream** command can be found in the *Command Reference for Cisco Aironet Access Points and Bridges*, which is available at cisco.com at the following URL:

http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/command/reference/cr12410b-chap2.html#wp3257080

Note The above rates work fine for Cisco phones and most WMM VoWLAN IP phones. However, some third party wireless phones.... Third parties wireless phones may have a different nominal rate or minimum PHY rate. You may need to enable additional nominal rates for these phones.

Optimized Voice Settings

Using the Admission Control check boxes, you can control client use of the access categories. When you enable admission control for an access category, clients associated to the access point must complete the WMM admission control procedure before they can use that access category. However, access points do not support the admission control procedure in this release, so clients cannot use the access category when you enable Admission Control.

Configuring Call Admission Control

Configuring Call Admission Control (CAC) on an access point involves the following:

1. Configuring the radio.
2. Enabling admission control on an SSID.

Configuring the Radio

This section describes how to configure admission control on an access point's radio.

For a list of Cisco IOS commands for configuring admission control using the CLI, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Follow these steps to configure admission control on a radio:

Step 1 Click the Access Categories page of the radio you want to configure.

Figure 15-4 shows an example of an Access Categories page.

Step 2 Select the **Admission Control** check box under **Voice(CoS 6-7)**.

Step 3 Enter the maximum percentage of the channel to be used for voice in the **Max Channel Capacity (%)** field.

Step 4 Enter the maximum percentage of the channel to use for roaming calls in the **Roam Channel Capacity (%)** field.

The percentage of the channel used by roaming calls up to the value specified in this field is deducted from the value you specified in the **Max Channel Capacity (%)** field.

For example, suppose you have entered 75% in the **Max Channel Capacity (%)** field and 6% in the **Roam Channel Capacity (%)**. If roaming calls are using 5% of the channel, a maximum of 70% of the channel can be used for voice calls (new calls initiated by clients in the cell).

Step 5 To enable call admission control for real time video traffic (AC_VO), check the **Admission Control** check box under **Video (CoS 5-6)**.

Note The admission control settings you have configured in this section will not take effect until you enable admission control on an SSID.

Enabling Admission Control on the SSID

This section describes how to enable admission control on an SSID.

For a list of Cisco IOS commands for enabling admission control using the CLI, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Follow these steps to enable admission control on an SSID:

Step 1 Open the SSID Manager page.

Step 2 Select an SSID.

Step 3 Under **General Settings**, select **Enable** in the **Call Admission Control** field.

Troubleshooting Admission Control

You can use two CLI commands to display information to help you troubleshoot admission control problems:

- To display current admission control settings on radio 0, enter the following command:

```
# show dot11 cac int dot11Radio 0
```

- To display current admission control settings on radio 1, enter the following command:

```
# show dot11 cac int dot11Radio 1
```

- To display information about admitted streams with admission control and MT, enter the following command:

```
# show dot11 traffic-streams
```

Configuring Streams

QoS policies mark or remark packets that go through the access point. When defining a QoS policy, you can also decide on limiting the rate of certain traffic.

QoS Elements for Wireless phones allows you to prioritize any voice packet regardless of any other consideration. This applies a low latency configuration to voice packets, without any upper limit.

Configuring streams is the third way of applying prioritization techniques to time-sensitive traffic, by determining which traffic should be sent with higher priority (low latency queue), and limit the amount of retries for these time-sensitive packets. Streams can be used in combination with other QoS configurations.

To configure these features, go to **Services > Streams** page (see Figure 15-5).

Step 1 From the Packet Handling per User Priority section, select the User Priorities queues that should be served with a low latency queuing logic.

- If **Reliable** is selected, unicasts packets are resent, if they are not acknowledged, as long as the destination is still reachable (wireless client associated or wireless bridge connected). The maximum amount of retries for a unicast packet that has not be acknowledged is determined at the radio level, with the Max data retries value configured in the Settings tab of each radio configuration section.

- If **Low Latency** is selected, you can configure the amount of retries that the AP should use before discarding the current packet and sending the next one. For low latency traffic, skipping a packet is usually preferable to interrupting the flow of traffic. In the Max Retries for Packet Discard, enter the max number of retries that the Ap should use for the matching User Priority set to Low Latency.

Step 2 Click **Apply** to validate.

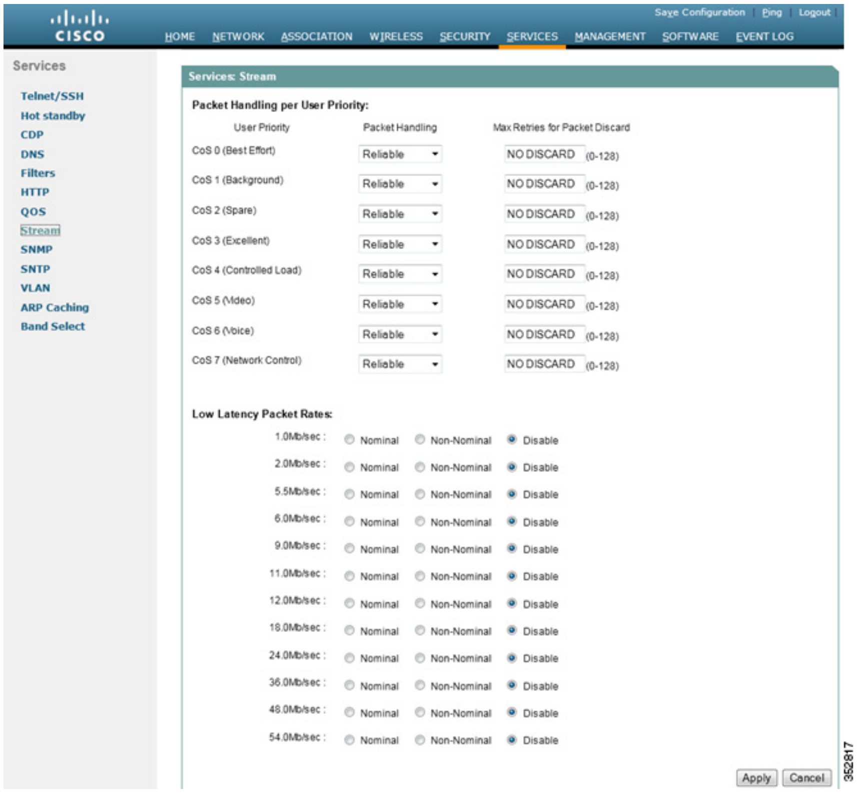
Step 3 At the bottom of the page, in the Low Latency Packet Rates section, you can also configure the rate at which the frames set for the Low Latency queues should be sent.

- Nominal—The AP will try to use this rate to send the Low Latency Packets (using the faster rate first, and depending on the client signal level).
- Non-nominal—The AP will try not to use that rate, but will revert to it if no nominal rate is possible.
- Disabled—The AP will not try to use that rate.

Step 4 Click **Apply** to validate.

To configure streams using the CLI, see Chapter 6, "Configuring Radio Settings."

Figure 15-5 Streams Page



Services: Stream

Packet Handling per User Priority:

User Priority	Packet Handling	Max Retries for Packet Discard
CoS 0 (Best Effort)	Reliable	NO DISCARD (0-128)
CoS 1 (Background)	Reliable	NO DISCARD (0-128)
CoS 2 (Spare)	Reliable	NO DISCARD (0-128)
CoS 3 (Excellent)	Reliable	NO DISCARD (0-128)
CoS 4 (Controlled Load)	Reliable	NO DISCARD (0-128)
CoS 5 (Video)	Reliable	NO DISCARD (0-128)
CoS 6 (Voice)	Reliable	NO DISCARD (0-128)
CoS 7 (Network Control)	Reliable	NO DISCARD (0-128)

Low Latency Packet Rates:

1.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
2.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
5.5Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
6.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
9.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
11.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
12.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
18.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
24.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
36.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
48.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable
54.0Mb/sec :	○ Nominal	○ Non-Nominal	● Disable

CHAPTER 16

Configuring Filters

This chapter describes how to configure and manage MAC address, IP, and EtherType filters on the access point using the web-browser interface.

Understanding Filters

Protocol filters (IP protocol, IP port, and EtherType) prevent or allow the use of specific protocols through the access point's Ethernet and radio ports. You can set up individual protocol filters or sets of filters. You can filter protocols for wireless client devices, users on the wired LAN, or both. For example, an SNMP filter on the access point's radio port prevents wireless client devices from using SNMP with or through the access point but does not block SNMP access from the wired LAN.

IP address and MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific IP or MAC addresses. You can create a filter that passes traffic to all addresses except those you specify, or you can create a filter that blocks traffic to all addresses except those you specify.

You can configure filters using the web-browser interface or by entering commands in the CLI.

Tip You can include filters in the access point's QoS policies. Refer to Chapter 15, "Configuring QoS,"for detailed instructions on setting up QoS policies.

Note Using the CLI, you can configure up to 2,048 MAC addresses for filtering. Using the web-browser interface, however, you can configure only up to 43 MAC addresses for filtering.

Configuring Filters Using the CLI

To configure filters using CLI commands, you use access control lists (ACLs) and bridge groups.

- For more information on bridge groups, see the *Configuring Transparent Bridging* chapter in the *Bridging and IBM Networking Configuration Guide*, at the following URL: http://www.cisco.com/c/en/us/td/docs/ios/bridging/configuration/guide/15-s/br-15-s-book/br_transprnt_brdg.html
- For more information on access control lists (ACLs), see the *IP Access List Overview* chapter, in the *Security Configuration Guide*, at the following URL: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/12-4t/sec-data-acl-12-4t-book/sec-access-list-ov.html

Note Avoid using both the CLI and the web-browser interfaces to configure the wireless device. If you configure the wireless device using the CLI, the web-browser interface might display an inaccurate interpretation of the configuration. However, the inaccuracy does not necessarily mean that the wireless device is misconfigured. For example, if you configure ACLs using the CLI, the web-browser interface might display this message: "Filter 700 was configured on interface Dot11Radio0 using CLI. It must be cleared via CLI to ensure proper operation of the web interface." If you see this message you should use the CLI to delete the ACLs and use the web-browser interface to reconfigure them.

Configuring Filters Using the Web-Browser Interface

This section describes how to configure and enable filters using the web-browser interface. You complete two steps to configure and enable a filter:

1. Name and configure the filter using the filter setup pages.
2. Enable the filter using the Apply Filters page.

Configuring and Enabling MAC Address Filters

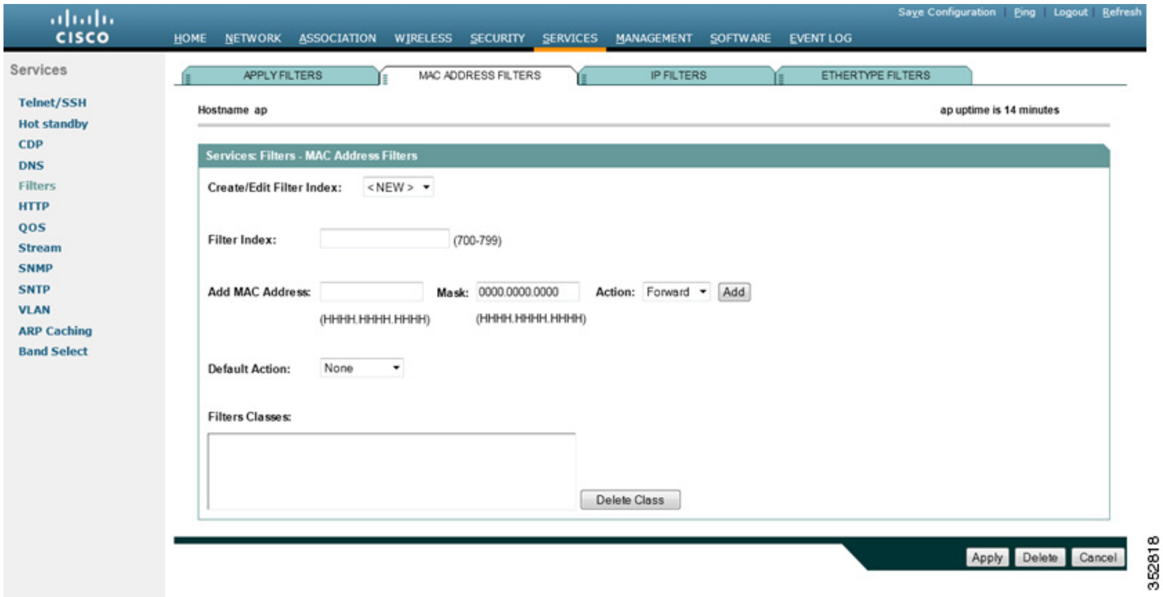
MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses except those you specify. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Note Using the CLI, you can configure MAC addresses for filtering, but because of a NVRAM limitation, you need FTP or TFTP for more than 600 MAC filters. Using the web-browser interface, however, you can configure only up to 43 MAC addresses for filtering.

Note MAC address filters are powerful, and if you make a mistake setting up the filters, you can lock yourself out of the access point while connecting to the AP using Telnet. If you accidentally lock yourself out of your access point, use the CLI from the console interface to disable the filters.

Use the MAC Address Filters page to create MAC address filters for the access point. Figure 16-1 shows the MAC Address Filters page.

Figure 16-1 MAC Address Filters Page



Hostname ap

ap uptime is 14 minutes

Services: Filters - MAC Address Filters

Create/Edit Filter Index: < NEW >

Filter Index: (700-799)

Add MAC Address: (HHHH.HHHH.HHHH) Mask: 0000.0000.0000 (HHHH.HHHH.HHHH) Action: Forward

Default Action: None

Filters Classes:

Follow this link path to reach the Address Filters page:

1. Click **Services** in the page navigation bar.
2. In the Services page list, click **Filters**.
3. On the Apply Filters page, click the **MAC Address Filters** tab at the top of the page.

Creating a MAC Address Filter

Follow these steps to create a MAC address filter:

Step 1 Follow the link path to the MAC Address Filters page.

Step 2 If you are creating a new MAC address filter, make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu. To edit a filter, select the filter number from the Create/Edit Filter Index menu.

Step 3 In the Filter Index field, name the filter with a number from 700 to 799. The number you assign creates an access control list (ACL) for the filter.

Step 4 Enter a MAC address in the Add MAC Address field. Enter the address with periods separating the three groups of four characters (0005.9a39.2110, for example).

Note To make sure the filter operates properly, use lower case for all the letters in the MAC addresses that you enter.

Step 5 Use the Mask entry field to indicate how many bits, from left to right, the filter checks against the MAC address. For example, to require an exact match with the MAC address (to check all bits) enter **0000.0000.0000**. To check only the first (highest weight) 8 bytes, enter **0.0.FFFF**.

Step 6 Select **Forward** or **Block** from the Action menu.

Step 7 Click **Add**. The MAC address appears in the Filters Classes field. To remove the MAC address from the Filters Classes list, select it and click **Delete Class**.

Step 8 Repeat Step 4 through Step 7 to add addresses to the filter.

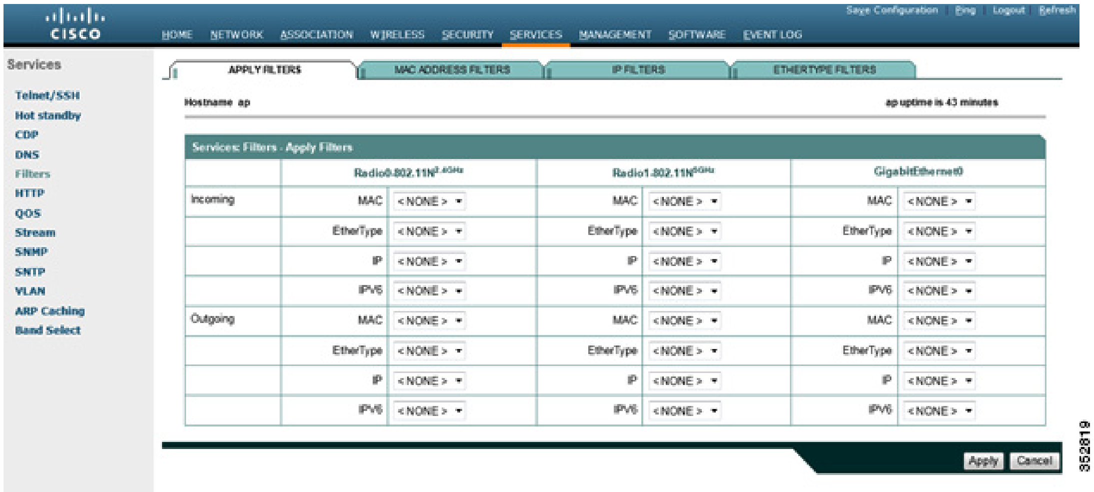
Step 9 Select **Forward All** or **Block All** from the Default Action menu. The filter's default action must be the opposite of the action for at least one of the addresses in the filter. For example, if you enter several addresses and you select **Block** as the action for all of them, you must choose **Forward All** as the filter's default action.

Tip You can create a list of allowed MAC addresses on an authentication server on your network. Consult the "Configuring Authentication Types" section on page 11-9 for instructions on using MAC-based authentication.

Step 10 Click **Apply**. The filter is saved on the access point, but it is not enabled until you apply it on the Apply Filters page.

Step 11 Click the **Apply Filters** tab to return to the Apply Filters page. Figure 16-2 shows the Apply Filters page.

Figure 16-2 Apply Filters Page



Hostname ap ap uptime is 43 minutes

Services: Filters - Apply Filters

	Radio0-802.11N$^{2.4GHz}$		Radio1-802.11N^{5GHz}		GigabitEthernet0	
Incoming	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >	IP	< NONE >
	IPV6	< NONE >	IPV6	< NONE >	IPV6	< NONE >
Outgoing	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >	IP	< NONE >
	IPV6	< NONE >	IPV6	< NONE >	IPV6	< NONE >

Step 12 Select the filter number from one of the MAC drop-down lists. You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.

Step 13 Click **Apply**. The filter is enabled on the selected ports.

If clients are not filtered immediately, click **Reload** on the System Configuration page to restart the access point. To reach the System Configuration page, click **Software** on the task menu and then click **System Configuration**.

Note Client devices with blocked MAC addresses cannot send or receive data through the access point, but they might remain in the Association Table as unauthenticated client devices. Client devices with blocked MAC addresses disappear from the Association Table when the access point stops monitoring them, when the access point reboots, or when the clients associate to another access point.

Creating a MAC Address Filter - Using CLI

To create a MAC address filter via CLI use the following command in global configuration mode:

access-list *number-700-799* **{permit | deny}** *macc-address mask*

The following MAC address access-list permits any MAC address starting with 1111.22, and blocks every other MAC address:

```
ap(config)# access-list 701 permit 1111.2200.0000   0000.00ff.ffff
ap(config)# access-list 701 deny   0000.0000.0000   ffff.ffff.ffff
```

To apply a MAC address access list to an interface, starting in global configuration mode use the following sequence of commands:

Step 1 **interface** *name*

Step 2 **l2-filter bridge-group-acl**

Step 3 **bridge-group** *bridge-group-number* **{input-address-list | output-address-list}** *ACL-number*

The following example applies the MAC address access list 701 created above to the Radio 0 interface, in the inbound direction. However, no VLAN was created on the interface, and so the ACL is applied to the default bridge group 1:

```
ap(config)# interface dot11Radio 0
ap(config-if)# l2-filter bridge-group-acl
ap(config-if)# bridge-group 1 input-address-list 701
```

In the following example, a VLAN 33 was created and associated to Radio 1. The matching bridge group 33 was created between the radio 1 subinterface 33 and the Ethernet subinterface 33. The MAC address filter is applied to the outgoing direction on radio 1 subinterface 33:

```
ap(config)# interface Dot11Radio1
ap(config-if)# l2-filter bridge-group-acl
ap(config-if)# exit
ap(config)# interface Dot11Radio1.33
ap(config-if)# bridge-group 33 output-address-list 701
```

Using MAC Address ACLs to Block or Allow Client Association to the Access Point

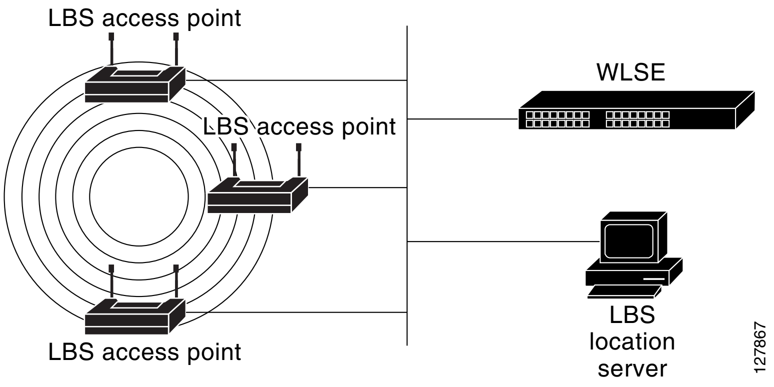
You can use MAC address ACLs to block or allow association to the access point. Instead of filtering traffic across an interface, you use the ACL to filter associations to the access point radio.

Follow these steps to use an ACL to filter associations to the access point radio:

Step 1 Follow Steps 1 through 10 in the "Creating a MAC Address Filter" section on page 16-4 to create an ACL. For MAC addresses that you want to allow to associate, select **Forward** from the Action menu. Select **Block** for addresses that you want to prevent from associating. Select **Block All** from the Default Action menu.

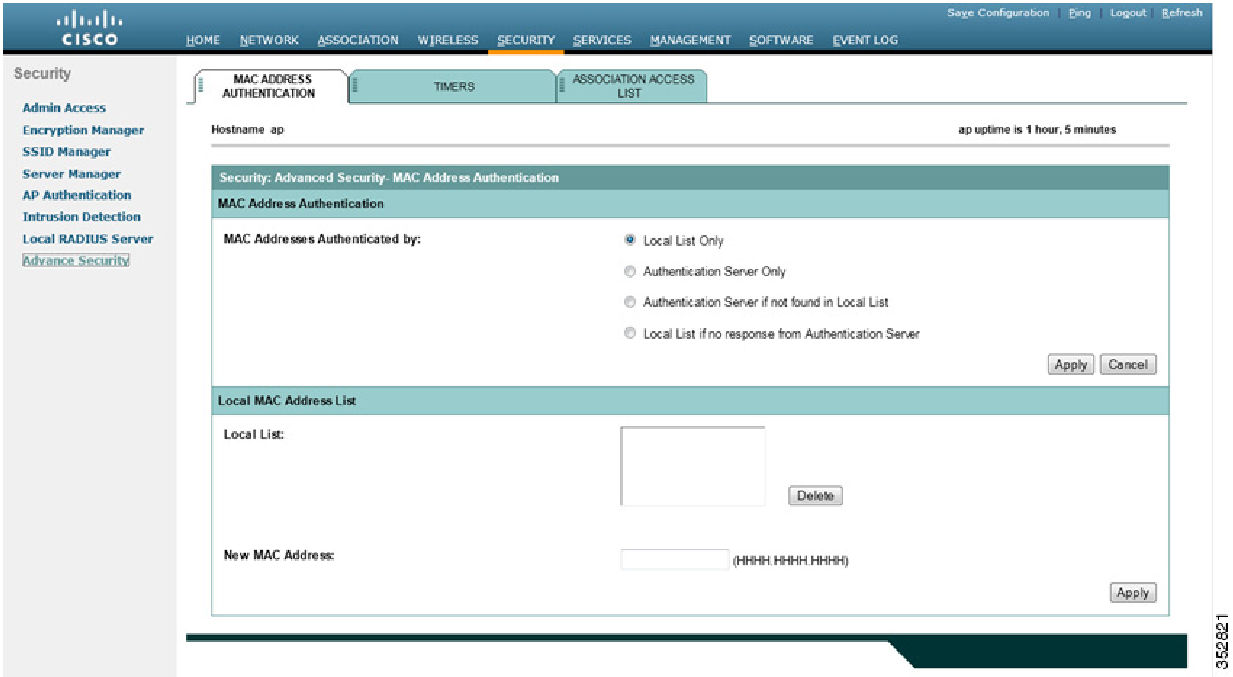
Step 2 Click **Security** to browse to the Security Summary page. Figure 16-3 shows the Security Summary page.

Figure 16-3 Security Summary Page



Step 3 Click **Advanced Security** to browse to the Advanced Security: MAC Address Authentication page. Figure 16-4 shows the MAC Address Authentication page.

Figure 16-4 Advanced Security: MAC Address Authentication Page



Hostname ap ap uptime is 1 hour, 5 minutes

Security: Advanced Security- MAC Address Authentication

MAC Address Authentication

MAC Addresses Authenticated by:
● Local List Only
○ Authentication Server Only
○ Authentication Server if not found in Local List
○ Local List if no response from Authentication Server

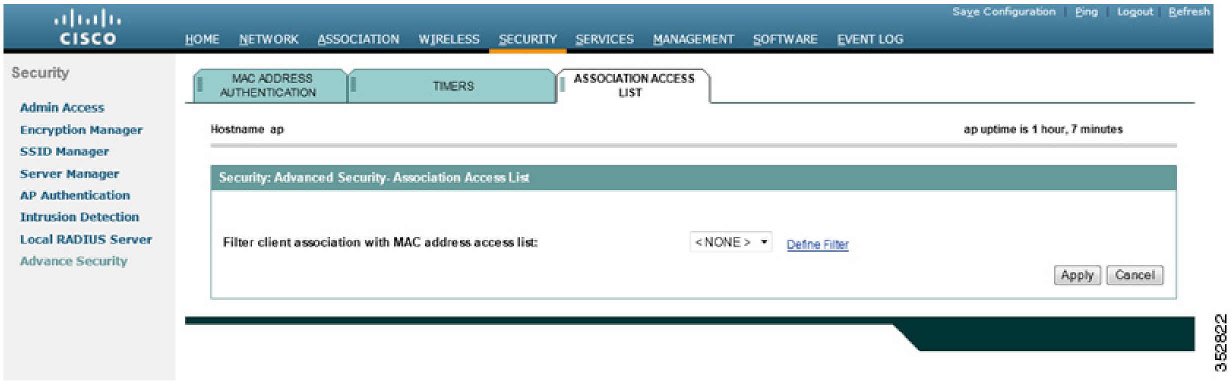
Local MAC Address List

Local List:

New MAC Address: (HHHH.HHHH.HHHH)

Step 4 Click the **Association Access List** tab to browse to the Association Access List page. Figure 16-5 shows the Association Access List page.

Figure 16-5 Association Access List Page



Hostname ap ap uptime is 1 hour, 7 minutes

Security: Advanced Security- Association Access List

Filter client association with MAC address access list: < NONE >

Step 5 Select your MAC address ACL from the drop-down list.

Step 6 Click **Apply**.

Using MAC Address ACLs to Block or Allow Client Association to the Access Point via CLI

To create an association filter via the CLI, use the following procedure:

Step 1 Creating a MAC address access-list using the command **access-list** *number-700-799*.

Step 2 Use the global configuration command **dott11 association mac-list** *list-number* to apply the use the MAC address access list as a filter for all wireless client associations, on all radios.
Clients not listed in the MAC address access-list will not be allowed to associate to any of the AP SSIDs, on any of the AP radios.

The following example uses MAC address access-list 702 as a global MAC address association filter:

```
ap(config)# dot11 association mac-list 702
ap(config)# end
```

Configuring MAC Address Authentication

A MAC address filter applied to an interface filters the MAC addresses which are sending traffic through that interface, regardless of the SSID in use. A MAC address filter applied at global association level filters those MAC addresses that are allowed to associate to one of the access point SSIDs, regardless of the SSID in use or regardless of the VLAN or interface associated to the SSID.

You can also use MAC addresses to filter the MAC addresses that are allowed to associate to a target SSID. This process is called MAC address authentication. The following table compares the three MAC address filtering methods available on Cisco IOS access points:

Method	Target	Notes
Interface MAC address filter	Specific interface or VLAN	Applies to all SSIDs mapped to the target interface or VLAN
Association MAC address	AP, globally	Applies to all SSIDs and all VLANs, for all wireless clients associating to the AP
SSID MAC address authentication	Specific SSID	Applies to a specific SSID, regardless of the radio, interface or VLAN to which the SSID is mapped

You can check MAC addresses used for authentication on the access point local list, or on an authentication server. The authentication server can be an external RADIUS server or the AP internal RADIUS server.

To configure your AP to use MAC address authentication on the SSID, you need to go through the following steps:

Step 1 Determine the source of MAC address authentication (local list, local AP RADIUS server, external RADIUS server)
If you use the AP local list of local RADIUS server, create the MAC addresses on the AP (in the AP local list of the RADIUS server, respectively)

Step 2 Configure the SSID to use the method you defined.

Determining the source of MAC Authentication

To define the source of MAC address verification for SSID MAC authentication, go to **Security > Advanced Security > MAC Address Authentication**.

In the MAC Address Authentication tab:

- To exclusively use the list of MAC addresses defined in the local page to authenticate client MAC addresses on target SSIDs, click the **Local List Only** option.
- To use the local MAC address list as the primary MAC address authentication method for SSID MAC-address authentication, when a list created on an external RADIUS server for MAC addresses not found in the local list, click the **Authentication Server if not found in the local list** option.
- To use primarily an external RADIUS server (or the access point internal RADIUS server), and to revert back to a local list on the same page only if the external server is not responding, click the **Local list if no response from Authentication server** option.
- To only use an external RADIUS server or the AP internal RADIUS server, and to never use the MAC addresses defined on the local page, click the **Authentication Server Only** option.

Click **Apply** to validate your choice.

Using the CLI, you can determine the source of MAC address verification using the global command **aaa authentication login mac_methods**.

The following example configures the AP to use the local list, and only revert to a group of RADIUS servers called rad_mac if the MAC address is not found in the local list:

```
ap(config)# aaa authentication login mac_methods local group rad_mac
```

For more details on how to create groups of RADIUS servers, see Chapter 11, “Configuring Authentication Types.”

Using a local MAC address list

If you want to use a list of MAC addresses defined on the MAC Address authentication page for SSID MAC address authentication, enter at the bottom of the page the MAC addresses (one at a time) that are authorized for authentication on the target SSIDs.

Note The list is global. A MAC address defined in the list will be authorized to join any SSID where MAC address authentication is enabled. If you want to use different lists of MAC addresses for different SSIDs on the AP, you must use an external RADIUS server.

From the CLI, a MAC address used for MAC address authentication is entered as a user, with the mac-address as the password. The user is then assigned an *exit* autocommand to prevent the user from accessing the AP interface. The following example creates the MAC address 1111.2222.3333 in the global list:

```
ap(config)# username 111122223333 password 0 111122223333
ap(config)# username 111122223333 autocommand exit
ap(config)# end
```

Using the AP internal RADIUS server for MAC address authentication

If you want to use a list of MAC addresses defined in the AP internal RADIUS server page, go to **Security > Local RADIUS Server > General Setup**.

In the General Setup page, enable the server for MAC authentication by checking the **MAC** check box in the **Enable Authentication Protocols** section. Then, click **Apply** to validate.

When using the AP internal RADIUS server, you need to define the AP as a RADIUS client. For this:

Step 1 In the **Network Access Server (AAA Clients)** section, enter the AP's IP address in the **Network Access Server** field.

Step 2 Enter a **Shared Secret**, which is a password used to authenticate the queries sourced from the AP IP address. You will need to define the same shared secret when configuring the AP as a RADIUS server in the Server Manager page.

Step 3 Click **Apply** to validate.

For more details on how to configure the AP local RADIUS server, including CLI commands, see Chapter 11, "Configuring Authentication Types.".

To create individual MAC addresses to be used for MAC authentication on target SSIDs, in the Individual Users section:

Step 1 Enter the target MAC address, without any separator in both the **Username** and **Password** fields.

Step 2 Check the **MAC authentication only**.

Step 3 Click **Apply** to validate.

Note The MAC addresses defined in the AP internal RADIUS server are global.
If you configure the AP to use an authentication server for MAC address verification, all SSIDs configured to use MAC authentication and the local AP RADIUS server will check the local list.
A major difference between using the AP global MAC address list and using the AP internal Authentication server as a source for SSID MAC authentication is that the global list applies to all SSIDs configured to use MAC address authentication. When choosing to use an authentication server for MAC authentication, some SSIDs can use the AP internal server list, while other SSIDs can use an external RADIUS server list.

From the CLI, you can add MAC address users by entering the local RADIUS server configuration submode, and then creating users. The username and password are the MAC address, without the separator. Add the keyword mac-only to specify that the user is used for MAC authentication.

The following example creates the MAC address user 333344445555:

```
ap(config)# radius-server local
ap(config-radsrv)# user 333344445555 password 0 333344445555 mac-auth-only
ap(config-radsrv)# end
```

When using the AP internal RADIUS server, you need to define the AP as a RADIUS server in the **Security > Server Manager** page.

In the Corporate Servers section, you can add a new server for your AP. For this:

Step 1 Enter the AP's IP address in the **Server** field

Step 2 Enter the same **Shared Secret** you entered when defining the AP as a RADIUS client in the previous page.

Step 3 Enter the **Authentication Port** as 1812.

Step 4 Enter the **Accounting Port** as 1813.

Step 5 Click **Apply** to validate.

Step 6 In the Default Server Priorities section, select the AP in the **Priority 1** field of the **MAC Authentication** priority list.

Step 7 Click **Apply** to validate.

Using an external RADIUS server for MAC address authentication

When using an external RADIUS server for MAC authentication, enter the external RADIUS server details in the **Security > Server Manager > Corporate Servers** section. Also select at least one server in the **Default Server Priorities > MAC Authentication** list.

Configuring the SSID for MAC Authentication

Once you have defined a source of MAC addresses and defined the MAC addresses (when using the local list or the AP internal RADIUS server), you need to configure the target SSIDs to use MAC authentication. For this:

Step 1 Go to the **Security > SSID Manager** page.

Step 2 Select or create a new SSID.

Step 3 In the Client Authentication Settings section, select the check boxes for each accepted authentication method. Then from the corresponding drop-down list, select **With MAC Authentication**.

Step 4 To use the default method defined in the **Security > Advanced Security** page and the default servers defined in **Security > Server Manager** page (if applicable), click the **Use Defaults** option in the MAC Authentication Servers section.
To use servers different from those defined in the **Security > Server Manager** page, click the **Customize** option and then select the servers to use.
The **Customize** option does not override the configuration from the **Security > Advanced Security** page that defines if the local list or the servers should be used. If you configured the AP to use only the internal list, choosing the Customize option in the SSID page will have no effect. The Customize option is only targeted at selecting what MAC server to choose, when MAC servers are selected in the **Security > Advanced Security** page.

Step 5 Click **Apply** to validate.

Creating a Time-Based ACL

Time-based ACLs are ACLs that can be enabled or disabled for a specific period of time. This capability provides robustness and the flexibility to define access control policies that either permit or deny certain kinds of traffic.

This example illustrates how to configure a time-based ACL through the CLI, where Telnet connection is permitted from the inside to the outside network on weekdays during business hours:

Note A time-based ACL can be defined either on the gigabit Ethernet port or on the Radio port of the Aironet AP, based on your requirements. It is never applied on the Bridge Group Virtual Interface (BVI).

Follow these steps to create a time-based ACL.

Step 1 Log in to the AP through the CLI.

Step 2 Use the console port or Telnet in order to access the ACL through the Ethernet interface or the wireless interface.

Step 3 Enter global configuration mode.

Step 4 Create a Time Range. For this example, Test:

```
ap(config-time-range)# time-range Test
```

Step 5 Create a time-range:

```
ap(config-time-range)# time-range periodic weekdays 7:00 to 19:00
```

Note Allows access to users during weekdays from 7:00 to 19:00 hrs.

Step 6 Create an ACL. For this example, 101:

```
ap(config)# ip access-list extended 101
ap(config-ext-nacl)# permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range Test
```

Note This ACL permits Telnet traffic to and from the network for the specified time-range Test. It also permits a Telnet session to the AP on weekdays, if the AP IP address is in the 172.16.1.0 subnet.

Step 7 Apply the time-based ACL to the Ethernet interface:

```
ap(config)# interface gigabitEthernet 0
ap(config-if)# ip address 172.16.1.10 255.255.255.0
ap(config-if)# ip access-group 101 in
```

ACL Logging

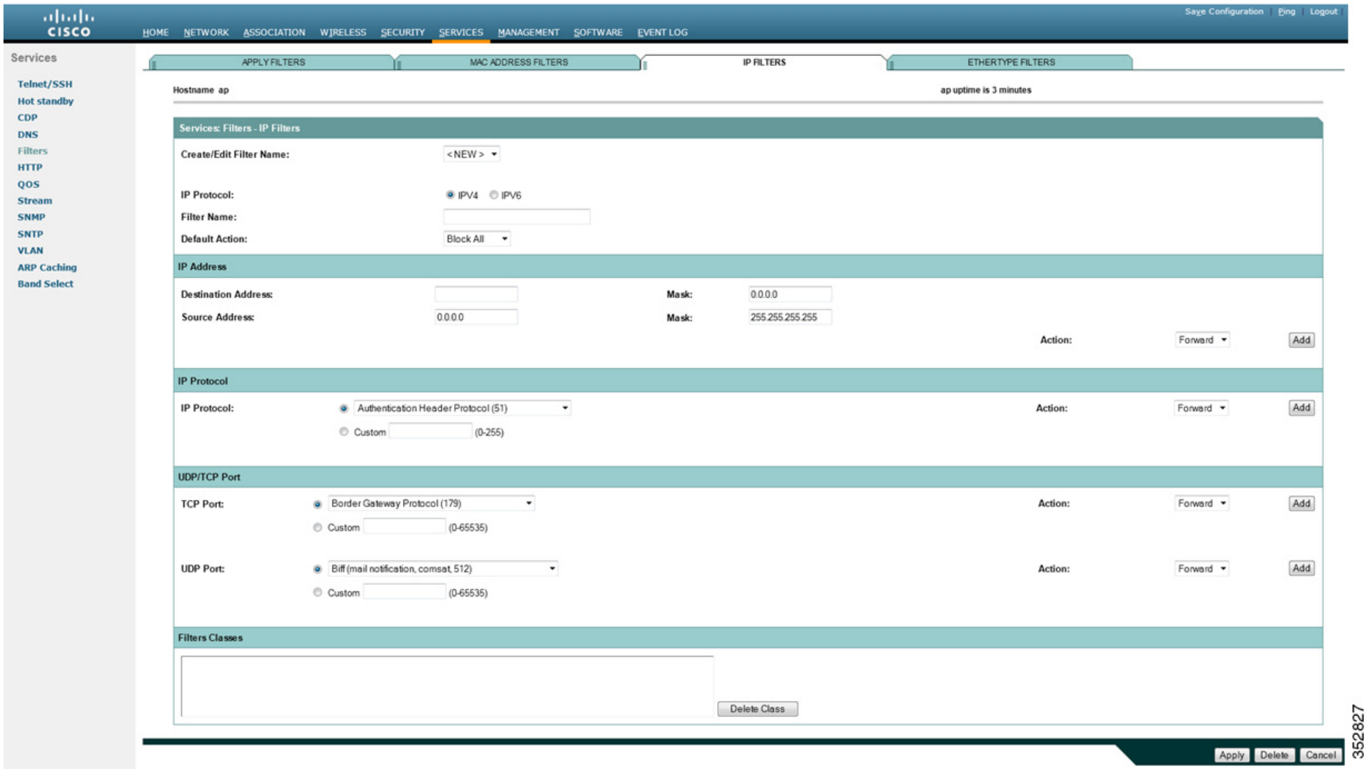
ACL logging is not supported on the bridging interfaces of AP platforms. When applied on bridging interface, it will work as if configured without “log” option and logging would not take effect. However, ACL logging will work well for the BVI interfaces as long as a separate ACL is used for the BVI interface.

Configuring and Enabling IP Filters

IP filters (IP address, IP protocol, and IP port) prevent or allow the use of specific protocols through the access point’s Ethernet and radio ports, and IP address filters allow or prevent the forwarding of unicast and multicast packets either sent from or addressed to specific IP addresses. You can create a filter that passes traffic to all addresses except those you specify, or you can create a filter that blocks traffic to all addresses except those you specify. You can create filters that contain elements of one, two, or all three IP filtering methods. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Use the IP Filters page to create IP filters for the access point. Figure 16-6 shows the IP Filters page.

Figure 16-6 IP Filters Page



Hostname ap

ap uptime is 3 minutes

Services: Filters - IP Filters

Create/Edit Filter Name: <NEW>

IP Protocol: ● IPV4 ○ IPV6

Filter Name:

Default Action: Block All

IP Address

Destination Address: Mask: 0.0.0.0

Source Address: 0.0.0.0 Mask: 255.255.255.255

Action: Forward

IP Protocol

IP Protocol: ● Authentication Header Protocol (51) Action: Forward

○ Custom (0-255)

UDP/TCP Port

TCP Port: ● Border Gateway Protocol (179) Action: Forward

○ Custom (0-65535)

UDP Port: ● Biff (mail notification, comsat, 512) Action: Forward

○ Custom (0-65535)

Filters Classes

Follow this link path to reach the IP Filters page:

1. Click **Services** in the page navigation bar.
2. In the Services page list, click **Filters**.
3. On the Apply Filters page, click the **IP Filters** tab at the top of the page.

Creating an IP Filter

Follow these steps to create an IP filter:

Step 1 Follow the link path to the IP Filters page.

Step 2 If you are creating a new filter, make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu. To edit an existing filter, select the filter name from the Create/Edit Filter Index menu.

Step 3 Enter a descriptive name for the new filter in the Filter Name field.

Step 4 Select **Forward all** or **Block all** as the filter's default action from the Default Action menu. The filter's default action must be the opposite of the action for at least one of the addresses in the filter. For example, if you create a filter containing an IP address, an IP protocol, and an IP port and you select **Block** as the action for all of them, you must choose **Forward All** as the filter's default action.

Step 5 To filter an IP address, enter an address in the IP Address field.

Note If you plan to block traffic to all IP addresses except those you specify as allowed, put the address of your own PC in the list of allowed addresses to avoid losing connectivity to the access point.

Step 6 Type the mask for the IP address in the Mask field. Enter the mask with periods separating the groups of characters (172.31.24.10, for example). If you enter 255.255.255.255 as the mask, the access point accepts any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address you entered in the IP Address field. The mask you enter in this field behaves the same way that a mask behaves when you enter it in the CLI.

Step 7 Select **Forward** or **Block** from the Action menu.

Step 8 Click **Add**. The address appears in the Filters Classes field. To remove the address from the Filters Classes list, select it and click **Delete Class**. Repeat Step 5 through Step 8 to add addresses to the filter.

If you do not need to add IP protocol or IP port elements to the filter, skip to Step 15 to save the filter on the access point.

Step 9 To filter an IP protocol, select one of the common protocols from the IP Protocol drop-down list, or select the **Custom** radio button and enter the number of an existing ACL in the Custom field. Enter an ACL number from 0 to 255. See Appendix A, "Protocol Filters," for a list of IP protocols and their numeric designators.

Step 10 Select **Forward** or **Block** from the Action menu.

Step 11 Click **Add**. The protocol appears in the Filters Classes field. To remove the protocol from the Filters Classes list, select it and click **Delete Class**. Repeat Step 9 to Step 11 to add protocols to the filter.

If you do not need to add IP port elements to the filter, skip to Step 15 to save the filter on the access point.

Step 12 To filter a TCP or UDP port protocol, select one of the common port protocols from the TCP Port or UDP Port drop-down lists, or select the **Custom** radio button and enter the number of an existing protocol in one of the Custom fields. Enter a protocol number from 0 to 65535. See Appendix A, "Protocol Filters," for a list of IP port protocols and their numeric designators.

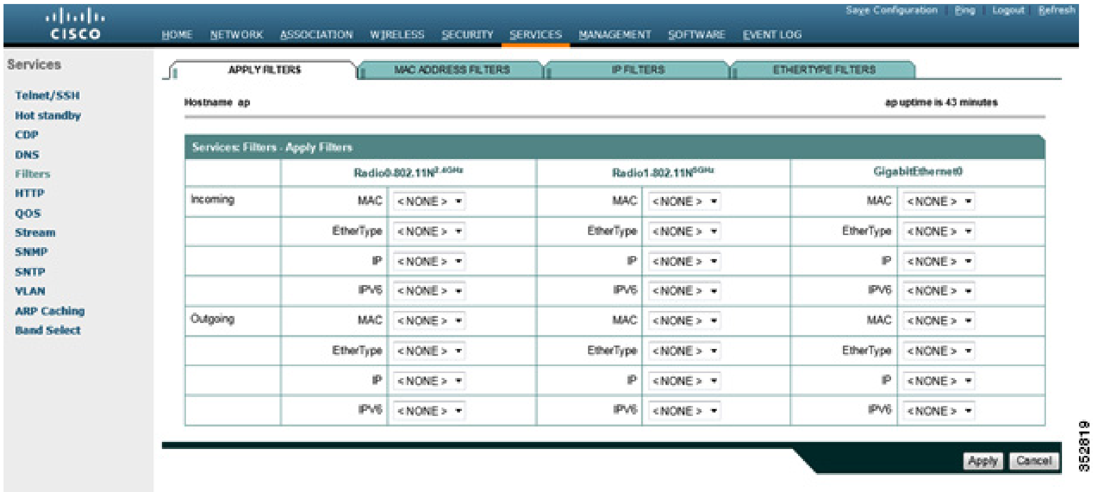
Step 13 Select **Forward** or **Block** from the Action menu.

Step 14 Click **Add**. The protocol appears in the Filters Classes field. To remove the protocol from the Filters Classes list, select it and click **Delete Class**. Repeat Step 12 to Step 14 to add protocols to the filter.

Step 15 When the filter is complete, click **Apply**. The filter is saved on the access point, but it is not enabled until you apply it on the Apply Filters page.

Step 16 Click the **Apply Filters** tab to return to the Apply Filters page. Figure 16-7 shows the Apply Filters page.

Figure 16-7 Apply Filters Page



Hostname ap

ap uptime is 43 minutes

Services: Filters - Apply Filters

	Radio0-802.11N$^{2.4GHz}$		Radio1-802.11N^{5GHz}		GigabitEthernet0	
Incoming	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >	IP	< NONE >
	IPV6	< NONE >	IPV6	< NONE >	IPV6	< NONE >
Outgoing	MAC	< NONE >	MAC	< NONE >	MAC	< NONE >
	EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE >
	IP	< NONE >	IP	< NONE >	IP	< NONE >
	IPV6	< NONE >	IPV6	< NONE >	IPV6	< NONE >

Step 17 Select the filter name from one of the IP drop-down lists. You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.

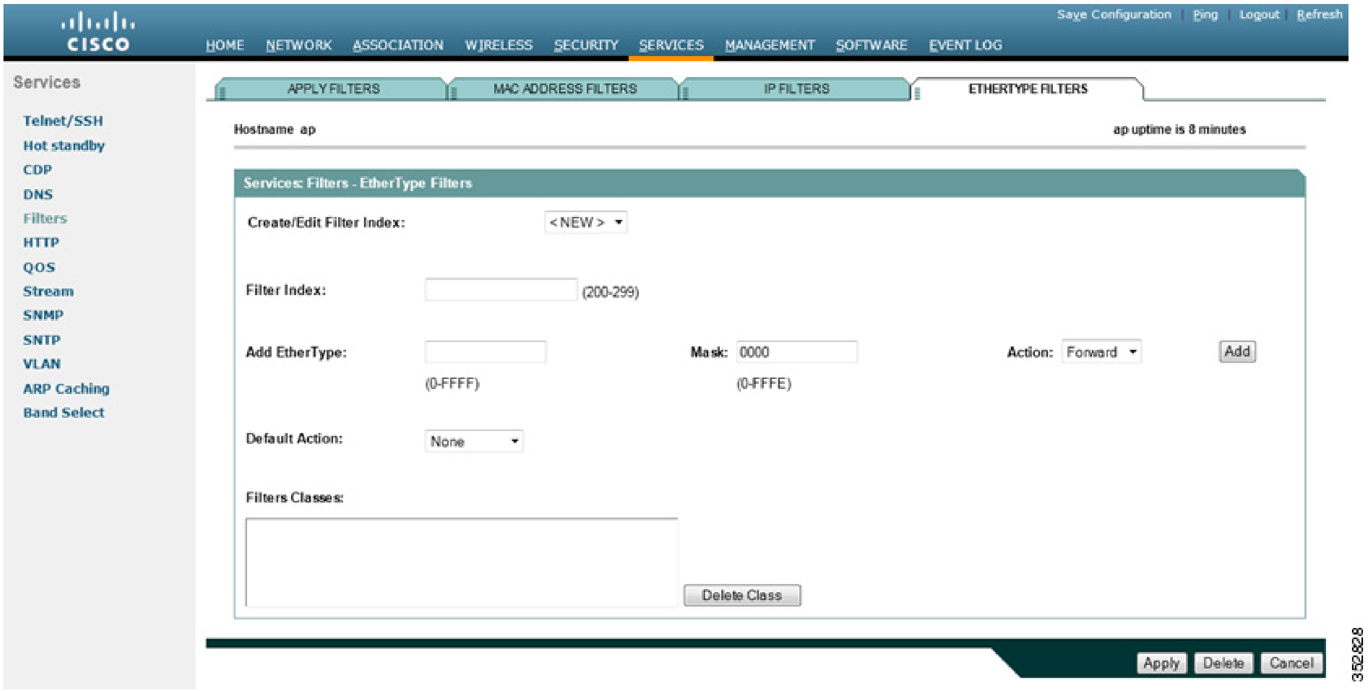
Step 18 Click **Apply**. The filter is enabled on the selected ports.

Configuring and Enabling EtherType Filters

EtherType filters prevent or allow the use of specific protocols through the access point's Ethernet and radio ports. You can apply the filters you create to either or both the Ethernet and radio ports and to either or both incoming and outgoing packets.

Use the EtherType Filters page to create EtherType filters for the access point. Figure 16-8 shows the EtherType Filters page.

Figure 16-8 EtherType Filters Page



Hostname ap

ap uptime is 8 minutes

Create/Edit Filter Index: < NEW >

Filter Index: (200-299)

Add EtherType: (0-FFFF)

Mask: 0000 (0-FFFE)

Action: Forward

Default Action: None

Filters Classes:

Follow this link path to reach the EtherType Filters page:

1. Click **Services** in the page navigation bar.
2. In the Services page list, click **Filters**.
3. On the Apply Filters page, click the **EtherType Filters** tab at the top of the page.

Creating an EtherType Filter

Follow these steps to create an EtherType filter:

Step 1 Follow the link path to the EtherType Filters page.

Step 2 If you are creating a new filter, make sure **<NEW>** (the default) is selected in the Create/Edit Filter Index menu. To edit an existing filter, select the filter number from the Create/Edit Filter Index menu.

Step 3 In the Filter Index field, name the filter with a number from 200 to 299. The number you assign creates an access control list (ACL) for the filter.

Step 4 Enter an EtherType number in the Add EtherType field. See Appendix A, "Protocol Filters," for a list of protocols and their numeric designators.

Step 5 Enter the mask for the EtherType in the Mask field. If you enter **0**, the mask requires an exact match of the EtherType.

Step 6 Select **Forward** or **Block** from the Action menu.

Step 7 Click **Add**. The EtherType appears in the Filters Classes field. To remove the EtherType from the Filters Classes list, select it and click **Delete Class**. Repeat Step 4 through Step 7 to add Ethertypes to the filter.

Step 8 Select **Forward All** or **Block All** from the Default Action menu. The filter's default action must be the opposite of the action for at least one of the Ethertypes in the filter. For example, if you enter several Ethertypes and you select **Block** as the action for all of them, you must choose **Forward All** as the filter's default action.

Step 9 Click **Apply**. The filter is saved on the access point, but it is not enabled until you apply it on the Apply Filters page.

Step 10 Click the **Apply Filters** tab to return to the Apply Filters page.

Step 11 Select the filter number from one of the EtherType drop-down lists. You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.

Step 12 Click **Apply**. The filter is enabled on the selected ports.

CHAPTER 17

Configuring CDP

This chapter describes how to configure Cisco Discovery Protocol (CDP) on your access point.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco Aironet IOS Command Reference for Access Points and Bridges* for this release and the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

Understanding CDP

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices. Information in CDP packets is used in network management software such as Cisco Prime Infrastructure2000.

CDP is used in network management to know about the neighbors of a given network device. CDP is enabled on the access point radio port only when the radio is associated to another wireless infrastructure device, such as an access point or a bridge. CDP is sent on the lowest VLAN number configured on the access point. When more than on VLAN is used in a wireless network, We recommend that the lowest VLAN number configured be used as the native VLAN

Note For best performance on your wireless LAN, disable CDP on all radio interfaces and on sub-interfaces if VLANs are enabled on the access point.

Configuring CDP

This section contains CDP configuration information and procedures:

- Default CDP Configuration, page 17-2
- Configuring the CDP Characteristics, page 17-2
- Disabling and Enabling CDP, page 17-3
- Disabling and Enabling CDP on an Interface, page 17-4

Default CDP Configuration

Table 17-1 lists the default CDP settings.

Table 17-1 Default CDP Configuration

Feature	Default Setting
CDP global state	Enabled
CDP interface state	Enabled
CDP holdtime (packet holdtime in seconds)	180
CDP timer (packets sent every x seconds)	60

Configuring the CDP Characteristics

You can configure the CDP holdtime (the number of seconds before the access point discards CDP packets) and the CDP timer (the number of seconds between each CDP packets the access point sends).

Beginning in Privileged Exec mode, follow these steps to configure the CDP holdtime and CDP timer.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cdp holdtime** *seconds*	(Optional) Specify the amount of time a receiving device should hold the information sent by your device before discarding it. The range is from 10 to 255 seconds; the default is 180 seconds.
Step 3	**cdp timer** *seconds*	(Optional) Set the transmission frequency of CDP updates in seconds. The range is from 5 to 254; the default is 60 seconds.
Step 4	**cdp advertise-v2**	(Optional) For CDP to send version-2 advertisements
Step 5	**cdp log mismatch duplex**	(Optional) Log the duplex-mismatches generated by CDP
Step 6	**cdp source-interface BVI1**	(Optional) Insert the BVI1 interface IP address in all CDP messages
Step 7	**end**	Return to Privileged Exec mode.

Use the **no** form of the CDP commands to return to the default settings.

This example shows how to configure and verify CDP characteristics:

```
AP# configure terminal
AP(config)# cdp holdtime 120
AP(config)# cdp timer 50
AP(config)# end

AP# show cdp

Global CDP information:
        Sending a holdtime value of 120 seconds
        Sending CDP packets every 50 seconds
```

For additional CDP **show** commands, see the "Monitoring and Maintaining CDP" section on page 17-5.

Disabling and Enabling CDP

CDP is enabled by default. Beginning in Privileged Exec mode, follow these steps to disable the CDP device discovery capability.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no cdp run**	Disable CDP.
Step 3	**end**	Return to Privileged Exec mode.

Beginning in privileged EXEC mode, follow these steps to enable CDP:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.

	Command	Purpose
Step 2	**cdp run**	Enable CDP after disabling it.
Step 3	**end**	Return to privileged EXEC mode.

This example shows how to enable CDP.

```
AP# configure terminal
AP(config)# cdp run
AP(config)# end
```

Disabling and Enabling CDP on an Interface

CDP is enabled by default on all supported interfaces to send and receive CDP information.

Beginning in privileged EXEC mode, follow these steps to disable CDP on an interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and enter the interface on which you are disabling CDP.
Step 3	**no cdp enable**	Disable CDP on an interface.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Beginning in privileged EXEC mode, follow these steps to enable CDP on an interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Enter interface configuration mode, and enter the interface on which you are enabling CDP.
Step 3	**cdp enable**	Enable CDP on an interface after disabling it.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to enable CDP on an interface.

```
AP# configure terminal
AP(config)# interface x
AP(config-if)# cdp enable
AP(config-if)# end
```

Monitoring and Maintaining CDP

To monitor and maintain CDP on your device, perform one or more of these tasks, beginning in privileged EXEC mode.

Command	Description
clear cdp counters	Reset the traffic counters to zero.
clear cdp table	Delete the CDP table of information about neighbors.
show cdp	Display global information, such as frequency of transmissions and the holdtime for packets being sent.
show cdp entry *entry-name* [**protocol** | **version**]	Display information about a specific neighbor. You can enter an asterisk (*) to display all CDP neighbors, or you can enter the name of the neighbor about which you want information. You can also limit the display to information about the protocols enabled on the specified neighbor or information about the version of software running on the device.
show cdp interface [*type number*]	Display information about interfaces where CDP is enabled. You can limit the display to the type of interface or the number of the interface about which you want information (for example, entering **gigabitethernet 0/1** displays information only about Gigabit Ethernet port 1).
show cdp neighbors [*type number*] [**detail**]	Display information about neighbors, including device type, interface type and number, holdtime settings, capabilities, platform, and port ID. You can limit the display to neighbors on a specific type or number of interface or expand the display to provide more detailed information.
show cdp traffic	Display CDP counters, including the number of packets sent and received and checksum errors.

Below are six examples of output from the CDP **show** privileged EXEC commands:

```
AP# show cdp
Global CDP information:
        Sending CDP packets every 50 seconds
        Sending a holdtime value of 120 seconds

AP# show cdp entry *
-------------------------
Device ID: AP
Entry address(es):
  IP address: 10.1.1.66
Platform: cisco WS-C3550-12T,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/2,  Port ID (outgoing port): GigabitEthernet0/2
Holdtime : 129 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I5Q3L2-M), Experimental Version 12.1(20010612:021
316) [jang-flamingo 120]
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 06-Jul-01 18:18 by jang

advertisement version: 2
```

```
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27, value=0000000
0FFFFFFFF010221FF000000000000000024B293A00FF0000
VTP Management Domain: ''
Duplex: full

-------------------------
Device ID: idf2-1-lab-l3.cisco.com
Entry address(es):
  IP address: 10.1.1.10
Platform: cisco WS-C3524-XL,  Capabilities: Trans-Bridge Switch
Interface: GigabitEthernet0/1,  Port ID (outgoing port): FastEthernet0/10
Holdtime : 141 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) C3500XL Software (C3500XL-C3H2S-M), Version 12.0(5.1)XP, MAINTENANCE IN
TERIM SOFTWARE
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Fri 10-Dec-99 11:16 by cchang

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=25, value=0000000
0FFFFFFFF010101FF000000000000000142EFA400FF
VTP Management Domain: ''

AP# show cdp entry * protocol
Protocol information for talSwitch14 :
  IP address: 172.20.135.194
Protocol information for tstswitch2 :
  IP address: 172.20.135.204
  IP address: 172.20.135.202
Protocol information for tstswitch2 :
  IP address: 172.20.135.204
  IP address: 172.20.135.202

AP# show cdp interface
GigabitEthernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/2 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/3 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/4 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/5 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/6 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/7 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

```
GigabitEthernet0/8 is up, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds

AP# show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device IDLocal InterfaceHoldtmeCapabilityPlatformPort ID
Perdido2Gig 0/6125R S IWS-C3550-1Gig0/6
Perdido2Gig 0/5125R S IWS-C3550-1Gig 0/5

AP# show cdp traffic
CDP counters :
        Total packets output: 50882, Input: 52510
        Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
        No memory: 0, Invalid packet: 0, Fragmented: 0
        CDP version 1 advertisements output: 0, Input: 0
        CDP version 2 advertisements output: 50882, Input: 52510
```

Enabling CDP Logging

You can enable CDP logging. To log errors related to duplex-mismatches identified through CDP, use the global configuration command **cdp log mismatch duplex**. To log errors related to duplex mismatches reported through CDP on a particular interface, use the same command at the interface level.

The following example enables logging for errors related to duplex-mismatches identified through CDP on the gigabit Ethernet interface, but disables logging for errors related to duplex-mismatches identified through CDP on the Radio 0 interface.

```
ap(config)# int gigabitEthernet 0
ap(config-if)# cdp log mismatch duplex
ap(config)# interface dot11Radio 0
ap(config-if)# no cdp log mismatch duplex
ap(config-if)# end
```

CHAPTER 18

Configuring SNMP

This chapter describes how to configure the Simple Network Management Protocol (SNMP) on your access point.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points* for this release.

Understanding SNMP

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. The SNMP manager can be part of a network management system (NMS) such as Cisco Prime Infrastructure. The agent and management information base (MIB) reside on the access point. To configure SNMP on the access point, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into the agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can mean improper user authentication, restarts, link status (up or down), MAC address tracking, closing of a TCP connection, loss of connection to a neighbor, or other significant events.

This section includes these concepts:

- SNMP Versions, page 18-2
- SNMP Manager Functions, page 18-3
- SNMP Agent Functions, page 18-4
- SNMP Community Strings, page 18-4
- Using SNMP to Access MIB Variables, page 18-4

SNMP Versions

This software release supports these SNMP versions:

- SNMPv1—The Simple Network Management Protocol, a full Internet standard, defined in RFC 1157.
- SNMPv2C, which has these features:
  - SNMPv2—Version 2 of the Simple Network Management Protocol, a draft Internet standard, defined in RFCs 1902 through 1907.
  - SNMPv2C—The Community-based Administrative Framework for SNMPv2, an experimental Internet protocol defined in RFC 1901.
- SNMPv3, which has these features:
  - Support for SHA and MD5 authentication protocols and DES56 encryption.
  - Three security levels: no authentication and no privacy (NoAuthNoPriv), authentication and no privacy (AuthNoPriv), and authentication and privacy (AuthPriv).

SNMPv3 supports the highest available levels of security for SNMP communication. Community strings for SNMPv1 and SNMPv2 are stored and transferred as plain text without encryption. In the SNMPv3 security model, SNMP users authenticate and join a user group. Access to system data is restricted based on the group.

You must configure the SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; therefore, you can configure the software to support communications with one management station using the SNMPv3 protocol and another using the SNMPv2 or SNMPv1 protocol.

Table 18-1 lists the SNMP versions and security levels supported on access points.

Table 18-1 SNMP Versions and Security Levels

SNMP Version	Security Level	Authentication	Encryption
v1	NoAuthNoPriv	Community string match	None
v2C	NoAuthNoPriv	Community string match	None
v3	NoAuthNoPriv	Username match	None
v3	AuthNoPriv	HMAC-MD5 or HMAC-SHA algorithms	None
v3	AuthPriv	HMAC-MD5 or HMAC-SHA algorithms	DES 56-bit encryption

SNMP Manager Functions

The SNMP manager uses information in the MIB to perform the operations described in Table 18-2.

Table 18-2 SNMP Operations

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves a value from a variable within a table.[1]
get-bulk-request[2]	Retrieves large blocks of data that would otherwise require the transmission of many small blocks of data, such as multiple rows in a table.
get-response	Replies to a get-request, get-next-request, and set-request sent by an NMS.
set-request	Stores a value in a specific variable.
trap	An unsolicited message sent by an SNMP agent to an SNMP manager when some event has occurred.

[1] With this operation, an SNMP manager does not need to know the exact variable name. A sequential search is performed to find the needed variable from within a table.

[2] The **get-bulk** command works only with SNMPv2.

SNMP Agent Functions

The SNMP agent responds to SNMP manager requests as follows:

- Get a MIB variable—The SNMP agent begins this function in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Set a MIB variable—The SNMP agent begins this function in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

The SNMP agent also sends unsolicited trap messages to notify an NMS that a significant event has occurred on the agent. Examples of trap conditions include, but are not limited to, when a port or module goes up or down, when spanning-tree topology changes occur, and when authentication failures occur.

SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. In order for the NMS to access the access point, the community string definitions on the NMS must match at least one of the three community string definitions on the access point.

Note SNMP communities are used with SNMPv1 and SNMPv2c. SNMPv3 does not use communities.

A community string can have one of these attributes:

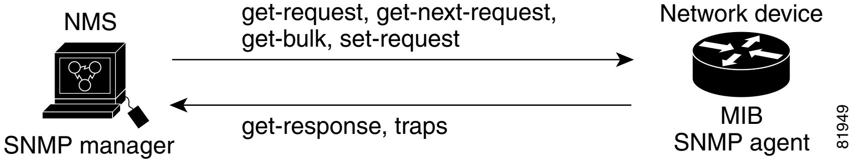
- Read-only—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access
- Read-write—Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings

Using SNMP to Access MIB Variables

An example of an NMS is the Cisco Prime Infrastructure network management software. Cisco Prime Infrastructure software uses the access point MIB variables to set device variables and to poll devices on the network for specific information. The results of a poll can be displayed and analyzed to troubleshoot internetworking problems, increase network performance, verify the configuration of devices, monitor traffic loads, and more.

As shown in Figure 18-1, the SNMP agent gathers data from the MIB. The agent can send traps (notification of certain events) to the SNMP manager, which receives and processes the traps. Traps are messages alerting the SNMP manager to a condition on the network such as improper user authentication, restarts, link status (up or down), MAC address tracking, and so forth. The SNMP agent also responds to MIB-related queries sent by the SNMP manager in *get-request*, *get-next-request*, and *set-request* format.

Figure 18-1 SNMP Network



For information on supported MIBs and how to access them, see Appendix B, "Supported MIBs."

Configuring SNMP

This section describes how to configure SNMP on your access point. It contains this configuration information:

- Default SNMP Configuration, page 18-5
- Enabling the SNMP Agent, page 18-6
- Configuring Community Strings, page 18-6
- Specifying SNMP-Server Group Names, page 18-8
- Configuring SNMP-Server Hosts, page 18-8
- Configuring SNMP-Server Users, page 18-8
- Configuring Trap Managers and Enabling Traps, page 18-8
- Setting the Agent Contact and Location Information, page 18-10
- Using the snmp-server view Command, page 18-11
- SNMP Examples, page 18-11

Default SNMP Configuration

Table 18-3 shows the default SNMP configuration.

Table 18-3 Default SNMP Configuration

Feature	Default Setting
SNMP agent	Disabled
SNMP community strings	No strings are configured by default. However, when you enable SNMP using the web-browser interface, the access point automatically creates the *public* community with read-only access to the IEEE802dot11 MIB.
SNMP trap receiver	None configured
SNMP traps	None enabled

Enabling the SNMP Agent

No specific CLI command exists to enable SNMP. The first **snmp-server** global configuration command that you enter enables the supported versions of SNMP.

You can also enable SNMP on the SNMP Properties page on the web-browser interface. When you enable SNMP on the web-browser interface, the access point automatically creates a community string called *public* with read-only access to the IEEE802dot11 MIB.

Configuring Community Strings

You use the SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the access point.

Optionally, you can specify one or more of these characteristics associated with the string:

- An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent
- A MIB view, which defines the subset of all MIB objects accessible to the given community
- Read and write or read-only permission for the MIB objects accessible to the community

Note In the current Cisco IOS MIB agent implementation, the default community string is for the Internet MIB object sub-tree. Because IEEE802dot11 is under another branch of the MIB object tree, you must enable either a separate community string and view on the IEEE802dot11 MIB or a common view and community string on the ISO object in the MIB object tree. ISO is the common parent node of IEEE (IEEE802dot11) and Internet. This MIB agent behavior is different from the MIB agent behavior on access points not running Cisco IOS software.

Beginning in privileged EXEC mode, follow these steps to configure a community string on the access point:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server community** *string* [*access-list-number*] [**view** *mib-view*] [**ro** | **rw**]	Configure the community string. • For *string*, specify a string that acts like a password and permits access to the SNMP protocol. You can configure one or more community strings of any length. • (Optional) For *access-list-number*, enter an IP standard access list numbered from 1 to 99 and 1300 to 1999. • (Optional) For **view** *mib-view*, specify a MIB view to which this community has access, such as **ieee802dot11**. See the "Using the snmp-server view Command" section on page 18-11 for instructions on using the **snmp-server view** command to access Standard IEEE 802.11 MIB objects through IEEE view. • (Optional) Specify either read-only (**ro**) if you want authorized management stations to retrieve MIB objects, or specify read/write (**rw**) if you want authorized management stations to retrieve and modify MIB objects. By default, the community string permits read-only access to all objects. **Note** To access the IEEE802dot11 MIB, you must enable either a separate community string and view on the IEEE802dot11 MIB or a common view and community string on the ISO object in the MIB object tree.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} *source* [*source-wildcard*]	(Optional) If you specified an IP standard access list number in Step 2, then create the list, repeating the command as many times as necessary. • For *access-list-number*, enter the access list number specified in Step 2. • The **deny** keyword denies access if the conditions are matched. The **permit** keyword permits access if the conditions are matched. • For *source*, enter the IP address of the SNMP managers that are permitted to use the community string to gain access to the agent. • (Optional) For *source-wildcard*, enter the wildcard bits in dotted decimal notation to be applied to the source. Place ones in the bit positions that you want to ignore. Recall that the access list is always terminated by an implicit deny statement for everything.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable access for an SNMP community, set the community string for that community to the null string (do not enter a value for the community string). To remove a specific community string, use the **no snmp-server community** *string* global configuration command.

This example shows how to assign the strings *open* and *ieee* to SNMP, to allow read-write access for both, and to specify that *open* is the community string for queries on all objects:

```
ap(config)# snmp-server community open rw
ap(config)# snmp-server community ieee view ieee802dot11 rw
```

Specifying SNMP-Server Group Names

To configure a new SNMP group, or a table that maps SNMP users to SNMP views, use the following command in global configuration mode:

Command	Purpose
snmp-server group [*groupname* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]}][**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]	Configures a new SNMP group, or a table that maps SNMP users to SNMP views.

Configuring SNMP-Server Hosts

To configure the recipient of an SNMP trap operation, use the following command in global configuration mode:

Command	Purpose
snmp-server host *host* [**traps** | **informs**][**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]	Configures the recipient of an SNMP trap operation.

Configuring SNMP-Server Users

To configure a new user to an SNMP group, use the following command in global configuration mode:

Command	Purpose
snmp-server user *username* [*groupname* **remote** *ip-address* [**udp-port** *port*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv des56** *priv password*]] [**access** *access-list*]	Configures a new user to an SNMP group.

Configuring Trap Managers and Enabling Traps

A trap manager is a management station that receives and processes traps. Traps are system alerts that the access point generates when certain events occur. By default, no trap manager is defined, and no traps are issued.

Access points running this Cisco IOS release can have an unlimited number of trap managers. Community strings can be any length.

Table 18-4 describes the supported access point traps (notification types). You can enable any or all of these traps and configure a trap manager to receive them.

Table 18-4 Notification Types

Notification Type	Description
aaa_server	Enable traps for AAA events
authenticate-fail	Enable traps for authentication failures.
config	Enable traps for SNMP configuration changes.
deauthenticate	Enable traps for client device deauthentications.
disassociate	Enable traps for client device disassociations.
dot11-qos	Enable traps for QoS changes.
entity	Enable traps for SNMP entity changes.
rogue-ap	Enable traps for rogue access point detections.
snmp	Enable traps for SNMP events.
switch-over	Enable traps for switch-overs.
syslog	Enable syslog traps.
wlan-wep	Enable WEP traps.
cef	Allows cef traps
config-copy	Allow SNMP config-copy traps
config-ctid	Allow SNMP config-ctid traps
cpu	Allow cpu related traps
dot11-mibs	Allow dot11 traps
entity	Allow SNMP entity traps
l2tun-pseudowire-status	Allow SNMP L2 pseudowire status traps
l2tun-session	Allow SNMP L2 session traps
syslog	Allow SNMP syslog traps
tty	Allow TCP connection traps
udp-port	The notification host's UDP port number
vrfmib	Allow SNMP vrfmib traps

Some notification types cannot be controlled with the **snmp-server enable** global configuration command, such as **udp-port**. These notification types are always enabled. You can use the **snmp-server host** global configuration command to a specific host to receive the notification types listed in Table 18-4.

Beginning in privileged EXEC mode, follow these steps to configure the access point to send traps to a host:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server host** *host-addr* {**traps** | **informs**} {**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}} *community-string* [**udp-port** *port*] *notification-type*	Specify the recipient of the trap message. • For *host-addr,* specify the name or address of the host (the targeted recipient). • Specify **traps** (the default) to send SNMP traps to the host. Specify **informs** to send SNMP informs to the host. • Specify the SNMP version to support. Version 1, the default, is not available with informs. Version 3 has three security levels: – **auth**—Specifies authentication of packets without encryption – **noauth**—Specifies no authentication and no encryption for packets – **priv**—Specifies authentication and encryption for packets • For *community-string,* specify the string to send with the notification operation. Though you can set this string using the **snmp-server host** command, We recommend that you define this string by using the **snmp-server community** command before using the **snmp-server host** command. • For *notification-type*, use the keywords listed in Table 18-4 on page 18-9.
Step 3	**snmp-server enable traps** *notification-types*	Enable the access point to send specific traps. For a list of traps, see Table 18-4 on page 18-9. To enable multiple types of traps, you must issue a separate **snmp-server enable traps** command for each trap type.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove the specified host from receiving traps, use the **no snmp-server host** *host* global configuration command. To disable a specific trap type, use the **no snmp-server enable traps** *notification-types* global configuration command.

Setting the Agent Contact and Location Information

Beginning in privileged EXEC mode, follow these steps to set the system contact and location of the SNMP agent so that these descriptions can be accessed through the configuration file:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**snmp-server contact** *text*	Set the system contact string. For example: `snmp-server contact Dial System Operator at beeper 21555.`
Step 3	**snmp-server location** *text*	Set the system location string. For example: `snmp-server location Building 3/Room 222`
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Using the snmp-server view Command

In global configuration mode, use the **snmp-server view** command to access Standard IEEE 802.11 MIB objects through IEEE view and the dot11 read-write community string.

This example shows how to enable IEEE view and dot11 read-write community string:

```
AP(config)# snmp-server view ieee ieee802dot11 included
AP(config)# snmp-server community dot11 view ieee RW
```

SNMP Examples

This example shows how to enable SNMPv1, SNMPv2C, and SNMPv3. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string *public*. This configuration does not cause the access point to send any traps.

```
AP(config)# snmp-server community public
```

This example shows how to assign the strings *open* and *ieee* to SNMP, to allow read-write access for both, and to specify that *open* is the community string for queries on non-IEEE802dot11-MIB objects and *ieee* is the community string for queries on IEEE802dot11-mib objects:

```
bridge(config)# snmp-server view dot11view ieee802dot11 included
bridge(config)# snmp-server community open rw
bridge(config)# snmp-server community ieee view ieee802dot11 rw
```

This example shows how to permit any SNMP manager to access all objects with read-only permission using the community string *public*. The access point also sends config traps to the hosts 192.180.1.111 and 192.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string *public* is sent with the traps.

```
AP(config)# snmp-server community public
AP(config)# snmp-server enable traps config
AP(config)# snmp-server host 192.180.1.27 version 2c public
AP(config)# snmp-server host 192.180.1.111 version 1 public
AP(config)# snmp-server host 192.180.1.33 public
```

This example shows how to allow read-only access for all objects to members of access list 4 that use the *comaccess* community string. No other SNMP managers have access to any objects. SNMP Authentication Failure traps are sent by SNMPv2C to the host *cisco.com* using the community string *public*.

```
AP(config)# snmp-server community comaccess ro 4
AP(config)# snmp-server enable traps snmp authentication
AP(config)# snmp-server host cisco.com version 2c public
```

This example shows how to send Entity MIB traps to the host *cisco.com*. The community string is restricted. The first line enables the access point to send Entity MIB traps in addition to any traps previously enabled. The second line specifies the destination of these traps and overwrites any previous **snmp-server host** commands for the host *cisco.com*.

```
AP(config)# snmp-server enable traps entity
AP(config)# snmp-server host cisco.com restricted entity
```

This example shows how to enable the access point to send all traps to the host *myhost.cisco.com* using the community string *public*:

```
AP(config)# snmp-server enable traps
AP(config)# snmp-server host myhost.cisco.com public
```

This example shows how to configure these SNMPv3 settings:

- a view name (*iso*)
- an SNMP engine ID (*1234567890*) that this agent uses to identify itself to the remote host at IP address *1.4.74.10*
- an SNMPv3 group (*admin*) which supports privacy encryption, and all users of the group have read and write access to all objects defined in the *iso* view
- an SNMP user (*joe*) that belongs to the admin group, uses MD5 authentication for queries, uses *xyz123* as a password for MD5, uses DES56 data query encryption, and uses *key007* as an encryption key
- an SNMP user (*fred*) that belongs to the admin group, uses MD5 authentication for queries, uses *abc789* as an encrypted password for MD5, uses DES56 data query encryption, and uses *key99* as an encryption key

```
AP(config)# snmp-server view iso iso included
AP(config)# snmp-server engineID remote 1.4.74.10 1234567890
AP(config)# snmp-server group admin v3 priv
AP(config)# snmp-server group admin v3 priv read iso write iso
AP(config)# snmp-server user joe admin v3 auth md5 xyz123 priv des56 key007
AP(config)# snmp-server user fred admin v3 encrypted auth md5 abc789 priv des56 key99
```

Note After you enter the last command in this example, the **show running-config** and **show startup-config** commands display only a partial SNMP configuration.

Displaying SNMP Status

To display SNMP input and output statistics, including the number of illegal community string entries, errors, and requested variables, use the **show snmp** privileged EXEC command. For information about the fields in this display, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

CHAPTER 19

Configuring Repeater and Standby Access Points and Workgroup Bridge Mode

This chapter describes how to configure your access point as a repeater, as a hot standby unit, or as a workgroup bridge.

Understanding Repeater Access Points

A repeater access point is not connected to the wired LAN; it is placed within radio range of an access point connected to the wired LAN to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. You can configure either the 2.4 GHz radio or the 5 GHz radio as a repeater. In access points with two radios, only one radio can be a repeater; the other radio must be shut down or be configured as a root, scanner, or spectrum radio.

The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client. When you configure an access point as a repeater, the access point's Ethernet port does not forward traffic.

You can set up a chain of several repeater access points, but throughput for client devices at the end of the repeater chain will be quite low. Because each repeater must receive and then re-transmit each packet on the same channel, throughput is cut in half for each repeater you add to the chain.

A repeater access point associates to the access point with which it has the best connectivity. However, you can specify the access point to which the repeater associates. Setting up a static, specific association between a repeater and a root access point improves repeater performance.

To set up repeaters, you must enable Aironet extensions on both the parent (root) access point and the repeater access points. Aironet extensions, which are enabled by default, improve the access point's ability to understand the capabilities of Cisco Aironet client devices associated with the access point. Disabling Aironet extensions sometimes improves the interoperability between the access point and non-Cisco client devices. Non-Cisco client devices might have difficulty communicating with repeater access points and the root access point to which repeaters are associated.

To use an SSID between an access point and a repeater, the **Infrastructure SSID** option has to be enabled on the SSID to allow AP to repeater communication.

The infrastructure SSID must be assigned to the native VLAN. If more than one VLAN is created on an access point or wireless bridge, an infrastructure SSID cannot be assigned to a non-native VLAN. The following message appears when the infrastructure SSID is configured on non-native VLAN:

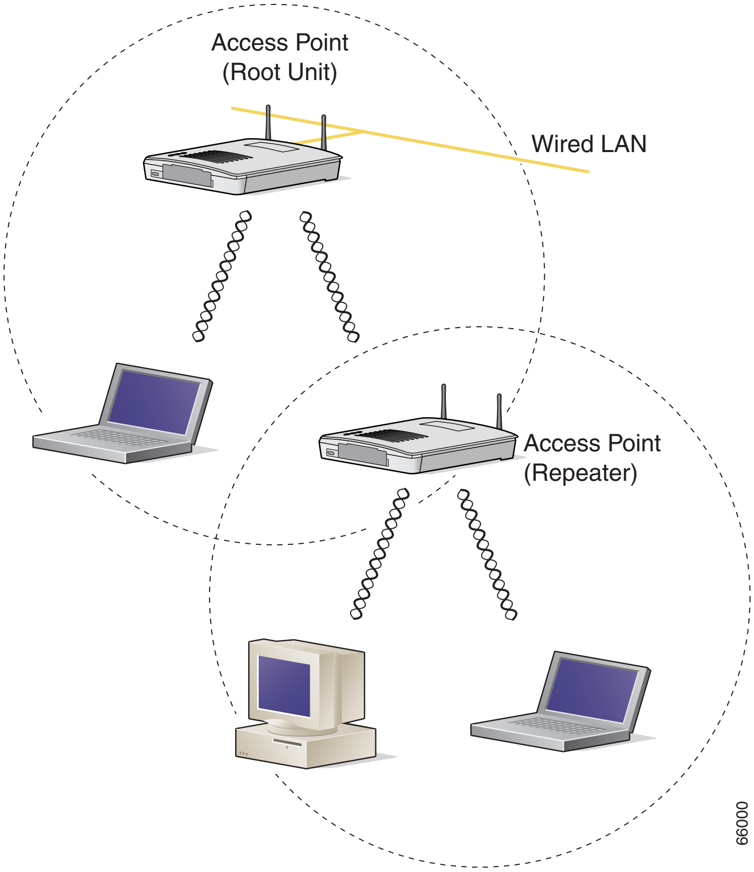
```
SSID [xxx] must be configured as native-vlan before enabling infrastructure-ssid
```

Note Access points create a virtual interface for each radio interface, and so repeater access points associate to the root access point twice: once for the actual interface and once for the virtual interface.

Note You cannot set a radio to act as a repeater and support other SSIDs at the same time. The repeater radio can only repeat the native VLAN. You cannot set a radio as a repeater, and then map to that radio an SSID that is mapped to a VLAN other than the native VLAN. However, the other radio can be configured to support several SSIDs and several VLANs.

Figure 19-1 shows an access point acting as a repeater.

Figure 19-1 Access Point as a Repeater



Configuring a Repeater Access Point

This section provides instructions for setting up an access point as a repeater and includes these sections:

- Default Configuration, page 19-4
- Guidelines for Repeaters, page 19-4
- Setting Up a Repeater, page 19-5
- Verifying Repeater Operation, page 19-7
- Aligning Antennas, page 19-6
- Setting Up a Repeater As a EAP-FAST Client, page 19-8
- Setting Up a Repeater As a WPA2 Client, page 19-7

Default Configuration

Access points are configured as root units by default. Table 19-1 shows the default values for settings that control the access point's role in the wireless LAN.

Table 19-1 Default Settings for Role in Wireless LAN

Feature	Default Setting
Station role	Root
Parent	none
Extensions	Aironet

Guidelines for Repeaters

Follow these guidelines when configuring repeater access points:

- Use repeaters to serve client devices that do not require high throughput. Repeaters extend the coverage area of your wireless LAN, but they drastically reduce throughput.
- Use repeaters when most if not all client devices that associate with the repeaters are Cisco Aironet clients. When non-Cisco clients are expected, verify that these clients support the Aironet IE extension, as this option is required on the SSID to allow for the communication between an AP and a repeater.
- Make sure that the data rates configured on the repeater access point match the data rates on the parent access point. For instructions on configuring data rates, see the "Configuring Radio Data Rates" section on page 6-9.
- The SSID configured on the repeater radio must be mapped to the native VLAN.

Note Repeater access points running Cisco IOS software cannot associate to parent access points that that do not run Cisco IOS software.

Note Repeater access points do not support wireless domain services (WDS). Do not configure a repeater access point as a WDS candidate, and do not configure a WDS access point to fall back to repeater mode in case of Ethernet failure. Repeaters can join a WDS infrastructure and act as WDS clients whenever needed.

Note If multiple BSSIDs are configured on a root access point that is designated as the parent of a repeater, the parent MAC address might change if a BSSID on the parent is added or deleted. If you use multiple BSSIDs on your wireless LAN and a repeater on your wireless LAN is configured to associate to a specific parent, check the association status of the repeater when you add or delete BSSIDs on the parent access point. If necessary, reconfigure the disassociated device to use the BSSID's new MAC address.

Setting Up a Repeater

Beginning in Privileged Exec mode, follow these steps to configure an access point as a repeater:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 3	**ssid** *ssid-string*	Call the SSID that the repeater uses to associate to a root access point; in the next step designate this SSID as an infrastructure SSID. If you created an infrastructure SSID on the root access point, create the same SSID on the repeater, also. Designate the SSID as an infrastructure SSID. The repeater uses this SSID to associate to the root access point. Infrastructure devices must associate to the repeater access point using this SSID unless you also enter the **optional** keyword. The infrastructure SSID must be assigned to the native VLAN. If more than one VLAN is created on an access point or wireless bridge, an infrastructure SSID cannot be assigned to a non-native VLAN. The following message appears when the infrastructure SSID is configured on non-native VLAN: `SSID [xxx] must be configured as native-vlan before enabling infrastructure-ssid`
Step 4	**station-role repeater**	Set the access point's role in the wireless LAN to repeater.
Step 5	**dot11 extension aironet**	If Aironet extensions are disabled, enable Aironet extensions.
Step 6	**parent** {*1-4*} *mac-address* [*timeout*]	(Optional) Enter the MAC address for the access point to which the repeater should associate. • You can enter MAC addresses for up to four parent access points, designated 1 to 4. The repeater always attempts to associate to the best access point from the list of its parent access points. The repeater does not associate with a MAC address that is not in its parent list unless you set the 'timeout' option. **Note** If multiple BSSIDs are configured on the parent access point, the MAC address for the parent might change if a BSSID on the parent is added or deleted. • (Optional) You can enter a timeout value in seconds, which determines how long the repeater attempts to associate to an access point that is in its parent list. If the repeater fails to associate within the timeout period, it will try to associate to parent access points that are not from its parent list. You can enter a timeout value ranging from 0 to 65535 seconds.

	Command	Purpose
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The following example shows how to set up a repeater access point with three potential parents, designated 1 to 3:

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid chicago
AP(config-if)# station-role repeater
AP(config-if)# dot11 extension aironet
AP(config-if)# parent 1 0987.1234.h345
AP(config-if)# parent 2 7809.b123.c345
AP(config-if)# parent 3 6543.a456.7421
AP(config-if)# end
```

This example shows how to remove a parent, here parent 2, from the parent list:

```
AP(config-if)# no parent 2
```

This example shows how to set a timeout of 60 seconds for the parent list:

```
AP(config-if)# parent timeout 60
```

This example shows how to disable the timeout value for the parent list:

```
AP(config-if)# no parent timeout
```

Aligning Antennas

When an access point is configured as a repeater, you can align its antenna with another remote antenna using the **dot11 antenna-alignment** CLI command.

The command invokes an alignment test. The radio disassociates from its parent, probes adjacent wireless devices, and records the MAC addresses and signal strengths of responses it receives. After the timeout, the radio reassociates with its parent.

Follow these steps to run an antenna alignment test:

	Command	Purpose
Step 1	**enable**	Enter privileged EXEC mod
Step 2	**dot11 dot11radio** { **0** | **1** } **antenna-alignment timeout** *timeout-in-seconds*	Enter interface configuration mode for the radio interface. • 0—For the 2.4-GHz radio and the 2.4-GHz 802.11n radio • 1—For the 5-GHz radio and the 5-GHz 802.11n radio. • *timeout-in-seconds*—Enter the time in seconds that the antenna alignment test runs before timing out. The default is 5 seconds.

Use the **show dot11 antenna-alignment** command to list the MAC addresses and signal level for the last 10 devices that responded to the probe.

Verifying Repeater Operation

After you set up the repeater, if your repeater is functioning correctly, the repeater access point should appear associated with the root access point in the root access point's Association Table.

Setting Up a Repeater As a WPA2 Client

WPA key management uses a combination of encryption methods to protect communication between client devices and the access point. You can set up a repeater access point to authenticate to your network like other WPA2-enabled client devices.

Beginning in Privileged Exec mode, follow these steps to set up the repeater as a WPA2 client:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ssid** *ssid-string*	Associate the SSID to the radio interface.
Step 3	**authentication open**	Enable open authentication for the SSID.
Step 4	**authentication key-management wpa**	Enable WPA authenticated key management for the SSID.
Step 5	**infrastructure ssid**	Designate the SSID as the SSID that the repeater uses to associate to other access points.
Step 6	**wpa-psk** { **hex** | **ascii** } [**0** | **7**] *encryption-key*	Enter a pre-shared key for the repeater. Enter the key using either hexadecimal or ASCII characters. If you use hexadecimal, you must enter 64 hexadecimal characters to complete the 256-bit key. If you use ASCII, you must enter from 8 to 63 ASCII characters, and the access point expands the key for you.
Step 7	**exit**	Exit the SSID configuration sub-mode.
Step 8	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 9	**encryption mode ciphers aes-ccm**	Enable AES CCMP encryption on the radio interface.
Step 10	**end**	Return to privileged EXEC mode.
Step 11	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Setting Up a Repeater As a EAP-FAST Client

You can set up a repeater access point to authenticate to your network like other wireless client devices. After you provide a network username and password for the repeater access point, it can authenticate to your network, through the root AP, using user credentials.

Setting up a repeater as a EAP-FAST, or other 802.1x/EAP authentication-method client requires three major steps:

1. Create an authentication username and password for the repeater on your authentication server.
2. Configure the authentication method to be supported on the root access point to which the repeater associates. The access point to which the repeater associates is called the parent access point. See Chapter 11, "Configuring Authentication Types," for instructions on setting up authentication.

   Note On the repeater access point, you must enable the same cipher suite or WEP encryption method and WEP features that are enabled on the parent access point.

3. Configure the repeater to act as a 802.1x/EAP client for the chosen method. The following example shows EAP-FAST configuration:

	Command	Purpose
Step 1	**eap profile** *profile-name*	Enter the name of a profile, that will be used by the repeater to determine which authentication method should be used.
Step 2	**method fast**	Configure EAP-FAST as the method to be used.
Step 3	**dot1x credentials** *name*	Configure user credentials that the repeater will use to authenticate to the wireless infrastructure.
Step 4	**username** *user-name*	Configure a username within the dot1x credentials.
Step 5	**password 0** *password*	Configure the password to use when the repeater will authenticate to the infrastructure.
Step 6	**exit**	Return to privileged EXEC mode.
Step 7	**dot11 ssid** *ssid-name*	Create a new SSID.
Step 8	**authentication open eap eap_methods**	Allow Open+ EAP authentication (EAP-FAST or other).
Step 9	**authentication network-eap eap_methods**	Allow LEAP authentication. LEAP is not the method of choice in this example, but LEAP is the default method. You need to enable LEP to trigger the 802.1x/EAP process. The EAP profile will determine which method should actually be used.
Step 10	**authentication key-management wpa version 2**	Set key management to WPA version 2.
Step 11	**dot1x credentials** *name*	Use the dot1x credentials created in for when the repeater authenticates to the wireless infrastructure. The credentials defined in the dot1x credentials profile will be used.
Step 12	**dot1x eap profile EAP-only**	Use the EAP-only profile created above for when the repeater authenticates to the wireless infrastructure. The method defined in the eap profile, EAP-FAST in this example, will be used

	Command	Purpose
Step 13	**infrastructure ssid** [**optional**]	(Optional) Designate the SSID as the SSID that other access points and workgroup bridges use to associate to this access point. If you do not designate an SSID as the infrastructure SSID, infrastructure devices can associate to the access point using any SSID. If you designate an SSID as the infrastructure SSID, infrastructure devices must associate to the access point using that SSID unless you also enter the **optional** keyword.
Step 14	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio and the 2.4-GHz 802.11n radio is 0. The 5-GHz radio and the 5-GHz 802.11n radio is 1.
Step 15	**ssid** *ssid-string*	Create an SSID and enter SSID configuration mode for the new SSID. The SSID can consist of up to 32 alphanumeric characters, but they should not include spaces. SSIDs are case-sensitive.
Step 16	**end**	Return to privileged EXEC mode.
Step 17	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Understanding Hot Standby

Hot Standby mode designates an access point as a backup for another access point. The standby access point is placed near the access point it monitors, configured exactly the same as the monitored access point. The standby access point associates with the monitored access point as a client and sends IAPP queries to the monitored access point through both the Ethernet and the radio ports. If the monitored access point fails to respond, the standby access point comes online and takes the monitored access point's place in the network.

Except for the IP address, the standby access point's settings should be identical to the settings on the monitored access point. If the monitored access point goes offline and the standby access point takes its place in the network, matching settings ensures that client devices can switch easily to the standby access point.

The standby access point monitors another access point in a device-to-device relationship, not in an interface-to-interface relationship. For example, you cannot configure the standby access point's 5-GHz radio to monitor the 5-GHz radio in access point alpha and the standby's 2.4-GHz radio to monitor the 2.4-GHz radio in access point bravo. You also cannot configure one radio in a dual-radio access point as a standby radio and configure the other radio to serve client devices.

Hot standby mode is disabled by default.

Note If the monitored access point malfunctions and the standby access point takes its place, repeat the hot standby setup on the standby access point when you repair or replace the monitored access point. The standby access point does not revert to standby mode automatically.

Note The MAC address of the monitored access point might change if a BSSID on the monitored unit is added or deleted. If you use multiple BSSIDs on your wireless LAN, check the status of the standby unit when you add or delete BSSIDs on the monitored access point. If necessary, reconfigure the standby unit to use the BSSID's new MAC address.

Note Hot standby is not supported on the BR1410 configured for AP mode.

Configuring a Hot Standby Access Point

When you set up the standby access point, you must enter radio mac address of the access point that the standby unit will monitor. To monitor access points with two radios, you need both radios MAC addresses. Record the MAC address of the monitored access point before you configure the standby access point.

The standby access point also must duplicate several key settings on the monitored access point. These settings are:

- Primary SSID (as well as additional SSIDs configured on the monitored access point)
- Default IP Subnet Mask
- Default Gateway
- Data rates
- Security settings
- Authentication types and authentication servers
- Radios configuration and status

Check the monitored access point and record these settings before you set up the standby access point.

Note Wireless client devices associated to the standby access point lose their connections during the hot standby setup process.

Tip To quickly duplicate the monitored access point's settings on the standby access point, save the monitored access point configuration and load it on the standby access point. See Chapter 20, "Working with Configuration Files," for instructions on uploading and downloading configuration files.

Beginning in Privileged Exec mode, follow these steps to enable hot standby mode on an access point:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**iapp standby** *mac-address*	Puts the access point into standby mode and specifies the MAC address of radio on the monitored access point. **Note** When you configure an access point with two radios to monitor an access point with two radios, you must enter the MAC addresses of both the monitored 2.4-GHz and 5-GHz radios. Enter the 2.4-GHz radio MAC address first, followed by the 5-GHz radio MAC address. **Note** The MAC address of the monitored access point might change if a BSSID on the monitored unit is added or deleted. If you use multiple BSSIDs on your wireless LAN, check the status of the standby unit when you add or delete BSSIDs on the monitored access point. If necessary, reconfigure the standby unit to use the BSSID's new MAC address. **Note** Hot standby is not supported on the BR1410 configured for AP mode.
Step 3	**iapp standby poll-frequency** *seconds*	Sets the number of seconds between queries that the standby access point sends to the monitored access point's radio and Ethernet ports. The default poll frequency is 2 seconds.
Step 4	**iapp standby timeout** *seconds*	Sets the number of seconds the standby access point waits for a response from the monitored access point before it assumes that the monitored access point has malfunctioned. The default timeout is 20 seconds. **Note** You should increase the standby timeout setting if the bridged path between the standby and monitored access points can be lost for periods greater than 20 seconds (during spanning tree recalculation, for example). **Note** If the monitored access point is configured to select the least congested radio channel, you might need to increase the standby timeout setting. The monitored unit might take up to 40 seconds to select the least congested channel.
Step 5	**iapp standby primary-shutdown**	(Optional) Configures the standby access point to send a Dumb Device Protocol (DDP) message to the monitored access point to disable the radios of the monitored access point when the standby unit becomes active. This feature prevents client devices that are associated to the monitored access point from remaining associated to the malfunctioning unit.

	Command	Purpose
Step 6	**show iapp standby-parms**	Verify your entries. If the access point is in standby mode, this command displays the standby parameters, including the MAC address of the monitored access point and the poll-frequency and timeout values. If the access point is not in standby mode, *no iapp standby mac-address* appears.
Step 7	**end**	Return to privileged EXEC mode.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

After you enable standby mode, configure the settings that you recorded from the monitored access point to match on the standby access point.

Verifying Standby Operation

Use this command to check the status of the standby access point:

show iapp standby-status

This command displays the status of the standby access point. Table 19-2 lists the standby status messages that can appear.

Table 19-2 Standby Status Messages

Message	Description
IAPP Standby is Disabled	The access point is not configured for standby mode.
IAPP—AP is in standby mode	The access point is in standby mode.
IAPP—AP is operating in active mode	The standby access point has taken over for the monitored access point and is functioning as a root access point.
IAPP—AP is operating in repeater mode	The standby access point has taken over for the monitored access point and is functioning as a repeater access point.
Standby status: Initializing	The standby access point is initializing link tests with the monitored access point.
Standby status: Takeover	The standby access point has transitioned to active mode.
Standby status: Stopped	Standby mode has been stopped by a configuration command.
Standby status: Ethernet Linktest Failed	An Ethernet link test failed from the standby access point to the monitored access point.
Standby status: Radio Linktest Failed	A radio link test failed from the standby access point to the monitored access point.
Standby status: Standby Error	An undefined error occurred.
Standby State: Init	The standby access point is initializing link tests with the monitored access point.
Standby State: Running	The standby access point is operating in standby mode and is running link tests to the monitored access point.
Standby State: Stopped	Standby mode has been stopped by a configuration command.
Standby State: Not Running	The access point is not in standby mode.

Use this command to check the standby configuration:

show iapp standby-parms

This command displays the MAC address of the standby access point, the standby timeout, and the poll-frequency values. If no standby access point is configured, this message appears:

```
no iapp standby mac-address
```

If a standby access point takes over for the monitored access point, you can use the **show iapp statistics** command to help determine the reason that the standby access point took over.

Understanding Workgroup Bridge Mode

You can configure access points as workgroup bridges, also termed as WGBs. In workgroup bridge (WGB) mode, the unit associates to another access point as a client and provides a network connection for the devices connected to its Ethernet port. For example, if you need to provide wireless connectivity for a group of network printers, you can connect the printers to a hub or to a switch, connect the hub or switch to the access point Ethernet port, and configure the access point as a workgroup bridge. The workgroup bridge associates to an access point on your network.

If your access point has two radios, either the 2.4-GHz radio or the 5-GHz radio can function in workgroup bridge mode. When you configure one radio interface as a workgroup bridge, the other radio remains up. However, both radios cannot be configured to operate simultaneously as a workgroup bridge. The other radio can either be disabled (shutdown), or be in root (access point or bridge), scanner, or spectrum mode.

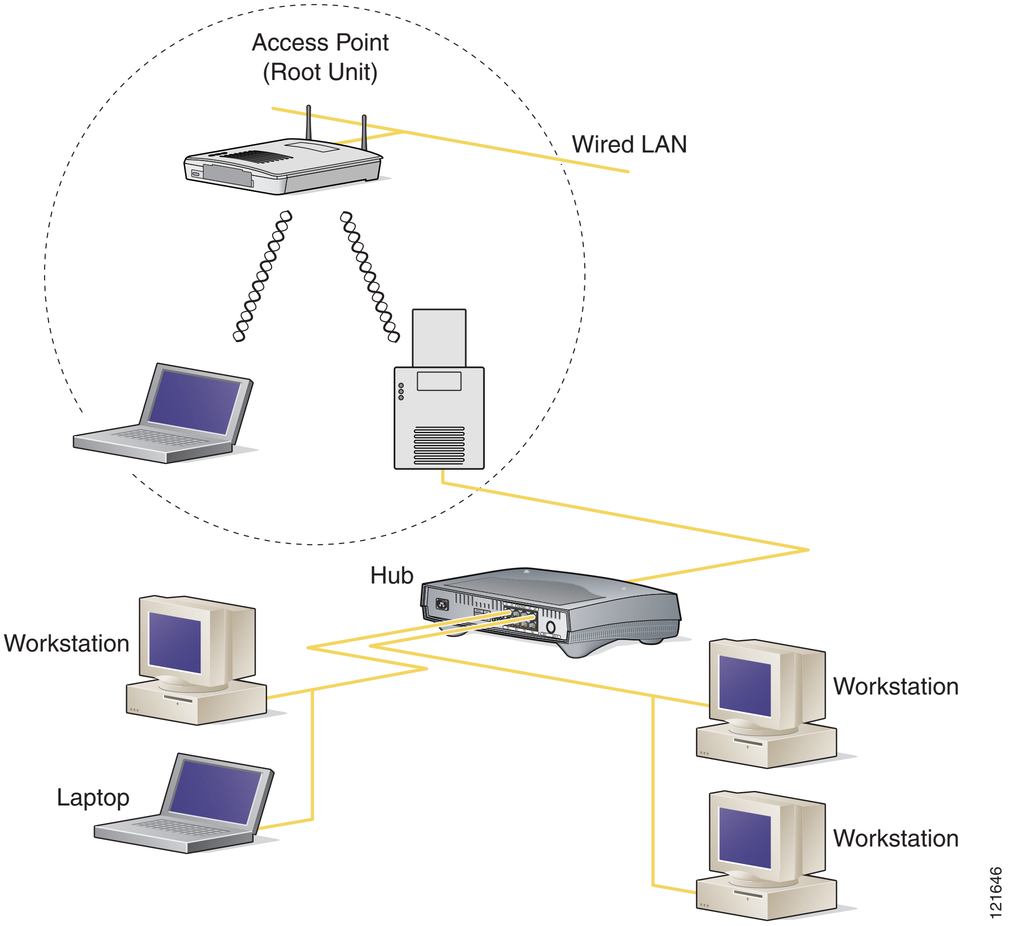
Caution An access point in workgroup bridge mode can introduce a bridge loop if you connect its Ethernet port to your wired LAN. To avoid a bridge loop on your network, disconnect the workgroup bridge from your wired LAN before or soon after you configure it as a workgroup bridge.

Note If multiple BSSIDs are configured on a root access point that is designated as the parent of a workgroup bridge, the parent MAC address might change if a BSSID on the parent is added or deleted. If you use multiple BSSIDs on your wireless LAN and a workgroup bridge on your wireless LAN is configured to associate to a specific parent, check the association status of the workgroup bridge when you add or delete BSSIDs on the parent access point. If necessary, reconfigure the workgroup bridge to use the BSSID’s new MAC address.

Note Although it functions as a bridge, an access point in workgroup bridge mode has a limited radio range. Workgroup bridges do not support the **distance** setting, which enables you to configure wireless bridges to communicate across several kilometers.

Figure 19-2 shows an access point in workgroup bridge mode.

Figure 19-2 Access Point in Workgroup Bridge Mode



Treating Workgroup Bridges as Infrastructure Devices or as Client Devices

The access point to which a workgroup bridge associates can treat the workgroup bridge as an infrastructure device or as a simple client device. By default, access points and bridges treat workgroup bridges as client devices.

For increased reliability, you can configure access points and bridges to treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. Treating a workgroup bridge as an infrastructure device means that the access point reliably delivers multicast packets, including Address Resolution Protocol (ARP) packets, to the workgroup bridge. You use the **infrastructure-client** configuration interface command to configure access points and bridges to treat workgroup bridges as infrastructure devices.

Configuring access points and bridges to treat a workgroup bridge as a client device allows more workgroup bridges to associate to the same access point, or to associate using an SSID that is not an infrastructure SSID. The performance cost of reliable multicast delivery—duplication of each multicast packet sent to each workgroup bridge—limits the number of infrastructure devices, including workgroup bridges, that can associate to an access point or bridge. To increase beyond 20 the number of workgroup bridges that can associate to the access point, the access point must reduce the delivery reliability of multicast packets to workgroup bridges. With reduced reliability, the access point cannot confirm whether multicast packets reach the intended workgroup bridge, so wired clients of workgroup bridges at the edge of the access point coverage area may not receive all multicast frames. When you treat workgroup bridges as client devices, you increase performance but reduce reliability. You use the **no infrastructure client** configuration interface command to configure access points and bridges to treat workgroup bridges as simple client devices. This is the default setting.

You should use a workgroup bridge as an infrastructure device if the devices connected to the workgroup bridge require network reliability equivalent to that of an access point or a bridge. You should use a workgroup bridge as a client device if these conditions are true:

- More than 20 workgroup bridges associate to the same access point or bridge
- The workgroup bridge associates using an SSID that is not an infrastructure SSID
- The workgroup bridge is mobile

Please notice that the **(no) infrastructure client** command is entered on the access point to which the workgroup bridge associates. This command determines whether the access point should add unicast copies of each multicast frames, sent in a reliable (unicast with acknowledgment) fashion to each workgroup bridge in the cell.

When infrastructure client is configured on the access point, each workgroup bridge potentially receives both the multicast initial frame and the unicast copy. Processing both frames (carrying the same upper layer content) creates processing inefficiency on the workgroup bridge. You can configure the workgroup bridge to consider the multicast frame and discard the unicast copy (default), or consider the unicast frame and discard the multicast original frame. To configure this behavior on the workgroup bridge radio, use the command **station-role workgroup-bridge multicast mode {client | infrastructure}**. The client option considers the multicast frame and discards the unicast copy. The infrastructure option echoes the Infrastructure Client configuration on the main access point, and sets the workgroup bridge to consider the unicast copies of multicast frames, and not process the multicast frames.

Configuring a Workgroup Bridge for Roaming

By default, workgroup bridges are expected to be static. Therefore, once they are associated to an access point SSID, they do not scan for other access points.

If your workgroup bridge is mobile, you can configure it to scan for a better radio connection to a parent access point or bridge. Use this command to configure the workgroup bridge as a mobile station:

```
ap(config)# mobile station
```

When you enable this setting, the workgroup bridge scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. Using these criteria, a workgroup bridge configured as a mobile station searches for a new parent association and roams to a new parent before it loses its current association. When the mobile station setting is disabled (the default setting) the workgroup bridge does not search for a new association until it loses its current association.

```
ap(config-if)#mobile station minimum-rate <data rate>
```

This is a configurable parameter to control when WGB triggers a new roaming event. If this cli is configured and if the current data rate is lower than the configured value, the new roaming process will be triggered. This will reduce unnecessary roaming and allows to have an expected rate value.

You can also configure the periodicity of scans. When the connection conditions deteriorate, the workgroup bridge scans for a better access point to connect to. If the scan does not allow the workgroup bridge to find a better connection point, use the **mobile station period** *number-of-seconds* command to determine the interval to the next scanning cycle.

Configuring a Workgroup Bridge for Limited Channel Scanning

In mobile environments such as railroads, a workgroup bridge instead of scanning all the channels will be restricted to scan only a set of limited channels in order to reduce the hand-off delay when the workgroup bridge roams from one access point to another. By limiting the number of channels the workgroup bridge scans to only those required, the mobile workgroup bridge achieves and maintains a continuous wireless LAN connection with fast and smooth roaming.

Configuring the Limited Channel Set

This limited channel set is configured using the **mobile station scan <set of channels>** CLI command to invoke scanning to all or specified channels. There is no limitation on the maximum number of channels that can be configured. The maximum number of channels that can be configured is restricted only by the number of channels a radio can support. When executed, the workgroup bridge only scans this limited channel set. This limited channel feature also affects the known channel list that the workgroup bridge receives from the access point to which it is currently associated. Channels are added to the known channel list only if they are also a part of the limited channel set.

The following example shows how the command is used. In the example, channels 1, 6, and 11 are specified to scan:

```
ap#
ap#confure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#int d0
ap(config-if)#ssid limited_scan
ap(config-if)#station-role workgroup-bridge
ap(config-if)#mobile station
ap(config-if)#mobile station scan 1 6 11
ap(config-if)#end
ap#
```

Use the **no mobile station scan** command to restore scanning to all the channels.

Ignoring the CCX Neighbor List

In addition, the workgroup bridge updates its known channel list using CCX reports such as the AP Adjacent report or Enhanced Neighbor List report. However, when a workgroup bridge is configured for limited channel scanning, it does not need to process the CCX reports to update its known channel list. Use the **mobile station ignore neighbor-list** command to disable processing of CCX neighbor list reports. This command is effective only if the workgroup bridge is configured for limited scanning channel scanning. The following example shows how this command is used

```
ap#
ap#confure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#int d0
ap(config-if)#mobile station ignore neighbor-list
ap(config-if)#end
```

Configuring a Client VLAN

If the devices connected to the workgroup bridge's Ethernet port should all be assigned to a particular VLAN, you can configure a VLAN for the connected devices. Enter this command on the workgroup bridge:

```
ap(config)# workgroup-bridge client-vlan vlan-id
```

All the devices connected to the workgroup bridge's Ethernet port are assigned to that VLAN.

Workgroup Bridge VLAN Tagging

The Workgroup-Bridge (WGB) VLAN tagging feature enables segregation of VLAN traffic based on the VLAN numbers for Unified WGB solution.

When this feature is enabled, the WGB removes the 802.1q header while sending the packet from a VLAN client to the wireless LAN controller (WLC). WGB gets the packet to a VLAN client without 802.1q header and WGB code has to be modified to add the 802.1q header while forwarding the frame to the switch behind WGB.

WGB updates the WLC with the wired-client VLAN information in the Internet Access Point Protocol (IAPP) Association message. WLC treats the WGB client as a VLAN-client and forwards the packet in the right VLAN interface based on the source-mac-address.

In the upstream direction, WGB removes the 802.1q header from the packet while sending to the WLC. In the downstream direction while forwarding the packet to the switch connecting the wired-client, the WLC sends the packet to WGB without the 802.1q tag and WGB adds a 4-byte 802.1q header based on the destination mac-address. (For detailed information on VLANs, refer to Chapter 14, "Configuring VLANs".)

Enter this command to enable WGB VLAN tagging:

```
WGB(config)#workgroup-bridge unified-vlan-client ?
        -replicate  Enable WGB broadcast to all vlans
        <cr>
```

Configuring Workgroup Bridge Mode

Beginning in privileged EXEC mode, follow these steps to configure an access point as a workgroup bridge:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** {**0** | **1**}	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	**station-role workgroup-bridge [universal** *mac-address***]**	Set the radio role to workgroup bridge. (Optional) When configured as a workgroup bridge, the access point sends specific messages to the primary access point to inform it about the MAC addresses of wired clients relayed through the workgroup bridge radio. When the primary access point is not a Cisco access point, these messages are not understood. To allow the workgroup bridge to successfully associate and communicate with a non-Cisco access point, you can use the **universal** optional argument. A restriction of this mode is that only one wired client is supported. When configuring this mode you need to configure the MAC address of the wired client, to which the traffic should be relayed through the workgroup bridge. Instead of sending the list of wired clients to the primary AP, the workgroup bridge will directly associate to the access point using the wired client's MAC address. If the wired client's MAC address is not found in the workgroup bridge's MAC address table, the workgroup bridge associates using its own MAC address. Then, when the wired client is connected and its MAC address appears in the workgroup bridge MAC address table, the WGB disassociates and then re-associates using the wired client's MAC address. This process supports non-Cisco access points that need a unique mapping between a wireless client and a MAC address.
Step 4	**station-role workgroup-bridge multicast mode {client | infrastructure}**	(Optional) When the primary access point is configured with the **infrastructure client** command, multicast frames are also sent to workgroup bridges via unicast. In such cases, the multicast frames relayed via unicast contain four MAC addresses in the header: Workgroup bridge unicast destination MAC address, Transmitting access point MAC address, Multicast destination MAC address, Original sender source MAC address). The original multicast frame header only contains three MAC addresses: Multicast destination MAC address, Transmitting access point MAC address, Original sender source MAC address. When using the **infrastructure client** command on the primary access point, use the station role workgroup-bridge multicast mode infrastructure to instruct the workgroup bridge to ignore the multicast frames and only process the relayed unicast copies of the multicast frames. Use the station role workgroup-bridge multicast mode client to instruct the workgroup bridge to only consider the standard frames, and ignore any relayed frame that would display four MAC addresses in the header. • client—Client-mode accepts only 3-MAC address header multicast packets • infrastructure—Infrastructure-mode accepts only 4-MAC address header multicast packets
Step 5	**ssid** *ssid-string*	Designates the SSID that the workgroup bridge should use to associate to a parent access point or a bridge.

	Command	Purpose
Step 6	**infrastructure-ssid**	Designate the SSID as an infrastructure SSID. **Note** The workgroup bridge must use an infrastructure SSID to associate to a root access point or bridge.
Step 7	**authentication client username** *username* **password** *password*	(Optional) If the parent access point is configured to require LEAP authentication, configure the username and password that the workgroup bridge uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the workgroup bridge on the authentication server.
Step 8	**exit**	Exit SSID configuration mode and return to radio interface configuration mode.
Step 9	**parent** {*1-4*} *mac-address* [*timeout*]	(Optional) Enter the MAC address for the access point to which the workgroup bridge should associate. • You can enter MAC addresses for up to four parent access points, designated 1 to 4. The workgroup bridge always attempts to associate to the best access point from the list of its parent access points. The workgroup bridge does not associate with a MAC address that is not in its parent list unless you set the 'timeout' option. **Note** If multiple BSSIDs are configured on the parent access point, the MAC address for the parent might change if a BSSID on the parent is added or deleted. • (Optional) You can enter a timeout value in seconds, which determines how long the workgroup bridge attempts to associate to an access point that is in its parent list. If the workgroup bridge fails to associate within the timeout period, it will try to associate to parent access points that are not from its parent list. You can enter a timeout value ranging from 0 to 65535 seconds.
Step 10	**mobile station**	(Optional) Configure the workgroup bridge as a mobile station. When you enable this setting, the workgroup bridge scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. When this setting is disabled (the default setting) the workgroup bridge does not search for a new association until it loses its current association.
Step 11	**mobile station period** *number-of-seconds*	(Optional) When the signal to the access point to which the workgroup bridge is associated, deteriorates, the workgroup bridge scans for an alternate access point. If this scan is unsuccessful (i.e. no access point with a better signal was found), the number of seconds entered here will be the interval to the next scan attempt.

	Command	Purpose
Step 12	**mobile station minimum-rate** *rate*	(Optional) When a workgroup bridge scans for an alternate access point, this command determines the minimum data rate that should be achievable to the new access point in order for the workgroup bridge to consider the alternate access point as a potential connection point.
Step 13	**mobile station scan**	(Optional) Restricts the list of channels that the workgroup bridge should scan in search of an alternate access point.
Step 14	**mobile station ignore neighbor-list**	(Optional) When the workgroup bridge is configured to restrict the list of scanned channels, this command instructs the workgroup bridge to ignore the CCX neighbor list messages that indicate potential neighboring access points and their channel.
Step 15	**exit**	Exit radio configuration mode and return to global configuration mode.
Step 16	**workgroup-bridge client-vlan** *vlan-id*	(Optional) Specify the VLAN to which the devices that are connected to the workgroup bridge's Ethernet port are assigned.
Step 17	**end**	Return to privileged EXEC mode.
Step 18	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure an access point as a workgroup bridge. In this example, the workgroup bridge uses the configured username and password to perform LEAP authentication, and the devices attached to its Ethernet port are assigned to VLAN 22:

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# station-role workgroup-bridge
AP(config-if)# ssid infra
AP(config-ssid)# infrastructure-ssid
AP(config-ssid)# authentication client username wgb1 password cisco123
AP(config-ssid)# exit
AP(config-if)# exit
AP(config)# workgroup-bridge client-vlan 22
AP(config)# end
```

This example shows how to set up a workgroup bridge with the parent access points, designated 1 and 2:

```
AP(config-if)# parent 1 0040.9631.81cf
AP(config-if)# parent 2 0040.9631.81da
```

This example shows how to remove a parent, here parent 2, from the parent list:

```
AP(config-if)# no parent 2
```

This example shows how to set a timeout of 60 seconds for the parent list:

```
AP(config-if)# parent timeout 60
```

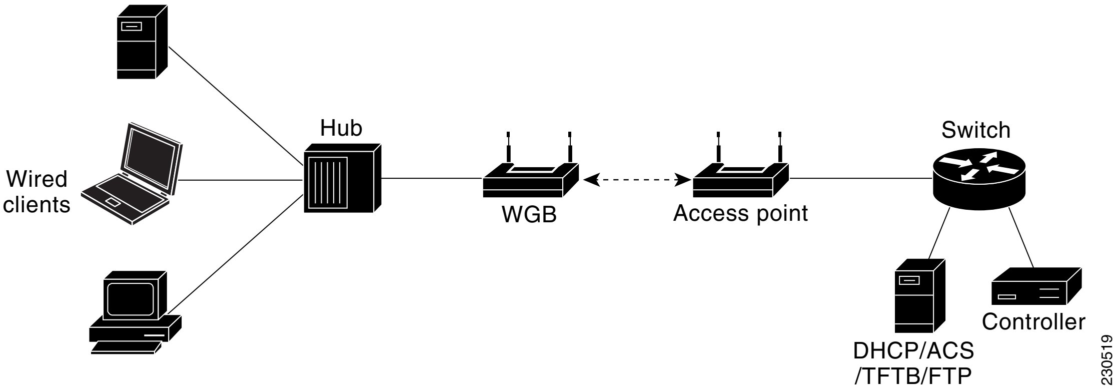
This example shows how to disable the timeout value for the parent list:

```
AP(config-if)# no parent timeout
```

Using Workgroup Bridges in a Lightweight Environment

You can configure an access point to operate as a workgroup bridge so that it can provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the workgroup bridge access point. A workgroup bridge connects to a wired network over a single wireless segment by learning the MAC address of its wired clients on the Ethernet interface and reporting them to the lightweight access point using Internet Access Point Protocol (IAPP) messaging. The workgroup bridge provides wireless access connectivity to wired clients by establishing a single connection to the lightweight access point. The lightweight access point treats the workgroup bridge as a wireless client.

Figure 19-3 Workgroup Bridge in a Lightweight Environment



Note If the lightweight access point fails, the workgroup bridge attempts to associate to another access point.

Guidelines for Using Workgroup Bridges in a Lightweight Environment

Follow these guidelines for using workgroup bridges on your lightweight network:

- The workgroup bridge can be any autonomous access point that supports the workgroup bridge mode and is running Cisco IOS Release JA or greater (on 32-MB access points) or Cisco IOS Release 12.3(8)JEB or greater (on 16-MB access points). These access points include the AP1040, AP1140, and AP1260. Cisco IOS Releases prior to 12.4(3g)JA and 12.3(8)JEB are not supported.

Note If your access point has two radios, you can configure only one for workgroup bridge mode. This radio is used to connect to the lightweight access point. We recommend that you disable the second radio.

Perform one of the following to enable the workgroup bridge mode on the workgroup bridge:

- On the workgroup bridge access point GUI, choose **Workgroup Bridge** for the role in radio network on the **Network > Network Interfaces > Radio0-802.11N 2.4GHz / Radio1-802.11N 5GHz > Settings** page.
  Alternatively, on the WGB access point CLI radio configuration submode, enter this command: **station-role workgroup-bridge**
- Only workgroup bridge in client mode (which is the default value) are supported. The lightweight access point will not relay multicast frames in a unicast fashion to associated workgroup bridges. Perform one of the following to enable client mode on the workgroup bridge:
  - On the radio configuration page, choose **Disabled** for the Reliable Multicast to workgroup bridge parameter.
  - From the radio configuration submode, enter this command: **no infrastructure client**.
- These lightweight features are supported for use with a workgroup bridge:
  - Guest N+1 redundancy
  - Local EAP
- These lightweight features are not supported for use with a workgroup bridge:
  - Cisco Centralized Key Management (CCKM)
  - Hybrid REAP
  - Idle timeout
  - Web authentication

Note If a workgroup bridge associates to a web-authentication WLAN, the workgroup bridge is added to the exclusion list, and all of the workgroup bridge wired clients are deleted.

- In a mesh network, a workgroup bridge can associate to any mesh access point, regardless of whether it acts as a root access point or a mesh access point.
- Wired clients connected to the workgroup bridge are not authenticated for security. Instead, the workgroup bridge is authenticated against the access point to which it associates. Therefore, We recommend that you physically secure the wired side of the workgroup bridge.
- With Layer 3 roaming, if you connect a wired client into the workgroup bridge network after the workgroup bridge has roamed to another controller (for example, to a foreign controller), the wired client’s IP address displays only on the anchor controller, not on the foreign controller.

- When you delete a workgroup bridge record from the controller, all of the workgroup bridge wired clients' records are also deleted.
- Wired clients connected to a workgroup bridge inherit the workgroup bridge's QoS and AAA override attributes.
- These features are not supported for wired clients connected to a workgroup bridge:
  - MAC filtering
  - Link tests
  - Idle timeout
- You do not need to configure anything on the controller to enable the workgroup bridge to communicate with the lightweight access point. However, to ensure proper communication, you should create a WLAN on the controller that matches the SSID and security method that was configured on the workgroup bridge.

Sample Workgroup Bridge Association Verification

To verify that the workgroup bridge is associated to an access point, enter this command on the workgroup bridge:

show dot11 association

If a wired client does not send traffic for an extended period of time, the workgroup bridge removes the client from its bridge table, even if traffic is continuously being sent to the wired client. As a result, the traffic flow to the wired client fails. To avoid the traffic loss, prevent the wired client from being removed from the bridge table by configuring the aging-out timer on the workgroup bridge to a large value using the following IOS commands on the workgroup bridge:

```
configure terminal
bridge bridge-group-number aging-time seconds
exit
end
```

where bridge-group-number is a value between 1 and 255, and seconds is a value between 10 and 1,000,000 seconds. We recommend configuring the seconds parameter to a value greater than the wired client's idle period.

Enabling VideoStream Support on Workgroup Bridges

VideoStream improves the reliability of an IP multicast stream by converting the multicast frame, over the air, to a unicast frame. Cisco IOS Releases 15.2(2)JA and later provide VideoStream support for wired devices connected to workgroup bridges. For access points running release 15.2(2)JA and later, the workgroup bridge is added to the wireless LAN controller (WLC) multicast table, and the workgroup bridge converts the VideoStream unicast frame into an Ethernet multicast frame and sends it out to its wired clients.

Enter this command on the WLC to enable VideoStream for workgroup bridges:

config media-stream wired-client enable

Configuring Workgroup Bridges for High-Speed Roaming

Consider the wireless network deployments which involve high-speed roaming of a workgroup bridge AP, such as in high-speed rail coaches. As the coaches move, the workgroup bridge AP in the coach roams from one parent AP (or root AP) to the next one mounted along the railway track. Such a scenario can involve trains moving at about 100 km/h, with the parent APs placed about 200-300m apart along the track.

For such scenarios ensure that the following configurations are done.

802.11v BSS Transition on the Wireless Controller

For high-speed roaming to work, on the wireless controller you must have 802.11v BSS Transition enabled. This allows for the workgroup bridge AP to request for and receive a neighbor list from the associated AP (i.e. the current parent AP). The workgroup bridge AP uses this list to identify the small set of channels on which it needs to scan to find the next parent AP.

Configuration on the WGB

To set how quickly a WGB detects that the current parent AP is suboptimal, while it is moving out of range, and that a roam needs to be initiated to discover the next parent AP, you can use the following command:
drssi roaming threshold *value* **period** *value* **packet** *value*

In this command:

- DRSSI roaming threshold is the RSSI threshold value. APs with RSSI values above this threshold are not considered for associating with.

  You are recommended to set the DRSSI roaming threshold to about 2 to 3 dBm below the average RSSI level in the middle point between two APs on the track. Note that a configured threshold of x, corresponding to -x dBm.
- Period controls how often the WGB decides to evaluate the quality of the link to the current parent. For example, if the train is moving very fast, you would like the WGB to evaluate the link quality more frequently. However if the speed is slow, the WGB can avoid frequent computations on evaluating the link quality.
- Packet is the threshold number of sample data packets from the current root AP that the WGB uses to keep track of the link quality with the AP. The WGB AP maintains a running average of the RSSI of the last received data packets from the root AP. If this running average falls below the threshold, the WGB initiates a roam. For example, if the train is moving very fast, a small number of samples can be used to decide when to switch.

As configured in the following example, a DRSSI roaming threshold value of 67, Period value of 1, and Packet value of 20 works well up to a speed of 100 km/h.

```
ap#confure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)#int d0
ap(config-if)#drssi roaming threshold 67 period 1 packet 20
ap(config-if)#end
```

You can also set the workgroup bridge to scan only the neighbor list that is received from the last associated AP, using the following command:
drssi scan-only current-neighbor-list

You can also disable this above command so that the workgroup bridge ages out the neighbors list gradually - the age out factor is reduced by 1 for every roam. Default age is 2. To disable, use the command **no drssi scan-only current-neighbor-list**.

Debug and Show commands

On the WGB, to view the current neighbor list table, use the following command:
show dot11 bss-trans neighbor-list

On the WGB, to enable debugging for 802.11v BSS transition:
debug dot11 dot11v {detail | errors | all}

CHAPTER 20

Managing Firmware and Configurations

This chapter describes how to manipulate the Flash file system, how to copy configuration files, and how to archive (upload and download) software images.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference for Access Points and Bridges* for this release and the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.4*.

Working with the Flash File System

The Flash file system on your access point provides several commands to help you manage software image and configuration files.

The Flash file system is a single Flash device on which you can store files. This Flash device is called *flash:*.

This section contains this information:

Displaying Available File Systems

To display the available file systems on your access point, use the **show file systems** privileged EXEC command as shown in this example:

```
ap# show file systems
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   arch:
*     31739904      16701952     flash     rw   flash:
      11999232       7754752     flash     rw   ram:
             -             -    opaque     rw   bs:
      31739904      16701952   unknown     rw   zflash:
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
         32768         26572     nvram     rw   nvram:
             -             -    opaque     rw   tmpsys:
             -             -   network     rw   tftp:
             -             -    opaque     rw   null:
             -             -    opaque     ro   xmodem:
             -             -    opaque     ro   ymodem:
             -             -   network     rw   rcp:
             -             -   network     rw   ftp:
             -             -   network     rw   http:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
```

Table 20-1 lists field descriptions for the **show file systems** command.

Table 20-1 show file systems Field Descriptions

Field	Value
Size(b)	Amount of memory in the file system in bytes.
Free(b)	Amount of free memory in the file system in bytes.
Type	Type of file system. **flash**—The file system is for a Flash memory device. **network**—The file system is for a network device. **nvram**—The file system is for a nonvolatile RAM (NVRAM) device. **opaque**—The file system is a locally generated *pseudo* file system (for example, the *system*) or a download interface, such as brimux. **unknown**—The file system is an unknown type.

Table 20-1 show file systems Field Descriptions (continued)

Field	Value
Flags	Permission for file system. **ro**—read-only. **rw**—read/write. **wo**—write-only.
Prefixes	Alias for file system. **arch:** **ram:** **bs:** **archive:** **tmpsys:** **xmoem:** **ymodem:** **scp:** **tar:** **https:** **flash:**—Flash file system. **ftp:**—File Transfer Protocol network server. Used to transfer files to or from the network device. **nvram:**—Non-volatile RAM memory (NVRAM). **null:**—Null destination for copies. You can copy a remote file to null to determine its size. **rcp:**—Remote Copy Protocol (RCP) network server. **system:**—Contains the system memory, including the running configuration. **tftp:**—Trivial File Transfer Protocol (TFTP) network server. **zflash:**—Read-only file decompression file system, which mirrors the contents of the Flash file system.

Setting the Default File System

You can specify the file system or directory that the system uses as the default file system by using the **cd** *filesystem:* privileged EXEC command. You can set the default file system to omit the *filesystem:* argument from related commands. For example, for all privileged EXEC commands that have the optional *filesystem:* argument, the system uses the file system specified by the **cd** command.

By default, the default file system is *flash:*.

You can display the current default file system as specified by the **cd** command by using the **pwd** privileged EXEC command.

Displaying Information About Files on a File System

You can view a list of the contents of a file system before manipulating its contents. For example, before copying a new configuration file to Flash memory, you might want to verify that the file system does not already contain a configuration file with the same name. Similarly, before copying a Flash configuration file to another location, you might want to verify its filename for use in another command.

To display information about files on a file system, use one of the privileged EXEC commands in Table 20-2.

Table 20-2 Commands for Displaying Information About Files

Command	Description
dir [**/all**] [*filesystem*:][*filename*]	Display a list of files on a file system.
show file systems	Display more information about each of the files on a file system.
show file information *file-url*	Display information about a specific file.
show file descriptors	Display a list of open file descriptors. File descriptors are the internal representations of open files. You can use this command to see if another user has a file open.

Changing Directories and Displaying the Working Directory

Beginning in privileged EXEC mode, follow these steps to change directories and display the working directory.

	Command	Purpose
Step 1	**dir** *filesystem*:	Display the directories on the specified file system. For *filesystem*:, use **flash:** for the system board Flash device.
Step 2	**cd** *directory_name*	Change to the directory of interest.
Step 3	**pwd**	Display the working directory.

Creating and Removing Directories

Beginning in privileged EXEC mode, follow these steps to create and remove a directory:

	Command	Purpose
Step 1	**dir** *filesystem*:	Display the directories on the specified file system. For *filesystem*:, use **flash:** for the system board Flash device.
Step 2	**mkdir** *directory_name*	Create a new directory. Directory names are case sensitive. Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.
Step 3	**dir** *filesystem*:	Verify your entry.

To delete a directory with all its files and subdirectories, use the **delete /force /recursive** *filesystem***:/***file-url* privileged EXEC command.

Use the **/recursive** keyword to delete the named directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the **/force** and **/recursive** keywords for deleting old software images that were installed by using the **archive download-sw** command but are no longer needed.

For *filesystem*, use **flash:** for the system board Flash device. For *file-url*, enter the name of the directory to be deleted. All the files in the directory and the directory are removed.

Caution When files and directories are deleted, their contents cannot be recovered.

Copying Files

To copy a file from a source to a destination, use the **copy** [**/erase**] *source-url destination-url* privileged EXEC command. For the source and destination URLs, you can use **running-config** and **startup-config** keyword shortcuts. For example, the **copy running-config startup-config** command saves the currently running configuration file to the NVRAM section of Flash memory to be used as the configuration during system initialization.

Note When adding the optional argument **/erase** to the copy command, the destination is overwritten. If a file with the same name exists at the destination, it is replaced with the new file that is being copied.

Network file system URLs include **ftp:**, **rcp:**, and **tftp:** and have the following syntax:

- File Transfer Protocol (FTP)—**ftp:**[[**//***username* [**:***password*]**@***location*]**/***directory*]**/***filename*
- Remote Copy Protocol (RCP)—**rcp:**[[**//***username***@***location*]**/***directory*]**/***filename*
- Trivial File Transfer Protocol (TFTP)—**tftp:**[[**//***location*]**/***directory*]**/***filename*

Local writable file systems include flash:.

Some invalid combinations of source and destination exist. Specifically, you cannot copy these combinations:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

For specific examples of using the **copy** command with configuration files, see the "Working with Configuration Files" section on page 20-9.

To copy software images either by downloading a new version or uploading the existing one, use the **archive download-sw** or the **archive upload-sw** privileged EXEC command. For more information, see the "Working with Software Images" section on page 20-20.

Deleting Files

When you no longer need a file on a Flash memory device, you can permanently delete it. To delete a file or directory from a specified Flash device, use the **delete** [**/force**] [**/recursive**] [*filesystem***:**]**/***file-url* privileged EXEC command.

Caution When files are deleted, their contents cannot be recovered.

Use the **/recursive** keyword for deleting a directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the **/force** and **/recursive** keywords for deleting old software images that were installed by using the **archive download-sw** command but are no longer needed.

If you omit the *filesystem***:** option, the access point uses the default device specified by the **cd** command. For *file-url*, you specify the path (directory) and the name of the file to be deleted.

This example shows how to delete the file *myconfig* from the default Flash memory device:

```
ap# delete myconfig
```

Creating, Displaying, and Extracting tar Files

You can create a tar file and write files into it, list the files in a tar file, and extract the files from a tar file as described in the next sections.

Creating a tar File

To create a tar file and write files into it, use this privileged EXEC command:

archive tar /create *destination-url* **flash:/***file-url*

For *destination-url*, specify the destination URL alias for the local or network file system and the name of the tar file to create. These options are supported:

- For the local Flash file system, the syntax is
  flash:/*file-url*
- For the File Transfer Protocol (FTP), the syntax is
  ftp:[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Remote Copy Protocol (RCP), the syntax is
  rcp:[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Trivial File Transfer Protocol (TFTP), the syntax is
  tftp:[[**//***location*]**/***directory*]**/***tar-filename***.tar**

The *tar-filename***.tar** is the tar file to be created.

For **flash:/***file-url*, specify the location on the local Flash file system from which the new tar file is created. You can also specify an optional list of files or directories within the source directory to write to the new tar file. If none are specified, all files and directories at this level are written to the newly created tar file.

This example shows how to create a tar file. This command writes the contents of the *new-configs* directory on the local Flash device to a file named *saved.tar* on the TFTP server at 172.20.10.30:

```
ap# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

Displaying the Contents of a tar File

To display the contents of a tar file on the screen, use this privileged EXEC command:

archive tar /table *source-url*

For *source-url*, specify the source URL alias for the local or network file system. These options are supported:

- For the local Flash file system, the syntax is **flash:**
- For the File Transfer Protocol (FTP), the syntax is **ftp:**[[**//***username*[**:***password*]@*location*]**/***directory*]**/***tar-filename***.tar**
- For the Remote Copy Protocol (RCP), the syntax is **rcp:**[[**//***username*@*location*]**/***directory*]**/***tar-filename***.tar**
- For the Trivial File Transfer Protocol (TFTP), the syntax is **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar**

The *tar-filename***.tar** is the tar file to display.

You can also limit the display of the files by specifying an optional list of files or directories after the tar file; then only these files are displayed. If none are specified, all files and directories are displayed.

This example shows how to display the contents of a *ap3g2-k9w7-tar.152-4.JB5.tar* file that is in Flash memory:

```
ap# archive tar /table flash:c1200-k9w7-mx.122-8.JA.tar
ap# archive tar /table flash:ap3g2-k9w7-tar.152-4.JB5.tar
info (286 bytes)
ap3g2-k9w7-mx.152-4.JB5/ (directory)
ap3g2-k9w7-mx.152-4.JB5/ap3g2-k9w7-mx.152-4.JB5 (208427 bytes)
ap3g2-k9w7-mx.152-4.JB5/ap3g2-k9w7-tx.152-4.JB5 (73 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/appsui.js (563 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/back.shtml (512 bytes)
.../...
```

This example shows how to display a *ap3g2-k9w7-mx.152-4.JB5/html/* directory and its contents:

```
ap# archive tar /table flash:/ap3g2-k9w7-tar.152-4.JB5.tar ap3g2-k9w7-mx.152-4.JB5/html
ap3g2-k9w7-mx.152-4.JB5/html/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/appsui.js (563 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/back.shtml (512 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/cookies.js (5032 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/forms.js (20125 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/sitewide.js (17089 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/stylesheet.css (3220 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/config.js (26330 bytes)
```

Extracting a tar File

To extract a tar file into a directory on the Flash file system, use this privileged EXEC command:

archive tar /xtract *source-url* **flash:/***file-url*

For *source-url*, specify the source URL alias for the local or network file system. These options are supported:

- For the local Flash file system, the syntax is
  flash:
- For the File Transfer Protocol (FTP), the syntax is
  ftp:[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Remote Copy Protocol (RCP), the syntax is
  rcp:[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar**
- For the Trivial File Transfer Protocol (TFTP), the syntax is
  tftp:[[**//***location*]**/***directory*]**/***tar-filename***.tar**

The *tar-filename***.tar** is the tar file from which to extract files.

For **flash:/***file-url*, specify the location on the local Flash file system into which the tar file is extracted. You can also specify an optional list of files or directories within the tar file for extraction. If none are specified, all files and directories are extracted.

This example shows how to extract the contents of a tar file located on the TFTP server at 172.20.10.30. This command extracts just the *new-configs* directory into the root directory on the local Flash file system. The remaining files in the *saved.tar* file are ignored.

```
ap# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

Displaying the Contents of a File

To display the contents of any readable file, including a file on a remote file system, use the **more** [**/ascii** | **/binary** | **/ebcdic**] *file-url* privileged EXEC command:

This example shows how to display the contents of a configuration file on a TFTP server:

```
ap# more tftp://serverA/hampton/savedconfig
!
! Saved configuration on server
!
version 11.3
service timestamps log datetime localtime
service linenumber
service udp-small-servers
service pt-vty-logging
!

<output truncated>
```

Working with Configuration Files

This section describes how to create, load, and maintain configuration files. Configuration files contain commands entered to customize the function of the Cisco IOS software. To better benefit from these instructions, your access point contains a minimal default running configuration for interacting with the system software.

You can copy (*download*) configuration files from a TFTP, FTP, or RCP server to the running configuration of the access point for various reasons:

- To restore a backed-up configuration file.
- To use the configuration file for another access point. For example, you might add another access point to your network and want it to have a configuration similar to the original access point. By copying the file to the new access point, you can change the relevant parts rather than recreating the whole file.
- To load the same configuration commands on all the access points in your network so that all the access points have similar configurations.

You can copy (*upload*) configuration files from the access point to a file server by using TFTP, FTP, or RCP. You might perform this task to back up a current configuration file to a server before changing its contents so that you can later restore the original configuration file from the server.

The protocol you use depends on which type of server you are using. The FTP and RCP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP and RCP are built on and use the Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which is connection oriented.

This section includes this information:

Guidelines for Creating and Using Configuration Files

Creating configuration files can aid in your access point configuration. Configuration files can contain some or all of the commands needed to configure one or more access points. For example, you might want to download the same configuration file to several access points that have the same hardware configuration.

Use these guidelines when creating a configuration file:

- If no passwords have been set on the access point, you must set them on each access point by entering the **enable secret** *secret-password* global configuration command. Enter a blank line for this command. The password is saved in the configuration file as clear text.

- If passwords already exist, you cannot enter the **enable secret** *secret-password* global configuration command in the file because the password verification will fail. If you enter a password in the configuration file, the access point mistakenly attempts to execute the passwords as commands as it executes the file.
- The **copy** {**ftp: | rcp: | tftp:**} **system:running-config** privileged EXEC command loads the configuration files on the access point as if you were entering the commands at the command line. The access point does not erase the existing running configuration before adding the commands. If a command in the copied configuration file replaces a command in the existing configuration file, the existing command is erased. For example, if the copied configuration file contains a different IP address in a particular command than the existing configuration, the IP address in the copied configuration is used. However, some commands in the existing configuration might not be replaced or negated. In this case, the resulting configuration file is a mixture of the existing configuration file and the copied configuration file, with the copied configuration file having precedence.

  To restore a configuration file to an exact copy of a file stored on a server, copy the configuration file directly to the startup configuration (by using the **copy** {**ftp: | rcp: | tftp:**} **nvram:startup-config** privileged EXEC command), and reload the access point.

Configuration File Types and Location

Startup configuration files are used during system startup to configure the software. Running configuration files contain the current configuration of the software. The two configuration files can be different. For example, you might want to change the configuration for a short time period rather than permanently. In this case, you would change the running configuration but not save the configuration by using the **copy running-config startup-config** privileged EXEC command.

The running configuration is saved in DRAM; the startup configuration is stored in the NVRAM section of Flash memory.

Creating a Configuration File by Using a Text Editor

When creating a configuration file, you must list commands logically so that the system can respond appropriately. This is one method of creating a configuration file:

Step 1 Copy an existing configuration from an access point to a server.

For more information, see the "Downloading the Configuration File by Using TFTP" section on page 20-11, the "Downloading a Configuration File by Using FTP" section on page 20-13, or the "Downloading a Configuration File by Using RCP" section on page 20-16.

Step 2 Open the configuration file in a text editor such as vi or emacs on UNIX or Notepad on a PC.

Step 3 Extract the portion of the configuration file with the desired commands, and save it in a new file.

Step 4 Copy the configuration file to the appropriate server location. For example, copy the file to the TFTP directory on the workstation (usually /tftpboot on a UNIX workstation).

Step 5 Make sure the permissions on the file are set to world-read.

Copying Configuration Files by Using TFTP

You can configure the access point by using configuration files you create, download from another access point, or download from a TFTP server. You can copy (upload) configuration files to a TFTP server for storage.

This section includes this information:

- Preparing to Download or Upload a Configuration File by Using TFTP, page 20-11
- Downloading the Configuration File by Using TFTP, page 20-11
- Uploading the Configuration File by Using TFTP, page 20-12

Preparing to Download or Upload a Configuration File by Using TFTP

Before you begin downloading or uploading a configuration file by using TFTP, perform these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured.
- Ensure that the access point has a route to the TFTP server. The access point and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the **ping** command.
- Ensure that the configuration file to be downloaded is in the correct directory on the TFTP server.
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- During upload operations, if you are overwriting an existing file on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

Downloading the Configuration File by Using TFTP

To configure the access point by using a configuration file downloaded from a TFTP server, follow these steps:

Step 1 Copy the configuration file to the appropriate TFTP directory on the workstation.

Step 2 Verify that the TFTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File by Using TFTP" section on page 20-11.

Step 3 Log into the access point through a Telnet session.

Step 4 Download the configuration file from the TFTP server to configure the access point.

Specify the IP address or host name of the TFTP server and the name of the file to download.

Use one of these privileged EXEC commands:

- **copy tftp:**[[[**//***location*]**/***directory*]**/***filename*] **system:running-config**
- **copy tftp:**[[[**//***location*]**/***directory*]**/***filename*] **nvram:startup-config**

The configuration file downloads, and the commands are executed as the file is parsed line-by-line.

This example shows how to configure the software from the file *tokyo-confg* at IP address 172.16.2.155:

```
ap# copy tftp://172.16.2.155/tokyo-confg system:running-config
Configure using tokyo-confg from 172.16.2.155? [confirm] y
```

```
Booting tokyo-confg from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

Uploading the Configuration File by Using TFTP

To upload a configuration file from an access point to a TFTP server for storage, follow these steps:

Step 1 Verify that the TFTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File by Using TFTP" section on page 20-11.

Step 2 Log into the access point through a Telnet session.

Step 3 Upload the access point configuration to the TFTP server. Specify the IP address or host name of the TFTP server and the destination filename.

Use one of these privileged EXEC commands:

- **copy system:running-config tftp:**[[[**//***location*]**/***directory*]**/***filename*]
- **copy nvram:startup-config tftp:**[[[**//***location*]**/***directory*]**/***filename*]

The file is uploaded to the TFTP server.

This example shows how to upload a configuration file from an access point to a TFTP server:

```
ap# copy system:running-config tftp://172.16.2.155/tokyo-confg
Write file tokyo-confg on host 172.16.2.155? [confirm] y
#
Writing tokyo-confg!!! [OK]
```

Copying Configuration Files by Using FTP

You can copy configuration files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy a configuration file from the access point to a server by using FTP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **copy** command if a username is specified.
- The username set by the **ip ftp username** *username* global configuration command if the command is configured.
- Anonymous.

The access point sends the first valid password in this list:

- The password specified in the **copy** command if a password is specified.
- The password set by the **ip ftp password** *password* global configuration command if the command is configured.
- The access point forms a password named *username@apname.domain*. The variable *username* is the username associated with the current session, *apname* is the configured host name, and *domain* is the domain of the access point.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept your FTP write request.

Use the **ip ftp username** and **ip ftp password** commands to specify a username and password for all copies. Include the username in the **copy** command if you want to specify only a username for that copy operation.

If the server has a directory structure, the configuration file is written to or copied from the directory associated with the username on the server. For example, if the configuration file resides in the home directory of a user on the server, specify that user's name as the remote username.

For more information, refer to the documentation for your FTP server.

This section includes this information:

- Preparing to Download or Upload a Configuration File by Using FTP, page 20-13
- Downloading a Configuration File by Using FTP, page 20-13
- Uploading a Configuration File by Using FTP, page 20-14

Preparing to Download or Upload a Configuration File by Using FTP

Before you begin downloading or uploading a configuration file by using FTP, perform these tasks:

- Ensure that the access point has a route to the FTP server. The access point and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the FTP server by using the **ping** command.
- If you are accessing the access point through a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new FTP username by using the **ip ftp username** *username* global configuration command during all copy operations. The new username is stored in NVRAM. If you are accessing the access point through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the **copy** command if you want to specify a username for only that copy operation.
- When you upload a configuration file to the FTP server, it must be properly configured to accept the write request from the user on the access point.

For more information, refer to the documentation for your FTP server.

Downloading a Configuration File by Using FTP

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using FTP:

	Command	Purpose
Step 1		Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File by Using FTP" section on page 20-13.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode on the access point. This step is required only if you override the default remote username or password (continue with Step 4 to Step 6).
Step 4	**ip ftp username** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(Optional) Change the default password.

	Command	Purpose
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**copy ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*] **/***filename*] **system:running-config** or **copy ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*] **/***filename*] **nvram:startup-config**	Using FTP, copy the configuration file from a network server to the running configuration or to the startup configuration file.

This example shows how to copy a configuration file named *host1-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 and to load and run those commands on the access point:

```
ap# copy ftp://netadmin1:mypass@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
ap#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

This example shows how to specify a remote username of *netadmin1*. The software copies the configuration file *host2-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 to the access point startup configuration.

```
ap# configure terminal
ap(config)# ip ftp username netadmin1
ap(config)# ip ftp password mypass
ap(config)# end
ap# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
ap#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by ftp from
172.16.101.101
```

Uploading a Configuration File by Using FTP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using FTP:

	Command	Purpose
Step 1		Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File by Using FTP" section on page 20-13.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username or password (continue with Step 4 to Step 6).

	Command	Purpose
Step 4	**ip ftp username** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(Optional) Change the default password.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**copy system:running-config ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*] **/***filename*] or **copy nvram:startup-config ftp:**[[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*] **/***filename*]	Using FTP, store the access point running or startup configuration file to the specified location.

This example shows how to copy the running configuration file named *ap2-confg* to the *netadmin1* directory on the remote host with an IP address of 172.16.101.101:

```
ap# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/ap2-confg
Write file ap2-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
ap#
```

This example shows how to store a startup configuration file on a server by using FTP to copy the file:

```
ap# configure terminal
ap(config)# ip ftp username netadmin2
ap(config)# ip ftp password mypass
ap(config)# end
ap# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [ap2-confg]?
Write file ap2-confg on host 172.16.101.101?[confirm]
![OK]
```

Copying Configuration Files by Using RCP

The Remote Copy Protocol (RCP) provides another method of downloading, uploading, and copying configuration files between remote hosts and the access point. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

The RCP requires a client to send a remote username with each RCP request to a server. When you copy a configuration file from the access point to a server, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **copy** command if a username is specified.
- The username set by the **ip rcmd remote-username** *username* global configuration command if the command is configured.

- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the access point software sends the Telnet username as the remote username.
- The access point host name.

For a successful RCP copy request, you must define an account on the network server for the remote username. If the server has a directory structure, the configuration file is written to or copied from the directory associated with the remote username on the server. For example, if the configuration file is in the home directory of a user on the server, specify that user's name as the remote username.

This section includes this information:

- Preparing to Download or Upload a Configuration File by Using RCP, page 20-16
- Downloading a Configuration File by Using RCP, page 20-16
- Uploading a Configuration File by Using RCP, page 20-17

Preparing to Download or Upload a Configuration File by Using RCP

Before you begin downloading or uploading a configuration file by using RCP, perform these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the access point has a route to the RCP server. The access point and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the **ping** command.
- If you are accessing the access point through a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new RCP username by using the **ip rcmd remote-username** *username* global configuration command to be used during all copy operations. The new username is stored in NVRAM. If you are accessing the access point through a Telnet session and you have a valid username, this username is used, and you do not need to set the RCP username. Include the username in the **copy** command if you want to specify a username for only that copy operation.
- When you upload a file to the RCP server, it must be properly configured to accept the RCP write request from the user on the access point. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server. For example, suppose that the access point contains these configuration lines:

  ```
  hostname ap1
  ip rcmd remote-username User0
  ```

  If the access point IP address translates to *ap1.company.com*, the .rhosts file for User0 on the RCP server should contain this line:

  ```
  ap1.company.com ap1
  ```

For more information, refer to the documentation for your RCP server.

Downloading a Configuration File by Using RCP

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using RCP:

	Command	Purpose
Step 1		Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File by Using RCP" section on page 20-16.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username (continue with Step 4 and Step 5).
Step 4	**ip rcmd remote-username** *username*	(Optional) Specify the remote username.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **system:running-config** or **copy rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] **nvram:startup-config**	Using RCP, copy the configuration file from a network server to the running configuration or to the startup configuration file.

This example shows how to copy a configuration file named *host1-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 and load and run those commands on the access point:

```
ap# copy rcp://netadmin1@172.16.101.101/host1-confg system:running-config
Configure using host1-confg from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-confg:![OK]
ap#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

This example shows how to specify a remote username of *netadmin1*. Then it copies the configuration file *host2-confg* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 to the startup configuration:

```
ap# configure terminal
ap(config)# ip rcmd remote-username netadmin1
ap(config)# end
ap# copy rcp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:![OK]
[OK]
ap#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

Uploading a Configuration File by Using RCP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using RCP:

	Command	Purpose
Step 1		Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File by Using RCP" section on page 20-16.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username (continue with Step 4 and Step 5).
Step 4	**ip rcmd remote-username** *username*	(Optional) Specify the remote username.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**copy system:running-config rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*] or **copy nvram:startup-config rcp:**[[[//[*username*@]*location*]/*directory*]/*filename*]	Using RCP, copy the configuration file from an access point running or startup configuration file to a network server.

This example shows how to copy the running configuration file named *ap2-confg* to the *netadmin1* directory on the remote host with an IP address of 172.16.101.101:

```
ap# copy system:running-config rcp://netadmin1@172.16.101.101/ap2-config
Write file ap-confg on host 172.16.101.101?[confirm]
Building configuration...[OK]
Connected to 172.16.101.101
ap#
```

This example shows how to store a startup configuration file on a server:

```
ap# configure terminal
ap(config)# ip rcmd remote-username netadmin2
ap(config)# end
ap# copy nvram:startup-config rcp:
Remote host[]? 172.16.101.101
Name of configuration file to write [ap2-confg]?
Write file ap2-confg on host 172.16.101.101?[confirm]
![OK]
```

Clearing Configuration Information

This section describes how to clear configuration information.

Deleting a Stored Configuration File

Caution You cannot restore a file after it has been deleted.

To delete a saved configuration from Flash memory, use the **delete flash:***filename* privileged EXEC command. Depending on the setting of the **file prompt** global configuration command, you might be prompted for confirmation before you delete a file. By default, the access point prompts for confirmation on destructive file operations. For more information about the **file prompt** command, refer to the *Cisco IOS Command Reference* guide.

Downloading Configuration File Always from TFTP Server

You can set the AP to download the configuration file (config.txt) always from the TFTP server, even when the NVRAM (flash) has a configuration file stored on it.

Before making this setting you must have the **AutoInstall using DHCP server** feature set for the access points on the router or switch. Without this the following configurations will not work.

To set the AP to download the configuration file always from the TFTP server, in global configuration mode, use the command **boot config-skip**. To disable this setting use the command **no boot config-skip**. This setting is disabled by default.

```
ap(config)# boot config-skip
ap(config)# no boot config-skip
```

In boot mode, you can use the following commands to enable or disable this setting:

- **ap: set BOOT_CONFIG_SKIP yes**, to enable.
- **ap: set BOOT_CONFIG no**, to disable.
- **ap: unset BOOT_CONFIG_SKIP**, to disable.

For setting this via the GUI:

Step 1 Go to **Software > System Configuration**.

Step 2 Against the **Boot Config Skip** option, click **Enable** or **Disable**, as required.

Step 3 Click **Apply**.

Working with Software Images

This section describes how to archive (download and upload) software image files, which contain the system software, Cisco IOS software, radio firmware, and the web management HTML files.

You download an access point image file from a TFTP, FTP, or RCP server to upgrade the access point software. You upload an access point image file to a TFTP, FTP, or RCP server for backup purposes. You can use this uploaded image for future downloads to the same access point or another of the same type.

The protocol you use depends on which type of server you are using. The FTP and RCP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP and RCP are built on and use the Transmission Control Protocol/Internet Protocol (TCP/IP) stack, which is connection-oriented.

This section includes this information:

- Image Location on the Access Point, page 20-20
- tar File Format of Images on a Server or Cisco.com, page 20-20
- Copying Image Files by Using TFTP, page 20-21
- Copying Image Files by Using FTP, page 20-24
- Copying Image Files by Using RCP, page 20-28
- Reloading the Image Using the Web Browser Interface, page 20-33

Note For a list of software images and supported upgrade paths, refer to the release notes for your access point.

Image Location on the Access Point

The Cisco IOS image is stored in a directory that shows the version number. A subdirectory contains the HTML files needed for web management. The image is stored on the system board Flash memory (flash:).

You can use the **show version** privileged EXEC command to see the software version that is currently running on your access point. In the display, check the line that begins with `System image file is...` It shows the directory name in Flash memory where the image is stored.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images you might have stored in Flash memory.

Note Starting with the Cisco IOS releases 15.2(4)JB and 12.4(25e)JAO, on Cisco Aironet 3600, 3700, and 2700 series APs, the backup IOS image is deleted from the system board's Flash memory when the new image is downloaded on to it. This is designed to be so because the system board's Flash memory, which has a total of 31 MB, does not have enough space to store the recovery image, the new image, and the backup image.

tar File Format of Images on a Server or Cisco.com

Software images located on a server or downloaded from Cisco.com are provided in a tar file format, which contains these files:

- *info* file

  The info file is always at the beginning of the tar file and contains information about the files within it.
- Cisco IOS image
- Web management files needed by the HTTP server on the access point
- radio firmware 5000.img file
- *info.ver* file

  The info.ver file is always at the end of the tar file and contains the same information as the info file. Because it is the last file in the tar file, its existence means that all files in the image have been downloaded.

Note The tar file sometimes ends with an extension other than *.tar*.

Copying Image Files by Using TFTP

You can download an access point image from a TFTP server or upload the image from the access point to a TFTP server.

You download an access point image file from a server to upgrade the access point software. You can overwrite the current image with the new one.

You upload an access point image file to a server for backup purposes; this uploaded image can be used for future downloads to the same or another access point of the same type.

This section includes this information:

- Preparing to Download or Upload an Image File by Using TFTP, page 20-21
- Downloading an Image File by Using TFTP, page 20-22
- Uploading an Image File by Using TFTP, page 20-23

Preparing to Download or Upload an Image File by Using TFTP

Before you begin downloading or uploading an image file by using TFTP, perform these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured.
- Ensure that the access point has a route to the TFTP server. The access point and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the **ping** command.
- Ensure that the image to be downloaded is in the correct directory on the TFTP server.
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- During upload operations, if you are overwriting an existing file on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

Downloading an Image File by Using TFTP

You can download a new image file and replace the current image or keep the current image.

Caution For the download and upload algorithms to operate properly, do *not* rename image directories.

Beginning in privileged EXEC mode, follow Steps 1 through 3 to download a new image from a TFTP server and overwrite the existing image.

	Command	Purpose
Step 1	.	Copy the image to the appropriate TFTP directory on the workstation. Make sure the TFTP server is properly configured; see the "Preparing to Download or Upload an Image File by Using TFTP" section on page 20-21
Step 2		Log into the access point through a Telnet session.
Step 3	**archive download-sw /overwrite /reload tftp:**[[//*location*]/*directory*]/*image-name*	Download the image file from the TFTP server to the access point, and overwrite the current image. • The **/overwrite** option overwrites the software image in Flash with the downloaded image. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved. • For //*location*, specify the IP address of the TFTP server. • For /*directory*/*image-name*, specify the directory (optional) and the image to download. Directory and image names are case sensitive.
Step 4	**archive download-sw /leave-old-sw /reload tftp:**[[//*location*]/*directory*]/*image-name*	Download the image file from the TFTP server to the access point, and keep the current image. • The **/leave-old-sw** option keeps the old software version after a download. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved. • For //*location*, specify the IP address of the TFTP server. • For /*directory*/*image-name*, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

Note To avoid an unsuccessful download, use the **archive download-sw /safe** command, which downloads the image first and does not delete the current running version until the download succeeds.

The download algorithm verifies that the image is appropriate for the access point model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the Flash device whether or not it is the same as the new one, downloads the new image, and then reloads the software.

Note The procedure to downgrade an access point IOS is the same procedure for performing an IOS upgrade. To downgrade an access point IOS, enter **archive download-sw /overwrite /reload tftp:**[[**//***location*]**/***directory*]**/***image-name.* The */overwrite* parameter erases the current IOS image, and the new downgraded version of IOS is loaded onto the access point. The */reload* option reloads the system after downloading the image unless the configuration has been changed and not saved.

Note If the Flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image on the system board Flash device (flash:). The image is placed into a new directory named with the software version string, and the system boot path variable is updated to point to the newly installed image.

If you kept the old image during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive** *filesystem***:/***file-url* privileged EXEC command. For *filesystem*, use **flash:** for the system board Flash device. For *file-url*, enter the directory name of the old image. All the files in the directory and the directory are removed.

Uploading an Image File by Using TFTP

You can upload an image from the access point to a TFTP server. You can later download this image to the access point or to another access point of the same type.

Caution For the download and upload algorithms to operate properly, do *not* rename image directories.

Beginning in privileged EXEC mode, follow these steps to upload an image to a TFTP server:

	Command	Purpose
Step 1		Make sure the TFTP server is properly configured; see the "Preparing to Download or Upload an Image File by Using TFTP" section on page 20-21.

	Command	Purpose
Step 1		Log into the access point through a Telnet session.
Step 2	**archive upload-sw tftp:**[[*//location*]*/directory*]*/image-name***.tar**	Upload the currently running access point image to the TFTP server. • For *//location*, specify the IP address of the TFTP server. • For */directory/image-name***.tar**, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The *image-name***.tar** is the name of the software image to be stored on the server.

The **archive upload-sw** privileged EXEC command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, the HTML files, and info.ver. After these files are uploaded, the upload algorithm creates the tar file format.

Copying Image Files by Using FTP

You can download an access point image from an FTP server or upload the image from the access point to an FTP server.

You download an access point image file from a server to upgrade the access point software. You can overwrite the current image with the new one or keep the current image after a download.

You upload an access point image file to a server for backup purposes. You can use this uploaded image for future downloads to the access point or another access point of the same type.

This section includes this information:

- Preparing to Download or Upload an Image File by Using FTP, page 20-24
- Downloading an Image File by Using FTP, page 20-25
- Uploading an Image File by Using FTP, page 20-27

Preparing to Download or Upload an Image File by Using FTP

You can copy images files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy an image file from the access point to a server by using FTP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a username is specified.
- The username set by the **ip ftp username** *username* global configuration command if the command is configured.
- Anonymous.

The access point sends the first valid password in this list:

- The password specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a password is specified.
- The password set by the **ip ftp password** *password* global configuration command if the command is configured.

- The access point forms a password named *username@apname.domain*. The variable *username* is the username associated with the current session, ap*name* is the configured host name, and *domain* is the domain of the access point.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from you.

Use the **ip ftp username** and **ip ftp password** commands to specify a username and password for all copies. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username only for that operation.

If the server has a directory structure, the image file is written to or copied from the directory associated with the username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using FTP, perform these tasks:

- Ensure that the access point has a route to the FTP server. The access point and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Verify connectivity to the FTP server by using the **ping** command.
- If you are accessing the access point through a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new FTP username by using the **ip ftp username** *username* global configuration command. This new name will be used during all archive operations. The new username is stored in NVRAM. If you are accessing the access point through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username for that operation only.
- When you upload an image file to the FTP server, it must be properly configured to accept the write request from the user on the access point.

For more information, refer to the documentation for your FTP server.

Downloading an Image File by Using FTP

You can download a new image file and overwrite the current image or keep the current image.

Caution For the download and upload algorithms to operate properly, do *not* rename image directories.

Beginning in privileged EXEC mode, follow Step 1 through Step 7 to download a new image from an FTP server and overwrite the existing image. To keep the current image, skip Step 7.

	Command	Purpose
Step 1		Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload an Image File by Using FTP" section on page 20-24.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username or password (see Steps 4, 5, and 6).

	Command	Purpose
Step 4	**ip ftp username** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(Optional) Change the default password.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**archive download-sw /overwrite /reload ftp:**[[*//username*[**:***password*]@*location*]*/directory*]*/image-name***.tar**	Download the image file from the FTP server to the access point, and overwrite the current image. • The **/overwrite** option overwrites the software image in Flash with the downloaded image. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved. • For *//username*[**:***password*], specify the username and password; these must be associated with an account on the FTP server. For more information, see the "Preparing to Download or Upload an Image File by Using FTP" section on page 20-24. • For @*location*, specify the IP address of the FTP server. • For *directory/image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.
Step 8	**archive download-sw /leave-old-sw /reload ftp:**[[*//username*[**:***password*]@*location*]*/directory*]*/image-name***.tar**	Download the image file from the FTP server to the access point, and keep the current image. • The **/leave-old-sw** option keeps the old software version after a download. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved. • For *//username*[**:***password*], specify the username and password. These must be associated with an account on the FTP server. For more information, see the "Preparing to Download or Upload an Image File by Using FTP" section on page 20-24. • For @*location*, specify the IP address of the FTP server. • For *directory/image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

Note To avoid an unsuccessful download, use the **archive download-sw /safe** command, which downloads the image first and does not delete the current running version until the download succeeds.

The download algorithm verifies that the image is appropriate for the access point model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the Flash device, whether or not it is the same as the new one, downloads the new image, and then reloads the software.

Note If the Flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough space to install the new image and keep the running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image onto the system board Flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT path-list is updated to point to the newly installed image. Use the privileged EXEC mode **show boot** command to display boot attributes, and use the global configuration **boot** command to change the boot attributes.

If you kept the old image during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive** *filesystem*:/*file-url* privileged EXEC command. For *filesystem*, use **flash:** for the system board Flash device. For *file-url*, enter the directory name of the old software image. All the files in the directory and the directory are removed.

Uploading an Image File by Using FTP

You can upload an image from the access point to an FTP server. You can later download this image to the same access point or to another access point of the same type.

Caution For the download and upload algorithms to operate properly, do *not* rename image directories.

The upload feature is available only if the HTML pages associated with the Cluster Management Suite (CMS) have been installed with the existing image.

Beginning in privileged EXEC mode, follow these steps to upload an image to an FTP server:

	Command	Purpose
Step 1		Verify that the FTP server is properly configured by referring to the "Preparing to Download or Upload a Configuration File by Using FTP" section on page 20-13.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username or password (continue with Step 4 to Step 6).
Step 4	**ip ftp username** *username*	(Optional) Change the default remote username.
Step 5	**ip ftp password** *password*	(Optional) Change the default password.

	Command	Purpose
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**archive upload-sw ftp:**[[**//**[*username*[**:***password*]**@**]*location*]**/***directory*]**/** *image-name***.tar**	Upload the currently running access point image to the FTP server. • For **//***username***:***password*, specify the username and password. These must be associated with an account on the FTP server. For more information, see the "Preparing to Download or Upload an Image File by Using FTP" section on page 20-24. • For **@***location*, specify the IP address of the FTP server. • For **/***directory***/***image-name***.tar**, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. The *image-name***.tar** is the name of the software image to be stored on the server.

The **archive upload-sw** command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, the HTML files, and info.ver. After these files are uploaded, the upload algorithm creates the tar file format.

Copying Image Files by Using RCP

You can download an access point image from an RCP server or upload the image from the access point to an RCP server.

You download an access point image file from a server to upgrade the access point software. You can overwrite the current image with the new one or keep the current image after a download.

You upload an access point image file to a server for backup purposes. You can use this uploaded image for future downloads to the same access point or another of the same type.

This section includes this information:

- Preparing to Download or Upload an Image File by Using RCP, page 20-28
- Downloading an Image File by Using RCP, page 20-30
- Uploading an Image File by Using RCP, page 20-32

Preparing to Download or Upload an Image File by Using RCP

RCP provides another method of downloading and uploading image files between remote hosts and the access point. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

RCP requires a client to send a remote username on each RCP request to a server. When you copy an image from the access point to a server by using RCP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a username is specified.
- The username set by the **ip rcmd remote-username** *username* global configuration command if the command is entered.
- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the access point software sends the Telnet username as the remote username.
- The access point host name.

For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. If the server has a directory structure, the image file is written to or copied from the directory associated with the remote username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using RCP, do these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the access point has a route to the RCP server. The access point and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the **ping** command.
- If you are accessing the access point through a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new RCP username by using the **ip rcmd remote-username** *username* global configuration command to be used during all archive operations. The new username is stored in NVRAM. If you are accessing the access point through a Telnet session and you have a valid username, this username is used, and there is no need to set the RCP username. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username only for that operation.
- When you upload an image to the RCP to the server, it must be properly configured to accept the RCP write request from the user on the access point. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server. For example, suppose the access point contains these configuration lines:

  ```
  hostname ap1
  ip rcmd remote-username User0
  ```

  If the access point IP address translates to *ap1.company.com*, the .rhosts file for User0 on the RCP server should contain this line:

  ```
  ap1.company.com ap1
  ```

For more information, refer to the documentation for your RCP server.

Downloading an Image File by Using RCP

You can download a new image file and replace or keep the current image.

Caution For the download and upload algorithms to operate properly, do *not* rename image directories.

Beginning in privileged EXEC mode, follow Steps 1 through 6 to download a new image from an RCP server and overwrite the existing image. To keep the current image, skip Step 6.

	Command	Purpose
Step 1		Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload an Image File by Using RCP" section on page 20-28.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username (continue with Step 4 and Step 5).
Step 4	**ip rcmd remote-username** *username*	(Optional) Specify the remote username.
Step 5	**end**	Return to privileged EXEC mode.

	Command	Purpose
Step 6	**archive download-sw /overwrite /reload rcp:**[[[**//**[*username*@]*location*]**/***directory*]**/***image-name***.tar**]	Download the image file from the RCP server to the access point, and overwrite the current image. • The **/overwrite** option overwrites the software image in Flash with the downloaded image. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved. • For **//***username*, specify the username. For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. For more information, see the "Preparing to Download or Upload an Image File by Using RCP" section on page 20-28. • For @*location*, specify the IP address of the RCP server. • For **/***directory***/***image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.
Step 7	**archive download-sw /leave-old-sw /reload rcp:**[[[**//**[*username*@]*location*]**/***directory*]**/***image-name***.tar**]	Download the image file from the RCP server to the access point, and keep the current image. • The **/leave-old-sw** option keeps the old software version after a download. • The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not saved. • For **//***username*, specify the username. For the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the "Preparing to Download or Upload an Image File by Using RCP" section on page 20-28. • For @*location*, specify the IP address of the RCP server. • For **/***directory*]**/***image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

Note To avoid an unsuccessful download, use the **archive download-sw /safe** command, which downloads the image first and does not delete the current running version until the download succeeds.

The download algorithm verifies that the image is appropriate for the access point model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the Flash device whether or not it is the same as the new one, downloads the new image, and then reloads the software.

Note If the Flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough room to install the new image an keep the running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image onto the system board Flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old software during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive** *filesystem***:/***file-url* privileged EXEC command. For *filesystem*, use **flash:** for the system board Flash device. For *file-url*, enter the directory name of the old software image. All the files in the directory and the directory are removed.

Uploading an Image File by Using RCP

You can upload an image from the access point to an RCP server. You can later download this image to the same access point or to another access point of the same type.

Caution For the download and upload algorithms to operate properly, do *not* rename image directories.

The upload feature is available only if the HTML pages associated with the Cluster Management Suite (CMS) have been installed with the existing image.

Beginning in privileged EXEC mode, follow these steps to upload an image to an RCP server:

	Command	Purpose
Step 1		Verify that the RCP server is properly configured by referring to the "Preparing to Download or Upload an Image File by Using RCP" section on page 20-28.
Step 2		Log into the access point through a Telnet session.
Step 3	**configure terminal**	Enter global configuration mode. This step is required only if you override the default remote username (continue with Step 4 and Step 5).
Step 4	**ip rcmd remote-username** *username*	(Optional) Specify the remote username.

	Command	Purpose
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**archive upload-sw rcp:**[[[//[*username*@]*location*]/*directory*]/*image-name*.**tar**]	Upload the currently running access point image to the RCP server. • For //*username*, specify the username; for the RCP copy request to execute, an account must be defined on the network server for the remote username. For more information, see the "Preparing to Download or Upload an Image File by Using RCP" section on page 20-28. • For @*location*, specify the IP address of the RCP server. • For /*directory*]/*image-name*.**tar**, specify the directory (optional) and the name of the software image to be uploaded. Directory and image names are case sensitive. • The *image-name*.**tar** is the name of software image to be stored on the server.

The **archive upload-sw** privileged EXEC command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, the HTML files, and info.ver. After these files are uploaded, the upload algorithm creates the tar file format.

Reloading the Image Using the Web Browser Interface

You can also use the Web browser interface to reload the access point image file. The Web browser interface supports loading the image file using HTTP or TFTP interfaces.

Note Your access point configuration is not changed when using the browser to reload the image file.

Browser HTTP Interface

The HTTP interface allows you to browse to the access point image file on your PC and download the image to the access point. Follow the instructions below to use the HTTP interface:

Step 1 Open your Internet browser.

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the Username field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Choose **Software** > **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click the **Browse** button to locate the image file on your PC.

Step 7 Click the **Upgrade** button.

For additional information, click the **Help** icon on the Software Upgrade screen.

Browser TFTP Interface

The TFTP interface allows you to use a TFTP server on a network device to load the access point image file. Follow the instructions below to use a TFTP server:

Step 1 Open your Internet browser.

Step 2 Enter the access point's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the Username field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Choose **Software** > **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click the **TFTP Upgrade** tab.

Step 7 Enter the IP address for the TFTP server in the TFTP Server field.

Step 8 Enter the file name for the access point image file in the Upload New System Image Tar File field. If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename. If the file is located in the TFTP root directory, enter only the filename.

Step 9 Click the **Upgrade** button.

For additional information click the Help icon on the Software Upgrade screen.

Downloading Software Image Always from TFTP Server

You can set the AP to download the software image file, always from the TFTP server, even when an image exists on the NVRAM (flash). Once this is set, whenever the AP is reloaded, the AP will always download the software image file from the TFTP server.

Before making this setting you must have the **AutoInstall using DHCP server** feature set for the access points on the router or switch. Without this, the following configurations will not work.

To set the AP to download the software image file always from the TFTP server, add the following command in the configuration file stored on a TFTP server:

Boot sytem ***imagename***

For example:

```
boot system ap3g1-k9w7-tar.wnbu_bt.0101011010
```

As the **AutoInstall using DHCP server** feature is enabled, when the AP reloads, it will get the TFTP IP address and configuration file name. The AP will then download the configuration file from the TFTP server and apply it. If the configuration file has the afore mentioned **Boot sytem** command, it will download the image from the TFTP server and reload with the new image.

Note The download of the software image from the TFTP server will happen only if the image on the server is not the same as the one currently running on the AP.

Example:Configuration file with Boot System Command

```
no aaa new-model
led display off
no ip source-route
no ip cef
ip domain name Sardinia
!
dot11 syslog
!
dot11 ssid myssid
!
dot11 ssid mysssid
   authentication open
!
boot system ap1g1-k9w7-tar.v153_80mr.201410081600

interface Dot11Radio0
 no ip address
 !
 ssid myssid
 !
 antenna gain 0
 packet retries 64 drop-packet
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
end
```

CHAPTER 21

Configuring L2TPv3 Over UDP/IP

Layer 2 Tunneling Protocol (L2TPv3), is a tunneling protocol that enables tunneling of Layer 2 packets over IP core networks.

L2TPv3 tunnel is a control connection between the end points. One L2TPv3 tunnel can have multiple data connections, and each data connection is termed as an L2TPv3 session. The control connection is used to establish, maintain, and release sessions. Each session is identified by a unique session ID.

To provide the tunneling service to Ethernet traffic, L2TPv3 feature employs:

- L2TPv3
- Pseudowire (PW) technology

Prerequisites

These are the prerequisites for configuring L2TPv3:

- IP routing must be enabled before configuring L2TP-class

  This command enables IP routing:

  ```
  ip routing
  ```

- IP CEF must be enabled

  This command enables IP CEF:

  ```
  ip cef
  ```

- Subinterfaces for Vlans must be created

  These commands create subinterfaces for VLANs:

  ```
  interface Dot11Radio interface number.sub-interface number

  encapsulation dot1Q vlan id

  bridge-group bridge id

  interface GigabitEthernet0.sub-interface number

  encapsulation dot1Q vlan id

  bridge-group bridge id
  ```

Note The bridge id on interfaces with same vlan id must be the same.

The following are not supported:

- Tunnel establishment using IPv6 address
- SNMP and GUI configuration
- Multiple tunnels to same LNS (L2TP Network Server)
- Configuring xconnect on physical interfaces like Gig and Dot11
- Prol2tp versions older than 1.6.1 when sequencing or cookies are enabled.
- Xconnect allows only IPv4 address. FQDN is not supported.
- Only dynamic cookie assignment is used.

Configuring L2TP Class

Configuring the L2TP creates a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes. These parameters can be configured:

- Authentication
- L2TPv3 hello interval
- Hostname
- Cookie length
- Enabling digest
- Retransmit and retries for the L2TPv3 control packets
- Timeout
- Receive-window size
- Hello interval

Beginning in privileged EXEC mode, follow these steps to configureL2TP Class

	Command	Purpose
Step 1	**digest hash** *[MD5, SHA]*	enable message digest.
Step 2	**receive-window** *size*	Receive window size of control connection.
Step 3	**hello** *interval*	Configure the interval between two hello messages.
Step 4	**cookie size** *cookie size*	Configure the cookie size. The values are 4 and 8.
Step 5	**digest secret** *secret*	Configure the secret for authentication.
Step 6	**retransmit retries** *retries*	Configure the number of times a control message is sent if no response is received.
Step 7	**retransmit timeout min** *minimum timeout*	Configure the minimum timeout beween retries.
Step 8	**retransmit timeout max** *maximum timeout*	Configure the maximum timeout between retries.

Note Multiple l2tp classes can be configured.

Examples

```
ap1# configure terminal
ap1(config)# l2tp-class myl2tpclass
ap1(config-l2tp-class)# hostname myhost1
ap1(config-l2tp-class)# hello 15
ap1(config-l2tp-class)# cookie size 4
ap1(config-l2tp-class)# digest secret cisco
ap1(config-l2tp-class)# retransmit retries 6
ap1(config-l2tp-class)# retransmit timeout 7
ap1(config-l2tp-class)# retransmit timeout max 5
ap1(config-l2tp-class)# retransmit timeout min 1
ap1(config-l2tp-class)# end
```

Configuring Pseudowire Class

Configuring the pseudowire class defines a layer 2 pseudowire class. These pseudowire parameters can be configured under pseudowire class:

- encapsulation method
- l2tp-class
- local interface
- sequencing
- IP related parameters like dfbit, tos and ttl

Beginning in privileged EXEC mode, follow these steps to configure Pseudowire Class

	Command	Purpose
Step 1	**pseudowire-class** *pseudowire class name*	Specifies the pseudowire class name.
Step 2	**encapsulation l2tpv3**	Enables the L2TPv3
Step 3	**protocol l2tpv3ietf** *l2tp class name*	Enables the standard L2TPv3 and attaches the L2TP class.
Step 4	**ip protocol udp**	Enables L2TPv3 over UDP.
Step 5	**ip local interface** *interface name*	Uses the interface address as the source address.

Examples

```
ap1# configure terminal
ap1(config)# pseudowire-class mypwclass
ap1(config-pw-class)# encapsulation l2tpv3
ap1(config-pw-class)# protocol l2tpv3ietf myl2tpclass
ap1(config-pw-class)# ip protocol udp
ap1(config-pw-class)# ip local interface BVI1
ap1(config-pw-class)# end
```

Relationship between L2TP Class and Pseudowire Class

Multiple pseudowire classes can be configured. A pseudowire class can configured with any one of the available L2TP Classes. Xconnect can be configured with any one of the configured pseudowire classes.

The following points should be kept in mind:

- A pseudowire class can have only one L2TP Class attached to it.
- An L2TP Class can be attached to multiple pseudowire-classes.
- An xconnect command has a pseudowire-class attached to it, so for one xconnect command only one pseudowire and one L2TP Class is sufficient.
- An L2TP Class not attached to a pseudowire-class and a pseudowire not attached to a xconnect command have no effect on working of an AP.
- L2TP Class attached with a Pseudowire Class cannot be modified. To modify, remove the xconnect from interface which is using this Pseudowire Class.

Configuring the Tunnel interface

This is a new interface for single tunnel support. You can configure xconnect here for all L2TPv3 traffic.

Beginning in privileged EXEC mode, follow these steps to configure the tunnel interface:

	Command	Purpose
Step 1	**interface VDT** *index*	Specifies the VDT interface.
Step 2	**no ip address**	Disables the IP addresses
Step 3	**xconnect** *LNS ip* | *vc-id* | **pw-class** *pseudowire class name*	Configures the LNS IP and attaches the Pseudowire Class.

The vc id is a number which is locally significant. Every xconnect command must be configured with a unique vc id. Traffic for ssids that have **xconnect** *VDT index* configured, get tunneled through a VDT interface with same index.

Examples

```
ap1# configure terminal
ap1(config)# interface VDT0
ap1(config-if)# xconnect 100.100.10.2 10 pw-class mypwclass
ap1(config-if)# end
```

Configure Tunnel management Interface

This is a new interface for secondary tunnel support.

Beginning in privileged EXEC mode, follow these steps to configure the tunnel management interface:

	Command	Purpose
Step 1	**interface VDT-Mgmt** index	Specifies the VDT management interface.
Step 2	**no ip dhcp client request router**	Disables the default route from dhcp.
Step 3	**ip address** *dhcp* | *ip netmask*	Specifies the dhcp IP or static IP.
Step 4	**vdt-mgmt vlan 10**	Configures the VLAN id.

This interface allows access to an AP through the tunnel. This interface is associated with a VDT interface with same index. Traffic from this interface is tunneled though a tunnel established with VDT interface with same index.

Note There will be two default routes leading to a communication failure if the default route from dhcp is not disabled using the **no ip dhcp client request router** command.

Examples

```
ap1# configure terminal
ap1(config)# interface VDT-Mgmt0
ap1(config-subif)# no ip dhcp client request router
ap1(config-subif)# ip address dhcp
ap1(config-subif)# vdt-mgmt vlan 10
ap1(config)# end
```

Mapping SSID to the Tunnel/Xconnect

Mapping the tunnel to the WLAN is done by adding Xconnect under the ssid configuration.

Beginning in privileged EXEC mode, follow these steps to map the tunnel to the VLAN:

	Command	Purpose
Step 1	**dot11 ssid** *ssid*	Specifies the ssid.
Step 2	**vlan** *vlan id*	Specifies the VLAN id.
Step 3	**xconnect** *index of VDT interface*	Enables L2TPv3 for the ssid.
Step 4	**authentication open**	Specifies the type of authentication.

Examples

```
ap1# configure terminal
ap1(config)# dot11 ssid myssid
ap1(config-ssid)# vlan 10
ap1(config-ssid)# authentication open
ap1(config-ssid)# xconnect 0
ap1(config-ssid)# end
```

Configuring TCP mss adjust

To configure TCP mss adjust for tunnel clients use the **dot11 l2tp tcp mss** *tcp mss value command* in the configuration mode.

dot11 l2tp tcp mss *tcp mss value*

Examples

```
ap# configure terminal
ap(config)# dot11 l2tp tcp mss 1360
ap1(config)# end
```

Configuring UDP checksum

To configure UDP checksum ignore for fragmented L2TPv3oUDP Data Packets use the **dot11 l2tpoUdp udp checksum zero** in the configuration mode.

dot11 l2tpoUdp udp checksum zero

Note This command is used when the prol2tp server version is older than 1.6.1 are used.

Examples

```
ap# configure terminal
ap(config)# dot11 l2tpoUdp udp checksum zero
ap(config)# end
```

CHAPTER 22

Configuring Ethernet over GRE

Ethernet over GRE (EoGRE), is a tunneling protocol that enables tunneling of Layer 2 packets encapsulated in GRE header over IP core networks. Generic Routing Encapsulation (GRE) is a tunneling protocol that encapsulates a wide variety of network layer protocols inside virtual point-to-point links over a Layer 3 IPv4 or Layer 3 IPv6 access network.

Prerequisites

The following are the prerequisites for configuring EoGRE:

- IP routing must be enabled. The following command enables IP routing:

  ip routing

- IP CEF must be enabled. The following command enables IP CEF:

  ip cef

- Sub-interfaces for VLANs must be created to tunnel Ethernet frames with the VLAN tag. The following commands create sub interfaces for VLANs:

  interface Dot11Radio *interface number.sub-interface number*

  encapsulation dot1Q *vlan id*

  bridge-group *bridge id*

  interface GigabitEthernet0.*sub-interface number*

  encapsulation dot1Q *vlan id*

  bridge-group *bridge id*

Note The bridge ID on interfaces with the same VLAN ID, must be the same.

The following are not supported:

- SNMP, and GUI through ACS configurations
- Tunnel establishment using IPv6 address

Configuring EoGRE

Configuring a tunnel profile defines configurable parameters to create a tunnel. The following parameters are to be configured under the dot11 tunnel:

- Tunnel address mode
- Source address
- Destination address
- Maximum segment size (MSS)
- Maximum transmission unit (MTU)
- Type of service (ToS) or Differentiated Services Code Point (DSCP)

Beginning in privileged EXEC mode, follow these steps to configure a tunnel profile under the dot11 tunnel.

Command	Purpose
mode [ipv4 | ipv6]	Set tunnel address mode to IPv4 or IPv6
source *address*	Source address, default is AP's BVI address
destination *address*	Tunnel destination address
mss *size*	Set TCP MSS value for incoming and outgoing TCP syn and syn/ack packets. Default size is 1360.
mtu *size*	Incoming IP packets will fragmented if the size of IP packet is larger than this value and then an ICMP Need Fragmentation error message is sent to the client. Default size is 1400.
tos *value*	To set a ToS or DSCP value in the transport IP address. Default value is zero (0).

Examples

```
ap(config)# dot11 tunnel sample
ap(config-dot11-tunnel)# mode ipv4
ap(config-dot11-tunnel)# destination 1.1.1.1
ap(config-dot11-tunnel)# mss 1360
ap(config-dot11-tunnel)# mtu 1400
ap(config-dot11-tunnel)# tos 5
ap(config-dot11-tunnel)# end
```

Mapping SSID to Tunnel

Mapping the tunnel to the WLAN is done by using the command **tunnel** *tunnel_profile* under the SSID configuration.

Beginning in privileged EXEC mode, follow these steps to map the SSID to the tunnel.

	Command	Purpose
Step 1	**dot11 ssid** *ssid*	Specifies the SSID
Step 2	**vlan** *vlan id*	Specifies the VLAN ID
Step 3	**tunnel** *tunnel profile*	Specifies the tunnel profile to be used
Step 4	**authentication {open | eap }**	Specifies the type of authentication

Examples

```
ap(config)# dot11 ssid doc
ap(config-ssid)# tunnel sample
ap(config-ssid)# authentication open
ap(config-ssid)# end
```

Configuring DHCP Snooping for EoGRE clients

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. By enabling DHCP snooping on the AP, the AP inserts the relay agent information option (DHCP option 82) which contains two sub-options Circuit ID and Remote ID.

Note DHCP Snooping is disabled by default.

Beginning in privileged EXEC mode, follow these steps to enable DHCP snooping for EoGRE clients under dot11 SSID.

	Command	Purpose
Step 1	**dhcp-snoop enable**	Enables DHCP snooping. By default, DHCP snooping is disabled.
Step 2	**dhcp-snoop circuit_id format {ap-mac | client-mac | eth-mac | name | ssid | type | vlan | raw** *word_string*}	Specify the format of the string sequence to used as the Circuit ID. To know the format to be specified, see Circuit ID and Remote ID Format and Strings, page 22-4. The Circuit ID gets inserted into the DHCP packets
Step 3	**dhcp-snoop circuit_id** *circuit-id-string_sequence*	Specify the string sequence to used as the Circuit ID, in the format you have set. Each string is separated from others using a character delimiter, the default being ‘;’

	Command	Purpose
Step 4	**dhcp-snoop remote_id format {ap-mac | client-mac | eth-mac | name | ssid | type | vlan | raw** *word_string***}**	You need to specify the format of the string sequence to used as the Remote ID. To know the values to be specified, see Circuit ID and Remote ID Format and Strings, page 22-4.
Step 5	**dhcp-snoop remote_id** *remote-id-string_sequence*	You need to specify the string sequence to used as the Remote ID, in the format you have set. Each string is separated from others using a character delimiter, the default being ‘;’

Examples

```
ap(config)# dot11 ssi
ap(config)# dot11 ssid doc
ap(config-ssid)# dhcp-snoop enable
ap(config-ssid)# dhcp-snoop circuit_id format ap-mac ssid type
ap(config-ssid)# dhcp-snoop circuit_id 00:10:A4:23:B6:C0;xfinityWiFi;s
ap(config-ssid)# dhcp-snoop remote_id format client-mac
ap(config-ssid)# dhcp-snoop remote_id 00:50:24:23:B7:D0
ap(config-ssid)# end
```

Additional Commands

The default DHCP Snooping encoding is in binary. You can set it to ASCII using the following command:

ap(config-ssid)# **dhcp-snoop encoding ascii**

The default DHCP Snooping string sequence delimiter is the single character ';'. To change this, use the following command:

ap(config-ssid)# **dhcp-snoop delimiter** *single_character_or_string*

The *single_character_or_string* can be up to 127 characters long.

Circuit ID and Remote ID Format and Strings

For both the Circuit ID and the Remote ID, you need to specify the format of the string sequence for each, before you assign the string for each.

The format and strings can be a combination of up to five out of eight values shown in the following table. When specifying the string sequence, the strings are separated by the delimiter character, the default being ‘;’.

Format	Nature of corresponding string
ap-mac	AP radio MAC address
client-mac	Client MAC address
eth-mac	AP Ethernet MAC address
name	AP name
raw *word_string*	Any string. If raw is specified in the format command, then the string to be entered is also specified alongside.

Format	Nature of corresponding string
ssid	Service Set Identifier (SSID)
type	Type of SSID. it is ‘o’ for Open SSID and ‘s’ for Secure SSID
vlan	VLAN name

Configuring Redundancy for Tunnel Gateway Address

Configuring a redundancy for the tunnel helps you to switchover from primary to secondary when the working gateway address fails or becomes unreachable.

The following parameters are to be configured under dot11 tunnel to configure redundancy:

- Backup destination
- Backup timeout
- Keep alive parameters

Beginning in privileged EXEC mode, follow these steps to configure redundancy address for the tunnel:

	Command	Purpose
Step 1	**Backup destination** *address*	Specifies the backup destination address
Step 2	**Backup timeout** *seconds*	Specifies the number of seconds after which the tunnel switches from backup to primary
Step 3	**Keepalive** *count interval dead-count timeout*	The *count* is the number of ping packets sent every *interval* seconds. After the *dead-count* pings fail, a tunnel endpoint is assumed to be dead. The *timeout* is the number of seconds the AP waits for ping replies after sending a ping. Default values for *count*, *interval*, *dead-count*, and *timeout* is 3, 60, 3, and 1 respectively.

Note During the switchover from primary to secondary, or vice versa, all associated clients will be deauthenticated and will reassociate after the switchover.
When both the primary and secondary are down, the SSIDs that are attached to the tunnel will also be down. Once either of the primary or secondary address can be reached by the AP, the SSID will come up and start serving clients.

Examples

```
ap(config)# dot11 tunnel sample
ap(config-dot11-tunnel)# backup destination 2.2.2.2
ap(config-dot11-tunnel)# backup timeout 60
ap(config-dot11-tunnel)# keepalive 3 60 3 3
ap(config-dot11-tunnel)# end
```

CHAPTER 23

Configuring System Message Logging

This chapter describes how to configure system message logging on your access point.

Note For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Configuration Fundamentals Command Reference* guide.

Understanding System Message Logging

By default, access points send the output from system messages and **debug** privileged EXEC commands to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer, terminal lines, or a syslog server, depending on your configuration. The process also sends messages to the console.

When the logging process is disabled, messages are sent only to the console. The messages are sent as they are generated, so message and debug output are interspersed with prompts or output from other commands. Messages are displayed on the console after the process that generated them has finished.

You can set the severity level of the messages to control the type of messages displayed on the console and each of the destinations. You can timestamp log messages or set the syslog source address to enhance real-time debugging and management.

You can access logged system messages by using the access point command-line interface (CLI) or by saving them to a properly configured syslog server. The access point software saves syslog messages in an internal buffer. You can remotely monitor system messages by accessing the access point through Telnet or by viewing the logs on a syslog server.

Configuring System Message Logging

This section describes how to configure system message logging. It contains this configuration information:

- System Log Message Format, page 23-2
- Default System Message Logging Configuration, page 23-3
- Disabling and Enabling Message Logging, page 23-4
- Setting the Message Display Destination Device, page 23-5
- Enabling and Disabling Timestamps on Log Messages, page 23-6
- Enabling and Disabling Sequence Numbers in Log Messages, page 23-6
- Defining the Message Severity Level, page 23-7
- Limiting Syslog Messages Sent to the History Table and to SNMP, page 23-8
- Setting a Logging Rate Limit, page 23-9
- Configuring the System Logging Facility, page 23-10

System Log Message Format

System log messages can contain up to 80 characters and a percent sign (%), which follows the optional sequence number or timestamp information, if configured. Messages are displayed in this format:

seq no:timestamp: %facility-severity-MNEMONIC:description

The part of the message preceding the percent sign depends on the setting of the **service sequence-numbers**, **service timestamps log datetime**, **service timestamps log datetime** [**localtime**] [**msec**] [**show-timezone**], or **service timestamps log uptime** global configuration command.

Table 23-1 describes the elements of syslog messages.

Table 23-1 System Log Message Elements

Element	Description
seq no:	Stamps log messages with a sequence number only if the **service sequence-numbers** global configuration command is configured. For more information, see the "Enabling and Disabling Sequence Numbers in Log Messages" section on page 23-6.
timestamp formats: *mm/dd hh:mm:ss* or *hh:mm:ss* (short uptime) or *d h* (long uptime)	Date and time of the message or event. This information appears only if the **service timestamps log** [**datetime** | **log**] global configuration command is configured. For more information, see the "Enabling and Disabling Timestamps on Log Messages" section on page 23-6.
facility	The facility to which the message refers (for example, SNMP, SYS, and so forth). A facility can be a hardware device, a protocol, or a module of the system software. It denotes the source or the cause of the system message.
severity	Single-digit code from 0 to 7 that is the severity of the message. For a description of the severity levels, see Table 23-3 on page 23-8.
MNEMONIC	Text string that uniquely describes the message.
description	Text string containing detailed information about the event being reported.

This example shows a partial access point system message:

```
*Mar  1 00:00:29.219: %LINK-6-UPDOWN: Interface GigabitEthernet0, changed state to up
*Mar  1 00:00:29.335: Starting Ethernet promiscuous mode
*Apr 13 15:29:28.000: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down
*Apr 13 15:29:28.000: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
administratively down
*Apr 13 15:29:28.007: %SYS-5-RESTART: System restarted --
```

Default System Message Logging Configuration

Table 23-2 shows the default system message logging configuration.

Table 23-2 Default System Message Logging Configuration

Feature	Default Setting
System message logging to the console	Enabled
Console severity	Debugging (and numerically lower levels; see Table 23-3 on page 23-8)
Logging buffer size	4096 bytes
Logging history size	1 message
Timestamps	Disabled

Table 23-2 Default System Message Logging Configuration (continued)

Feature	Default Setting
Synchronous logging	Disabled
Logging server	Disabled
Syslog server IP address	None configured
Server facility	Local7 (see Table 23-4 on page 23-10)
Server severity	Informational (and numerically lower levels; see Table 23-3 on page 23-8)

Disabling and Enabling Message Logging

Message logging is enabled by default. It must be enabled to send messages to any destination other than the console. When enabled, log messages are sent to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages.

Beginning in privileged EXEC mode, follow these steps to disable message logging:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no logging on**	Disable message logging.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config** or **show logging**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Disabling the logging process can slow down the access point because a process must wait until the messages are written to the console before continuing. When the logging process is disabled, messages are displayed on the console as soon as they are produced, often appearing in the middle of command output.

The **logging synchronous** global configuration command also affects the display of messages to the console. When this command is enabled, messages appear only after you press Return. For more information, see the "Enabling and Disabling Timestamps on Log Messages" section on page 23-6.

To re-enable message logging after it has been disabled, use the **logging on** global configuration command.

Setting the Message Display Destination Device

If message logging is enabled, you can send messages to specific locations in addition to the console. Beginning in privileged EXEC mode, use one or more of the following commands to specify the locations that receive messages:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging buffered** [*size*] [*level*]	Log messages to an internal buffer. The default buffer size is 4096. The range is 4096 to 2147483647 bytes. Levels include emergencies 0, alerts 1, critical 2, errors 3, warnings 4, notifications 5, informational 6, and debugging 7. **Note** Do not make the buffer size too large because the access point could run out of memory for other tasks. Use the **show memory** privileged EXEC command to view the free processor memory on the access point; however, this value is the maximum available, and you should *not* set the buffer size to this amount.
Step 3	**logging** *host*	Log messages to a syslog server host. For *host*, specify the name or IP address of the host to be used as the syslog server. To build a list of syslog servers that receive logging messages, enter this command more than once. For complete syslog server configuration steps, see the "Configuring the System Logging Facility" section on page 23-10.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**terminal monitor**	Log messages to a non-console terminal during the current session. Terminal parameter-setting commands are set locally and do not remain in effect after the session has ended. You must perform this step for each session to see the debugging messages.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

The **logging buffered** global configuration command copies logging messages to an internal buffer. The buffer is circular, so newer messages overwrite older messages after the buffer is full. To display the messages that are logged in the buffer, use the **show logging** privileged EXEC command. The first message displayed is the oldest message in the buffer. To clear the contents of the buffer, use the **clear logging** privileged EXEC command.

To disable logging to the console, use the **no logging console** global configuration command.

Enabling and Disabling Timestamps on Log Messages

By default, log messages are not timestamped.

Beginning in privileged EXEC mode, follow these steps to enable timestamping of log messages:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**service timestamps log uptime** or **service timestamps log datetime** [**msec**] [**localtime**] [**show-timezone**]	Enable log timestamps. The first command enables timestamps on log messages, showing the time since the system was rebooted. The second command enables timestamps on log messages. Depending on the options selected, the timestamp can include the date, time in milliseconds relative to the local time zone, and the time zone name.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable timestamps for both debug and log messages, use the **no service timestamps** global configuration command.

This example shows part of a logging display with the **service timestamps log datetime** global configuration command enabled:

```
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

This example shows part of a logging display with the s**ervice timestamps log uptime** global configuration command enabled:

```
*Apr 13 15:29:28.000: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down
```

Enabling and Disabling Sequence Numbers in Log Messages

Because there is a chance that more than one log message can have the same timestamp, you can display messages with sequence numbers so that you can unambiguously refer to a single message. By default, sequence numbers in log messages are not displayed.

Beginning in privileged EXEC mode, follow these steps to enable sequence numbers in log messages:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**service sequence-numbers**	Enable sequence numbers.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable sequence numbers, use the **no service sequence-numbers** global configuration command.

This example shows part of a logging display with sequence numbers enabled:

```
000019: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

Defining the Message Severity Level

You can limit messages displayed to the selected device by specifying the severity level of the message, which are described in Table 23-3.

Beginning in privileged EXEC mode, follow these steps to define the message severity level:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging console** *level*	Limit messages logged to the console. By default, the console receives debugging messages and numerically lower levels (see Table 23-3 on page 23-8).
Step 3	**logging monitor** *level*	Limit messages logged to the terminal lines. By default, the terminal receives debugging messages and numerically lower levels (see Table 23-3 on page 23-8).
Step 4	**logging trap** *level*	Limit messages logged to the syslog servers. By default, syslog servers receive informational messages and numerically lower levels (see Table 23-3 on page 23-8). For complete syslog server configuration steps, see the "Configuring the System Logging Facility" section on page 23-10.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config** or **show logging**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note Specifying a *level* causes messages at that level and numerically lower levels to be displayed at the destination.

To disable logging to the console, use the **no logging console** global configuration command. To disable logging to a terminal other than the console, use the **no logging monitor** global configuration command. To disable logging to syslog servers, use the **no logging trap** global configuration command.

Table 23-3 describes the *level* keywords. It also lists the corresponding syslog definitions from the most severe level to the least severe level.

Table 23-3 Message Logging Level Keywords

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

The software generates four other categories of messages:

- Error messages about software or hardware malfunctions, displayed at levels **warnings** through **emergencies**. These types of messages mean that the functionality of the access point is affected.
- Output from the **debug** commands, displayed at the **debugging** level.
- Interface up or down transitions and system restart messages, displayed at the **notifications** level. This message is only for information; access point functionality is not affected.
- Reload requests and low-process stack messages, displayed at the **informational** level. This message is only for information; access point functionality is not affected.

Note Authentication request log messages are not logged on to a syslog server. This feature is not supported on Cisco Aironet access points.

Limiting Syslog Messages Sent to the History Table and to SNMP

If you have enabled syslog message traps to be sent to an SNMP network management station by using the **snmp-server enable trap** global configuration command, you can change the level of messages sent and stored in the access point history table. You can also change the number of messages that are stored in the history table.

Messages are stored in the history table because SNMP traps are not guaranteed to reach their destination. By default, one message of the level **warning** and numerically lower levels (see Table 23-3 on page 23-8) are stored in the history table even if syslog traps are not enabled.

Beginning in privileged EXEC mode, follow these steps to change the level and history table size defaults:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging history** *level*[1]	Change the default level of syslog messages stored in the history file and sent to the SNMP server. See Table 23-3 on page 23-8 for a list of *level* keywords. By default, **warnings**, **errors**, **critical**, **alerts**, and **emergencies** messages are sent.
Step 3	**logging history size** *number*	Specify the number of syslog messages that can be stored in the history table. The default is to store one message. The range is 1 to 500 messages.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

[1] Table 23-3 lists the level keywords and severity level. For SNMP usage, the severity level values increase by 1. For example, emergencies equal 1, not 0, and critical equals 3, not 2.

When the history table is full (it contains the maximum number of message entries specified with the **logging history size** global configuration command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

To return the logging of syslog messages to the default level, use the **no logging history** global configuration command. To return the number of messages in the history table to the default value, use the **no logging history size** global configuration command.

Setting a Logging Rate Limit

You can enable a limit on the number of messages that the access point logs per second. You can enable the limit for all messages or for messages sent to the console, and you can specify that messages of a specific severity are exempt from the limit.

Beginning in privileged EXEC mode, follow these steps to enable a logging rate limit:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging rate-limit** *seconds* [**all | console**] [**except** *severity*]	Enable a logging rate limit in seconds. • (Optional) Apply the limit to all logging or only to messages logged to the console. • (Optional) Exempt a specific severity from the limit.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable the rate limit, use the **no logging rate-limit** global configuration command.

Configuring the System Logging Facility

When sending system log messages to an external device, you can cause the access point to identify its messages as originating from any of the syslog facilities.

Beginning in privileged EXEC mode, follow these steps to configure system facility message logging:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging** *host*	Log messages to a syslog server host by entering its IP address. To build a list of syslog servers that receive logging messages, enter this command more than once.
Step 3	**logging trap** *level*	Limit messages logged to the syslog servers. Be default, syslog servers receive informational messages and lower. See Table 23-3 on page 23-8 for *level* keywords.
Step 4	**logging facility** *facility-type*	Configure the syslog facility. See Table 23-4 on page 23-10 for *facility-type* keywords. The default is **local7**.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To remove a syslog server, use the **no logging** *host* global configuration command, and specify the syslog server IP address. To disable logging to syslog servers, enter the **no logging trap** global configuration command.

Table 23-4 lists the system facilities supported by the Cisco IOS software. For more information about these facilities, consult the operator's manual for your syslog server.

Table 23-4 Logging Facility-Type Keywords

Facility Type Keyword	Description
auth	Authorization system
cron	Cron facility
daemon	System daemon
kern	Kernel
local0-7	Locally defined messages
lpr	Line printer system
mail	Mail system
news	USENET news
sys9	System use
sys10	System use
sys11	System use
sys12	System use

Table 23-4 Logging Facility-Type Keywords (continued)

Facility Type Keyword	Description
sys13	System use
sys14	System use
syslog	System log
user	User process
uucp	UNIX-to-UNIX copy system

Displaying the Logging Configuration

To display the current logging configuration and the contents of the log buffer, use the **show logging** privileged EXEC command. For information about the fields in this display, refer to the *Cisco IOS Configuration Fundamentals Command Reference* guide.

To display the logging history file, use the **show logging history** privileged EXEC command.

CHAPTER 24

Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the wireless device. For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at the following URL (select **Top Issues** and then select **Wireless Technologies**):

http://www.cisco.com/tac

Checking the LED Indicators

If your wireless device is not communicating, first check the LED indicators on the device to quickly assess the device’s status.

The LED indicator setup is not the same across all Cisco Aironet series access points. Depending on the series, your access point may have a single Status LED indicator, or three indicators – Ethernet LED, Status LED, and Radio LED. Refer to your access point’s *Getting Started Guide* or the *Hardware Installation Guide* (for Outdoor Access Points) for information on its LED indicator setup.

Note There will be small variations in LED color intensity and hue from unit to unit. This is expected and within the normal range of the LED manufacturer’s specifications and is not a defect.

Checking Power

You can verify the availability of power to the access point/bridge by checking the power injector’s LED indicator:

- Green color indicates input power is being supplied to the bridge.
- Red color indicates an overcurrent or overvoltage error condition—disconnect input power from the power injector, check all coax cable connections for a possible short, wait approximately 1 minute, and reconnect input power to the power injector. If the LED turns red again, contact technical support for assistance.

  Note The power injector requires approximately 50 seconds to recover from an overcurrent or overvoltage condition.

Off indicates input power is not available—verify that the power module is connected to the power injector and that AC power is available or that 12- to 40-VDC input power is connected to the power injector.

Low Power Condition

Access points can be powered from the 48-VDC power module or from an in-line power source.

For full operation, the 1040, 1140, 1260, and 700W series access points require 12.95 W of power. The power module and Cisco Aironet power injectors are capable of supplying the required power for full operation, but some inline power sources are not capable of supplying 12.95 W. Also, some high-power inline power sources, might not be able to provide 12.95 W of power to all ports at the same time.

The 2600, 3600, 2700 and 3700 series access points need 18.5 Watts, and therefore 802.3at or PoE+. However, these access points can also function with 802.3af power, by disabling one of the radio chains on each radio module.

Note An 802.3af compliant switch (Cisco or non-Cisco) is capable of supplying sufficient power for full operation.

Note When an AP 2700 or AP 3700 is running in low power mode with PoE 802.3af power, one of the radios is shutdown. As the saved power from the shut down radio is utilized for the running radio, that radio is reset. During the reset, communication with associated WLAN clients will get disrupted. After the radio comes back online after reset, the WLAN clients will re-associate with it afresh.

On power on, the access points are placed into low power mode (both radios are disabled), Cisco IOS software loads and runs, and power negotiation determines if sufficient power is available. If there is sufficient power then the radios are turned on; otherwise, the access point remains in low power mode with the radios disabled to prevent a possible over-current condition. In low power mode, the access point activates the Status LED low power error indication, displays a low power message on the browser and serial interfaces, and creates an event log entry.

Checking Basic Settings

Mismatched basic settings are the most common causes of lost connectivity with wireless clients. If the wireless device does not communicate with client devices, check the areas described in this section.

SSID

Wireless clients attempting to associate with the wireless device must use the same SSID as the wireless device. If a client device's SSID does not match the SSID of an wireless device in radio range, the client device will not associate.

WEP Keys

The WEP key you use to transmit data must be set up exactly the same on the wireless device and any wireless devices with which it associates. For example, if you set WEP Key 3 on your client adapter to 0987654321 and select it as the transmit key, you must set WEP Key 3 on the wireless device to exactly the same value. The wireless device does not need to use Key 3 as its transmit key, however.

Refer to Chapter 10, "Configuring WLAN Authentication and Encryption,"for instructions on setting the wireless device's WEP keys.

Security Settings

Wireless clients attempting to authenticate with the wireless device must support the same security options configured in the wireless device, such as EAP or LEAP, MAC address authentication, Message Integrity Check (MIC), WEP key hashing, and 802.1X protocol versions.

If your radio clients are using EAP-FAST authentication, you must configure open authentication with EAP. If you do not configure open authentication with EAP, a warning message appears. If you are using the CLI. the following warning appears:

SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.

If you are using the GUI, this warning message appears:

WARNING:
"Network EAP is used for LEAP authentication only. If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured."

If a wireless client is unable to authenticate with the wireless device, contact the system administrator for proper security settings in the client adapter and for the client adapter driver and firmware versions that are compatible with the wireless device settings.

Resetting to the Default Configuration

If you forget the password that allows you to configure the wireless device, you may need to completely reset the configuration. On all access points, you can use the MODE button on the access point or the web-browser interface. On 350 series access points, you can use the web-browser or CLI interfaces.

Note The following steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID. The default username and password are both **Cisco**, which is case-sensitive.

Using the MODE Button

Follow these steps to delete the current configuration and return all access point settings to the factory defaults using the MODE button.

Note To reset the configuration to defaults, intead of using the MODE button, follow the instructions in the "Using the Web Browser Interface" section on page 24-5, or in the "Using the CLI" section on page 24-5.
You cannot use the MODE button to reset the configuration to defaults on 350 series access points.

Step 1 Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

Step 2 Press and hold the **MODE** button while you reconnect power to the access point.

Step 3 Hold the MODE button until the Status LED turns blue.

Step 4 After the access point reboots, you must reconfigure the access point by using the Web-browser interface or the CLI.

Note The access point is configured with the factory default values including the IP address (set to receive an IP address using DHCP). The default username and password are **Cisco**, which is case-sensitive.

Using the Web Browser Interface

Follow these steps to delete the current configuration and return all wireless device settings to the factory defaults using the web browser interface:

Step 1 Open your Internet browser.

Step 2 Enter the wireless device's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the Username field.

Step 4 Enter the wireless device password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click **Software** and the System Software screen appears.

Step 6 Click **System Configuration** and the System Configuration screen appears.

Step 7 Click the **Reset to Defaults** or **Reset to Defaults (Except IP)** button.

Note Select **Reset to Defaults (Except IP)** if you want to retain a static IP address.

Step 8 Click **Restart**. The system reboots.

Step 9 After the wireless device reboots, you must reconfigure the wireless device by using the Web-browser interface or the CLI. The default username and password are **Cisco**, which is case-sensitive.

Using the CLI

Follow the steps below to delete the current configuration and return all wireless device settings to the factory defaults using the CLI.

Step 1 Open the CLI using a Telnet session or a connection to the wireless device console port.

Step 2 Reboot the wireless device by removing power and reapplying power.

Step 3 Let the wireless device boot until the command prompt appears and the wireless device begins to inflate the image. When you see these lines on the CLI, press **Esc**:

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...###########################################################################
################################################################################
################################################################################
####################
```

Step 4 At the ap: prompt, enter the **flash_init** command to initialize the Flash.

```
ap: flash_init
Initializing Flash...
flashfs[0]: 142 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7612416
flashfs[0]: Bytes used: 3407360
flashfs[0]: Bytes available: 4205056
flashfs[0]: flashfs fsck took 0 seconds.
```

```
...done initializing Flash.
```

Step 5 Use the **dir flash:** command to display the contents of Flash and find the config.txt configuration file.

```
ap: dir flash:
Directory of flash:/
3 .rwx 223 <date> env_vars
4 .rwx 2190 <date> config.txt
5 .rwx 27 <date> private.config
150 drwx 320 <date> c350.k9w7.mx.122.13.JA
4207616 bytes available (3404800 bytes used)
```

Step 6 Use the **rename** command to change the name of the config.txt file to config.old.

```
ap: rename flash:config.txt flash:config.old
```

Step 7 Use the **reset** command to reboot the wireless device.

```
ap: reset
Are you sure you want to reset the system (y/n)?y
System resetting...
    using  eeprom values
WRDTR,CLKTR: 0x80000800 0x80000000
RQDC ,RFDC : 0x80000033 0x000001cb
    ddr init done
IOS Bootloader - Starting system.
Xmodem file system is available.
DDR values used from system serial eeprom.
WRDTR,CLKTR: 0x80000800, 0x80000000
RQDC, RFDC : 0x80000033, 0x000001cb
```

Step 8 When the access point has finished rebooting the software, establish a new Telnet session to the access point.

Note The wireless device is configured with factory default values, including the IP address (set to receive an IP address using DHCP) and the default username and password (**Cisco**).

Step 9 When IOS software is loaded, you can use the **del** privileged EXEC command to delete the config.old file from Flash.

```
ap# del flash:config.old
Delete filename [config.old]
Delete flash:config.old [confirm]
ap#
```

Reloading the Access Point Image

If the wireless device has a firmware failure, you must reload the image file using the Web browser interface or on all access points, by pressing and holding the MODE button for around 30 seconds. You can use the browser interface if the wireless device firmware is still fully operational and you want to upgrade the firmware image. However, you can use the MODE button when the access point has a corrupt firmware image.

Using the MODE button

You can use the MODE button on all access points to reload the access point image file from an active Trivial File Transfer Protocol (TFTP) server on your network or on a PC connected to the access point Ethernet port.

If the wireless device experiences a firmware failure or a corrupt firmware image, indicated by three red LED indicators, you must reload the image from a connected TFTP server.

Note This process resets *all* configuration settings to factory defaults, including passwords, security configurations, the wireless device IP address, and SSIDs.

Follow these steps to reload the access point image file:

Step 1 The PC you intend to use must be configured with a static IP address in the range of 10.0.0.2 to 10.0.0.30.

Step 2 Make sure that the PC contains the access point image file (such as such as *ap3g2-k9w7-tar.152-4.JB5.tar*) in the TFTP server folder and that the TFTP server is activated. For additional information, refer to the "Obtaining the Access Point Image File" and "Obtaining TFTP Server Software" sections.

Step 3 Rename the access point image file in the TFTP server folder. For example, if the image file is **ap3g2-k9w7-tar.152-4.JB5.tar**, rename the file to **ap3g2-k9w7-tar.default**.

Step 4 Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.

Step 5 Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

Step 6 Press and hold the **MODE** button while you reconnect power to the access point.

Step 7 Hold the **MODE** button until the status LED turns red (approximately 20 to 30 seconds), and release the MODE button.

Step 8 Wait until the access point reboots as indicated by all LEDs turning green followed by the Status LED blinking green.

Step 9 After the access point reboots, you must reconfigure the access point by using the Web-browser interface or the CLI.

Using the Web Browser Interface

You can also use the Web browser interface to reload the wireless device image file. The Web browser interface supports loading the image file using HTTP or TFTP interfaces.

Note Your wireless device configuration does not change when you use the browser to reload the image file.

Browser HTTP Interface

The HTTP interface enables you to browse to the wireless device image file on your PC and download the image to the wireless device. Follow the instructions below to use the HTTP interface:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer or Netscape Navigator (version 7.x).

Step 2 Enter the wireless device's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the Username field.

Step 4 Enter the wireless device password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click the **Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click **Browse** to find the image file on your PC.

Step 7 Click **Upload**.

For additional information, click the **Help** icon on the Software Upgrade screen.

Browser TFTP Interface

The TFTP interface allows you to use a TFTP server on a network device to load the wireless device image file. Follow the instructions below to use a TFTP server:

Step 1 Open your Internet browser.

Step 2 Enter the wireless device's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the Username field.

Step 4 Enter the wireless device password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click the **Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click the **TFTP Upgrade** tab.

Step 7 Enter the IP address for the TFTP server in the TFTP Server field.

Step 8 Enter the file name for the image file in the Upload New System Image Tar File field. If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename. If the file is located in the TFTP root directory, enter only the filename.

Step 9 Click **Upload**.

For additional information click the **Help** icon on the Software Upgrade screen.

Using the CLI

Follow the steps below to reload the wireless device image using the CLI. When the wireless device begins to boot, you interrupt the boot process and use boot loader commands to load an image from a TFTP server to replace the image in the wireless device.

Note Your wireless device configuration is not changed when using the CLI to reload the image file.

Step 1 Open the CLI using a connection to the wireless device console port.

Step 2 Reboot the wireless device by removing power and reapplying power.

Step 3 Let the wireless device boot until it begins to inflate the image. When you see these lines on the CLI, press **Esc**:

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...###########################################################################
################################################################################
################################################################################
####################
```

Step 4 When the ap: command prompt appears, enter the **set** command to assign an IP address, subnet mask, and default gateway to the wireless device.

Note You must use upper-case characters when you enter the **IP-ADDR**, **NETMASK**, and **DEFAULT_ROUTER** options with the **set** command.

Your entries might look like this example:

```
ap: set IP_ADDR 192.168.133.160
ap: set NETMASK 255.255.255.0
ap: set DEFAULT_ROUTER 192.168.133.1
```

Step 5 Enter the **tftp_init** command to prepare the wireless device for TFTP.

```
ap: tftp_init
```

Step 6 Enter the **tar** command to load and inflate the new image from your TFTP server. The command must include this information:

- the **-xtract** option, which inflates the image when it is loaded
- the IP address of your TFTP server
- the directory on the TFTP server that contains the image
- the name of the image
- the destination for the image (the wireless device Flash)

Your entry might look like this example:

```
ap: tar -xtract tftp://192.168.130.222/images/ap3g2-k9w7-tar.152-4.JB5.tar flash
```

Step 7 When the display becomes full, the CLI pauses and displays `--MORE--`. Press the spacebar to continue.

```
extracting info (286 bytes)
ap3g2-k9w7-mx.152-4.JB5/ (directory)
ap3g2-k9w7-mx.152-4.JB5/ap3g2-k9w7-mx.152-4.JB5 (208427 bytes)
ap3g2-k9w7-mx.152-4.JB5/ap3g2-k9w7-tx.152-4.JB5 (73 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/appsui.js (563 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/back.shtml (512 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/cookies.js (5032 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/forms.js (20125 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/sitewide.js (17089 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/stylesheet.css (3220 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/config.js (26330 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/popup_capabilitycodes.shtml.gz (1020 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/filter.js.gz (1862 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/filter_vlan.js.gz (1459 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/filter_mac_ether.js.gz (1793 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/security.js.gz (962 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/vlan.js.gz (1121 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ssid.js.gz (4286 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/network-if.js.gz (2084 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/dot1x.js.gz (988 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/stp.js.gz (957 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_assoc.shtml.gz (5653 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_event-log.shtml.gz (3907 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_home.shtml.gz (7071 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_network-if.shtml.gz (3565 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_network-map.shtml.gz (3880 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_services.shtml.gz (3697 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_system-sw.shtml.gz (2888 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_contextmgr.shtml.gz (3834 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/ap_title_appname.gif (2092 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/2600_title_appname.gif (2100 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button.gif (1211 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_1st.gif (1171 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_cbottom.gif (318 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_current.gif (1206 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_endcap.gif (878 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_encap_last.gif (333 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_last.gif (386 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_nth.gif (1177 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_leftnav_dkgreen.gif (869 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_leftnav_green.gif (879 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_leftnav_upright.gif (64 bytes)
.../...
```

Step 8 Enter the **set BOOT** command to designate the new image as the image that the wireless device uses when it reboots. The wireless device creates a directory for the image that has the same name as the image, and you must include the directory in the command. Your entry might look like this example:

```
ap: set BOOT flash:/ap3g2-k9w7-tar.152-4.JB5/ap3g2-k9w7-tar.152-4.JB5
```

Step 9 Enter the **set** command to check your bootloader entries.

```
ap: set
BOOT=flash:/ap3g2-k9w7-tar.152-4.JB5/ap3g2-k9w7-tar.152-4.JB5
DEFAULT_ROUTER=192.168.133.1
```

```
IP_ADDR=192.168.133.160
NETMASK=255.255.255.0
```

Step 10 Enter the **boot** command to reboot the wireless device. When the wireless device reboots, it loads the new image.

```
ap: boot
```

Obtaining the Access Point Image File

You can obtain the wireless device image file from the Cisco.com by following these steps:

Step 1 Use your Internet browser to access the Download Software page for wireless products, at the following URL:

http://software.cisco.com/download/navigator.html?mdfid=278875243&i=!h

Step 2 Login to the Cisco.com site.
Click **Log In** at the top right corner of the page and enter your CCO login and password.

Step 3 In Select a Product area, from the right-most column click **Access Points**.

Step 4 Click the appropriate access point.

Step 5 Click the appropriate access point version.

Step 6 Click **Autonomous AP IOS Software**.
A list of available software versions appear.

Step 7 Choose the version you wish to download.
The download page for the version you chose appears.

Step 8 Click **Download**. The Software Download Rules page appears.

Step 9 Read the Software Download Rules carefully and click **Agree**.

Step 10 Save the file to your hard drive.

Obtaining TFTP Server Software

You can download TFTP server software from several websites. We recommend the shareware TFTP utility available at this URL:

http://tftpd32.jounin.net

Follow the instructions on the website for installing and using the utility.

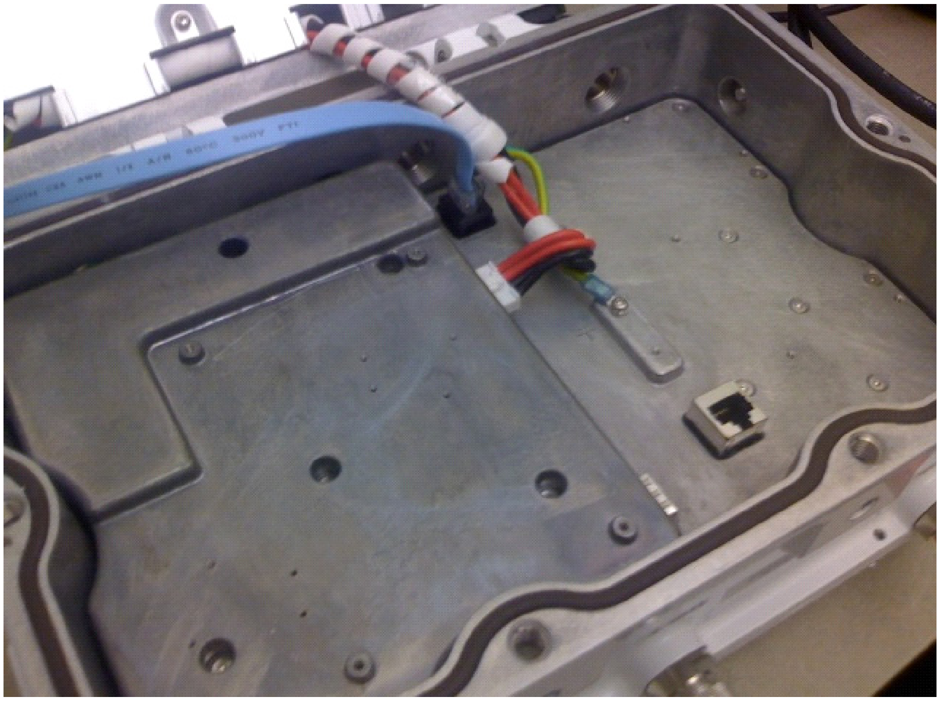
Image Recovery on the 1520 Access Point

The process for image recovery on an 1520 access point is similar to the process for any IOS access point with a console port.

To perform image recovery on the 1520 access point, follow these steps:

Step 1 With the access point powered off, connect an RJ45 console cable to the console port (). The console port is the black plastic RJ45 jack inside the unit.

Figure 24-1 Connecting an RJ45 Console Cable to the Console Port



Step 2 Configure the terminal emulator for 8 databits, no parity, no flow control, 9600 bps.

Step 3 Apply power to the access point.

Step 4 When the bootloader displays "Base Ethernet MAC Address", hit the <esc> key to break to the **ap:** prompt:

```
IOS Bootloader - Starting system.
Xmodem file system is available.
flashfs[0]: 13 files, 2 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 31868928
flashfs[0]: Bytes used: 9721344
flashfs[0]: Bytes available: 22147584
flashfs[0]: flashfs fsck took 20 seconds.
Reading cookie from flash parameter block...done.
Base Ethernet MAC address: 00:1f:27:75:db:00

The system boot has been aborted.  The following
commands will finish loading the operating system
software:
    ether_init
    tftp_init
    boot
ap:
```

Note If the **ENABLE_BREAK=no environmental** variable is set, you will not be able to escape to the bootloader.

Step 5 Cable the 1520 access point's LAN port ("PoE In") to a TFTP server. For example, a Windows PC with tftpd32 installed.

Step 6 Install a good copy of the **k9w7** IOS image on the TFTP server.

Step 7 Configure the TFTP server's LAN interface with a static IP address. For example, 10.1.1.1.

Step 8 On the access point enter:

```
ap: dir flash:
```

Verify there is enough free space on flash to hold the new code (or if the flash file system is corrupt), then enter:

```
ap: format flash:
```

Step 9 Copy the image using TFTP to the 1520 access point's flash.

CHAPTER 25

Miscellaneous AP-Specific Configurations

This chapter contains miscellaneous configurations that are specific to certain access points.

Cisco Aironet 700W Series

Using the LAN ports on 700W APs

The Cisco Aironet 700W series access points have one 10/100/1000BASE-T PoE Uplink/WAN port and four 10/100/1000BASE-T RJ-45 local Ethernet ports for wired device connectivity. The fourth port functions as a PoE-Out port when the AP is powered by 802.3at Ethernet switch, Cisco power injector AIR-PWRJ4=, or Cisco Power Supply.

By default, all four local Ethernet ports are disabled. You can be enable them when required.

You can also configure the local Ethernet ports to a VLAN ID using the interface configuration command, **vlan** *vlan-id*.

Enable LAN ports on 702W

Step 1 Enter global configuration mode.

```
ap#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

Step 2 Enable the LAN port.

```
ap(config)#lan-Port port-id 1
ap(config-lan-port)#no shutdown
ap(config-lan-port)#end
```

Assign a VLAN to the LAN ports

Use the commands given in the example below.

```
ap#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)#lan-Port port-id 1
ap(config-lan-port)#vlan 25
ap(config-lan-port)#end
```

Verifying the LAN Port Configurations

Use the command given in the example below.

```
voip#sh lan  config

LAN table entries:

 Port    Status       Vlan valid    Vlan Id
  ----    ---------    ----------    -------
  LAN1    DISABLED     25            NA
  LAN2    ENABLED      NO            NA
  LAN3    DISABLED     NO            NA
  LAN4    ENABLED      NO            NA
LAN POE out state = ENABLED
```

700W AP as Workgroup Bridge

Like other Cisco Access points 702W AP series also can be configured as a Workgroup Bridge (WGB).

A WGB can provide a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter in order to connect to the wireless network can be connected to the WGB through the Ethernet port.

The WGB supports up to 20 Ethernet-enabled devices to a Wireless LAN (WLAN). The WGB associates to the root AP through the wireless interface. In this way, wired clients obtain access to the wireless network. A WGB can associate to:

- An AP
- A root bridge (in AP mode)
- A controller through a lightweight AP

When a Cisco 702W access point acts as a WGB, the wired Ethernet clients behind the WGB can be either connected to the LAN or WAN ports present on the 702W AP.

APPENDIX A

Protocol Filters

The tables in this appendix list some of the protocols that you can filter on the access point. In each table, the Protocol column lists the protocol name, the Additional Identifier column lists other names for the same protocol, and the ISO Designator column lists the numeric designator for each protocol.

Table A-1 EtherType Protocols

Protocol	Additional Identifier	ISO Designator
ARP	—	0x0806
RARP	—	0x8035
IP	—	0x0800
Berkeley Trailer Negotiation	—	0x1000
LAN Test	—	0x0708
X.25 Level3	X.25	0x0805
Banyan	—	0x0BAD
CDP	—	0x2000
DEC XNS	XNS	0x6000
DEC MOP Dump/Load	—	0x6001
DEC MOP	MOP	0x6002
DEC LAT	LAT	0x6004
Ethertalk	—	0x809B
Appletalk ARP	Appletalk AARP	0x80F3
IPX 802.2	—	0x00E0
IPX 802.3	—	0x00FF
Novell IPX (old)	—	0x8137
Novell IPX (new)	IPX	0x8138
EAPOL (old)	—	0x8180
EAPOL (new)	—	0x888E
Telxon TXP	TXP	0x8729
Aironet DDP	DDP	0x872D
Enet Config Test	—	0x9000
NetBUI	—	0xF0F0

Table A-2 IP Protocols

Protocol	Additional Identifier	ISO Designator
dummy	—	0
Internet Control Message Protocol	ICMP	1
Internet Group Management Protocol	IGMP	2
Transmission Control Protocol	TCP	6
Exterior Gateway Protocol	EGP	8
PUP	—	12
CHAOS	—	16
User Datagram Protocol	UDP	17
XNS-IDP	IDP	22
ISO-TP4	TP4	29
ISO-CNLP	CNLP	80
Banyan VINES	VINES	83
Encapsulation Header	encap_hdr	98
Spectralink Voice Protocol	SVP Spectralink	119
raw	—	255

Table A-3 IP Port Protocols

Protocol	Additional Identifier	ISO Designator
TCP port service multiplexer	tcpmux	1
echo	—	7
discard (9)	—	9
systat (11)	—	11
daytime (13)	—	13
netstat (15)	—	15
Quote of the Day	qotd quote	17
Message Send Protocol	msp	18
ttytst source	chargen	19
FTP Data	ftp-data	20
FTP Control (21)	ftp	21
Secure Shell (22)	ssh	22
Telnet	—	23
Simple Mail Transport Protocol	SMTP mail	25
time	timserver	37
Resource Location Protocol	RLP	39
IEN 116 Name Server	name	42
whois	nicname 43	43
Domain Name Server	DNS domain	53
MTP	—	57
BOOTP Server	—	67
BOOTP Client	—	68
TFTP	—	69
gopher	—	70
rje	netrjs	77
finger	—	79
Hypertext Transport Protocol	HTTP www	80
ttylink	link	87
Kerberos v5	Kerberos krb5	88
supdup	—	95
hostname	hostnames	101

Table A-3 IP Port Protocols (continued)

Protocol	Additional Identifier	ISO Designator
TSAP	iso-tsap	102
CSO Name Server	cso-ns csnet-ns	105
Remote Telnet	rtelnet	107
Postoffice v2	POP2 POP v2	109
Postoffice v3	POP3 POP v3	110
Sun RPC	sunrpc	111
tap ident authentication	auth	113
sftp	—	115
uucp-path	—	117
Network News Transfer Protocol	Network News readnews nntp	119
USENET News Transfer Protocol	Network News readnews nntp	119
Network Time Protocol	ntp	123
NETBIOS Name Service	netbios-ns	137
NETBIOS Datagram Service	netbios-dgm	138
NETBIOS Session Service	netbios-ssn	139
Interim Mail Access Protocol v2	Interim Mail Access Protocol IMAP2	143
Simple Network Management Protocol	SNMP	161
SNMP Traps	snmp-trap	162
ISO CMIP Management Over IP	CMIP Management Over IP cmip-man CMOT	163
ISO CMIP Agent Over IP	cmip-agent	164
X Display Manager Control Protocol	xdmcp	177
NeXTStep Window Server	NeXTStep	178
Border Gateway Protocol	BGP	179
Prospero	—	191
Internet Relay Chap	IRC	194

Table A-3 IP Port Protocols (continued)

Protocol	Additional Identifier	ISO Designator
SNMP Unix Multiplexer	smux	199
AppleTalk Routing	at-rtmp	201
AppleTalk name binding	at-nbp	202
AppleTalk echo	at-echo	204
AppleTalk Zone Information	at-zis	206
NISO Z39.50 database	z3950	210
IPX	—	213
Interactive Mail Access Protocol v3	imap3	220
Unix Listserv	ulistserv	372
syslog	—	514
Unix spooler	spooler	515
talk	—	517
ntalk	—	518
route	RIP	520
timeserver	timed	525
newdate	tempo	526
courier	RPC	530
conference	chat	531
netnews	—	532
netwall	wall	533
UUCP Daemon	UUCP uucpd	540
Kerberos rlogin	klogin	543
Kerberos rsh	kshell	544
rfs_server	remotefs	556
Kerberos kadmin	kerberos-adm	749
network dictionary	webster	765
SUP server	supfilesrv	871
swat for SAMBA	swat	901
SUP debugging	supfiledbg	1127
ingreslock	—	1524
Prospero non-priveleged	prospero-np	1525
RADIUS	—	1812
Concurrent Versions System	CVS	2401
Cisco IAPP	—	2887
Radio Free Ethernet	RFE	5002

APPENDIX B

Supported MIBs

This appendix lists the Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) that the access point supports for this software release. The Cisco IOS SNMP agent supports SNMPv1, SNMPv2, and SNMPv3.

MIB List

- IEEE802dot11-MIB
- Q-BRIDGE-MIB
- P-BRIDGE-MIB
- CISCO-DOT11-LBS-MIB
- CISCO-DOT11-IF-MIB
- CISCO-WLAN-VLAN-MIB
- CISCO-IETF-DOT11-QOS-MIB
- CISCO-IETF-DOT11-QOS-EXT-MIB
- CISCO-DOT11-ASSOCIATION-MIB
- CISCO-L2-DEV-MONITORING-MIB
- CISCO-DDP-IAPP-MIB
- CISCO-IP-PROTOCOL-FILTER-MIB
- CISCO-SYSLOG-EVENT-EXT-MIB
- CISCO-TBRIDGE-DEV-IF-MIB
- BRIDGE-MIB
- CISCO-CDP-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-FLASH-MIB
- CISCO-IMAGE-MIB
- CISCO-MEMORY-POOL-MIB

- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-SMI-MIB
- CISCO-TC-MIB
- CISCO-SYSLOG-MIB
- CISCO-WDS-INFO-MIB
- ENTITY-MIB
- IF-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-SYSTEM-MIB
- OLD-CISCO-TS-MIB
- RFC1213-MIB
- RFC1398-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPv2-TC

Using FTP to Access the MIB Files

Follow these steps to obtain each MIB file by using FTP:

Step 1 Use FTP to access the server **ftp.cisco.com**.

Step 2 Log in with the username **anonymous**.

Step 3 Enter your e-mail username when prompted for the password.

Step 4 At the `ftp>` prompt, change directories to **/pub/mibs/v1** or **/pub/mibs/v2**.

Step 5 Use the **get** *MIB_filename* command to obtain a copy of the MIB file.

Note You can also access information about MIBs on the Cisco web site: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

APPENDIX C

Error and Event Messages

This appendix lists the CLI error and event messages.

Conventions

System error messages are displayed in the format shown in Table C-1.

Table C-1 System Error Message Format

Message Component	Description	Example
Error identifier	A string categorizing the error.	STATION-ROLE
Software component	A string identifying the software component of the error.	AUTO_INSTALL
Severity Level	A numerical string indicating the severity of the error.	0-LOG-EMERG—emergency situation, nothing is functional 1-LOG-ALERT—alerts user to a very serious problem 2-LOG-CRIT—warns of a possible serious critical error 3-LOG-ERR—warning of error condition, most features functional; user should exercise care 4-LOG-WARNING—warning that user can ignore if they prefer 5-LOG-NOTICE—notice that may be of concern to user 6-LOG-INFO—informational (not serious) 7-LOG-DEBUG—debug information (not serious)
Action Flags	Internal to the code for which additional action is displayed.	0—No action flag MSG-TRACEBACK—includes traceback with message MSG-PROCESS—includes process information with message MSG-CLEAR—indicates condition had cleared MSG-SECURITY—indicates as security message MSG-NOSCAN—suppresses EEM pattern screening
%d	An integer number.	2450
%e	A MAC address.	000b.fcff.b04e
%s	A message string which provides more detail of the error.	"Attempt to protect port 1640 failed."
%x	A hexadecimal number.	0x001

Software Auto Upgrade Messages

Error Message `SW-AUTO-UPGRADE-2-FATAL_FAILURE: "Attempt to upgrade software failed, software on flash may be deleted. Please copy software into flash.`

Explanation Auto upgrade of the software failed. The software on the flash might have been deleted. Copy software into the flash.

Recommended Action Copy software before rebooting the unit.

Error Message `SW-AUTO-UPGRADE-7-DHCP_CLIENT_FAILURE: "%s": Auto upgrade of the software failed."`

Explanation Auto upgrade of the software failed.

Recommended Action Make sure that the DHCP client is running.

Error Message `SW-AUTO-UPGRADE-7-DHCP_SERVER_FAILURE: "%s": Auto upgrade of the software failed."`

Explanation Auto upgrade of the software failed.

Recommended Action Make sure that the DHCP server is configured correctly.

Error Message `SW-AUTO-UPGRADE-7_BOOT_FAILURE: "%s": Auto upgrade of the software failed."`

Explanation Auto upgrade of the software failed.

Recommended Action Reboot the unit. If the message appears again, copy the error message exactly as it appears and report it to your technical support representative.

Error Message `DOT11-4-UPGRADE: "Send your company name and the following report to migrateapj52w52@cisco.com." The following AP has been migrated from J(j52) to U(w52) Regulatory Domain:AP name AP Model Ethernet MAC %s %s %e \U\Regulatory Doman`

Explanation A Japan regulatory domain field upgrade from J to U has been accomplished.

Recommended Action None.

Error Message `AUTO-INSTALL-4-STATION_ROLE: "%s": The radio is operating in automatic install mode."`

Explanation The radio is operating in automatic install mode.

Recommended Action Use the **station-role** configuration interface command to configure the radio for a role other than install mode.

Error Message `AUTO-INSTALL-4-IP_ADDRESS_DHCP: "The radio is operating in automatic install mode and has set ip address dhcp."`

Explanation The radio is operating in automatic install mode and is configured to receive an IP address through DHCP.

Recommended Action Use the **station-role** configuration interface command to configure the radio for a role other than install mode.

Error Message `AUTO-INSTALL-6_STATUS: "%s" %s. RSSI=-%d dBm.: "The radio is operating in install mode."`

Explanation The radio is operating in automatic install mode.

Recommended Action Use the **station-role** configuration interface command to configure the radio for a role other than install mode.

Error Message `AVR_IMAGE_UPDATE-7-UPDATE_COMPLETE: "The AVR "$d" firmware was successfully updated."`

Explanation The access point AVR firmware was successfully updated.

Recommended Action None.

Error Message `AVR_IMAGE_UPDATE-2-UPDATE_FAILURE: "The AVR "$d" firmware is not current. Update error: "$s"."`

Explanation The AVR firmware is not current and the update failed

Recommended Action Copy the error message and report it to your technical support representative.

Error Message `AVR_IMAGE_UPDATE-4-UPDATE_SKIPPED: "AVR "$d" update processing was skipped:"$s"."`

Explanation AVR update processing was skipped due to an error.

Recommended Action None.

Error Message `AVR_IMAGE_UPDATE-4-UPDATE_START: "The system is updating the AVR "$d" firmware. Please wait . . . "`

Explanation The system is updating the AVR firmware.

Recommended Action None.

Association Management Messages

Error Message `DOT11-3-BADSTATE: "%s %s ->%s."`

Explanation 802.11 association and management uses a table-driven state machine to keep track and transition an association through various states. A state transition occurs when an association receives one of many possible events. When this error occurs, it means that an association received an event that it did not expect while in this state.

Recommended Action The system can continue but may lose the association that generates this error. Copy the message exactly as it appears and report it to your technical service representative.

Error Message `DOT11-6-ASSOC: "Interface %s, Station %s e% %s KEY_MGMT (%s), MSGDEF_LIMIT_MEDIUM."`

Explanation The indicated station associated to an access point on the indicated interface.

Recommended Action None.

Error Message `DOT11-6-ADD: "Interface %s, Station %e associated to parent %e."`

Explanation The indicated station associated to the parent access point on the indicated interface.

Recommended Action None.

Error Message `DOT11-6-DISASSOC: Interface %s, Deauthenticating Station %e #s`

Explanation Station disassociated from the access point.

Recommended Action None.

Error Message `DOT11-6-ROAMED: "Station %e roamed to %e."`

Explanation The indicated station roamed to the indicated new access point.

Recommended Action None.

Error Message `DOT11-4-ENCRYPT_MISMATCH: "Possible encryption key mismatch between interface %s and station %e."`

Explanation The encryption setting of the indicated interface and indicated station may be mismatched.

Recommended Action Check the encryption configuration of this interface and the failing station to ensure that the configurations match.

Error Message `DOT11-4-DIVER_USED: Interface $s, Mcs rates 8-15 disabled due to only one transmit or recieve antenna enabled`

Explanation These rates require that at least 2 receive and transmit antennas be enabled.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl. Also perform a search of the Bug Toolkit http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl. If you still require assistance, open a case with the Technical Assistance Center via the Internet http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl, or contact your Cisco technical support representative and provide the representative with the gathered information.

Error Message `DOT11-4-NO_HT: Interface %s, Mcs rates disabled on vlan %d due to %s`

Explanation The correct configuration was not in use to allow the HT rates to be used.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Research and attempt to resolve the error using the Output Interpreter https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl. Also perform a search of the Bug Toolkit http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl. If you still require assistance, open a case with the Technical Assistance Center via the Internet http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl, or contact your Cisco technical support representative and provide the representative with the gathered information.

Error Message `DOT11-4-NO_MBSSID_BACKUP_VLAN: Backup VLANs cannot be configured if MBSSID is not enabled:"$s" not started`

Explanation To enable backup VLAN, MBSSID mode should be configured.

Recommended Action Configure MBSSID on the device.

Unzip Messages

Error Message `SOAP-4-UNZIP_OVERFLOW: “Failed to unzip %s, exceeds maximum uncompressed html size.”`

Explanation The HTTP server cannot retrieve a compressed file in response to an HTTP GET request because the file is too large for the buffers used in the uncompression process.

Recommended Action Make sure that the file is a valid HTML page. If it is, you need to copy an uncompressed version of the file into Flash to retrieve it through HTTP.

System Log Messages

Error Message `%DOT11-4-LOADING_RADIO: Interface [chars], loading the radio firmware ([chars])`

Explanation The radio has been stopped to load new firmware.

Recommended Action None.

Error Message `%LINEPROTO-5-UPDOWN: Line protocol on Interface [chars], changed state to [chars]`

Explanation The data link level line protocol has changed state.

Recommended Action None.

Error Message `%SYS-5-RESTART: System restarted --[chars]`

Explanation A reload or restart was requested.

Recommended Action Notification message only. None.

Error Message `%SYS-5-CONFIG_I: Configured from [chars] by [chars]`

Explanation The router configuration has been changed.

Recommended Action This is a notification message only. None.

Error Message `%LINEPROTO-5-UPDOWN: Line protocol on Interface [chars], changed state to [chars]`

Explanation The data link level line protocol has changed state on the interface shown.

Recommended Action None.

Error Message `%SNMP-5-COLDSTART: SNMP agent on host [chars] is undergoing a cold start`

Explanation The SNMP server completed a coldstart.

Recommended Action Notification message only. None.

Error Message `%SYS-6-CLOCKUPDATE: System clock has been updated from [chars] to [chars], configured from [chars] by [chars].`

Explanation The system clock has been modified.

Recommended Action This is an informational message only. None.

802.11 Subsystem Messages

Error Message `DOT11-6-FREQ_USED: "Interface %s, frequency %d selected."`

Explanation After scanning for an unused frequency, the indicated interface selected the displayed frequency.

Recommended Action None.

Error Message `DOT11-4-NO-VALID_INFRA_SSID: "No infrastructure SSID configured. %s not started."`

Explanation No infrastructure SSID was configured and the indicated interface was not started.

Recommended Action Add at least one infrastructure SSID to the radio configuration.

Error Message `DOT11-4-VERSION_UPGRADE: "Interface %d, upgrading radio firmware."`

Explanation When starting the indicated interface, the access point found the wrong firmware version. The radio will be loaded with the required version.

Recommended Action None.

Error Message `DOT11-2-VERSION_INVALID: "Interface %d, unable to find required radio version %x.%x/ %d/`

Explanation When trying to re-flash the radio firmware on the indicated interface, the access point recognized that the indicated radio firmware packaged with the Cisco IOS software had the incorrect version.

Recommended Action None.

Error Message `DOT11-3-RADIO_OVER_TEMPERATURE: "Interface %s Radio over temperature detected."`

Explanation The radio's internal temperature exceeds maximum limits on the indicated radio interface.

Recommended Action Take steps necessary to reduce the internal temperature. These steps will vary based on your specific installation.

Error Message `DOT11-6-RADIO_TEMPERATURE_NORMAL: "Interface %s radio temperature returned to normal."`

Explanation The radio's internal temperature has returned to normal limits on the indicated radio interface.

Recommended Action None.

Error Message `DOT11-3-TX_PWR_OUT_OF_RANGE: "Interface %s Radio transmit power out of range."`

Explanation The transmitter power level is outside the normal range on the indicated radio interface.

Recommended Action Remove unit from the network and service.

Error Message `DOT11-3-RADIO_RF_LO: "Interface %s Radio cannot lock RF freq."`

Explanation The radio phase lock loop (PLL) circuit is unable to lock the correct frequency on the indicated interface.

Recommended Action Remove unit from network and service.

Error Message `DOT11-3-RADIO_IF_LO: "Interface %s Radio cannot lock IF freq."`

Explanation The radio intermediate frequency (IF) PLL is unable to lock the correct frequency on the indicated interface.

Recommended Action Remove unit from network and service.

Error Message `DOT11-6-FREQ_SCAN: "Interface %s Scanning frequencies for %d seconds."`

Explanation Starting a scan for a least congested frequency on the interface indicated for a the time period indicated.

Recommended Action None.

Error Message `DOT11-2-NO_CHAN_AVAIL: "Interface %s, no channel available."`

Explanation No frequency is available, likely because RADAR has been detected within the previous 30 minutes.

Recommended Action None.

Error Message `DOT11-6-CHAN_NOT_AVAIL: "DFS configured frequency %d Mhz unavailable for %d minute(s).`

Explanation Radar has been detected on the current channel. Dynamic Frequency Selection (DFS) regulations require no transmission for 30 seconds on the channel.

Recommended Action None.

Error Message `DOT11-6-DFS_SCAN_COMPLETE: "DFS scan complete on frequency %d MHz."`

Explanation The device has completed its Dynamic Frequency Scan (DFS) frequency scanning process on the displayed frequency.

Recommended Action None.

Error Message `DOT11-6-DFS_SCAN_START: "DFS: Scanning frequency %d MHz for %d seconds."`

Explanation The device has begun its DFS scanning process.

Recommended Action None.

Error Message `DOT11-6-DFS_TRIGGERED: "DFS: triggered on frequency %d MHz."`

Explanation DFS has detected RADAR signals on the indicated frequency.

Recommended Action None. The channel will be placed on the non-occupancy list for 30 minutes and a new channel will be selected.

Error Message `DOT11-4-DFS_STORE_FAIL: "DFS: could not store the frequency statistics."`

Explanation A failure occurred writing the DFS statistics to flash.

Recommended Action None.

Error Message `DOT11-4-NO_SSID: "No SSIDs configured, %d not started."`

Explanation All SSIDs were deleted from the configuration. At least one must be configured for the radio to run.

Recommended Action Configure at least one SSID on the access point.

Error Message `DOT11-4-NO_SSID_VLAN: "No SSID with VLAN configured. %s not started."`

Explanation No SSID was configured for a VLAN. The indicated interface was not started.

Recommended Action At least one SSID must be configured per VLAN. Add at least one SSID for the VLAN on the indicated interface.

Error Message `DOT11-4-NO_MBSSID_VLAN: "No VLANs configured in MBSSID mode. %s not started."`

Explanation No VLAN configured in MBSSID mode. The indicated interface was not started.

Recommended Action Add at least one SSID with the VLAN on the indicated interface configuration.

Error Message `DOT11-4-NO_MBSSID_SHR_AUTH: "More than 1 SSID with shared authentication method in non-MBSSID mode % is down".`

Explanation Not more than 1 SSID can have shared authentication method when MBSSID is not enabled.

Recommended Action Remove Dot11Radio radio interface or change authentication mode for SSID to open configuration.

Error Message `DOT114-NO_MBSSID_BACKUP_VLAN: "Backup VLANs cannot be configured if MBSSID is not enabled. %s not started.`

Explanation To enable a backup VLAN, MBSSID mode should be configured.

Recommended Action Configure MBSSID on the device.

Error Message `IF-4-MISPLACED_VLAN_TAG: "Detected a misplaced VLAN tag on source Interface %. Dropping packet.`

Explanation Received an 802.1Q VLAN tag was detected on the indicated interface which could not be parsed correctly. The received packet was encapsulated or deencapsulated incorrectly.

Recommended Action None.

Error Message `DOT11-2-FW_LOAD_NET: "Interface %s cannot load on boot. Place image in flash root directory and reload."`

Explanation The radio images cannot be loaded from a network when the access point boots.

Recommended Action Place the image on the root directory of the flash file system.

Error Message `DOT11-4-FW_LOAD_DELAYED: "Interface %s, network filesys not ready. Delaying firmware (%s) load."`

Explanation The network filesystem was not running or not ready when trying to flash new firmware into the indicated interface. Loading the identified firmware file has been delayed.

Recommended Action Make sure the network is up and ready before attempting to reflash the new firmware.

Error Message `DOT11-3-FLASH_UNKNOWN_RADIO: "Interface %s has an unknown radio."`

Explanation The radio type could not be determined when the user attempted to flash new firmware into the indicated interface.

Recommended Action Reboot the system and see if the firmware upgrade completes.

Error Message `DOT11-4-UPLINK_ESTABLISHED: "Interface %s associated to AP %s %e %s.`

Explanation The indicated repeater has associated to the indicated root access point. Clients can now associate to the indicated repeater and traffic can pass.

Recommended Action None.

Error Message `DOT11-2-UPLINK_FAILED: "Uplink to parent failed: %s."`

Explanation The connection to the parent access point failed for the displayed reason. The uplink will stop its connection attempts.

Recommended Action Try resetting the uplink interface. Contact Technical Support if the problem persists.

Error Message `DOT11-4-CANT_ASSOC: "Interface %, cannot associate %s."`

Explanation The indicated interface device could not associate to an indicated parent access point.

Recommended Action Check the configuration of the parent access point and this unit to make sure there is a match.

Error Message `DOT11-4-CANT_ASSOC: "Interface Dot11Radio 0, cannot associate."`

Explanation Parent does not support client MFP. This error message displays on the access point only in workgroup bridge, repeater, or non-root bridge mode and is seen if the WGB, repeater, or non-root is configured with Client MFP SD required (or mandatory) but root Client MFP is disabled.

Recommended Action Check the configuration of the parent access point and this unit to make sure there is a match.

Error Message `DOT11-2-PROCESS_INITIALIZATION_FAILED: "The background process for the radio could not be started: %s)`

Explanation The initialization process used by the indicated interface failed for some reason, possibly a transient error.

Recommended Action Perform a reload of the access point. If this fails to rectify the problem, perform a power cycle. If this still fails, try downgrading the access point firmware to the previous version.

Error Message `DOT11-2-RADIO_HW_RESET: "Radio subsystem is undergoing hardware reset to recover from problem."`

Explanation An unrecoverable error occurred that could not be resolved by a soft reset.

Recommended Action None.

Error Message `DOT11-2-RESET_RADIO: "Interface %s, Radio %s, Trying hardware reset on radio."`

Explanation Using a software reset to start a radio failed. Trying a hardware reset which will reset all radios on the unit.

Recommended Action None.

Error Message `DOT11-4-MAXRETRIES: "Packet to client %e reached max retries, removing the client."`

Explanation The maximum packet send retry limit has been reached and the client is being removed. This error message indicates that the access point attempts to poll the client a certain number of times, but does not receive a response. Therefore, the client is removed from the association table. This issue is commonly seen when the client and access point are attempting to communicate in a noisy RF environment.

Recommended Action To resolve this issue, see if a snapshot reveals noise in the radio spectrum by trying to run a carrier busy test on the access point. Attempt to alleviate any unwanted noise. For more information, see the "Performing a Carrier Busy Test" procedure on page 6-34. If there are several access points in the same area, they could be overlapping the channel signal or with any other wireless device in the surrounding area. Change the channels under Network Interfaces and select Radio-802.11. There are three non-overlapping channels: 1, 6, and 11.

Error Message `DOT11-4-RM_INCAPABLE: "Interface %s`

Explanation Indicated interface does not support the radio management feature.

Recommended Action None.

Error Message `DOT11-4-RM_INCORRECT_INTERFACE: "Invalid interface, either not existing or non-radio."`

Explanation A radio management request discovered that the interface either does not exist or is not a radio interface.

Recommended Action None.

Error Message `DOT11-3-POWERS_INVALID: "Interface %s, no valid power levels available."`

Explanation The radio driver found no valid power level settings.

Recommended Action Investigate and correct the power source and settings.

Error Message `DOT11-4-RADIO_INVALID_FREQ: "Operating frequency (%d) invalid - performing a channel scan."`

Explanation The indicated frequency is invalid for operation. A channel scan is being performed to select a valid frequency.

Recommended Action None.

Error Message `DOT11-4-RADIO_NO_FREQ: "Interface &s, all frequencies have been blocked, interface not started."`

Explanation The frequencies set for operation are invalid and a channel scan is being forced in order to select a valid operating frequency.

Recommended Action None.

Error Message `DOT11-4-BCN_BURST_NO_MBSSID: "Beacon burst mode is enabled but MBSSID is not enabled, %s is down."`

Explanation Beacon burst mode can only be enabled when MBSSID is enabled on the indicated interface.

Recommended Action Enable the MBSSID or disable beacon bursting on the indicated interface.

Error Message `DOT11-4-BCN_BURST_TOO_MANY_DTIMS: "Beacon burst mode is enabled and there are too many different DTIM periods defined. %s is down.`

Explanation Beacon burst mode can only support up to 4 unique DTIM values, each with a maximum of 4 BSSes.

Recommended Action Change the number of unique DTIMs on the SSIDs configured for the interface to a more reasonable set of values.

Error Message `DOT11-2-RADIO_INITIALIZATION_ERROR: "The radio subsystem could not be initialized (%s)."`

Explanation A critical error was detected while attempting to initialize the radio subsystem.

Recommended Action Reload the system.

Error Message `DOT11-4-UPLINK_NO_ID_PWD: "Interface %s, no username/password supplied for uplink authentication."`

Explanation The user failed to enter a username and/or password.

Recommended Action Enter the username and/or password and try again.

Error Message `DOT11-5-NO_IE_CFG: "No IEs configured for %s (ssid index %u)."`

Explanation When attempting to apply a beacon or probe response to the radio, the beacon or probe was undefined on the indicated SSID index.

Recommended Action Check the IE configuration.

Error Message `DOT11-4-FLASHING_RADIO: "Interface %s, flashing radio firmware (%s)."`

Explanation The indicated interface radio has been stopped to load the indicated new firmware.

Recommended Action None.

Error Message `DOT11-4-LOADING_RADIO: "Interface %s, loading the radio firmware (%s)."`

Explanation The indicated interface radio has been stopped to load new indicated firmware.

Recommended Action None.

Error Message `DOT11-2-NO_FIRMWARE: "Interface %s, no radio firmware file (%s) was found."`

Explanation When trying to flash new firmware, the file for the radio was not found in the Flash file system. Or, the IOS on the access point is corrupt.

Recommended Action The wrong image has been loaded into the unit. Locate the correct image based on the type of radio used. To resolve this issue you may have to reload the access point with a new Cisco IOS image. Instructions for reloading an image are found in "Reloading the Access Point Image" section on page 24-6.

If the IOS on the access point is corrupt, reload the access point image using the Mode button method. Refer to the "Using the MODE Button" section on page 24-4.

Error Message `DOT11-2-BAD_FIRMWARE: "Interface %s, radio firmware file (%s) is invalid."`

Explanation When trying to Flash new firmware into the indicated interface the indicated radio firmware file was found to be invalid.

Recommended Action Make sure the correct firmware image file is located in the place where the unit expects to find it.

Error Message `DOT11-2-RADIO_FAILED: "Interface %s, failed - %s."`

Explanation The radio driver on the indicated interface found a severe error and is shutting down for the indicated reason.

Recommended Action None.

Error Message `DOT11-4-FLASH_RADIO_DONE: "Interface %s, flashing radio firmware completed."`

Explanation The indicated interface radio firmware flash is complete, and the radio will be restarted with the new firmware.

Recommended Action None.

Error Message `DOT11-4-UPLINK_LINK_DOWN: "Interface %s, parent lost: %s."`

Explanation The connection to the parent access point on the indicated interface was lost for the reason indicated. The unit will try to find a new parent access point.

Recommended Action None.

Error Message `DOT11-4-CANT_ASSOC: Cannot associate: $s`

Explanation The unit could not establish a connection to a parent access point for the displayed reason.

Recommended Action Verify that the basic configuration settings (SSID, WEP, and others) of the parent access point and this unit match.

Error Message `DOT11-4-CLIENT_NOT_FOUND: "Client was not found."`

Explanation Client was not found while checking mic.

Recommended Action None.

Error Message `DOT11-4-MAXRETRIES: Packet to client [mac] reached max retries, remove the client`

Explanation A packet sent to the client has not been successfully delivered many times, and the max retries limit has been reached. The client is deleted from the association table.

Recommended Action None.

Error Message `DOT11-4-BRIDGE_LOOP: "Bridge loop detected between WGB %e and device %e."`

Explanation The indicated workgroup bridge reported the address of one of its indicated Ethernet clients and the access point already had that address marked as being somewhere else on the network.

Recommended Action Click **Refresh** on the Associations page on the access point GUI, or enter the **clear dot11 statistics** command on the CLI.

Error Message `DOT11-4-ANTENNA_INVALID: "Interface %s, current antenna position not supported, radio disabled."`

Explanation The Indicated AIR-RM21A radio module does not support the high-gain position for the external antenna (the high-gain position is folded flat against the access point). The access point automatically disables the radio when the antenna is in the high-gain position.

Recommended Action Fold the antenna on the AIR-RM21A radio module so that it is oriented 90 degrees to the body of the access point.

Error Message `DOT11-6-ANTENNA_GAIN: "Interface %s, antenna position/gain changed, adjusting transmitter power."`

Explanation The antenna gain has changed so the list of allowed power levels must be adjusted.

Recommended Action None.

Error Message `DOT11-4-DIVER_USED: "Interface %s Mcs rates 8-15 disabled due to only one transmit or receive antenna enabled."`

Explanation The rates listed require at least 2 receive or transmit antennas be enabled.

Recommended Action Install and enable at least 2 receive or transmit antennas on the access point.

Error Message `DOT11-3-RF-LOOPBACK_FAILURE: "Interface %s Radio failed to pass RF loopback test."`

Explanation Radio loopback test failed for the interface indicated.

Recommended Action None.

Error Message `DOT11-3-RF-LOOPBACK_FREQ_FAILURE: "Interface %s failed to pass RF loopback test."`

Explanation Radio loopback test failed at a given frequency for the indicated interface.

Recommended Action None.

Error Message `DOT11-7-AUTH_FAILED: "Station %e Authentication failed"`

Explanation The indicated station failed authentication.

Recommended Action Verify that the user entered the correct username and password, and verify that the authentication server is online.

Error Message `DOT11-7-CCKM_AUTH_FAILED: "Station %e CCKM authentication failed."`

Explanation The indicated station failed CCKM authentication.

Recommended Action Verify that the topology of the access points configured to use the WDS access point is functional.

Error Message `DOT11-4-CCMP_REPLAY: "AES-CCMP TSC replay was detected on packet (TSC 0x%11x received from &e)."`

Explanation AES-CCMP TSC replay was indicated on a frame. A replay of the AES-CCMP TSC in a received packet almost indicates an active attack.

Recommended Action None.

Error Message `DOT11-4-CKIP_MIC_FAILURE: "CKIP MIC failure was detected on a packet (Digest 0x%x) received from %e)."`

Explanation CKIP MIC failure was detected on a frame. A failure of the CKIP MIC in a received packet almost indicates an active attack.

Recommended Action None.

Error Message `DOT11-4-CKIP_REPLAY: "CKIP SEQ replay was detected on a packet (SEQ 0x&x) received from %e."`

Explanation CKIP SEQ replay was detected on a frame. A replay of the CKIP SEQ in a received packet almost indicates an active attack."

Recommended Action None.

Error Message `DOT11-4-TKIP_MIC_FAILURE: "Received TKIP Michael MIC failure report from the station %e on the packet (TSC=0x%11x) encrypted and protected by %s key."`

Explanation TKIP Michael MIC failure was detected from the indicated station on a unicast frame decrypted locally with the indicated pairwise key.

Recommended Action A failure of the Michael MIC in a received packet might indicate an active attack on your network. Search for and remove potential rogue devices from your wireless LAN. This failure might also indicate a misconfigured client or a faulty client.

Error Message `DOT11-4-TKIP_MIC_FAILURE_REPORT: "Received TKIP Michael MIC failure report from the station %e on the packet (TSC=0x0) encrypted and protected by %s key`

Explanation The access point received an EAPOL-key from the indicated station notifying the access point that TKIP Michael MIC failed on a packet transmitted by this access point.

Recommended Action None.

Error Message `DOT11-3-TKIP_MIC_FAILURE_REPEATED: "Two TKIP Michael MIC failures were detected within %s seconds on %s interface. The interface will be put on MIC failure hold state for next %d seconds"`

Explanation Two TKIP Michael MIC failures were detected within the indicated time on the indicated interface. Because this usually indicates an active attack on your network, the interface will be put on hold for the indicated time. During this hold time, stations using TKIP ciphers are disassociated and cannot reassociate until the hold time ends. At the end of the hold time, the interface operates normally.

Recommended Action MIC failures usually indicate an active attack on your network. Search for and remove potential rogue devices from your wireless LAN. If this is a false alarm and the interface should not be on hold this long, use the **countermeasure tkip hold-time** command to adjust the hold time.

Error Message `DOT11-4-TKIP_REPLAY: "TKIP TSC replay was detected on a packet (TSC 0x%ssx received from %e)."`

Explanation TKIP TSC replay was detected on a frame. A replay of the TKIP TSC in a received packet almost indicates an active attack.

Recommended Action None.

Error Message `DOT11-4-WLAN_RESOURCE_LIMIT: "WLAN limit exceeded on interface %s and network-id %d."`

Explanation This access point has reached its limit of 16 VLANs or WLANs.

Recommended Action Unconfigure or reduce static VLANS if access point is trying to associate with RADIUS assigned Network-ID turned on.

Error Message `SOAP-3-WGB_CLIENT_VLAN_SOAP: "Workgroup Bridge Ethernet client VLAN not configured."`

Explanation No VLAN is configured for client devices attached to the workgroup bridge.

Recommended Action Configure a VLAN to accommodate client devices attached to the workgroup bridge.

Error Message `DOT11-4-NO_VLAN_NAME: "VLAN name %s from RADIUS server is not configured for station %e."`

Explanation The VLAN name returned by the RADIUS server must be configured in the access point.

Recommended Action Configure the VLAN name in the access point.

Error Message `DOT11-4-NO_VLAN_ID: "VLAN id %d from Radius server is not configured for station %e."`

Explanation The VLAN ID returned by the Radius server must be configured on the access point.

Recommended Action Configure the VLAN ID on the access point.

Error Message `SOAP-3-ERROR: "Reported on line %d in file %s.%s."`

Explanation An internal error occurred on the indicated line number in the indicated filename in the controller ASIC.

Recommended Action None.

Error Message `SOAP_FIPS-2-INIT_FAILURE: "SOAP FIPS initialization failure: %s."`

Explanation SOAP FIPS initialization failure.

Recommended Action None.

Error Message `SOAP_FIPS-4-PROC_FAILURE: "SOAP FIPS test failure: %s."`

Explanation SOAP FIPS test critical failure.

Recommended Action None.

Error Message `SOAP_FIPS-4-PROC_WARNING: "SOAP FIPS test warning: %s."`

Explanation SOAP FIPS test non-critical failure.

Recommended Action None.

Error Message `SOAP_FIPS-2-SELF_TEST_IOS_FAILURE: "IOS crypto FIPS self test failed at %s."`

Explanation SOAP FIPS self test on IOS crypto routine failed.

Recommended Action Check IOS image.

Error Message `SOAP_FIPS-2-SELF_TEST_RAD_FAILURE: "RADIO crypto FIPS self test failed at %s on interface %s %d."`

Explanation SOAP FIPS self test on radio crypto routine failed.

Recommended Action Check radio image.

Error Message `SOAP_FIPS-2-SELF_TEST_IOS_SUCCESS: "IOS crypto FIPS self test passed."`

Explanation SOAP FIPS self test passed.

Recommended Action None.

Error Message `SOAP_FIPS-2-SELF_TEST_RAD_SUCCESS: "RADIO crypto FIPS self test passed on interface %s %d."`

Explanation SOAP FIPS self test passed on a radio interface.

Recommended Action None.

Error Message `DOT11-6-MCAST_DISCARD: "%s mode multicast packets are discarded in %s multicast mode."`

Explanation The access point configured as a workgroup bridge and drops infrastructure mode multicast packets in client mode and drops client mode multicast packets in infrastructure mode.

Recommended Action None.

Inter-Access Point Protocol Messages

Error Message `DOT11-6-STANDBY_ACTIVE: "Standby to Active, Reason = %s (%d)."`

Explanation The access point is transitioning from standby mode to active mode for the indicated reason.

Recommended Action None.

Error Message `DOT11-6-STANDBY_REQUEST: "Hot Standby request to shutdown radios from %e."`

Explanation The indicated standby access point has requested that this access point shut down its radio interfaces because a failure has been detected on one of this access point's radio interfaces.

Recommended Action None.

Error Message `DOT11-6-ROGUE_AP: "Rogue AP %e reported. Reason: %s."`

Explanation A station has reported a potential rogue access point for the indicated reason.

Recommended Action None.

Local Authenticator Messages

Error Message `RADSRV-4-NAS_UNKNOWN: Unknown authenticator: [ip-address]`

Explanation The local RADIUS server received an authentication request but does not recognize the IP address of the network access server (NAS) that forwarded the request.

Recommended Action Make sure that every access point on your wireless LAN is configured as a NAS on your local RADIUS server.

Error Message `RADSRV-4-NAS_KEYMIS: NAS shared key mismatch.`

Explanation The local RADIUS server received an authentication request but the message signature indicates that the shared key text does not match.

Recommended Action Correct the shared key configuration on either the NAS or on the local RADIUS server.

Error Message `RADSRV-4_BLOCKED: Client blocked due to repeated failed authentications`

Explanation A user failed authentication the number of times configured to trigger a block, and the account been disabled.

Recommended Action Use the **clear radius local-server user** *username* privileged EXEC command to unblock the user, or allow the block on the user to expire by the configured lockout time.

Error Message

Error Message `DOT1X-SHIM-6-AUTH_OK: "Interface %s authenticated [%s]."`

Explanation The 802.1x authentication was successful.

Recommended Action None.

Error Message `DOT1X-SHIM-3-AUTH_FAIL: "Interface %s authentication failed."`

Explanation The 802.1x authentication failed to the attached device.

Recommended Action Check the configuration of the 802.1x credentials on the client as well as the RADIUS server.

Error Message `DOT1X-SHIM-3-INIT_FAIL: "Unable to init - %s."`

Explanation An error occurred during the initialization of the shim layer.

Recommended Action

Error Message `DOT1X-SHIM-3-UNSUPPORTED_KM: "Unsupported key management: %X."`

Explanation Am error occurred during the initialization of the shim layer. An unsupported key management type was found.

Recommended Action None.

Error Message `DPT1X-SHIM-4-PLUMB_KEY_ERR: "Unable to plumb keys - %s."`

Explanation An unexpected error occurred when the shim layer tried to plumb the keys.

Recommended Action None.

Error Message `DOT1X-SHIM-3-PKT_TX_ERR: "Unable to tx packet -%s."`

Explanation An unexpected error occurred when the shim layer tried to transmit the dot1x packet.

Recommended Action None.

Error Message `DOT1X-SHIM-3-ENCAP_ERR: "Packet encap failed for %e."`

Explanation An unexpected error occurred when the shim layer tried to transmit the dot1x packet. The packet encapsulation failed.

Recommended Action None.

Error Message `DOT1X-SHIM-3-SUPP_START_FAIL: "Unable to start supplicant on %s."`

Explanation An unexpected error occurred when the shim layer tried to start the dot1x suppliant on the indicated interface.

Recommended Action None.

Error Message `DOT1X-SHIM=3-NO_UPLINK: "No uplink found for %s."`

Explanation While processing a dot1x event or message on a dot11 interface, a situation was encountered where an uplink was expected, but not found.

Recommended Action None.

Error Message `Information Group rad_acct: Radius server <ip address> is responding again (previously dead). Error Group acct: No active radius servers found. Id 106`

Explanation This message is seen if the **radius-server deadtime 10** command is configured on the access point.This command is configured to set an interval during which the access point does not attempt to use servers that do not respond. Thus avoids the time needed to wait for a request to time out before trying the next configured server. A Radius server marked as dead is skipped by additional requests for the duration of the minutes unless all servers are marked dead. Configuring dead time for 10 minutes means that the server cannot be used for 10 minutes.

Recommended Action You can disable this command if you want this log to disappear. Actually this message is not really a major problem, it is just an informational log.

WDS Messages

Error Message `WLCCP-WDS-6-REPEATER_STOP: WLCCP WDS on Repeater unsupported, WDS is disabled.`

Explanation Repeater access points do not support WDS.

Recommended Action None.

Error Message `WLCCP-WDS-6-PREV_VER_AP: A previous version of AP is detected.`

Explanation The WDS device detected a previous version of the access point.

Recommended Action None.

Error Message `WLCCP-AP-6-INFRA: WLCCP Infrastructure Authenticated`

Explanation The access point successfully authenticated to the WDS device.

Recommended Action None.

Error Message `WLCCP-AP-6-STAND_ALONE: Connection lost to WLCCP server, changing to Stand-Alone Mode`

Explanation The access point lost its connection to the WDS device and is in stand-alone mode.

Recommended Action None.

Error Message `WLCCP-AP-6-PREV_VER_WDS: A previous version of WDS is detected`

Explanation The access point detected a previous version of WDS.

Recommended Action Check for an unsupported version of WDS on your network.

Error Message `WLCCP-AP-6-UNSUP_VER_WDS: An unsupported version of WDS is detected`

Explanation The access point detected an unsupported version of WDS.

Recommended Action Check for an unsupported version of WDS on your network.

Error Message `WLCCP-NM-3-WNM_LINK_DOWN: Link to WNM is down`

Explanation The network manager is not responding to keep-active messages.

Recommended Action Check for a problem with the network manager or with the network path to the network manager.

Error Message `WLCCP-NM-6-WNM_LINK_UP: Link to WNM is up`

Explanation The network manager is now responding to keep-active messages.

Recommended Action None.

Error Message `WLCCP-NM-6-RESET: Resetting WLCCP-NM`

Explanation A change in the network manager IP address or a temporary out-of-resource state might have caused a reset on the WDS network manager subsystem, but operation will return to normal shortly.

Recommended Action None.

Error Message `WLCCP-WDS-3-RECOVER: "%s`

Explanation WDS graceful recovery errors.

Recommended Action None.

Mini IOS Messages

Error Message `MTS-2-PROTECT_PORT_FAILURE: An attempt to protect port [number] failed`

Explanation Initialization failed on attempting to protect port.

Recommended Action None.

Error Message `MTS-2-SET_PW_FAILURE: Error %d enabling secret password.`

Explanation Initialization failed when the user attempted to enable a secret password.

Recommended Action None.

Error Message `Saving this config to nvram may corrupt any network management or security files stored at the end of nvram. Continue? [no]:`

Explanation This warning message displays on the access point CLI interface while saving configuration changes through the CLI. This is due to insufficient space in flash memory. When a radio crashes, .rcore files are created. These files indicate a firmware or a hardware problem in the radio, although a hardware problem is less likely.

Recommended Action This warning message can be prohibited by removing the rcore files generated in flash memory. The rcore files have a .rcore extension. The files can be deleted because they simply show that the radio went down at some point. The .rcore files can be listed on the CLI session and appear similar to this:

r15_5705_AB50_A8341F30.rcore

Access Point/Bridge Messages

Error Message `APBR-4-SEND_PCKT_FAILED:   Failed to Send Packet on port ifDescr (error= errornum)errornum: status error number`

```
HASH(0x2096974)
```

Explanation The access point or bridge failed to send a packet. This condition might be seen if there is external noise or interference.

Recommended Action Check for sources of noise or interference.

Error Message `APBR-6-DDP_CLNT_RESET:  Detected probable reset of hosthost: host MAC address HASH(0x2080f04)`

Explanation The access point or bridge detects that another infrastructre device has restarted.

Recommended Action If this message appears continuously, reboot the access point.

Cisco Discovery Protocol Messages

Error Message `CDP_PD-2-POWER_LOW: %s - %s %s (%e)`

Explanation The system is not supplied with sufficient power.

Recommended Action Reconfigure or replace the source of inline power.

External Radius Server Error Messages

Error Message `RADUYS:response-authenticator decrypt fail, paklen 32`

Explanation This error message means that there is a mismatch in the RADIUS shared key between the RADIUS server and the access point.

Recommended Action Make sure that the shared key used on the RADIUS server and the access point are the same.

LWAPP Error Messages

Error Message `LWAPP-3-CDP: Failure sending CDP Update to Controller. Reason "s"`

Explanation Could not send access point CDP update to controller

Recommended Action None.

Error Message `LWAPP-3-CLIENTERRORLOG: "s"`

Explanation This log message indicates an LWAPP client error event. The message is logged to help in troubleshooting LWAPP access point join problems.

Recommended Action None.

Error Message `LWAPP-3-CLIENTEVENTLOG: "s"`

Explanation This log message indicates an LWAPP client notification event. The message is logged to help in troubleshooting LWAPP access point join problems.

Recommended Action None.

Error Message `LWAPP-3-UNSUPPORTEDRM: Got unsupported CCX RM Measurement "s" request "d" from Controller.`

Explanation Got unsupported CCX radio managment measurement request from controller.

Recommended Action None.

Error Message `LWAPP-5-WRONG_DFS_SLOT: DFS action on non-DFS radio "d"`

Explanation DFS action on radio b/g

Recommended Action None.

Sensor Messages

Error Message `SENSOR-3-TEMP_CRITICAL: System sensor "d" has exceeded CRITCAL temperature thresholds`

Explanation One of the measured environmental test points exceeds the extreme threshold.

Recommended Action Correct the specified condition, or the system may shut itself down as a preventive measure. Enter the **show environment all** to help determine if this is due to temperature or volatage condition. If this is a critical temperature warning, please ensure that the router fans are are operating and that the room cooling and air-conditioning are functioning. This condition could cause the system to fail to operate properly.

Error Message `SENSOR-3-TEMP_NORMAL: "s" temperature sensor is now normal`

Explanation One of the measured environmental test points is under normal operating temperature.

Recommended Action None.

Error Message `SENSOR-3-TEMP_SHUTDOWN: Shuting down the system because of dangerously HIGH temperature at sensor "d".`

Explanation One of the measured environmental test points exceeds the operating temperature environment of the router.

Recommended Action Investigate the cause of the high temperature.

Error Message `SENSOR-3-TEMP_WARNING: "s" temparature sensor "d" has exceeded WARNING temperature thresholds`

Explanation One of the measured environmental test points exceeds the warning threshold.

Recommended Action Closely monitor the condition and correct if possible, by cooling the environment.

Error Message `SENSOR-3-VOLT_CRITICAL: System sensor "d" has exceeded CRITCAL voltage thresholds`

Explanation One of the measured environmental test points exceeds the extreme voltage threshold.

Recommended Action Correct the specified condition, or the system may shut itself down as a preventive measure. Enter the **show environment all** to help determine if this is due to volatage condition. This condition could cause the system to fail to operate properly.

Error Message `SENSOR-3-VOLT_NORMAL: System sensor "d"("d") is now operating under NORMAL voltage`

Explanation One of the measured environmental test points is under normal operating voltage.

Recommended Action None.

Error Message `SENSOR-3-VOLT_WARNING: Voltage monitor "d"("d") has exceeded voltage thresholds`

Explanation One of the measured voltage test points indicates that voltage is out of normal range.

Explanation Check Power Supplies or contact TAC

SNMP Error Messages

Error Message `SNMP-3-AUTHFAILIPV6: Authentication failure for SNMP request from host`Unrecognized format ' %P'

Explanation An SNMP request was sent by this host which was not properly authenticated.

Recommended Action Make sure that the community/user name used in the SNMP req has been configured on the router.

Error Message `SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full`

Explanation Snmp packet dropped due to input queue full error

Recommended Action Use the command **show snmp** to see the number of packets dropped. Stop any SNMP access to the device until the error condition is recovered.

Error Message `SNMP-3-INTERRUPT_CALL_ERR: "s" function, cannot be called from interrupt handler`

Explanation This message indicates that a call has been made to the function from an interrupt handler. This is not permitted because it will fail and device will reboot down the stack in malloc call.

Recommended Action If this messages recurs, copy it exactly as it appears and report it to your technical support representative.

Error Message SNMP-4-NOENGINEIDV6: Remote snmpEngineID for Unrecognized format ‘ %P’ not found when creating user: “s”

Explanation An attempt to create a user failed.This is likely because the engine ID of the remote agent (or SNMP manager) was not configured.

Recommended Action Configure the remote snmpEngineID and reconfigure the user. If the problem persists, copy the error message exactly as it appears, and report it to your technical support representative.

Error Message SNMP_MGR-3-MISSINGHOSTIPV6: Cannot locate information on SNMP informs host:Unrecognized format ‘ %P’

Explanation A table entry for the mentioned SNMP informs destination cannot be found. As a result, inform notifications will not be sent to this destination.

Recommended Action Run the **show snmp host** and **show snmp** commands. Copy the error message and output from the show commands exactly as they appear, and report it to your technical support representative. Deleting and re-adding the informs destination via the **snmp-server host** configuration command may clear the condition. Otherwise, reloading the system may be necessary.

SSH Error Messages

Error Message SSH-5-SSH2_CLOSE: SSH2 Session from ”%s” (tty = “%d”) for user ’”%s”’ using crypto cipher ’”%s”’, hmac ’”%s”’ closed

Explanation The SSH Session closure information

Recommended Action None - informational message

Error Message SSH-5-SSH2_SESSION: SSH2 Session request from ”%s” (tty = “%d”) using crypto cipher ’”%s”’, hmac ’”%s”’ ”%s”

Explanation The SSH session request information

Recommended Action None - informational message

Error Message SSH-5-SSH2_USERAUTH: User ’”%s”’ authentication for SSH2 Session from ”%s” (tty = “%d”) using crypto cipher ’”%s”’, hmac ’”%s”’ ”%s”

Explanation The SSH user authentication status information

Recommended Action None - informational message

Error Message `SSH-5-SSH_CLOSE: SSH Session from “%s”(tty = “%d”) for user ’”%s”’ using crypto cipher ’”%s”’ closed`

Explanation The SSH Session closure information

Recommended Action None - informational message

Error Message `SSH-5-SSH_SESSION: SSH Session request from ”%s” (tty = “%d”) using crypto cipher ’”%s”’ ”%s”`

Explanation The SSH session request information

Recommended Action None - informational message

Error Message `SSH-5-SSH_USERAUTH: User ’”%s”’ authentication for SSH Session from ”%s” (tty = “%d”) using crypto cipher ’”%s”’ ”%s”`

Explanation The SSH user authentication status information

Recommended Action None - informational message