Cisco IOS Software Configuration Guide for Cisco Aironet Access Points

Cisco IOS Releases 12.4(3g)JA and 12.3(8)JEB
April 2007

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

Text Part Number: 0L-11350-01

Cisco IOS Software Configuration Guide for Cisco Aironet Access Points

CONTENTS

Preface

Audience

This guide is for the networking professional who installs and manages Cisco Aironet Access Points. 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 two Cisco IOS releases: 12.4(3g)JA and 12.3(8)JEB. Cisco IOS Release 12.4(3g)JA supports the following autonomous 32 Mb platforms:

- 1130 series access point
- 1240 series access point
- 1300 outdoor access point/bridge

Cisco IOS Release 12.3(8)JEB is a maintenance release and supports the following autonomous 16 Mb platforms:

- 1100 series access point
- 1200 series access point
- 1230 series access point

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**. On the Cisco Support Documentation home page, select **Release 12.4** from the Cisco IOS Software drop-down list.

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.

Organization

This guide is organized into these chapters:

Chapter 1, "Overview," lists the software and hardware features of the access point and describes the access point's 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, "Administering the Access PointWireless Device Access," 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, data rates, 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 Cipher Suites and WEP," 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 WDS, Fast Secure Roaming, Radio Management, and Wireless Intrusion Detection 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 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 System Message Logging," describes how to configure system message logging on your access point.

Chapter 22, "Wireless Device Troubleshooting," provides troubleshooting procedures for basic problems with the access point.

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:

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.

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.

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix "Translated Safety Warnings.")**

Waarschuwing **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.)**

Varoitus **Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)**

Attention **Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).**

Warnung **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)**

Avvertenza **Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).**

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").**

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)**

Related Publications

These documents provide complete information about the access point:

- *Quick Start Guide: Cisco Aironet 1100 Series Access Points*
- *Quick Start Guide: Cisco Aironet 1130AG Series Access Point*
- *Quick Start Guide: Cisco Aironet 1200 Series Access Points*
- *Quick Start Guide: Cisco Aironet 1240 Series Access Point*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*
- *Installation Instructions for Cisco Aironet Power Injectors*
- *Cisco Aironet 802.11g Radio Upgrade Instructions*
- *Release Notes for Cisco Aironet 1240 and 1300 Series Access Points for Cisco IOS Release 12.4(3g)JA*
- *Release Notes for Cisco Aironet 1100 and 1200 Series Access Points for Cisco IOS Release 12.3(8)JEB*
- *Cisco 1800 Series Routers Hardware Installation Guide*
- *Cisco AP HWIC Wireless Configuration Guide*
- *Cisco Router and Security Device Manager (SDM) Quick Start Guide*

Related documents from the Cisco TAC Web pages include:

- Antenna Cabling

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

CHAPTER 1

Overview

Cisco Aironet Access PointsCisco wireless devices (hereafter called *access points* or *wireless devices*) 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 pointwireless devices are Wi-Fi certified, 802.11a-compliant, 802.11b-compliant, and 802.11g-compliant wireless LAN transceivers.

An access pointwireless device 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 radio range of an access pointwireless device can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

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). Use the **interface dot11radio** global configuration CLI command to place the wireless device into the radio configuration mode.

Each access point platform contains one or two radios:

- The 1100 series access point uses a single, 802.11b, 2.4-GHz mini-PCI radio that can be upgraded to an 802.11g, 2.4-GHz radio.
- The 1130 series access point has integrated 802.11g and 802.11a radios and antennas.
- The 1200 series access point can contain two radios: a 2.4-GHz radio in an internal mini-PCI slot and a 5-GHz radio module in an external, modified cardbus slot. The 1200 series access point supports one radio of each type, but it does not support two 2.4-GHz or two 5-GHz radios.
- The 1230 series access point is pre-configured to include both an 802.11g and an 802.11a radio. It has antenna connectors for externally attached antennas for both radios.
- The 1240 series access point uses externally connected antennas for each band instead of built-in antennas.
- The 1300 series outdoor access point/bridge uses an integrated antenna and can be configured to use external, dual-diversity antennas.

This chapter provides information on the following topics:

Features

This section lists features supported on access pointWireless devices running Cisco IOS software.

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

Note Cisco IOS Release 12.3(8)JEB is a maintenance release only. No new features are included in this release.

Features Introduced in This Release

Table 1-1 lists the new features in Cisco IOS Release 12.4(3g)JA and the supported platforms.

Table 1-1 New Cisco IOS Software Features for Cisco IOS Release 12.4(3g)JA

Feature	Cisco Aironet 1240 Series Access Points	Cisco Aironet 1300 Series Outoor Access Point/Bridge	Cisco Aironet 1400 Series Wireless Bridge
Japan upgrade utility[1]	x	x	x
Multiple VLAN and rate limiting support for point-to-multipoint bridging	x	x	–
Universal workgroup bridge	x	x	–
Client MFP support	x	x	–
Regulatory changes for Taiwan	x	x	x

1. The utility also operates on 1130 series access points and 1200 series access points with RM21 and RM22A radios.

Japan Upgrade Utility

The Japanese government has changed their 5-GHz radio spectrum regulations to allow a field upgrade of 802.11a radios. Japan allows three different frequency sets organized into regulatory domains as shown in Table 1-2.

Table 1-2 Japan Frequency Sets

Frequency Set	Channel (Freq)	Channel (Freq)	Channel (Freq)	Channel (Freq)
J52	34 (5170 MHz)	38 (5190 MHz)	42 (5210 MHz	46 (5230 MHz)
W52	36 (5180 MHz)	40 (5200 MHz)	44 (5220 MHz)	48 (5240 MHz)
W53	52 (5260 MHz)	56 (5280 MHz)	60 (5300 MHz)	64 (5320 MHz)

These frequency sets have 3 legal combinations in which Cisco has organized into regulatory domains:

- J regulatory domain = J52
- P regulatory domain = W52+W53

- U regulatory domain = W52

The upgrade utility allows users to migrate their 802.11a radios from J52 to W52. The utility operates on the following devices:

- 1130 series access points
- 1200 series access points with RM21 and RM22A radios
- 1240 series access points

Users must migrate all 802.11a radios in their wireless network from J52 to W52. There cannot be a mix of radios in the network operating in the J52 and W52 bands because of overlap.

See the "Migrating to Japan W52 Domain" section on page 5-37 for more information about this utility.

Multiple VLAN and Rate Limiting Support for Point-to-Multipoint Bridging

This feature modifies the way point-to-multipoint bridging can be configured to operate on multiple VLANs with the ability to control traffic rates on each VLAN. The feature is available on 32 Mb access points configured as bridges (1240 series) and the 1300 series access point/bridge. The feature is not available on 16 Mb access points (1100, 1200, and 350 series)

In a typical scenario, multiple VLAN support permits users to set up point-to-multipoint bridge links with remote sites, with each remote site on a separate VLAN. This configuration provides the user to separate and control traffic to each site. Rate limiting ensures that no remote site consumes more than a specified amount of the entire link band width. Only uplink traffic can be controlled by the FastEthernet ingress ports of non-root bridges.

See the "Configuring Multiple VLAN and Rate Limiting for Point-to-Multipoint Bridging" section on page 5-39 for more information on this feature.

Client MFP Support

Client MFP encrypts class 3 management frames sent between access points and CCXv5-capable client stations, so that both access point and client can take preventative action by dropping spoofed class 3 management frames (management frames passed between an access point and a client that are 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 station in the (re)association request's Robust Security Network Information Element (RSNIE) is used to protect both unicast data and class 3 management frames. access points in workgroup bridge, repeater, and non-root bridge modes must negotiate either TKIP or AES-CCMP in order to use Client MFP.

Regulatory Changes for Taiwan

In June 2006, the FCC finalized rules governing the use of frequencies in the 5.250 – 5.725 GHz range. Products using these frequencies must employ Dynamic Frequency Selection (DFS). With Cisco IOS Release 12.3(8)JA, FCC DFC compliance was enabled in the North American domain for 1130, 1200, and 1240 series access points.

Taiwan's regulatory agencies have elected to adhere to the United State's FCC regulations regarding DFS. This release supports DFS for the Taiwan (-T) regulatory domain. This also enables the use of additional channels in the 5.250 – 5.725 GHz band.

See the "Dynamic Frequency Selection" section on page 6-17 for more information on DFS.

Universal Workgroup Bridge

This feature provides the means for Cisco access points configured as workgroup bridges (WGBs) to associate with non-Cisco access points. In addition, the feature provides the WGB with the ability to be continuously in World Mode.

See the "Configuring the Role in Radio Network" section on page 6-2 for more information on universal workgroup bridge configuration.

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 a client's signal quality drops, 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's 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 CCKM and a device providing 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.

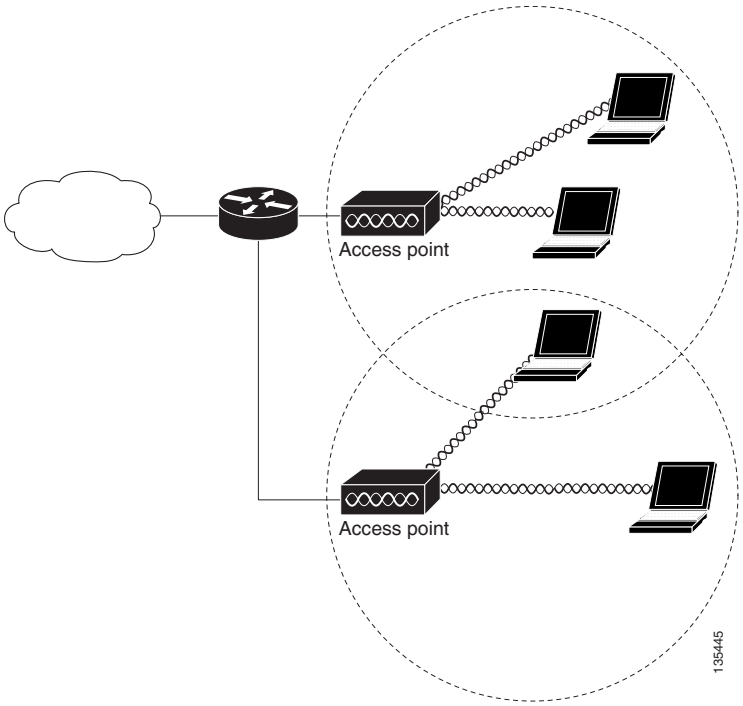
Network Configuration Examples

This section describes the access point's role in common wireless network configurations. The access point's 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

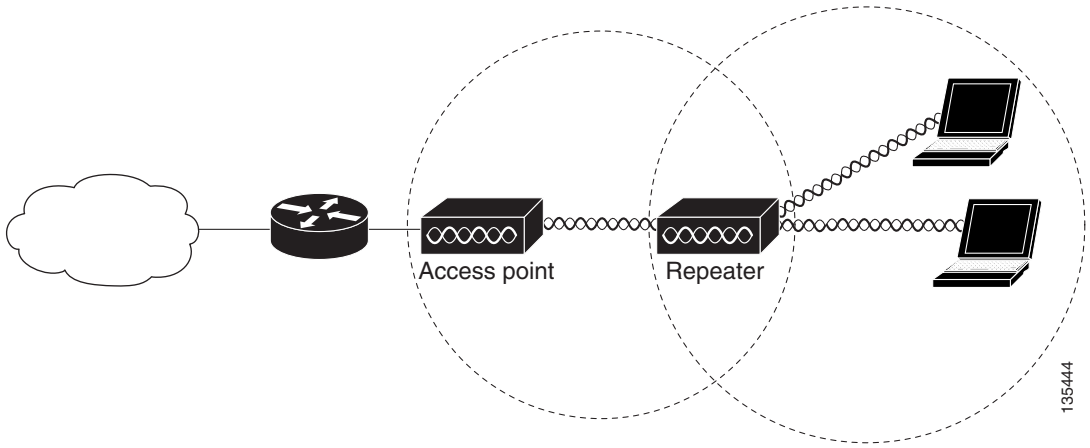


Repeater Access Point

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

The 1200 and 1240 access points and the 1300 access point/bridge 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 6-2 for instructions on setting up an access point as a bridge.

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

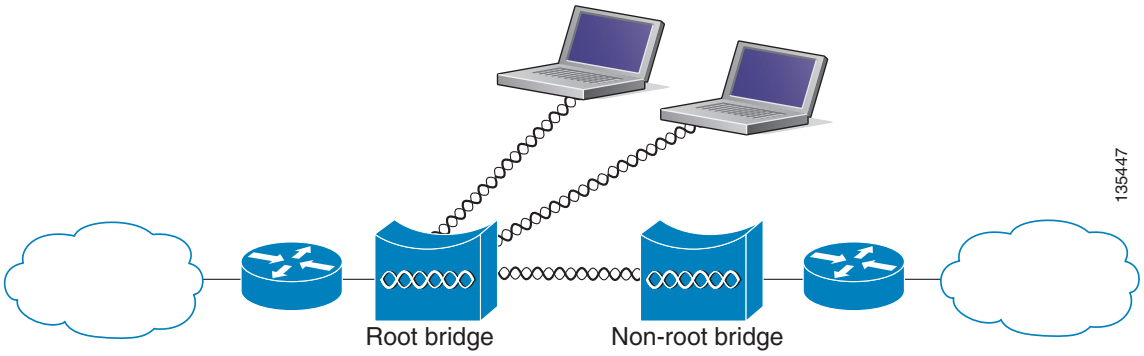
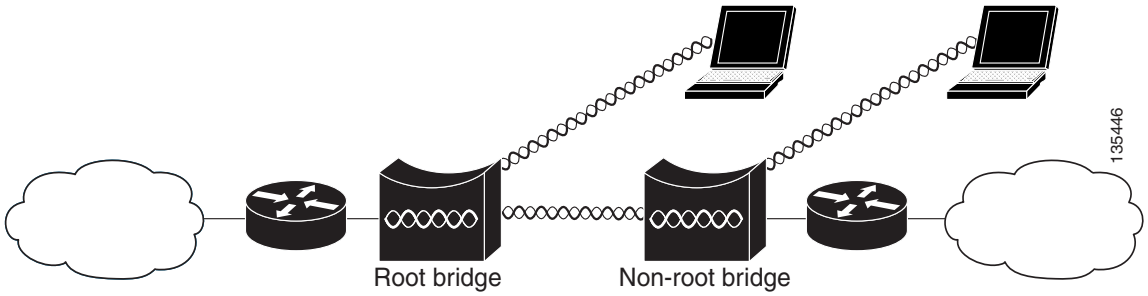


Figure 1-4 Access Points as Root and Non-root Bridges with Clients



When wirless 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. 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.

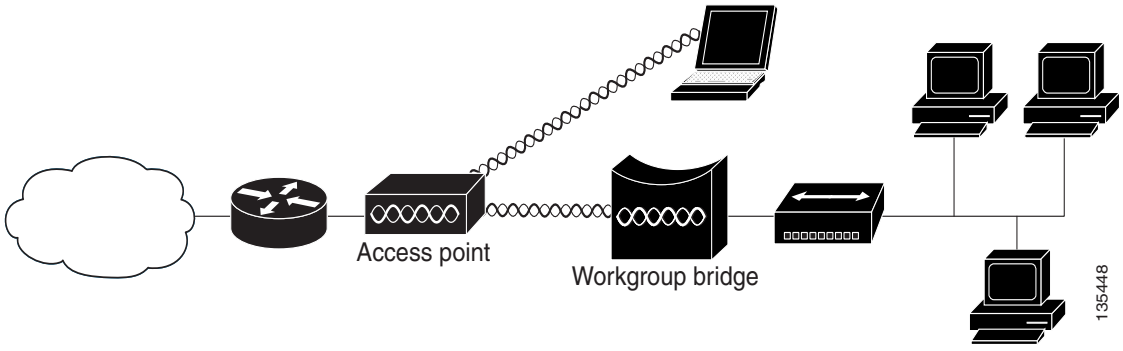
Workgroup Bridge

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. When you configure one radio interface as a workgroup bridge, the other radio interface is automatically disabled.

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 19-16 for information on configuring your access point as a workgroup bridge.

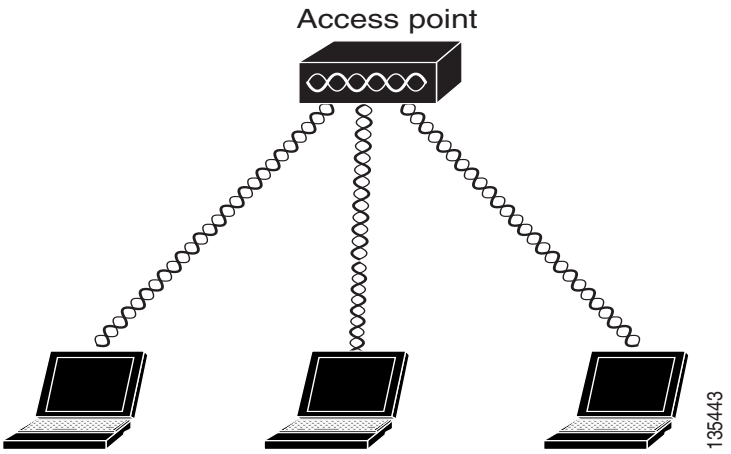
Figure 1-5 Access Point as a Workgroup Bridge



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 details regarding the configuration parameters are contained in the help system. This chapter contains these sections:

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.

The following parameters can be configured by using the web browser interface.

- VLAN Configuration
- SSID configuration
- VLAN-to-SSID mappings
- Gain and power settings
- Maximum reach
- Maximum throughput
- Light Extensible Authentication Protocol (LEAP) configuration (including LEAP/RADIUS server)
- Local user profiles for local LEAP server
- Encryption modes
- Wireless MAC filter
- Detect MACs for filter (capture network discovered MAC addresses and export to MAC filter list)
- Broadcast SSID

Note The wireless device web-browser interface is fully compatible with Microsoft Internet Explorer version 5.56.0 on Windows 98, 2000, and XP platforms, and with Netscape version 7.17.0 on Windows 98, 2000, XP, and Solaris platforms.

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's IP address to browse to the management system. See the "Obtaining and Assigning an IP Address" section on page 4-4 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's IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer) and press **Enter**. The Summary StatusHome page appears.

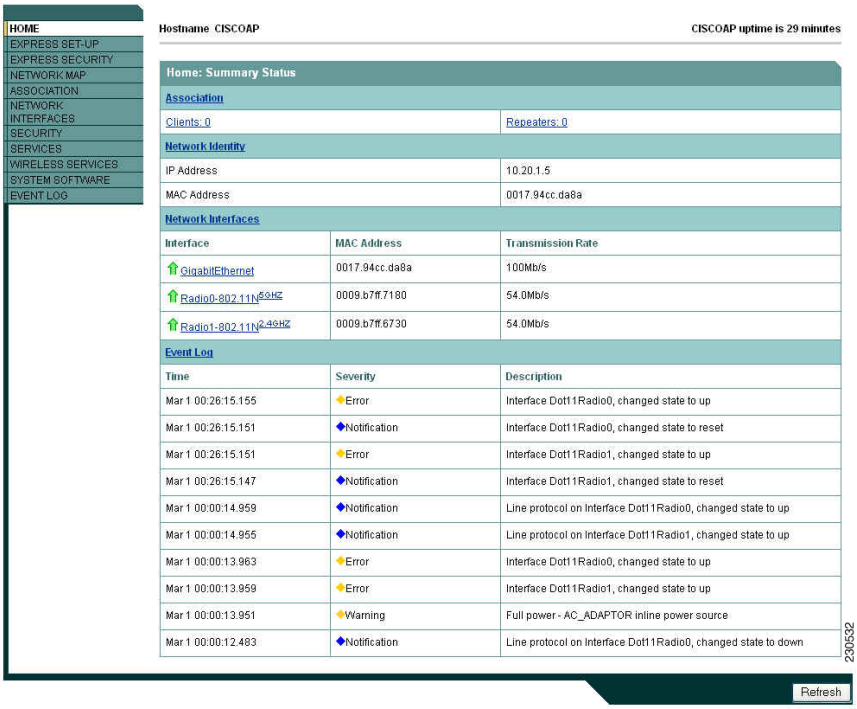
Using the Management Pages in the Web-Browser Interface

The system management pages use consistent techniques to present and save configuration information. A navigation bar is on the left side of the page, and configuration action buttons appear at the bottom. You use the navigation bar to browse to other management pages, and you use the configuration action buttons to save or cancel changes to the configuration.

Note It is important to remember that clicking your web-browser's **Back** button returns you to the previous page without saving any changes you have made. Clicking **Cancel** cancels any changes you made on 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



Using Action Buttons

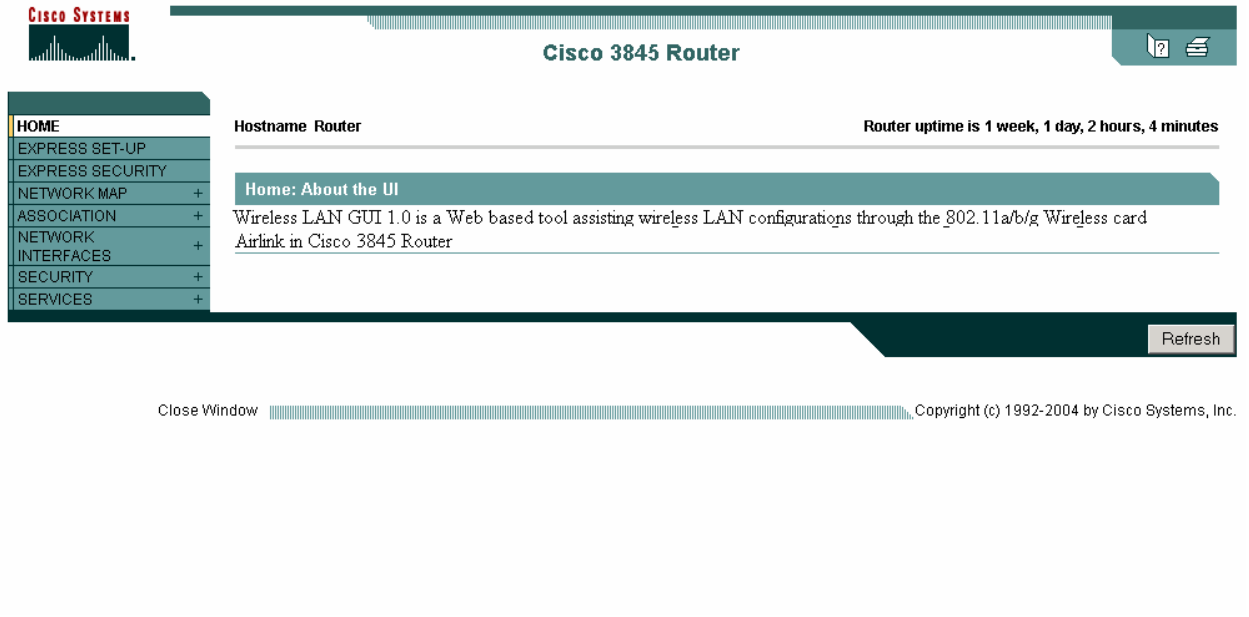


Table 2-1 lists the page links and buttons that appear on most management pages.

Table 2-1 Common Buttons on Management Pages

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.
Express Setup	Displays the Express Setup page that includes basic settings such as system name, IP address, and role in radio network.
Express Security	Displays the Express Security page that you use to create SSID and assign security settings to them.
Network Map	Displays a list of infrastructure devices on your wireless LAN.
Association	Displays a list of all devices on your wireless LAN, listing their system names, network roles, and parent-client relationships.
Network Interfaces	Displays status and statistics for the Ethernet and radio interfaces and provides links to configuration pages for each interface.
Security	Displays a summary of security settings and provides links to security configuration pages.
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.
Wireless Services	Displays a summary of wireless services used with CCKM and provides links to WDS configuration pages.

Table 2-1 Common Buttons on Management Pages (continued)

Button/Link	Description
System 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.

Character Restrictions in Entry Fields

Because the 1200 series access point uses Cisco IOS software, tThere are certain characters that you cannot use in the entry fields on the web-browser interface. You cannot use these characters in entry fields:

“

]

+

/

Tab

Trailing space

Enabling HTTPS for Secure Browsing

You can protect 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’s address line from http://*ip_address* to **https://*ip_address*** and log into the access point again.

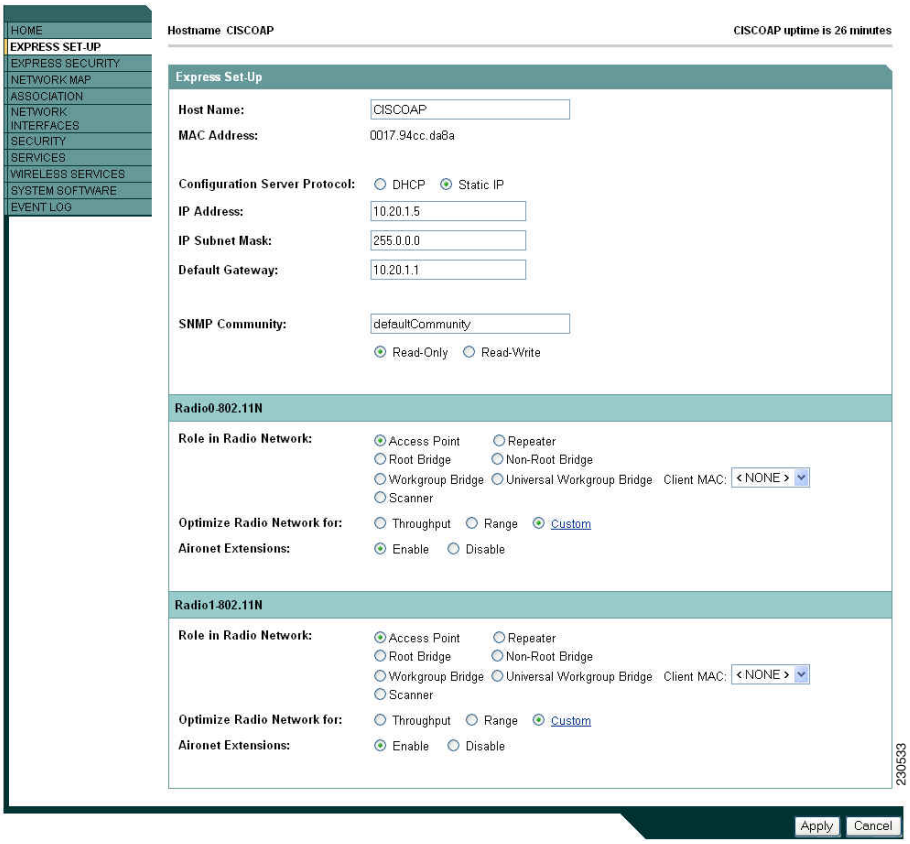
Note When you enable HTTPS, most browsers prompt you for approval each time you browse to a device that does not have a fully qualified domain name (FQDN). To avoid the approval prompts, complete Step 2 through Step 9 in these instructions to create an FQDN for the access point. However, if you do not want to create an FQDN, skip to Step 10.

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 Browse to the Express Setup page. Figure 2-2 shows the Express Setup page.

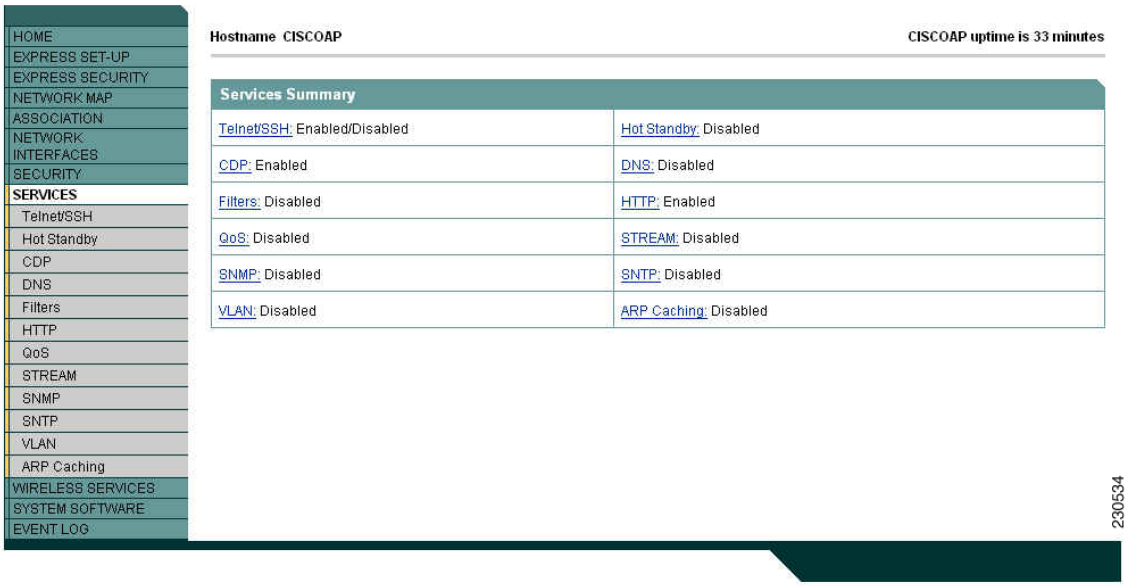
Figure 2-2 Express Setup Page



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

Step 4 Browse to the Services – DNS page. Figure 2-3 shows the Services – DNS page.

Figure 2-3 Services – DNS Page



Step 5 Select **Enable** for Domain Name System.

Step 6 In the Domain Name field, enter your company's domain name. At Cisco Systems, for example, the domain name is *cisco.com*.

Step 7 Enter at least one IP address for your DNS server in the Name Server IP Addresses entry fields.

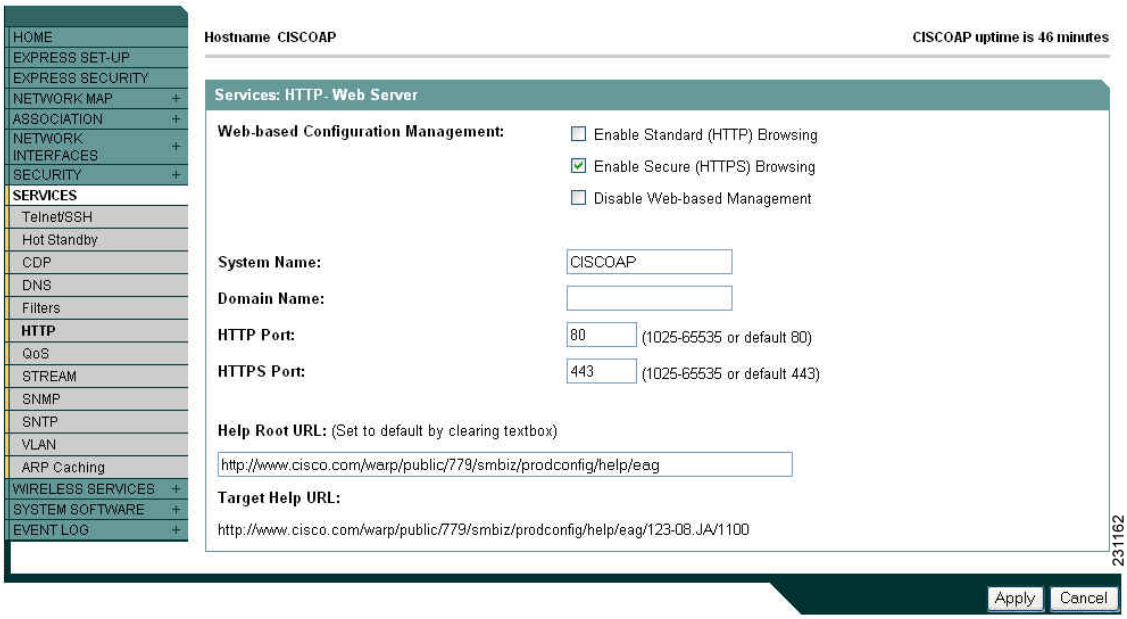
Step 8 Click **Apply**. The access point's FQDN is a combination of the system name and the domain name. For example, if your system name is *ap1100* and your domain name is *company.com*, the FQDN is *ap1100.company.com*.

Step 9 Enter the FQDN on your DNS server.

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

Step 10 Browse to the Services: HTTP Web Server page. Figure 2-4 shows the HTTP Web Server page:

Figure 2-4 Services: HTTP Web Server Page



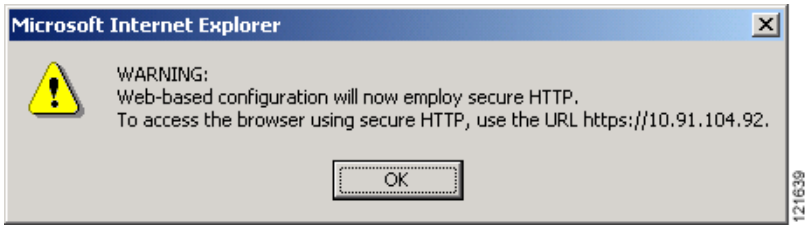
Step 11 Select the Enable Secure (HTTPS) Browsing check box and click **Apply**.

Step 12 Enter a domain name and click **Apply**.

Note Although you can enable both standard HTTP and HTTPS, Cisco recommends that you enable one or the other.

A warning window appears stating that you will use HTTPS to browse to the access point. The window also instructs you to change the URL that you use to browse to the access point from *http* to *https*. Figure 2-5 shows the warning window:

Figure 2-5 HTTPS Warning Window



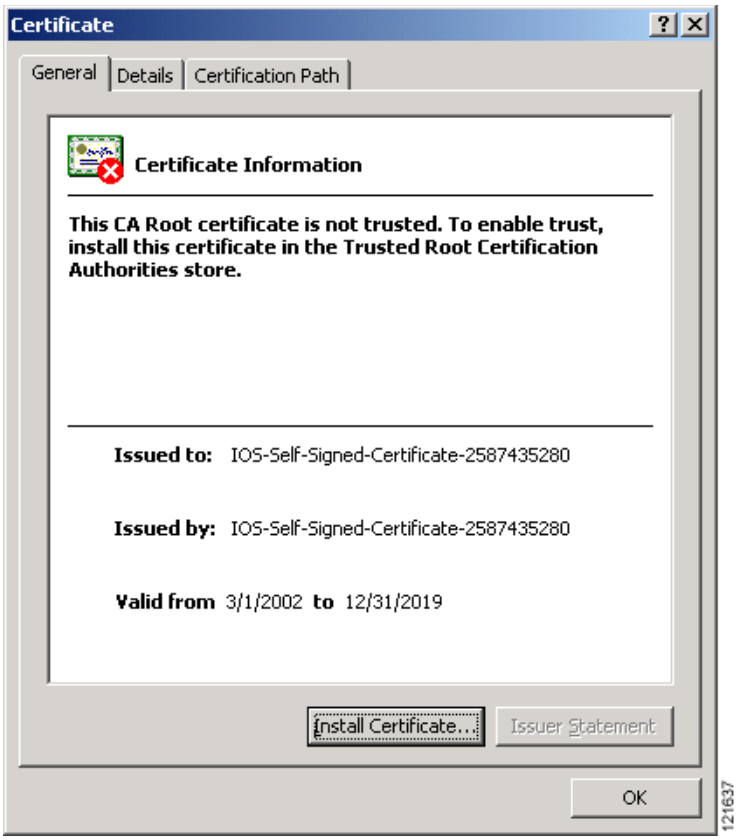
Step 13 Click **OK**. The address in your browser's address line changes from **http://*ip-address*** to **https://*ip-address***.

Step 14 Another warning window appears stating that the access point's security certificate is valid but is not from a known source. However, you can accept the certificate with confidence because the site in question is your own access point. Figure 2-6 shows the certificate warning window:

Figure 2-6 Certificate Warning Window

Step 15 Click **View Certificate** to accept the certificate before proceeding. (To proceed without accepting the certificate, click **Yes**, and skip to Step 24 in these instructions.) Figure 2-7 shows the Certificate window.

Figure 2-7 Certificate Window

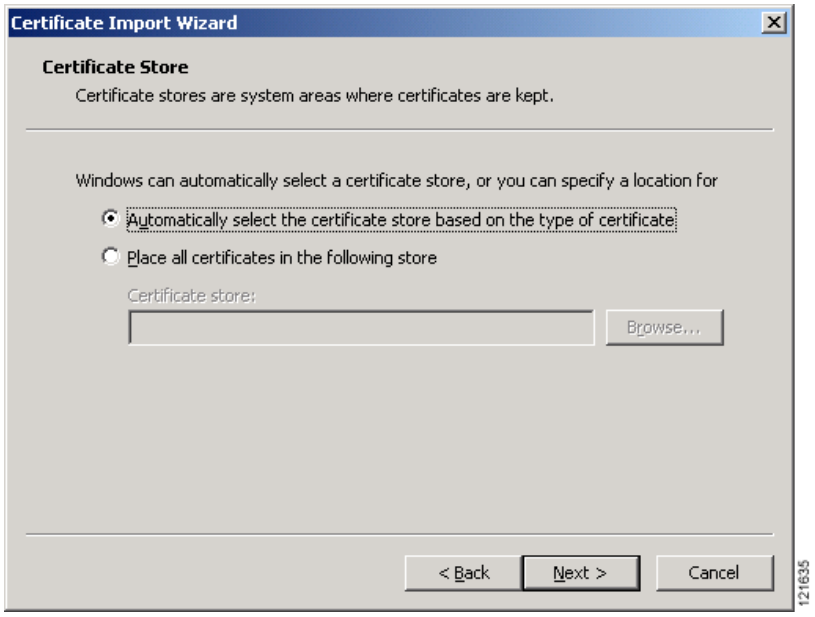


Step 16 On the Certificate window, click **Install Certificate**. The Microsoft Windows Certificate Import Wizard appears. Figure 2-8 shows the Certificate Import Wizard window.

Figure 2-8 Certificate Import Wizard Window

Step 17 Click **Next**. The next window asks where you want to store the certificate. Cisco recommends that you use the default storage area on your system. Figure 2-9 shows the window that asks about the certificate storage area.

Figure 2-9 Certificate Storage Area Window



Step 18 Click **Next** to accept the default storage area. A window appears that states that you successfully imported the certificate. Figure 2-10 shows the completion window.

Figure 2-10 Certificate Completion Window

Step 19 Click **Finish**. Windows displays a final security warning. Figure 2-11 shows the security warning.

Figure 2-11 Certificate Security Warning

Step 20 Click **Yes**. Windows displays another window stating that the installation is successful. Figure 2-12 shows the completion window.

Figure 2-12 Import Successful Window

Step 21 Click **OK**.

Step 22 On the Certificate window shown in Figure 2-7, which is still displayed, click **OK**.

Step 23 On the Security Alert window shown in Figure 2-6, click **Yes**.

Step 24 The access point login window appears and you must log into the access point again. The default user name is *Cisco* (case-sensitive) and the default password is *Cisco* (case-sensitive).

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 ap1100
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 *ap1100*, 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 12.3. Click this link to browse to the master list of commands:

http://www.cisco.com/en/US/docs/ios/mcl/123mcl/TD-Book-Wrapper.html

Deleting an HTTPS Certificate

The access point generates a certificate automatically when you enable HTTPS. However, if you need to change the access point's fully qualified domain name (FQDN) 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 Certificate** to delete the certificate.

Step 4 Re-enable HTTPS. The access point generates a new certificate using the new FQDN.

Using Online Help

Click the help icon at the top of any page in the web-browser interface to display online help. Figure 2-13 shows the help and print icons.

Figure 2-13 Help and Print Icons

When a help page appears in a new browser window, use the Select a topic drop-down menu to display the help index or instructions for common configuration tasks, such as configuring VLANs.

Changing the Location of Help Files

Cisco maintains up-to-date HTML help files for access points on the Cisco web site. By default, the access point opens a help file on Cisco.com when you click the help button on the access point web-browser interface. However, you can install the help files on your network so your access points can access them there. Follow these steps to install the help files locally:

Step 1 Download the help files from the Software Center on Cisco.com:

http://www.cisco.com/cisco/software/navigator.html

Select the help files that match the software version on your access point.

Step 2 Unzip the help files on your network in a directory accessible to your access point. When you unzip the help files, the HTML help pages are stored in a folder named according to the help version number and access point model number.

Step 3 Browse to the Services: HTTP Web Server page in the access point web-browser interface.

Step 4 In the Default Help Root URL entry field, enter the complete path to the location where you unzipped the help files. When you click the access point help button, the access point automatically appends the help version number and model number to the path that you enter.

Note Do not add the help version number and device model number to the Default Help Root URL entry. The access point automatically adds the help version and model number to the help root URL.

If you unzip the help files on your network file server at *//myserver/myhelp*, your Default Help Root URL looks like this:

http://myserver/myhelp

Table 2-2 shows an example help location and Help Root URL for an 1100 series access point.

Table 2-2 Example Help Root URL and Help Location

Files Unzipped at This Location	Default Help Root URL	Actual Location of Help Files
//myserver/myhelp	http://myserver/myhelp	//myserver/myhelp/123-02.JA/1100

Step 5 Click **Apply**.

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
```

CHAPTER 3

Using the Command-Line Interface

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

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 is radio 0, and the 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 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

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's 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 When the Telnet window appears, click **Connect** and select **Remote System**.

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

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

Step 4 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 5-25 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's web-browser interface to complete the initial configuration and then use the CLI to enter additional settings for a more detailed configuration.

This chapter contains these sections:

Note In this release, 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:

- The login and password for the access point. The default login is Cisco and the default password is Cisco (both case sensitive)
- 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

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 default settings using the access point GUI:

Step 1 Open your Internet browser. The web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98, 2000 and XP platforms, and with Netscape version 7.0 on Windows 98, 2000, XP, and Solaris platforms.

Step 2 Enter the wireless device's 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 **System 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 protocal 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). To obtain the access point/bridge's new IP address, you can use the *show interface bvi1* CLI command.

Obtaining and Assigning an IP Address

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

- If you have an 1130AG, 1200, 1240 series access point or 1300 series access point/bridge, 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's console port:
  - Connecting to the 1100 Series Access Point Locally, page 4-5
  - Connecting to the 1130 Series Access Point Locally, page 4-6
  - Connecting to the 1200, 1230, and 1240 Series Access Points Locally, page 4-6.
  - Connecting to the 1300 Series Access Point/Bridge Locally, page 4-7

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:
  - If you have a 1200 series access point, 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 the 1100 Series Access Point Locally" section on page 4-5 or in the "Connecting to the 1200, 1230, and 1240 Series Access Points Locally" section on page 4-6 to connect to the console port.
  - Provide your network administrator with the wireless device's 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's MAC address is on label attached to the bottom of the access point.
  - Use the Cisco IP Setup Utility (IPSU) to identify the assigned address. IPSU runs on most Microsoft Windows operating systems: Windows 9x, 2000, Me, NT, and XP.

    You can download IPSU from the Software Center on Cisco.com. Click this link to browse to the Software Center:

    http://www.cisco.com/cisco/software/navigator.html

Default IP Address Behavior

When you connect a 1130AG, 1200, 1240 access point, or 1300 series access point/bridge 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.

When you connect an 1100 series access point with a default configuration to your LAN, the 1100 series access point makes several attempts to get an IP address from the DHCP server. If it does not receive an address, it assigns itself the IP address 10.0.0.1 for five minutes. During this five-minute window, you can browse to the default IP address and configure a static address. If after five minutes the access point is not reconfigured, it discards the 10.0.0.1 address and reverts to requesting an address from the DHCP server. If it does not receive an address, it sends requests indefinitely. If you miss the five-minute window for browsing to the access point at 10.0.0.1, you can power-cycle the access point to repeat the process.

The 1300 series access point/bridge assumes a radio network role of a root access point. To configure it as a bridge, you must manually place it in install mode in order to align the antennas and establish a link. To establish the link you must have two access point/bridges configured in the install mode. In the install mode, one access point/bridge must be configured as a root bridge and the other a non-root bridge. To facilitate the configuration, an automatic option is available when the access point/bridge is in the install mode. After the wireless link is established and the bridge antennas are aligned, you take both access point/bridges out of install mode and place them on your LAN as root and non-root bridges.

Connecting to the 1100 Series Access Point Locally

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 Ethernet port using a Category 5 Ethernet cable. You can use a local connection to the Ethernet port much as you would use a serial port connection.

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

If the access point is configured with default values and it does not receive an IP address from the DHCP server, it defaults to IP address 10.0.0.1 for five minutes. During that five minutes, you can browse to that IP address to configure the unit. If after five minutes the unit has not been reconfigured, it discards the 10.0.0.1 address and reverts to requesting an address from the DHCP server. If it does not receive an address, it sends requests indefinitely. If you miss the five-minute window for browsing to the access point at 10.0.0.1, you can power-cycle the access point to repeat the process.

Follow these steps to connect to the access point locally:

Step 1 Make sure that the PC you intend to use to configure the access point is configured with an IP address from 10.0.0.2 to 10.0.0.10.

Step 2 Connect your PC to the access point using a Category 5 Ethernet cable. You can use either a crossover cable or a straight-through cable.

Step 3 Power up the access point.

Step 4 Follow the steps in the "Assigning Basic Settings" section on page 4-8. If you make a mistake and need to start over, follow the steps in the "Resetting the Device to Default Settings" section on page 4-2.

Step 5 After configuring the access point, remove the Ethernet cable from your PC and connect the access point to your wired LAN.

Note When you connect your PC to the access point 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.

Connecting to the 1130 Series Access Point Locally

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 Open the access point cover.

Step 2 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 3 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 no flow control does not work, try Xon/Xoff flow control.

Connecting to the 1200, 1230, and 1240 Series Access Points Locally

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.

Note 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 no flow control does not work, try Xon/Xoff flow control.

Step 3 Connect power to the access point. The access point displays the power up configuration sequence.

Step 4 When the power up sequence ends, press **Enter** and the access point CLI command prompt displays, such as **AP>**.

Note The access point default username is **Cisco** and the default password is **Cisco**.

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

Connecting to the 1300 Series Access Point/Bridge Locally

If you need to configure the access point/bridge locally (without connecting the access point/bridge 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's Ethernet port much 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 up the access point/bridge.

Step 5 Follow the steps in the "Assigning Basic Settings" section on page 4-8. If you make a mistake and need to start over, follow the steps in the "Resetting the Device to Default Settings" procedure on page 4-2.

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's 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.

See Chapter 6, "Configuring Radio Settings" for additional information.

Assigning Basic Settings

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

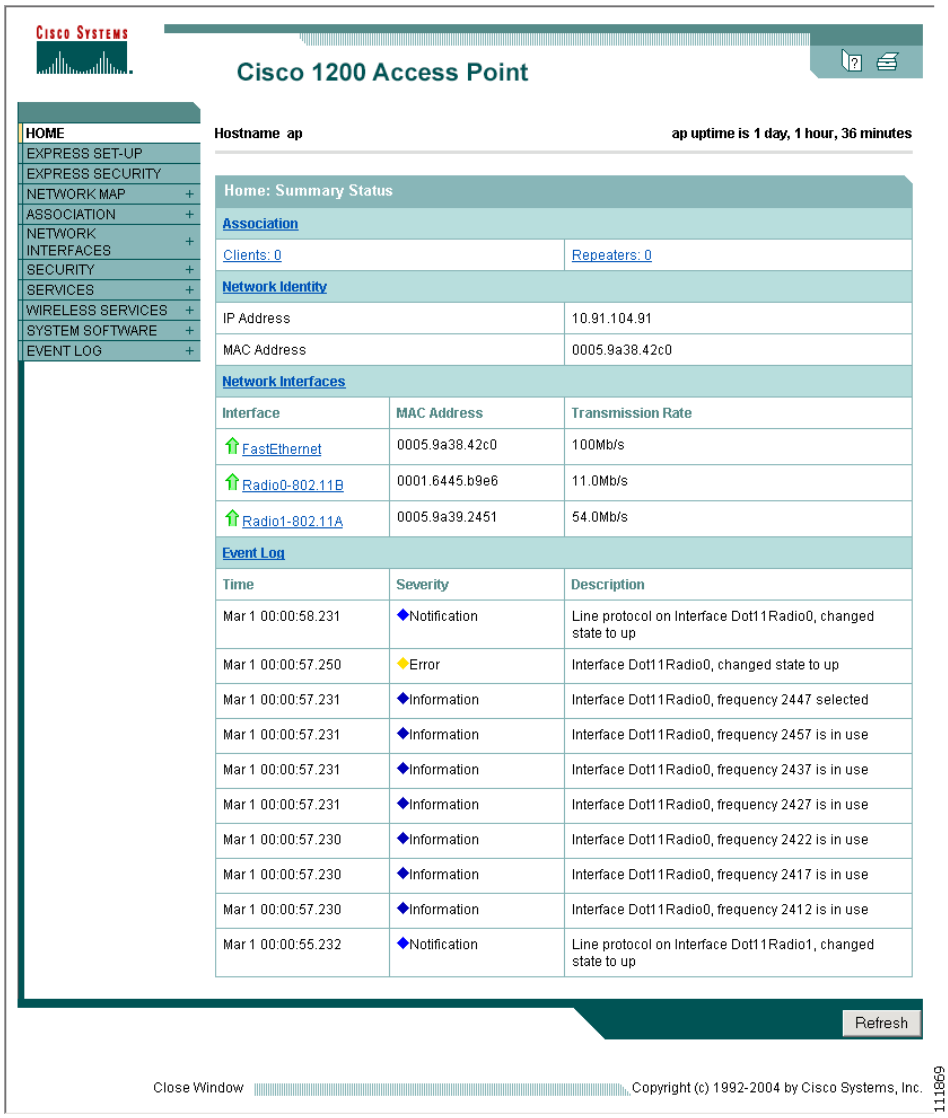
Step 1 Open your Internet browser. The wireless device web-browser interface is fully compatible with Microsoft Internet Explorer version 6.0 on Windows 98, 2000, XP platforms, and with Netscape version 7.0 on Windows 98, 2000, XP, and Solaris platforms.

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

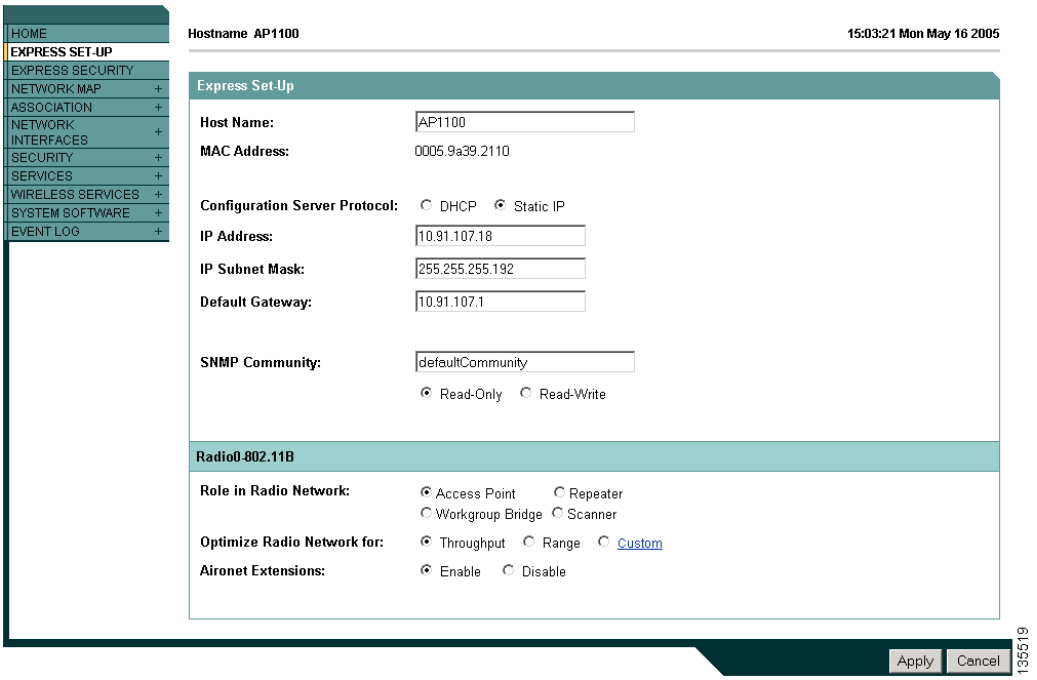
Step 4 Enter the case-sensitive password *Cisco* and press **Enter**. The Summary Status page appears, as shown in Figure 4-1.

Figure 4-1 Summary Status Page



Step 5 Click **Express Setup**. The Express Setup screen appears. Figure 4-2 and Figure 4-3 shows the Express Setup page for the 1100 series access points. Your pages may differ depending on the access point model and configuration you are using.

Figure 4-2 Express Setup Page for 1100 Series Access Points



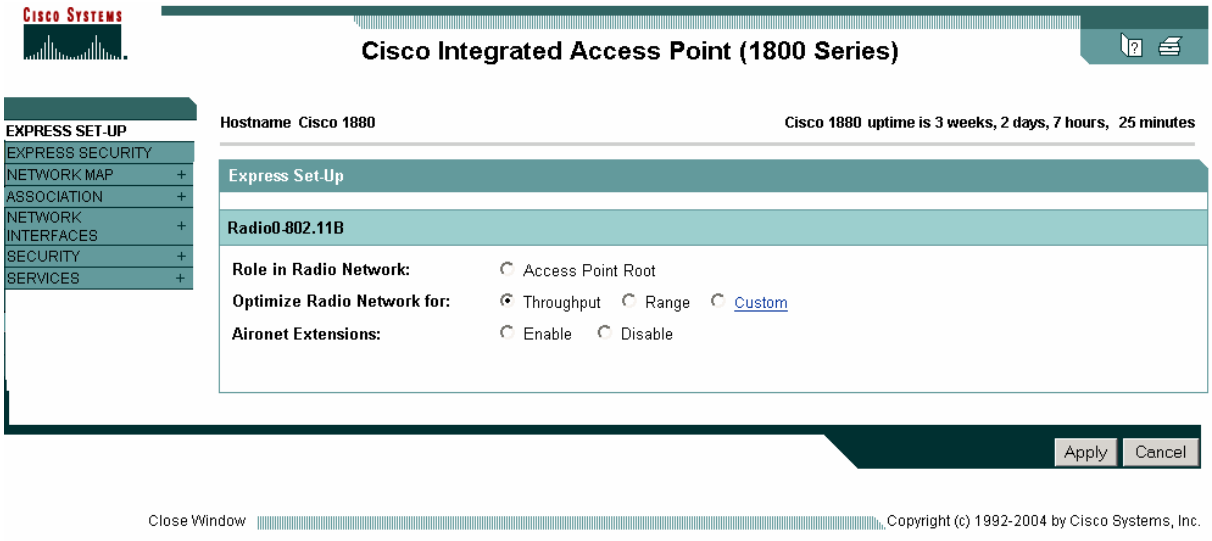
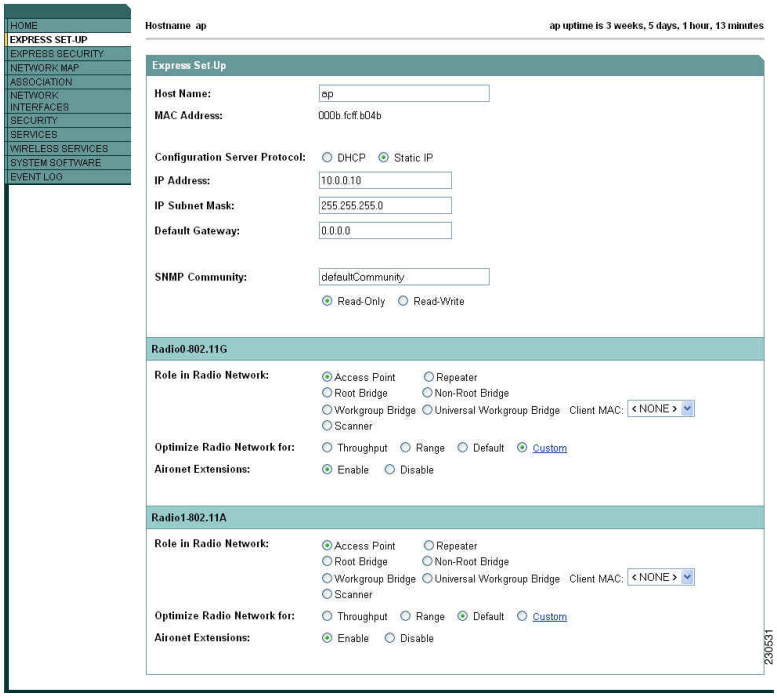
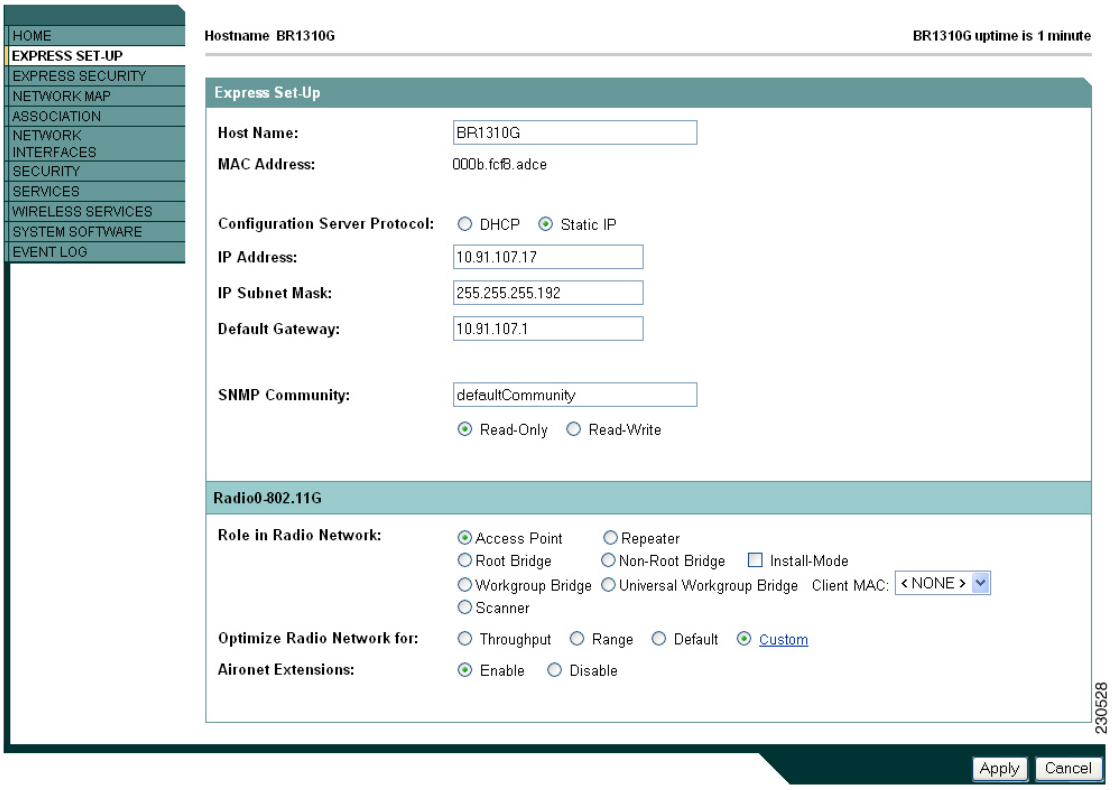


Figure 4-3 Express Setup Page for 1130, 1200, and 1240 Series Access Points



Note Figure 4-3 shows the Express Setup page for an 1130 series access point. The 1200 series is similar, but does not support the universal workgroup bridge role.

Figure 4-4 Express Setup Page for the 1300 Series Access Point/Bridge



Step 6 Enter the configuration settings 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 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.

- **Configuration Server Protocol**—Click on the button that matches the network's method of IP address assignment.
  - **DHCP**—IP addresses are automatically assigned by your network's 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's IP address. If DHCP is enabled for your network, leave this field blank.

Note If the wireless device's 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 4-2 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.
- **Role in Radio Network**—Click on 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.
  - **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. This setting is available only for the 1200 and 1240 series access points.
  - **Non-Root Bridge**—In this mode, the device establishes a link with a root bridge. This setting is available only for the 1200 and 1240 series access points.
  - **Install Mode**—Places the 1300 series access point/bridge in auto installation mode so you can align and adjust a bridge link for optimum efficiency.
  - **Workgroup Bridge**—Emulates a Cisco Aironet 350 Series 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 wokgroup bridge can have have a maximum of 254 clients, presuming that no other wireless clients are associated to the root bridge or access point. This setting is available for the 1100, 1200, and 1300 series access points.
  - **Universal Workgroup Bridge**—Configures the access point as a workgroup bridge capable of associating with non-Cisco access points. This setting is available on 1130, and 1240 series access points and 1300 series access point/bridges.
  - **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's range but might reduce throughput.

  - **Custom**—The wireless device uses the settings you enter on the Network Interfaces: Radio-802.11b Settings page. Clicking **Custom** takes you to the Network Interfaces: Radio-802.11b Settings page.

- **Aironet Extensions**—Enable this setting if there are only Cisco Aironetwireless devices on your wireless LAN.
- **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).

Step 7 Click **Apply** to save your settings.

Step 8 Click **Network Interfaces** to browse to the Network Interfaces Summary page.

Step 9 Click the radio interface to browse to the Network Interfaces: Radio Status page.

Step 10 Click the **Settings** tab to browse to the Settings page for the radio interface.

Step 11 Click **Enable** to enable the radio.

Step 12 Click **Apply**.

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

Note You can restore 1100 and 1200 series 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 Express 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
SNMP Community	defaultCommunity (Read-only)
Role in Radio Network (for each radio installed)	Access point

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

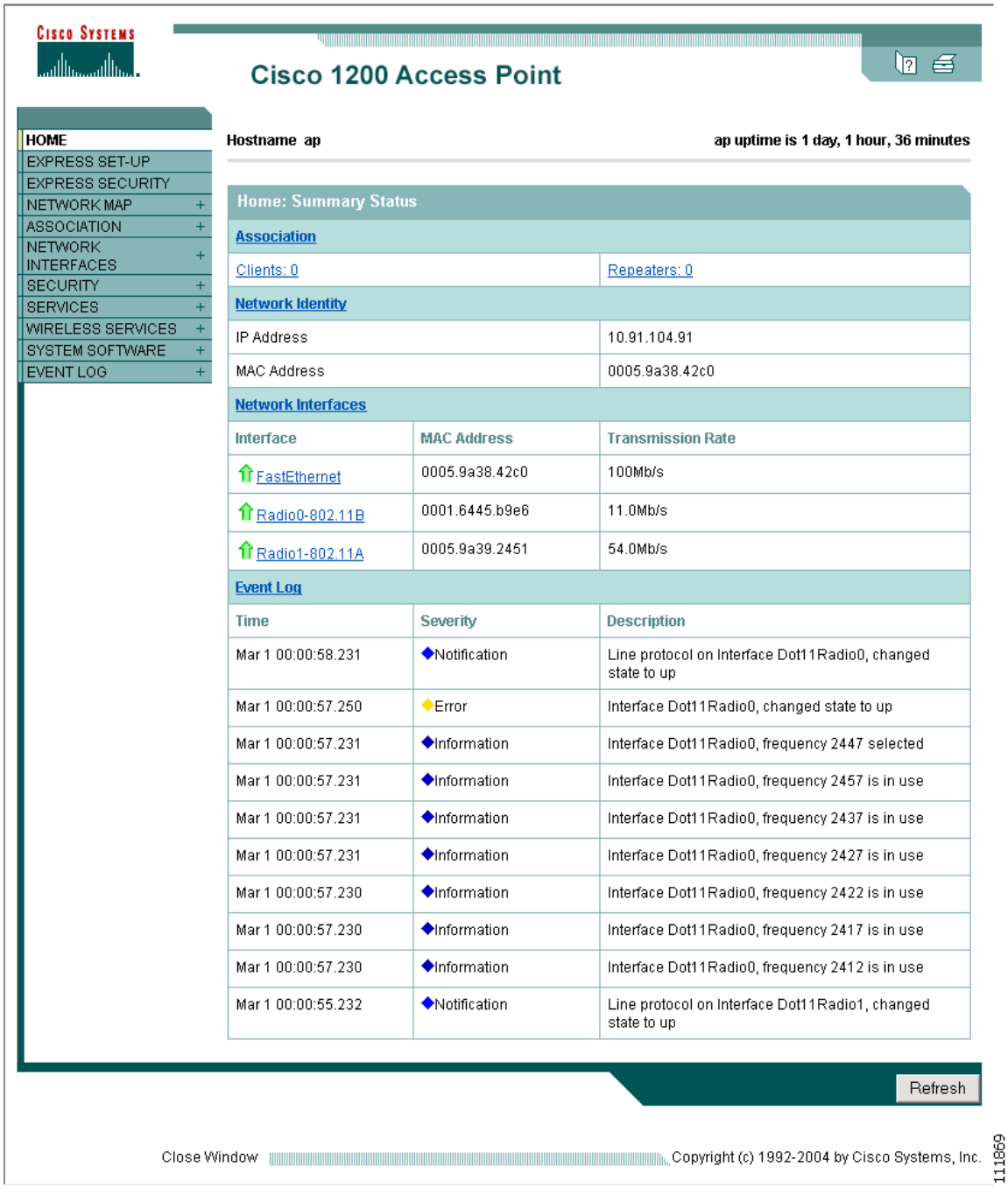
Setting	Default
Optimize Radio Network for	Throughput
Aironet Extensions	Enable

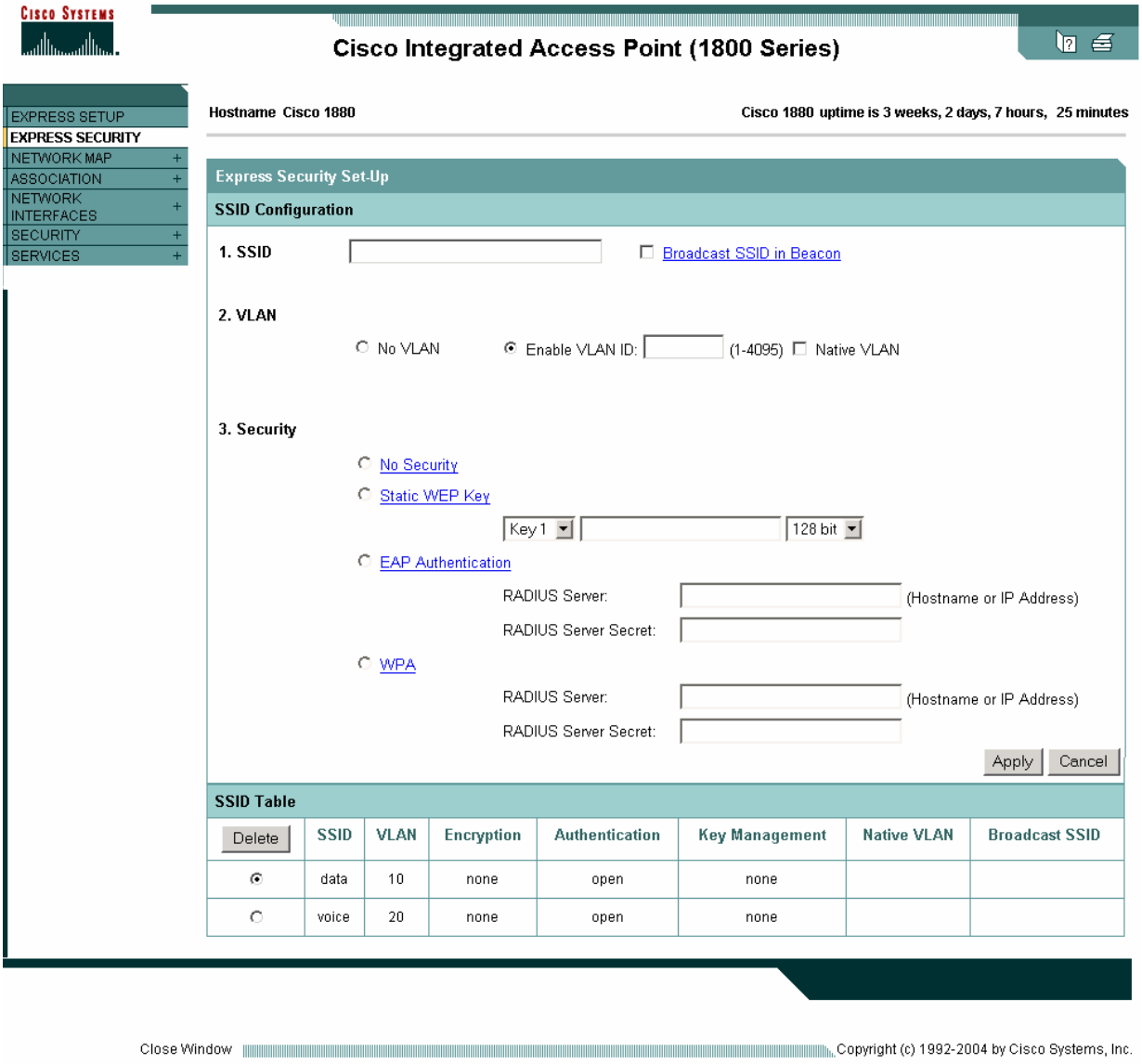
Configuring Basic Security Settings

After you assign basic settings to the wireless device, you must configure security settings to prevent unauthorized access to your network. Because it is a radio device, the wireless device can communicate beyond the physical boundaries of your worksite.

Just as you use the Express Setup page to assign basic settings, you can use the Express Security page to create unique SSIDs and assign one of four security types to them. Figure 4-5 shows the Express Security page.

Figure 4-5 Express Security Page





The Express Security page helps you configure basic security settings. You can use the web-browser interface's main Security pages to configure more advanced security settings.

Understanding Express Security Settings

The SSIDs that you create using the Express security page appear in the SSID table at the bottom of the page. You can create up to 16 SSIDs on the wireless device. On dual-radio wireless devices, the SSIDs that you create are enabled on both radio interfaces.

Note In Cisco IOS Release 12.4(3g)JA and 12.3(8)JEB, 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.

Express Security Types

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 "Using MAC Address ACLs to Block or Allow Client Association to the Access Point" on page 16-6) 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's 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 don't 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 don't 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.

Express Security Limitations

Because the Express Security page is designed for simple configuration of basic security, the options available are a subset of the wireless device's 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 assign SSIDs to specific radio interfaces. The SSIDs that you create are enabled on all radio interfaces. To assign SSIDs to specific radio interfaces, use the Security SSID Manager page.
- 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.

Using the Express Security Page

Follow these steps to create an SSID using the Express Security page:

Step 1 Type the SSID in the SSID entry field. The SSID can contain up to 32 alphanumeric characters.

Step 2 To broadcast the SSID in the wireless device beacon, check the Broadcast SSID in Beacon check box. 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.

Step 3 (Optional) Check the Enable VLAN ID check box and enter a VLAN number (1 through 4095) to assign the SSID to a VLAN. You cannot assign an SSID to an existing VLAN.

Step 4 (Optional) Check the Native VLAN check box to mark the VLAN as the native VLAN.

Step 5 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 and shared 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 4-18 for details.

Step 6 Click **Apply**. The SSID appears in the SSID table at the bottom of the page.

CLI Configuration Examples

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

Example: No Security

This example shows part of the configuration that results from using the Express Security page to create an SSID called *no_security_ssid*, including the SSID in the beacon, assigning it to VLAN 10, and selecting VLAN 10 as the native VLAN:

```
!
dot11 ssid no_security_ssid
authentication open
vlan 10
!
interface Dot11Radio0/1.10
 encapsulation dot1Q 10 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 Dot11Radio1/1
 no ip address
 no ip route-cache
!
ssid no_security_ssid
!
speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 rts threshold 2312
 station-role root
!
interface Dot11Radio1/1.10
 encapsulation dot1Q 10 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
```

Example: Static WEP

This example shows part of the configuration that results from using the Express Security page to create 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:

```
ssid static_wep_ssid
    vlan 20
    authentication open
!
interface Dot11Radio0/1
 no ip address
 no ip route-cache
 !
 encryption vlan 20 key 3 size 128bit 7 FFD518A21653687A4251AEE1230C transmit-key
 encryption vlan 20 mode wep mandatory
!
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 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

 ssid statuc_wep_ssid
!
interface Dot11Radio0/1.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 subscriber-loop-control
 bridge-group 20 block-unknown-source
 no bridge-group 20 source-learning
 no bridge-group 20 unicast-flooding
 bridge-group 20 spanning-disabled
!
interface Dot11Radio1/1
 no ip address
 no ip route-cache
 !
 encryption vlan 20 key 3 size 128bit 7 741F07447BA1D4382450CB68F37A transmit-key
 encryption vlan 20 mode wep mandatory
 !
 ssid static_wep_ssid
!
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 rts threshold 2312
 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 Dot11Radio1/1.20
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 20
 bridge-group 20 subscriber-loop-control
```

```
 bridge-group 20 block-unknown-source
 no bridge-group 20 source-learning
 no bridge-group 20 unicast-flooding
 bridge-group 20 spanning-disabled
```

Example: EAP Authentication

This example shows part of the configuration that results from using the Express Security page to create 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 don't 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
!
interface Dot11Radio0/1
 no ip address
 no ip route-cache
 !
 encryption vlan 30 mode wep mandatory
 !
 ssid eap_ssid
!
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 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 Dot11Radio0/1.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
 bridge-group 30 spanning-disabled
!
interface Dot11Radio0/1
 no ip address
 no ip route-cache
 !
 encryption vlan 30 mode wep mandatory
 !
 ssid eap_ssid
!
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 rts threshold 2312
 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 Dot11Radio0/1.30
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 bridge-group 30 subscriber-loop-control
 bridge-group 30 block-unknown-source
 no bridge-group 30 source-learning
 no bridge-group 30 unicast-flooding
 bridge-group 30 spanning-disabled
!
interface FastEthernet0
 mtu 1500
 no ip address
 ip mtu 1564
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.30
 mtu 1500
 encapsulation dot1Q 30
 no ip route-cache
 bridge-group 30
 no bridge-group 30 source-learning
 bridge-group 30 spanning-disabled
!
interface BVI1
 ip address 10.91.104.91 255.255.255.192
 no ip route-cache
!
ip http server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
ip radius source-interface BVI1
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.91.104.92 auth-port 1645 acct-port 1646 key 7 091D1C5A4D5041
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
```

Example: WPA

This example shows part of the configuration that results from using the Express Security page to create an SSID called *wpa_ssid*, excluding the SSID from the beacon, and assigning the SSID to VLAN 40:

```
ssid wpa_ssid
    vlan 40
    authentication open eap eap_methods
    authentication network-eap eap_methods
    authentication key-management wpa
 !
```

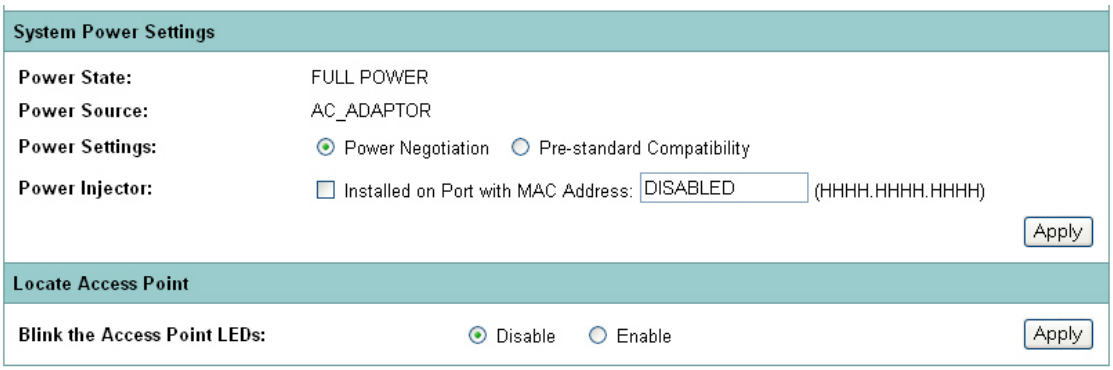
```
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.91.104.92 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
!
!
bridge irb
!
!
interface Dot11Radio0/1
 no ip address
 no ip route-cache
 !
 encryption vlan 40 mode ciphers tkip
 !
  ssid wpa_ssid
!
speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 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 Dot11Radio0/1.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 bridge-group 40 subscriber-loop-control
 bridge-group 40 block-unknown-source
 no bridge-group 40 source-learning
 no bridge-group 40 unicast-flooding
 bridge-group 40 spanning-disabled
!
  ssid wpa_ssid
!
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 FastEthernet0.40
 encapsulation dot1Q 40
 no ip route-cache
 bridge-group 40
 no bridge-group 40 source-learning
 bridge-group 40 spanning-disabled
```

Configuring System Power Settings for 1130 and 1240 Series Access Points

The 1130 and 1240 access points 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. Use the System Software: System Configuration page on the web-browser interface to select a power option. Figure 4-6 shows the System Power Settings section of the System Configuration page.

Figure 4-6 Power Options on the System Software: System Configuration Page



Using the AC Power Adapter

If you use the AC power adapter to provide power to the 1130 or 1240 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 1130 or 1240 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 1130 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 1130 or 1240 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.

Using the IP Setup Utility

IPSU enables you to find a wireless device's IP address when it has been assigned by a DHCP server. This section explains how to install the utility and how to use it to find the wireless device's IP address.

Note IPSU discovers the access point's IP address only if the unit receives an address from the DHCP server or if you set the IP address manually. By default, access points that have a console port send DHCP requests to the DHCP server indefinitely. IPSU cannot report the IP address until the access point receives one.

Note IPSU can be used only on the following operating systems: Windows 95, 98, NT, 2000, ME, or XP.

Tip Another simple way to find the wireless device's IP address is to look on the Status screen in the Aironet Client Utility on a client device associated to the wireless device.

Obtaining IPSU

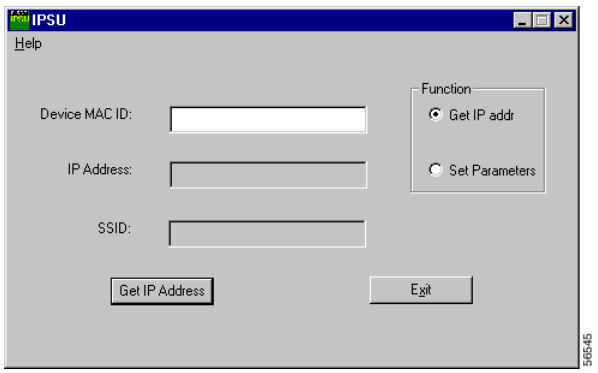
IPSU is available on the Cisco web site. Click this link to browse to the Software Center on Cisco.com: http://www.cisco.com/cisco/software/navigator.html

Using IPSU to Find the Access Point's IP Address

If the wireless device receives an IP address from a DHCP server, you can use IPSU to find its IP address. Because IPSU sends a reverse-ARP request based on the wireless device MAC address, you must run IPSU from a computer on the same subnet as the wireless device. Follow these steps to find the wireless device's IP address:

Step 1 Double-click the **IPSU** icon on your computer desktop to start the utility. The IPSU screen appears (see Figure 4-7).

Figure 4-7 IPSU Get IP Address Screen



Step 2 When the utility window opens, make sure the *Get IP addr* radio button in the Function box is selected.

Step 3 Enter the wireless device's MAC address in the Device MAC ID field. The wireless device's MAC address is printed on the label on the bottom of the unit. It should contain six pairs of hexadecimal digits. Your wireless device's MAC address might look like the following example:

000BFCFFB24E

Note The MAC address field is not case-sensitive.

Step 4 Click **Get IP Address**.

Step 5 When the wireless device's IP address appears in the IP Address field, write it down.

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's Ethernet and radio ports, the network uses the BVI. Refer to the "Using the Command-Line Interface" section on page 3-1 for information on using the CLI interface.

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's BVI:

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

	Command	Purpose
Step 2	**interface bvi1**	Enter interface configuration mode for the BVI.
Step 3	**ip address** *address mask*	Assign 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 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 When the Telnet window appears, click **Connect** and select **Remote System**.

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

Step 3 In the Host Name field, type the wireless device's 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.

Note The 8021X supplicant is available on 1130AG, 1240AG, and 1300 series access points. It is not available on 1100 and 1200 series access points.

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*:

```
ap1240AG>enable
Password:xxxxxxx
ap1240AG#config terminal
Enter configuration commands, one per line. End with CTRL-Z.
ap1240AG(config)# dot1x credentials test
ap1240AG(config-dot1x-creden)#username Cisco
ap1240AG(config-dot1x-creden)#password Cisco
ap1240AG(config-dot1x-creden)#exit
ap1240AG(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's wired port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface fastethernet 0**	Enter the interface configuration mode for the access point's Fast Ethernet port. **Note** You can also use **interface fa0** to enter the fast 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's Fast Ethernet port:

```
ap1240AG>enable
Password:xxxxxxx
ap1240AG#config terminal
Enter configuration commands, one per line. End with CTRL-Z.
ap1240AG(config)#interface fa0
ap1240AG(config-if)#dot1x credentials test
ap1240AG(config-if)#end
ap1240AG#
```

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 "Creating and Applying EAP Method Profiles for the 802.1X Supplicant" on page 11-17.

CHAPTER 5

Administering the Access PointWireless Device Access

This chapter describes how to administer the wireless device. This chapter contains these sections:

Disabling the Mode Button

You can disable the mode button on access points having a console port by using the **[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's mode button.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no boot mode-button**	Disables the access point's 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:/c1200-k9w7-mx-v123_7_ja.20050430/c1200-k9w7-mx.v123_7_ja.20050430
Config file: flash:/config.txt
Private Config file: flash:/private-config
Enable Break: no
Manual boot:no
Mode button:on
Enable IOS break: no
HELPER path-list:
NVRAM/Config file
    buffer size: 32768

ap#show boot mode-button
on
ap#
```

Note As long as the privileged EXEC password is known, you can restore the mode button to normal operation using the **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 security server. For more information, see the "Controlling Access Point Access with RADIUS" section on page 5-9.

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.

Cisco recommends 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*}	Define a new password or change an existing password for access to privileged EXEC mode.
	or	or
	enable secret [**level** *level*] {*password* | *encryption-type encrypted-password*}	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*, only type 5, a Cisco proprietary encryption algorithm, is available. If you specify an encryption type, you must provide an encrypted password—an encrypted password you copy from another access pointwireless device configuration. **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 *1FaD0$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	**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 3	**login local**	Enable local password checking at login time. Authentication is based on the username specified in Step 2.
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 no username for the only username, you can be locked out of the wireless device.

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 5-8
- 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.

	Command	Purpose
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.

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 5-10
- Configuring RADIUS Login Authentication, page 5-10 (required)
- Defining AAA Server Groups, page 5-12 (optional)
- Configuring RADIUS Authorization for User Privileged Access and Network Services, page 5-14 (optional)
- Displaying the RADIUS Configuration, page 5-15

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.

	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: • **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 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 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 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
```

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'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.

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 wireless device for user RADIUS authorization for all network-related service requests.
Step 3	**aaa authorization exec 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 for Release 12.3*.

These sections describe TACACS+ configuration:

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's profile, which is located either 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.

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict a user'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 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 tacacs+**	Configure the wireless device for user TACACS+ authorization for all network-related service requests.
Step 3	**aaa authorization exec 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. Cisco recommends 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 fastethernet0**	Enter configuration interface mode.
Step 3	**speed** {**10** | **100** | **auto**}	Configure the Ethernet speed. Cisco recommends that you use **auto**, the default setting.
Step 4	**duplex** {**auto** | **full** | **half**}	Configure the duplex setting. Cisco recommends 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 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 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, 12.3(7)JA* 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 5-22
- Monitoring and Maintaining the DHCP Server Access Point, page 5-24

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.

The 1100 series access point becomes a mini-DHCP server by default when it is configured with factory default settings and it cannot receive IP settings from a DHCP server. As a mini-DHCP server, the 1100 series access point provides up to 20 IP addresses between 10.0.0.11 and 10.0.0.30 to a PC connected to its Ethernet port and to wireless client devices configured to use no SSID, and with all security settings disabled. The mini-DHCP server feature is disabled automatically when you assign a static IP address to the 1100 series access point. Because it has a console port to simplify initial setup, the 1200 series access point does not become a DHCP server automatically.

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's 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

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's 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 5-9)
- Local authentication and authorization (for more information, see the "Configuring the Access Point for Local Authentication and Authorization" section on page 5-19)

For more information about SSH, refer to Part 5, "Other Security Features" in the *Cisco IOS Security Configuration Guide for Release 12.3.*

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, refer to Part 5, "Other Security Features" in the *Cisco IOS Security Configuration Guide for Release 12.3*, which is available on Cisco.com at the following link:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_installation_and_configuration_guides_list.html

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 5-26
- Configuring ARP Caching, page 5-27

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's 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

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/tech/tk648/tk362/technologies_tech_note09186a0080a23d02.shtml

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 of these commands in 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. Cisco recommends 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

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, 2000, at 02:00, and end on April 26, 2001, at 02:00:

```
AP(config)# clock summer-time pdt date 12 October 2000 2:00 26 April 2001 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.

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**.

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 for Release 12.3*.

This section contains this configuration information:

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 pointwireless devices, 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 5-33
- Setting Up DNS, page 5-34
- Displaying the DNS Configuration, page 5-35

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's 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

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

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, go to the following URL:
http://cisco-images.cisco.com/en/US/docs/wireless/access_point/conversion/lwapp/upgrade/guide/lwapnote.html

Migrating to Japan W52 Domain

This utility is used to migrate 802.11a radios from the J52 to W52 domains. The utility operates on the 1130, 1200 (with RM21 and RM22A radios), and 1240 access points. Migration is not supported on access points that do not ship with 802.11a radios.

The following interface global configuration mode CLI command is used to migrate an access point 802.11a radio to the W52 domain:

dot11 migrate j52 w52

After displaying appropriate warnings and entering **y**, the migration process starts and completes after the access reboots twice. The firmware initialization code reads and initializes the regulatory domain when the radio hardware is reset. The hardware reset reloads the firmware and flashes the image onto the radio and then allows the initialization to proceed. To make sure that the radio selects the regulatory domain, the access point reboots a second time.

The following example shows how the migration is accomplished:

```
ap>enable
Password:
ap#config terminal
ap(config)interface dot11radio0
ap(config-if)#dot11 migrate j52 w52
Migrate APs with 802.11A Radios in the "J"
                Regulatory Domain to the "U" Regulatory Domain.
The "J" domain allows J52 frequencies, the "U" domain allows W52 frequencies

WARNING: This migration is permanent and is not reversible, as required by law.
WARNING: Once migrated, the 802.11A radios will not operate with previous OS versions.
WARNING: All migrated APs will reboot.
WARNING: All migrated APs must be promptly reported to the manufacturer.
This AP is eligible for migration:
ap      AIR-AP1242AG-A-K9       0013.5f0e.d1e0  "J" Regulatory Domain
Begin to migrate Access Point from J (J52) to U (W52).do you want to Continue ?
(yes/[no]):yes
Burning cookie into serial eeprom:
Reading cookie from system serial eeprom...done.
Editing copy...done.
Writing cookie into system serial eeprom...done.

*Mar  1 00:09:13.844: %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
ap             AIR-AP1242AG-A-K9     0013.5f0e.d1e0 "U" Regulatory Domain
*Mar  1 00:09:13.844: Convert Regulatory Domain from J (J52) to U (W52). Writing AP nvram.
*Mar  1 00:09:14.060: %SYS-5-RELOAD: Reload requested by Exec. Reload Reason: CONVERT
REGULATORY DOMAIN FROM J to U
```

If you choose **no**, the operation terminates as shown in this example:

```
...
Begin to migrate Access Point from J (J52) to U (W52).do you want to Continue ?
(yes/[no]):no
AP not migrated.

ap(config-if)#
```

Verifying the Migration

Use the **show controllers** command to confirm the migration as shown in this typical example:

```
ap#show controllers dot11Radio 1
!
interface Dot11Radio1
Radio AIR-AP1242A, Base Address 0013.5f0e.d1e0, BBlock version
0.00, Software version 5.95.7
Serial number: ALP0916W015
Number of supported simultaneous BSSID on Dot11Radio1: 8
Carrier Set: Japan (UNI1) (JP )
Uniform Spreading Required: No
Current Frequency: 0 MHz  Channel 0
Allowed Frequencies: 5180(36) 5200(40) 5220(44) 5240(48)

Listen Frequencies: 5170(34) 5190(38) 5210(42) 5230(46) 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)
Beacon Flags: 0; Beacons are disabled; Probes are disabled High Density mode disabled
  Local Rx sensitivity (Config -127, Max -57, Min -17, Active 0) dBm
        CCA Sensitivity -64 dBm
  Cell  Rx sensitivity -80 dBm, CCA Sensitivity -60 dBm, Tx Power 127 dBm
Current Power: 17 dBm
Allowed Power Levels: -1 2 5 8 11 14 15 17
Allowed Client Power Levels: 2 5 8 11 14 15 17
Current Rates:  basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
Active Rates:
Allowed Rates:  6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Range Rates:  basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Throughput Rates:  basic-6.0 basic-9.0 basic-12.0 basic-
18.0 basic-24.0 basic-36.0 basic-48.0 basic-54.0
```

Note The country code is updated from JP to JU after migration. Radios not migrated are still shown as country code JP.

Configuring Multiple VLAN and Rate Limiting for Point-to-Multipoint Bridging

This feature modifies the way point-to-multipoint bridging can be configured to operate on multiple VLANs with the ability to control traffic rates on each VLAN. The feature is available on 32 Mb access points configured as bridges (1240 series) and the 1300 series access point/bridge. The feature is not available on 16 Mb access points (1100, 1200, and 350 series)

Note Rate limiting policy can only be applied to ingress ports of Fast Ethernet ingress ports on non-root bridges.

In a typical scenario, multiple VLAN support permits users to set up point-to-multipoint bridge links with remote sites, with each remote site on a separate VLAN. This configuration provides the user to separate and control traffic to each site. Rate limiting ensures that no remote site consumes more than a specified amount of the entire link band width. Only uplink traffic can be controlled using the FastEthernet ingress ports of non-root bridges.

Using the class-based policing feature, you can specify the rate limit and apply it to ingress of the Ethernet interface of a non-root bridge. Applying the rate at the ingress of the Ethernet interface ensures that all incoming Ethernet packets conform to the configured rate.

The following configuration shows how to define a traffic class using the **class-map** command and associate the criteria from the traffic class with the traffic policing configuration, which is configured in the service policy using the **policy-map** command. In this example, traffic policing is configured with an average rate of 8000 bits per second and a normal burst size of 1000 bytes for all incoming packets on the FastEthernet 0 interface.

```
AP enable
AP#config terminal
AP(config)#class-map sample_class
AP(config-cmap)#match any
AP(config-cmap)#exit
AP(config)#policy-map police setting
AP(config-pmap)#class sample_class
AP(config-pmap)#police 8000 1000 conform-action transmit exceed-action drop
AP(config-pmap-c)#exit
AP(config-pmap)#exit
AP(config)#interface fa0
AP(config-if)#service-policy input police-setting
```

Note There are many options available under the **class-map policy** command, however only the **match any** option is supported by this release.

CLI Command

Use the **bridge non-root client vlan** <vlan id> command to add the 802.11Q tag to all incoming Ethernet packets. This command can only be applied to non-root bridges.

CHAPTER 6

Configuring Radio Settings

This chapter describes how to configure radio settings for the wireless device. This chapter includes these sections:

Enabling the Radio Interface

The wireless device radios are disabled by default.

Note In Cisco IOS Release 12.3(8)JA there is no default SSID. You must create a Radio Service Set Identifier (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 radio is radio 0, and the 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	AP1200	AP1100	AP1130	AP1240	1300AP/ BR
Access point	X	X	X	X	X
Access point (fallback to radio shutdown)	X	X	X	X	X
Access point (fallback to repeater)	X	X	X	X	X
Repeater	X	X	X	X	X
Root bridge	X	–	–	X	X
Non-root bridge	X	–	–	X	X
Root bridge with wireless clients	X	–	–	X	X
Non-root bridge with wireless clients	X	–	–	X	X
Workgroup bridge	X	X	X	X	X

Table 6-1 Device Role in Radio Network Configuration (continued)

Role in Radio Network	AP1200	AP1100	AP1130	AP1240	1300AP/ BR
Universal workgroup bridge[1]	—	—	X	X	X
Scanner	X	X	X	X	X

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 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.

Beginning in privileged EXEC mode, follow these steps to set the wireless device's 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. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 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. • Bridge modes are available only on the 1200 and 1240 series access points. When in bridge mode, they are interoperable with the 1300 series outdoor access point/bridge only on supported bridge features. See the "Bridge Features Not Supported" section on page 6-7. • The bridge mode radio supports point-to-point configuration only. • A 1300 series 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's 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's MAC address. Also, the universal workgroup bridge role supports only one wired client. • Spanning Tree Protocol (STP) is configurable on 1200, 1240 series access points in bridge modes. • (Optional) Select the root access point's fallback role. If the wireless device's 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 Bridge/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 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 roll, you must include the client's 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's MAC address. In universal workgroup bridge mode, the workgroup bridge uses the Ethernet client's 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.

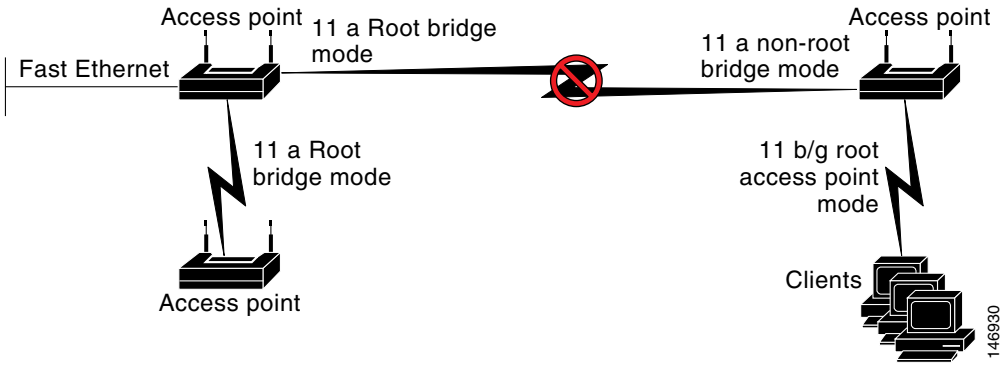
You can enable a recovery mechanism and make the workgroup bridge manageable again by disabling the Ethernet client, causing the universal workgroup bridge to associate with an access point using its own BVI address.

A *roaming* keyword has been added to the **world-mode** command to support an "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.

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 won't be able to send or receive data from the network.

Figure 6-1 Dual-Radio Fallback



Note This feature is supported by the dual-radio access points such as AP1240, AP1230, and AP 1130.

Note 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:

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

- To track radio 1, enter the following command:

```
# 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 6-2.

Note Fast Ethernet tracking does not support the Repeater mode.

- To configure the access point for fast Ethernet tracking, enter the following command:

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

MAC-Address Tracking

You can configure the radio whose role is root access point to go up or down by tracking a client access point, 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 client whose MAC address is 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
```

Bridge Features Not Supported

The following features are not supported when a 1200 or 1240 series access point is configured as a bridge:

- Clear Channel Assessment (CCA)
- Interoperability with 1400 series bridge
- Concatenation
- Install mode
- EtherChannel and PageP configuration on switch

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 always attempts to transmit at the highest data rate set to **Basic**, also called **Require** on the browser-based interface. If there are obstacles or interference, the wireless device steps down to the highest 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. For example, to set the 2.4-GHz radio for 11 megabits per second (Mbps) service only, set the 11-Mbps rate to **Basic** and set the other data rates to **Disabled**. To set the wireless device to serve only client devices operating at 1 and 2 Mbps, set 1 and 2 to **Basic** and set the rest of the data rates to **Disabled**. 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**. To set the 5-GHz radio for 54 Mbps service only, set the 54-Mbps rate to **Basic** and set the other data rates to **Disabled**.

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 four data rates to **basic**.

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 54 Mbps data rate and do not operate if data rates higher than 11Mbps are set to require on the connecting access point.

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 is radio 0, and the 5-GHz radio is radio 1.

	Command	Purpose
Step 3	**speed** These options are available for the 802.11b, 2.4-GHz radio: {[**1.0**] [**11.0**] [**2.0**] [**5.5**] [**basic-1.0**] [**basic-11.0**] [**basic-2.0**] [**basic-5.5**] | **range** | **throughput**} These options are available for the 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** } These options are available for the 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** }	Set each data rate to **basic** or **enabled**, or enter **range** to optimize range or **throughput** to optimize throughput. • (Optional) Enter **1.0**, **2.0**, **5.5**, and **11.0** to set these data rates to **enabled** on the 802.11b, 2.4-GHz radio. Enter **1.0**, **2.0**, **5.5**, **6.0**, **9.0**, **11.0**, **12.0**, **18.0**, **24.0**, **36.0**, **48.0**, and **54.0** to set these data rates to **enabled** on the 802.11g, 2.4-GHz radio. Enter **6.0**, **9.0**, **12.0**, **18.0**, **24.0**, **36.0**, **48.0**, and **54.0** to set these data rates to **enabled** on the 5-GHz radio. • (Optional) Enter **basic-1.0**, **basic-2.0**, **basic-5.5**, and **basic-11.0** to set these data rates to **basic** on the 802.11b, 2.4-GHz radio. 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's 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) 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's 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
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:

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# no speed basic-2.0 basic-5.5
ap1200(config-if)# end
```

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.
Step 3	**power local** These options are available for the 802.11b, 2.4-GHz radio (in mW): { **1** | **5** | **20** | **30** | **50** | **100** | **maximum** } These options are available for the 5-GHz radio (in mW): { **5** | **10** | **20** | **40** | **maximum** } These options are available for the 802.11a, 5-GHz radio (in dBm): {**-1** | **2** | **5** | **8** | **11** | **14** | **15** | **17** | **maximum** } If your access point contains an AIR-RM21A 5-GHz radio module, these power options are available (in dBm): { **-1** | **2** | **5** | **8** | **11** | **14** | **16** | **17** | **20** | **maximum** }	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.*"Power local for 802.11b - please remove. No such command, e.g. power local {1 | 5 | ....}" - Tania Chen*
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** }	Set the transmit power for the 802.11g, 2.4-GHz radio to one of the power levels allowed in your regulatory domain. All settings are in mW. 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 transmits at up to 100 mW for the 1, 2, 5.5, and 11Mbps data rates. However, for the 6, 9, 12, 18, 24, 36, 48, and 54Mbps data rates, the maximum transmit power for the 802.11g radio is 3050 mW.
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.
Step 3	**power client** These options are available for 802.11b, 2.4-GHz clients (in mW): { **1** | **5** | **20** | **30** | **50** | **100** | **local** | **maximum**} These options are available for 802.11g, 2.4-GHz clients (in mW): { **1** | **5** | **10** | **20** | **30** | **50** | **100** | **local** | **maximum**} These options are available for 5-GHz clients (in mW): { **5** | **10** | **20** | **40** | **local** | **maximum** } If your access point contains an AIR-RM21A 5-GHz radio module, these power options are available for 5-GHz clients (in dBm): { **-1** | **2** | **5** | **8** | **11** | **14** | **16** | **17** | **20** | **loca**l | **maximum** }	Set the maximum power level allowed on client devices that associate to the wireless device. **Note** The settings allowed in your regulatory domain might differ from the settings listed here. The **local** parameter tells the client to set its transmitter power to match the access point's local power setting. This limits the client to the higher OFDM or CCK power set on the access point. **Note** The maximum transmit power depends on your regulatory domain and the antenna gain for your access point or bridge. This command requires the client radio to be turned on and enabled to determine the valid power settings configured on your 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.

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's hardware installation guide for the frequencies allowed in your domain.

Note In places where RF interferrence might be causing clients to occassionally get disconnected from the wirless network, setting the wireless interface to run on a different channel, such as channel 1 (2412), might avoid the interference.

Note Cisco Aironet CB20A client radios sometimes fail to associate to the AIR-RM21A radio module because the CB20A client does not support all the channels supported by the AIR-RM21A radio module. The default channel setting for the AIR-RM21A radio module, least congested, often results in the access point settling on one of these frequencies that the CB20A client radio does not support: channel 149 (5745 GHz), channel 153 (5765 GHz), channel 157 (5785 GHz), and channel 161 (5805 GHz). To avoid this problem, set the channel on the AIR-RM21A radio module to one of the channels supported by the CB20A client.

Each 2.4-GHz channel covers 22 MHz. The bandwidth for channels 1, 6, and 11 does 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 eight channels from 5180 to 5320 MHzup to 27 channels from 5170 to 5850 MHz depending on regulatory domain. 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.

Beginning in privileged EXEC mode, follow these steps to set the wireless device's radio channel:

	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.

	Command	Purpose
Step 3	**channel** *frequency* | **least-congested**	Set the default channel for the wireless device radio. Table 6-3 through Table 6-6 show the available channels and frequencies for all radios. Table 6-3 and Table 6-4 show the channels and frequencies. To search for the least-congested channel on startup, enter **least-congested**. **Note** The **channel** command is disabled for 5-GHz radios that comply with European Union regulations on dynamic frequency selection (DFS). See the "Dynamic Frequency Selection" section on page 6-17 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.

Table 6-3 shows the available channels and frequencies for the IEEE 802.11b 2.4-GHz radio.

Table 6-3 Channels and Frequencies for IEEE 802.11b 2.4 GHz Radio

Channel Identifier	Center Frequency (MHz)	Regulatory Domains				
		Americas (–A)	China (–C)	EMEA (–E)	Israel (–I)	Japan (–J)
1	2412	X	X	X	–	X
2	2417	X	X	X	–	X
3	2422	X	X	X	–	X
4	2427	X	X	X	–	X
5	2432	X	X	X	X	X
6	2437	X	X	X	X	X
7	2442	X	X	X	X	X
8	2447	X	X	X	X	X
9	2452	X	X	X	–	X
10	2457	X	X	X	–	X
11	2462	X	X	X	–	X
12	2467	–	–	X	–	X
13	2472	–	–	X	–	X
14	2484	–	–	–	–	X

Table 6-4 shows the available frequencies for the 802.11g 2.4 GHz radio.

Table 6-4 Channels and Available Frequencies for IEEE 802.11g 2.4 GHz Radio

Channel Identifier	Center Frequency (MHz)	Regulatory Domains							
		Americas (–A)		EMEA (–E)		Israel (–I)		Japan (–J)	
		CCK	OFDM	CCK	OFDM	CCK	OFDM	CCK	OFDM
1	2412	X	X	X	X	–	–	X	X
2	2417	X	X	X	X	–	–	X	X
3	2422	X	X	X	X	–	–	X	X
4	2427	X	X	X	X	–	–	X	X
5	2432	X	X	X	X	X	X	X	X
6	2437	X	X	X	X	X	X	X	X
7	2442	X	X	X	X	X	X	X	X
8	2447	X	X	X	X	X	X	X	X
9	2452	X	X	X	X	X	–	X	X
10	2457	X	X	X	X	X	–	X	X
11	2462	X	X	X	X	X	–	X	X
12	2467	–	–	X	X	X	–	X	X
13	2472	–	–	X	X	X	–	X	X
14	2484	–	–	–	–	–	–	X	–

Table 6-5 shows the available channels and frequencies for the RM20A IEEE 802.11a radio

Table 6-5 Channels and Available Frequencies for the RM20A IEEE 802.11a Radio

Channel Identifier	Center Frequency (MHz)	Regulatory Domains			
		Americas (–A)	Japan	Singapore (-S)	Taiwan (-T)
34	5170	–	x	–	–
36	5180	x	–	x	–
38	5190	–	x	–	–
40	5200	x	–	x	–
42	5210	–	x	–	–
44	5220	x	–	x	–
46	5230	–	x	–	–
48	5240	x	–	x	–
52	5260	x	–	–	x
56	5280	x	–	–	x
60	5300	x	–	–	x
64	5320	x	–	–	x

Table 6-6 shows the available frequencies for the RM21A and RM22A IEEE 802.11a 5-GHz radios.

Table 6-6 Channels and Available Frequencies for the RM21A and RM22A IEEE 802.11a 5-GHz Radios

Channel ID	Center Freq (MHz)	Americas (–A)	China (–C)	EMEA (–E)	Japan (–J)	South Korea (–K)	North America (–N)	Japan (–P)	Singapore (–S)	Tiawan (–T)
34	5170	–	–	–	x	–	–	–	–	–
36	5180	x	–	x	–	x	x	x	x	–
38	5190	–	–	–	x	–	–	–	–	–
40	5200	x	–	x	–	x	x	x	x	–
42	5210	–	–	–	x	–	–	–	–	–
44	5220	x	–	x	–	x	x	x	x	–
46	5230	–	–	–	x	–	–	–	–	–
48	5240	x	–	x		x	x	x	x	–
52	5260	x	–	x	–	x	x	x	x	–
56	5280	x	–	x	–	x	x	x	x	x
60	5300	x	–	x	–	x	x	x	x	x
64	5320	x	–	x	–	x	x	x	x	x
100	5500	–	–	x	–	x	–	–	–	x
104	5520	–	–	x	–	x	–	–	–	x
108	5540	–	–	x	–	x	–	–	–	x
112	5560	–	–	x	–	x	–	–	–	x
116	5580	–	–	x	–	x	–	–	–	x
120	5600	–	–	x	–	x	–	–	–	x
124	5620	–	–	x	–	x	–	–	–	x
128	5640	–	–	x	–	–	–	–	–	x
132	5660	–	–	x	–	–	–	–	–	x
136	5680	–	–	x	–	–	–	–	–	x
140	5700	–	–	x	–	–	–	–	–	x
149	5745	x	x	–	–	x	x	–	x	x
153	5765	x	x	–	–	x	x	–	x	x
157	5785	x	x	–	–	x	x	–	x	x
161	5805	x	x	–	–	x	x	–	x	x
165	5825	–	–	–	–	–	–	–	–	–

Note The frequencies allowed in your regulatory domain might differ from the frequencies listed here.

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 6-7, 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 6-7, 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 Europe and Singapore. The access points randomly selects a channel. However, in Japan, you can manually select a channel if a radar has not been detected on it for the previous 30 minutes. If you attempt to select a channel that is unavailable due to radar detection, the CLI displays a message stating the channel is unavailable.

The full list of channels that require DFS is shown in Table 6-7.

Table 6-7 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 6-7. The user interface prevents you from manually configuring these channels. The channels not listed in Table 6-7 do not require random selection and may be manually configured.

Prior to transmitting on any channels listed in Table 6-7, 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 6-7, in addition to performing 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 my 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 Cisco recommends 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.

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#show controller dot11radio1
!
interface Dot11Radio1
Radio AIR-RM1251A, Base Address 011.9290ec0, BBlock version 0.00, Software version 6.00.0
Serial number FOCO83114WK
Number of supported simultaneous BSSID on Dot11Radio1: 8
Carrier Set: Americas (OFDM) (US )
```

```
Uniform Spreading Required: Yes
Current Frequency: 5300 MHz Channel 60 (DFS enabled)
Current Frequency: 5300 MHz  Channel 60 (DFS enabled)
Allowed Frequencies: 5180(36) 5200(40) 5220(44) 5240(48) *5260(52) *5280(56) *53
00(60) *5320(64) *5500(100) *5520(104) *5540(108) *5560(112) *5580(116) *5660(13
2) *5680(136) *5700(140) 5745(149) 5765(153) 5785(157) 5805(161)
* = May only be selected by Dynamic Frequency Selection (DFS)

Listen Frequencies: 5170(34) 5190(38) 5210(42) 5230(46) 5180(36) 5200(40) 5220(4
4) 5240(48) 5260(52) 5280(56) 5300(60) 5320(64) 5500(100) 5520(104) 5540(108) 55
60(112) 5580(116) 5600(120) 5620(124) 5640(128) 5660(132) 5680(136) 5700(140) 57
45(149) 5765(153) 5785(157) 5805(161) 5825(165)

DFS Blocked Frequencies: none
Beacon Flags: 0; Beacons are enabled; Probes are enabled
Current Power: 17 dBm
Allowed Power Levels: -1 2 5 8 11 14 15 17
Allowed Client Power Levels: 2 5 8 11 14 15 17
...
```

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**	Enter the configuration interface for the 802.11a radio
Step 3	**channel** *number* | **dfs** |**band** <*1 - 5*>}	For *number*, enter one of the following channels: 36, 40, 44, 48, 149, 153, 157, 161, 5180, 5200, 5220, 5240, 5745, 5765, 5785, or 5805. 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)`
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 selects channel 36 and configures it to use DFS on a frequency band 1:

```
ap#configure terminal
ap(config)interface dot11radio1
ap(config-if) channel 36
ap(config-if)
```

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.
- **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
```

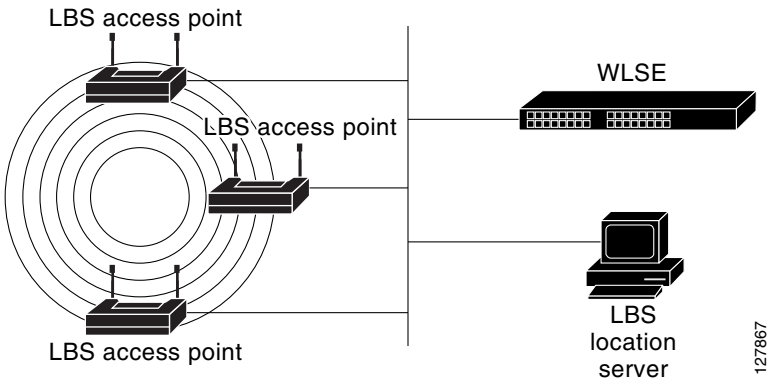
Configuring Location-Based Services

This section describes how to configure location-based services using the access point CLI. As with other access point features, you can use a WLSE on your network to configure LBS on multiple access points. LBS settings do not appear on the access point GUI in this release.

Understanding Location-Based Services

Cisco recommends that you configure a minimum of three access points for LBS. When you configure location-based services (LBS) on your access points, the access points monitor location packets sent by LBS positioning tags attached to assets that you want to track. When an access point receives a positioning packet, it measures the received signal strength indication (RSSI) and creates a UDP packet that contains the RSSI value and the time that the location packet was received. The access point forwards the UDP packets to a location server. The location server calculates the LBS tag's position based on the location information that it receives from the LBS-enabled access points. If your network has a WLSE, the location server can query the WLSE for the status of LBS-enabled access points. Figure 6-2 shows the basic parts of an LBS-enabled network.

Figure 6-2 Basic LBS Network Configuration



The access points that you configure for LBS should be in the same vicinity. If only one or two access points report messages from a tag, the location server can report that the location of the tag is somewhere in the coverage area of the two reporting access points. Consult the documentation for your LBS tags and location server for additional configuration details.

Configuring LBS on Access Points

Use the CLI to configure LBS on your access point. Beginning in privileged EXEC mode, follow these steps to configure LBS:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 lbs** *profile-name*	Create an LBS profile for the access point and enter LBS configuration mode.

	Command	Purpose
Step 3	**server-address** *ip-address* **port** *port*	Enter the IP address of the location server and the port on the server to which the access point sends UDP packets that contain location information.
Step 4	**method** {**rssi**}	(Optional) Select the location method that the access point uses when reporting location information to the location server. In this release, **rssi** (in which the access point measures the location packet's RSSI) is the only option and is also the default.
Step 5	**packet-type** {**short** | **extended**}	(Optional) Select the packet type that the access point accepts from the LBS tag. • **short**—The access point accepts short location packets from the tag. In short packets, the LBS information is missing from the tag packet's frame body and the packet indicates the tag's transmit channel. • **extended**—This is the default setting. The access point accepts extended packets from the tag. An extended packet contains two bytes of LBS information in the frame body. If the packet does not contain those two bytes in the frame body, the access point drops the packet.
Step 6	**channel-match**	(Optional) Specifies that the LBS packet sent by the tag must match the radio channel on which the access point receives the packet. If the channel used by the tag and the channel used by the access point do not match, the access point drops the packet. Channel match is enabled by default.
Step 7	**multicast-address** *mac-address*	(Optional) Specifies the multicast address that the tag uses when it sends LBS packets. The default multicast address is 01:40:96:00:00:10.
Step 8	**interface dot11** { **0** | **1** }	Specify the radio interface on which this LBS profile is enabled. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1. The profile remains inactive until you enter this command.
Step 9	**exit**	Return to global configuration mode.

In this example, the profile *southside* is enabled on the access point's 802.11g radio:

```
ap# configure terminal
ap(config)# dot11 lbs southside
ap(dot11-lbs)# server-address 10.91.105.90 port 1066
ap(dot11-lbs)# interface dot11 0
ap(dot11-lbs)# exit
```

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 wireless device 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. Cisco client devices running firmware version 5.30.17 or later detect whether the wireless device is using 802.11d or Cisco legacy world mode and automatically use world mode that matches the mode used by the wireless device.

You can also configure world mode to be always on. In this configuration, the access point essentially roams between countries changing its settings as required.

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 (sometimes called a *header*) is a section of data at the head of a packet that contains information that the wireless device and client devices need when sending and receiving packets. 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. Early models of Cisco Aironet's Wireless LAN Adapter (PC4800 and PC4800A) require long preambles.

- Long—A long preamble ensures compatibility between the wireless device and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A). 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.
- 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.
- 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.

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.

	Command	Purpose
Step 3	**gain** *dB*	Specifies the resultant gain of the antenna attached to the device. Enter a value from –128 to 128 dB. If necessary, you can use a decimal in the value, such as 1.5. **Note** This setting does not affect the behavior of the wireless device; it only informs the WLSE on your network of the device's antenna gain.
Step 4	**antenna receive** {**diversity** | **left** | **right**}	Set the receive 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**.
Step 5	**antenna transmit** {**diversity** | **left** | **right**}	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**.
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 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.

	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.

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.
Step 3	**no dot11 extension aironet**	Disable Aironet extensions.

	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.

Use the **dot11 extension aironet** command to enable Aironet extensions if they are disabled.

Configuring the Ethernet Encapsulation Transformation Method

When the wireless device receives data packets that are not 802.3 packets, the wireless device must format the packets to 802.3 using an encapsulation transformation method. These are the two transformation methods:

- 802.1H
- RFC1042—This is the default setting. Use this setting to ensure interoperability with non-Cisco Aironet wireless equipment.

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.
Step 3	**payload-encapsulation** **snap** | **dot1h**	Set the encapsulation transformation method to RFC1042 (**snap**) or 802.1h (**dot1h**, the default setting).
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 approximately 20 Cisco Aironet Workgroup Bridges that are associated to the wireless device. The default setting, **disabled**, reduces the reliability of multicast delivery to allow 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, including Address Resolution Protocol (ARP) packets, to the workgroup bridge.

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.

This feature is not supported on the 5-GHz radio.

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 }**	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.

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 6-29 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.
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 to different access points on your wireless LAN, you must set up protected ports on the switch to which the wireless devices are connected.

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.

For detailed information on protected ports and port blocking, refer to the "Configuring Port-Based Traffic Control" chapter in the *Catalyst 3550 Multilayer Switch Software Configuration Guide, 12.1(12c)EA1*. Click this link to browse to that guide:
http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_12c_ea1/configuration/guide/3550scg.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 data beacon rate is set at 2, its default setting, then the wireless device sends a beacon containing a DTIM every 200 Kμsecs. 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 is radio 0, and the 5-GHz radio is radio 1.
Step 3	**beacon period** *value*	Set the beacon period. Enter a value in Kilomicroseconds.
Step 4	**beacon dtim-period** *value*	Set the DTIM. 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 is radio 0, and the 5-GHz radio is radio 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 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 is radio 0, and the 5-GHz radio is radio 1.
Step 3	**packet retries** *value*	Set the maximum data retries. Enter a setting from 1 to 128.
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 is radio 0, and the 5-GHz radio is radio 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.

	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.

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 disabled by default.

In radio interface mode, enter this command to enable short slot time:

```
ap(config-if)# slot-time-short
```

Enter **no slot-time-short** 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.

Use the **show dot11 carrier busy** command to re-display the carrier busy test results.

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 the CoS 5 (Video) and CoS 6 (Voice) user priorities.

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 on the left side of the web-browser interface.

Step 3 When the list of Services expands, 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 menu and enter a value for maximum retries for packet discard in the corresponding field.

The default value for maximum retries is 3 for the Low Latency setting (Figure 6-3). This value indicates how many times the access point will try to retrieve 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 6-3 Packet Handling Configuration

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*.

Viewing VoWLAN Metrics

VoWLAN metrics provide you with diagnostic information pertinent to VoIP performance. This information helps you determine whether problems are being introduced by the WLAN or the wired network. VoWLAN metrics are stored on WLSE.

Note The WLSE updates VoWLAN metrics every 90 seconds and stores metrics for up to 1.5 hours.

Viewing Voice Reports

You can use a browser to access voice reports listing VoWLAN metrics stored on a WLSE. You can view reports for access point groups and for individual access points.

To view voice reports, follow these steps:

Step 1 Log in to a WLSE.

Step 2 Click the **Reports** tab.

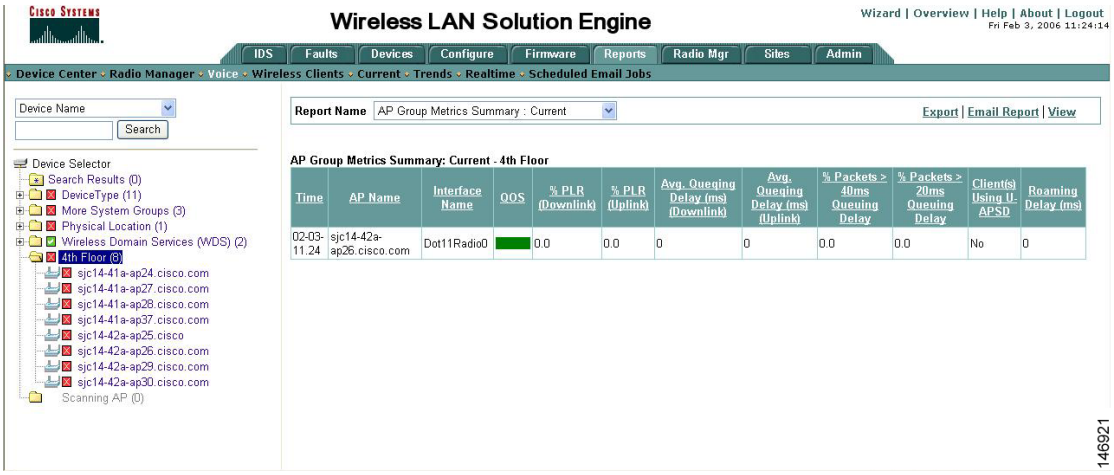
Step 3 Click **Voice**.

Step 4 From the Report Name drop-down menu, choose **AP Group Metrics Summary: Current**.

Step 5 On the left-hand side, click an access point group.

The group metrics appear on the right-hand side as shown in the example in Figure 6-4. Each line represents an access point in the group.

Figure 6-4 Access Point Metrics Summary



The information presented in the group metrics summary is an aggregate of metrics from all the voice clients of individual access points that belong to the group.

Step 6 To view voice metrics for an access point or a group of access points, select the group or device from the Device Selector tree on the left-hand side and choose the report name to view from the Report Name drop-down menu:

- To view the current metrics from the access point, choose **AP Detail: Current** from the Report Name drop-down menu. The resulting report displays the metrics for each client connected to the access points.
- To view an aggregate of the metrics recorded during the last hour, choose **AP Detail: Last Hour** from the Report Name drop-down menu.
- To view queuing delay graphs during the last hour, choose **Voice Queuing Delay** from the Report Name drop-down menu.
- To view packet loss graphs during the last hour, choose **Voice Packet Loss** from the Report Name drop-down menu.
- To view voice roaming graphs during the last hour, choose **Voice Roaming** from the Report Name drop-down menu.

- To view a graph of voice bandwidth in use during the last hour, choose **Bandwidth In Use (% Allowed)** from the Report Name drop-down menu.
- To view graphs of voice streams in progress, choose **Voice Streams In Progress** from the Report Name drop-down menu.
- To view a graph of rejected voice streams, choose **Rejected Voice Streams** from the Report Name drop-down menu.

Figure 6-5 is an example of a voice queuing delay graph.

Figure 6-5 % of Packets > 40 ms Queuing Delay

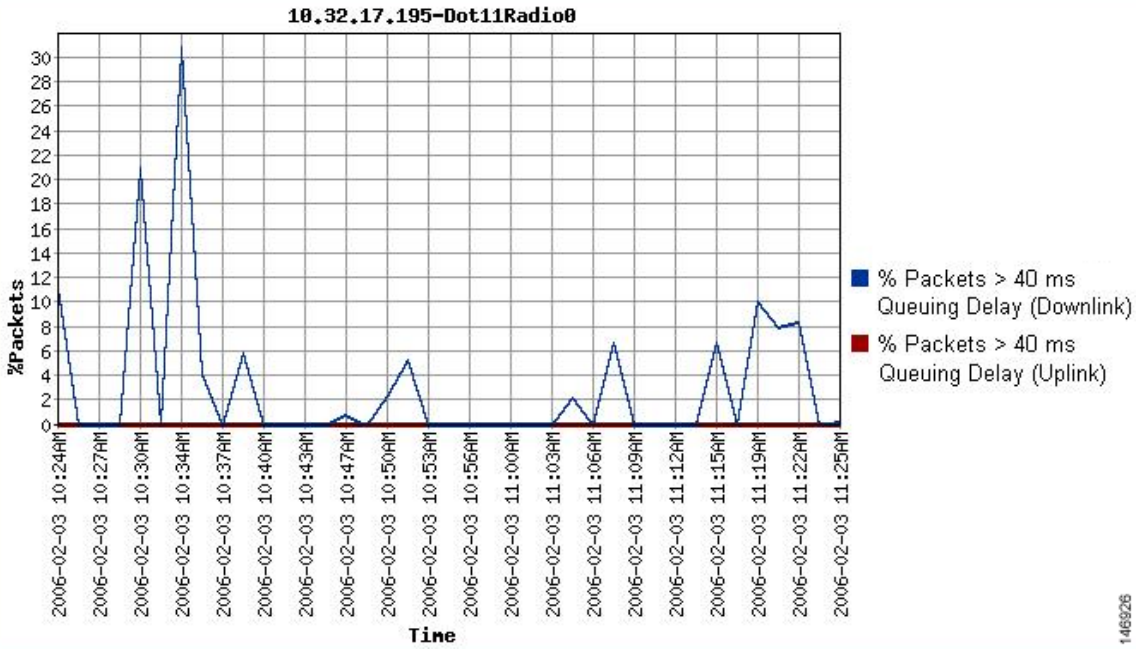
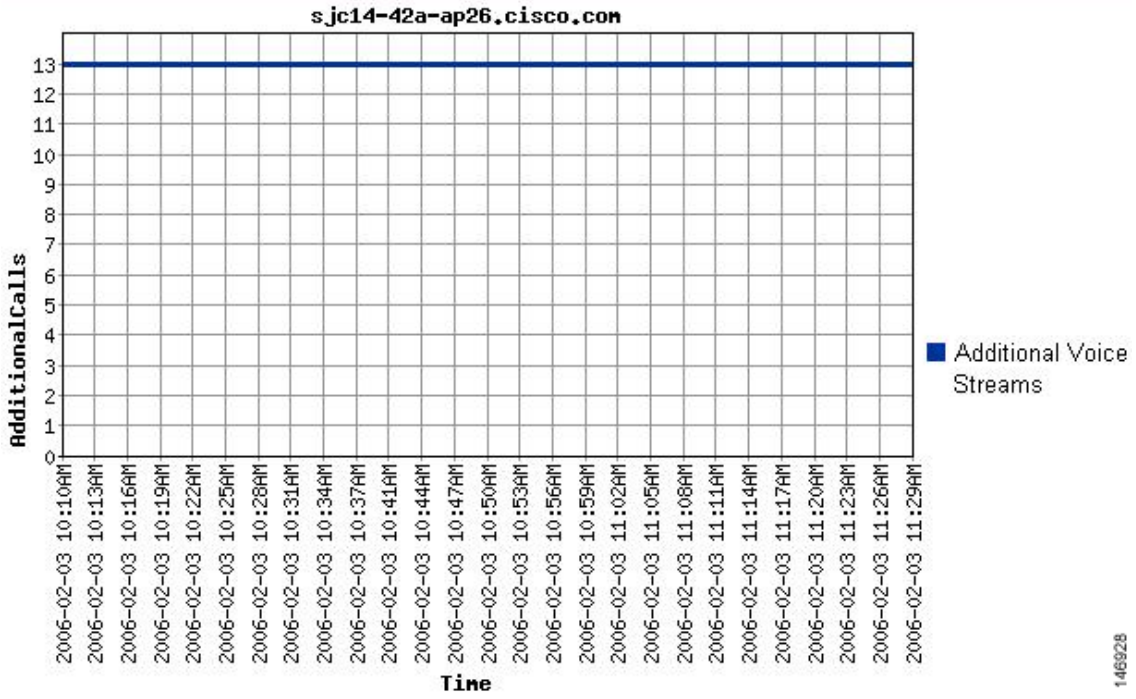


Figure 6-6 is an example of a graph showing voice streaming in progress.

Figure 6-6 Voice Streaming Progress



Viewing Wireless Client Reports

In addition to viewing voice reports from an access point perspective, you can view them from a client perspective. For every client, the WLSE displays the access points the client associated with and the WoLAN metrics that were recorded.

To view voice reports for wireless clients, follow these steps:

Step 1 Log in to a WLSE.

Step 2 Click the **Reports** tab.

Step 3 Click **Wireless Clients**.

Step 4 From the Report Name drop-down menu, choose the type of report to view.

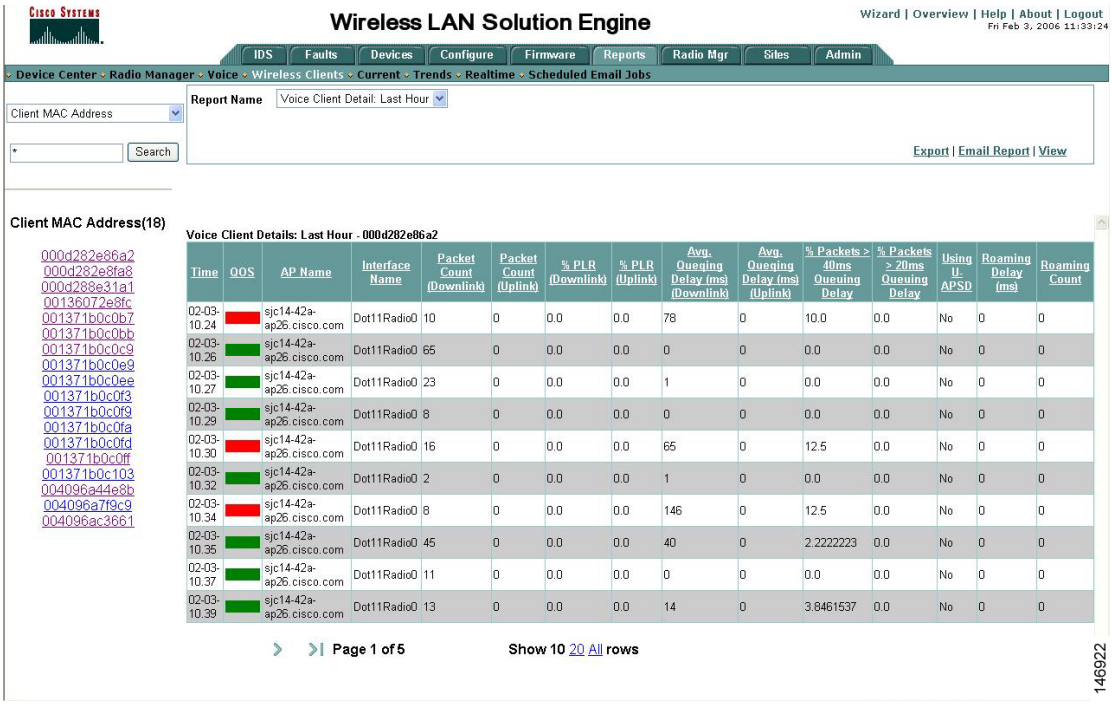
For example, to view the VoWLAN metrics for the last hour, choose **Voice Client Detail: Last Hour**.

Step 5 On the left-hand side, use the Search field to search for clients whose MAC addresses match a certain criteria.

Step 6 On the left-hand side, click the MAC address of a client to display the corresponding VoWLAN metrics.

The metrics appear on the right-hand side as shown in the example in Figure 6-7.

Figure 6-7 Wireless Client Metrics



Viewing Voice Fault Summary

The Faults > Voice Summary page in WLSE displays a summary of the faults detected with the following voice fault types:

- Excessive Voice Bandwidth (CAC)
- Degraded Voice QOS (TSM)

To view a summary of voice faults, follow these steps:

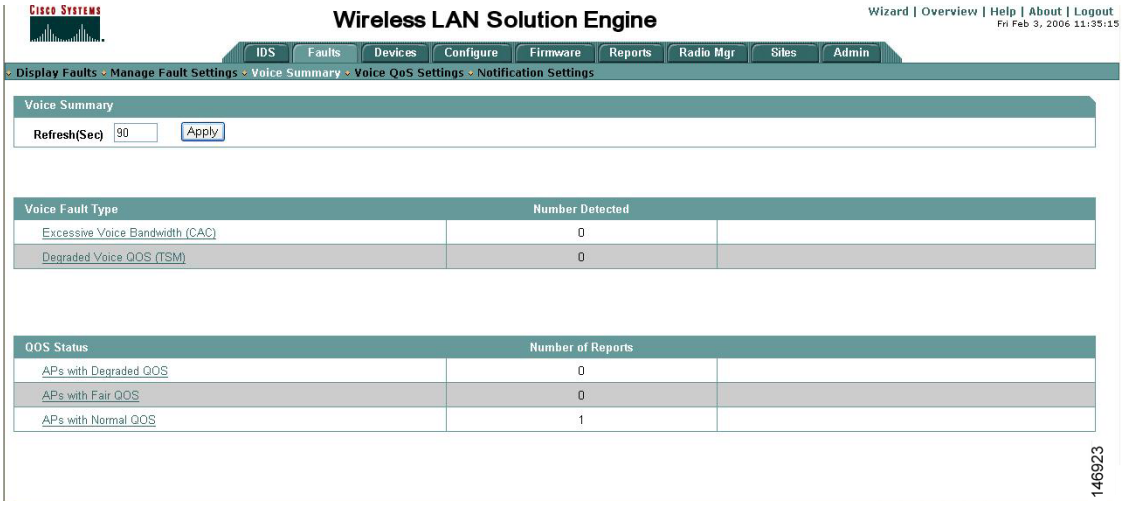
Step 1 Log in to a WLSE.

Step 2 Click the **Faults** tab.

Step 3 Click **Voice Summary**.

For both fault types, the screen lists the number of faults detected as shown in the example in Figure 6-8.

Figure 6-8 Voice Fault Summary



Configuring Voice QoS Settings

You can use WLSE's Faults > Voice QoS Settings screen to define the voice QoS thresholds for the following parameters:

- Downstream Delay with U-ASPD not used
- Downstream Delay with U-ASPD used
- Upstream Delay
- Downstream Packet Loss Rate
- Upstream Packet Loss Rate
- Roaming Time

To view a summary of voice faults, follow these steps:

Step 1 Log in to a WLSE.

Step 2 Click the **Faults** tab.

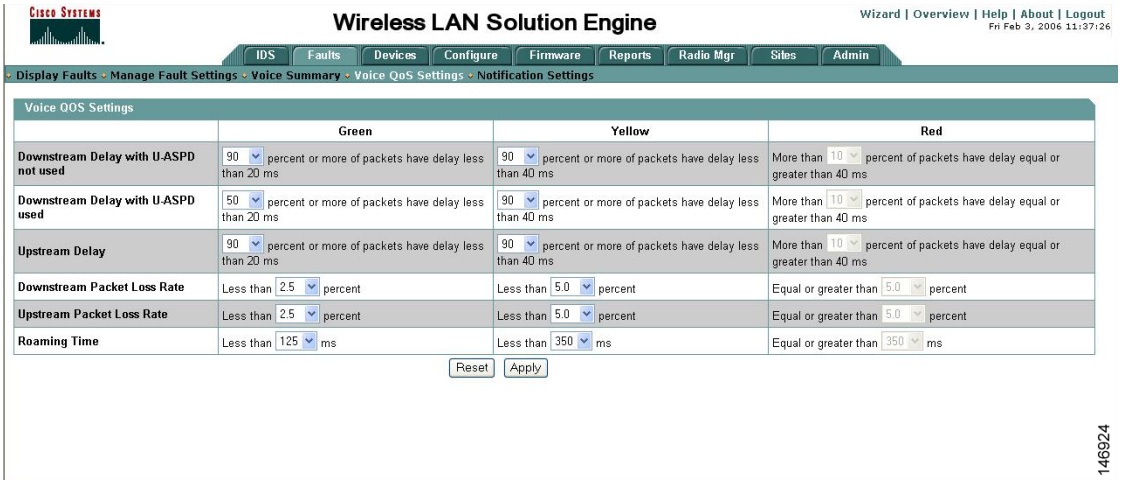
Step 3 Click **Voice QoS Settings**.

Step 4 To change a setting, choose a new value from the corresponding drop-down menu.

For example, to set the QoS indicator for Upstream Delay parameter so that the green color is shown when 90% or more of packets have a delays of less than 20 ms, choose 90 from the parameter's drop-down menu in the Green column, as shown in the example in Figure 6-9.

Step 5 Click **Apply** when done.

Figure 6-9 Voice QoS Settings



Configuring Voice Fault Settings

You can use WLSE's Faults > Manage Fault Settings screen to enable fault generation and specify the priority of the faults generated.

To configure fault settings, follow these steps:

Step 1 Log in to a WLSE.

Step 2 Click the **Faults** tab.

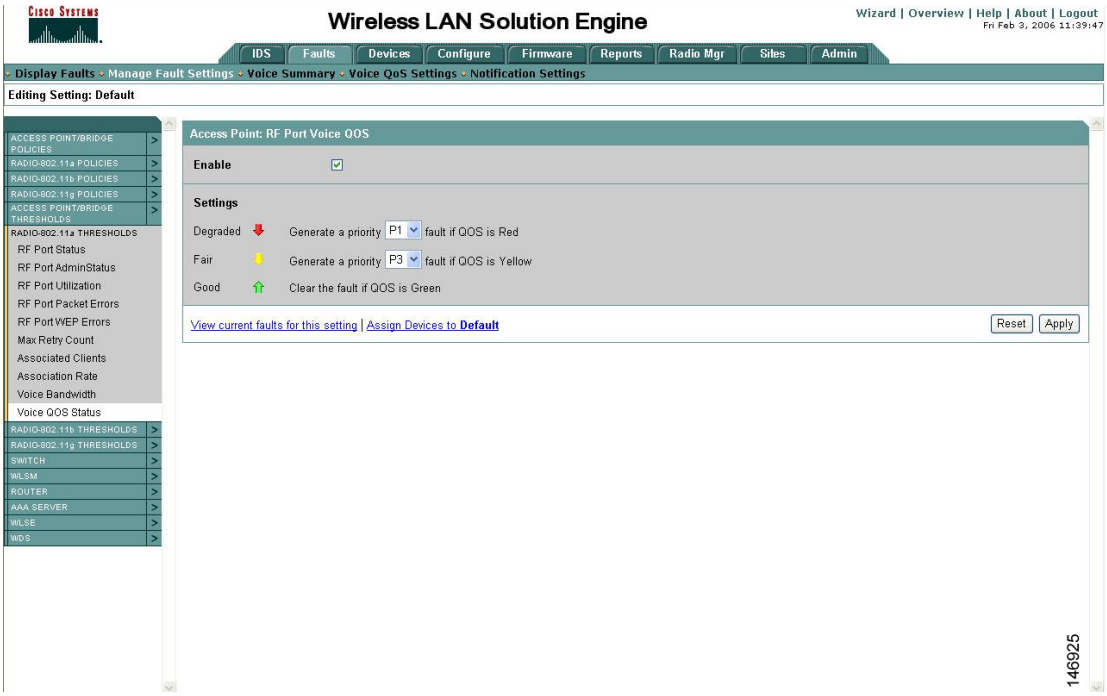
Step 3 Click **Manage Fault Settings**.

Step 4 Choose the priority of the faults generated if QoS is red (fair) from the corresponding drop-down menu.

Step 5 Click **Apply** when done.

In the example in Figure 6-8, the system generates P1 faults when QoS is degraded and P3 faults when QoS is fair. If QoS is green, the system clears the faults generated.

Figure 6-10 Fault Settings



CHAPTER 7

Configuring Multiple SSIDs

This chapter describes how to configure and manage multiple service set identifiers (SSIDs) on the access point. This chapter contains these sections:

Understanding Multiple SSIDs

The SSID is a unique identifier 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. Do not include spaces in your SSIDs.

You can configure up to 16 SSIDs on your 1200 series access point and assign different configuration settings to each SSID. All the SSIDs are 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 method

Note For detailed information on client authentication types, see Chapter 11, "Configuring Authentication Types."

- Maximum number of client associations using the SSID
- RADIUS accounting for traffic using the SSID
- Guest mode
- Repeater mode, including authentication username and password
- Redirection of packets received from client devices

If you want the access point to allow associations from client devices that do not specify an SSID in their configurations, you can set up a guest SSID. The access point includes the guest SSID in its beacon. If the guest mode is disabled, the SSID will not be broadcast in the beacon messages. If you do not want clients that do not have a preconfigured SSID to connect to the wireless network, disable the guest SSID feature. For information on how to configure guest mode SSID and disable Guest mode SSID, see the "Creating an SSID Globally" section on page 7-4.

If your access point will be a repeater or will be a root access point that acts as a parent for a repeater, you can set up an SSID for use in repeater mode. 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 one SSID to a VLAN, and client devices using the SSID are grouped in that VLAN.

Effect of Software Versions on SSIDs

Cisco introduced global-mode SSID configuration in Cisco IOS Release 12.3(2)JA to simplify configuration of SSID parameters under multiple interfaces. Configuration of SSID parameters at the interface level was supported in Cisco IOS Release 12.3(2)JA release for backward compatibility, but configuration of SSID parameters at the interface level disabled in releases after Cisco IOS Release 12.3(4)JA. Table 7-1 lists the SSID configuration methods supported in Cisco IOS Releases.

Table 7-1 SSID Configuration Methods Supported in Cisco IOS Releases

Cisco IOS Release	Supported SSID Configuration Method
12.2(15)JA	Interface-level only
12.3(2)JA	Both interface-level and global

Table 7-1 SSID Configuration Methods Supported in Cisco IOS Releases (continued)

Cisco IOS Release	Supported SSID Configuration Method
12.3(4)JA and 12.3(7)JA	Both interface-level and global; all SSIDs saved in global mode
post-12.3(4)JA	Global only

Cisco IOS Release 12.3(7)JA supports configuration of SSID parameters at the interface level on the CLI, but the SSIDs are stored in global mode. Storing all SSIDs in global mode ensures that the SSID configuration remains correct when you upgrade to release later than Cisco IOS Release 12.3(7)JA.

If you need to upgrade from Cisco IOS Release 12.3(2)JA or earlier to a release later than 12.3(4)JA, you should first upgrade to Cisco IOS Release 12.3(4)JA, save the configuration file, upgrade to the target release, and load the saved configuration file. This process ensures that your interface-level SSID configuration correctly translates to global mode. If you upgrade directly from a pre-12.3(4)JA release to a post-12.3(4)JA release, your interface-level SSID configuration is deleted.

If you downgrade the software version from Cisco IOS Release 12.3(7)JA, any SSIDs that you created become invalid. To avoid reconfiguring the SSIDs after a downgrade, save a copy of a configuration file in an earlier software version before you upgrade to Cisco IOS Release 12.3(7)JA; if you downgrade software versions from Cisco IOS Release 12.3(7)JA, load the saved configuration file after the downgrade.

Table 7-2 shows an example SSID configuration on an access point running Cisco IOS Release 12.2(15)JA and the configuration as it appears after upgrading to Cisco IOS Release 12.3(7)JA.

Table 7-2 Example: SSID Configuration Converted to Global Mode after Upgrade

SSID Configuration in 12.2(15)JA	SSID Configuration after Upgrade to 12.3(7)JA
interface dot11Radio 0 ssid engineering authentication open vlan 4 interface dot11Radio 1 ssid engineering authentication open vlan 5	dot11 ssid engineering authentication open vlan 5 ! interface dot11Radio 0 ssid engineering interface dot11Radio 1 ssid engineering

Note that the VLAN configuration under each interface is retained in the global SSID configuration.

Note SSIDs, VLANs, and encryption schemes are mapped together on a one-to-one-to-one basis; one SSID can be mapped to one VLAN, and one VLAN can be mapped to one encryption scheme. When using a global SSID configuration, you cannot configure one SSID with two different encryption schemes. For example, you cannot apply SSID *north* with TKIP on interface dot11 0 and also apply SSID *north* with WEP128 on interface dot11 1.

Configuring Multiple SSIDs

These sections contain configuration information for multiple SSIDs:

Note In Cisco IOS Release 12.3(4)JA and later, you configure SSIDs globally and then apply them to a specific radio interface. Follow the instructions in the "Creating an SSID Globally" section on page 7-4 to configure SSIDs globally.

Default SSID Configuration

In Cisco IOS Release 12.3(7)JA there is no default SSID. You must configure a minimum of one SSID to establish a Wireless LAN connection. This section explains how to configure the SSID globally.

Creating an SSID Globally

In Cisco IOS Releases 12.3(2)JA and later, you can configure SSIDs globally or for a specific radio interface. When you use the **dot11 ssid** global configuration command to create an SSID, 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.

Note SSIDs created in Cisco IOS Releases 12.3(7)JA and later become invalid if you downgrade the software version to an earlier release.

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** The first character cannot contain the !, #, or ; character. **Note** +,], /, ", TAB, and trailing spaces are invalid characters for SSIDs.

	Command	Purpose
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. Set the username and password on the SSID that the repeater access point uses to associate to a root access point, or with another repeater.
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/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfacct.htm#xtocid2
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 only one SSID to a VLAN.
Step 6	**guest-mode**	(Optional) Designate the SSID as your access point's guest-mode SSID. The access point includes the SSID in its beacon and allows associations from client devices that do not specify an SSID.
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, workgroup bridge, and non-root bridge roles. However, 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.
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 is radio 0, and the 5-GHz radio is radio 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's 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 Spaces in SSIDs

In Cisco IOS Release 12.3(7)JA and later, You can include spaces in an SSID, but trailing spaces (spaces at the end of an SSID) are invalid. However, any SSIDs created in previous versions having trailing spaces are recognized. Trailing spaces make it appear that you have identical SSIDs configured on the same access point. If you think identical SSIDs are on the access point, use the **show dot11 associations** privileged EXEC command to check any SSIDs created in a previous release for trailing spaces.

For example, this sample output from a **show configuration** privileged EXEC command does not show spaces in SSIDs:

```
ssid buffalo
    vlan 77
    authentication open

ssid buffalo
    vlan 17
    authentication open

ssid buffalo
    vlan 7
    authentication open
```

However, this sample output from a **show dot11 associations** privileged EXEC command shows the spaces in the SSIDs:

```
SSID [buffalo] :
```

```
SSID [buffalo ] :
SSID [buffalo  ] :
```

Note This command shows only the first 15 characters of the SSID. Use the **show dot11 associations client** command to see SSIDs having more than 15 characters.

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. Cisco's 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 and 802.11g radios now support up to 8 basic SSIDs (BSSIDs), which are similar to MAC addresses. You use multiple BSSIDs to assign a unique DTIM setting for each SSID and to broadcast more than one SSID in beacons. 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 BSSID's new 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
- Access points must contain an 802.11a or 802.11g radio that supports multiple BSSIDs. To determine whether a radio supports multiple basic SSIDs, 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: 8`

Guidelines for Using Multiple BSSIDs

Keep these guidelines in mind when configuring multiple BSSIDs:

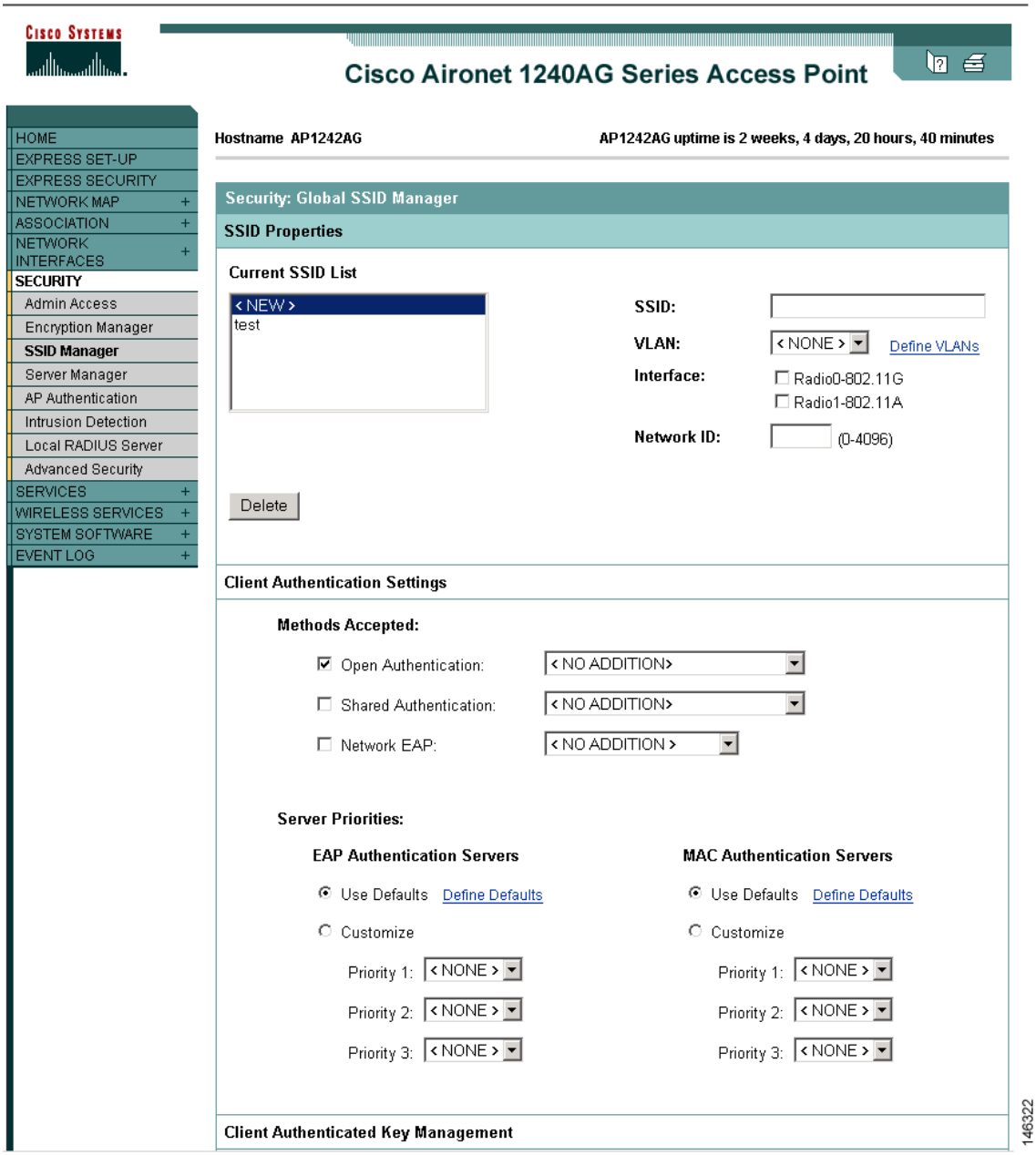
- RADIUS-assigned VLANs are not supported when you enable multiple BSSIDs.
- When you enable BSSIDs, the access point automatically maps a BSSID to each SSID. You cannot manually map a BSSID to a specific SSID.
- When multiple BSSIDs are enabled on the access point, the SSIDL IE does not contain a list 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:

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



Step 2 Enter the SSID name in the **SSID** field.

Step 3 Use the **VLAN** drop-down menu 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 enable it for a radio interface.

Step 5 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. BSSIDs 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 d0
ap(config-if)# mbssid
ap(config-if)# exit
ap(config)# dot11 ssid visitor
ap(config-ssid)# mbssid guest-mode dtim-period 75
ap(config-ssid)# exit
ap(config)# interface d0
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

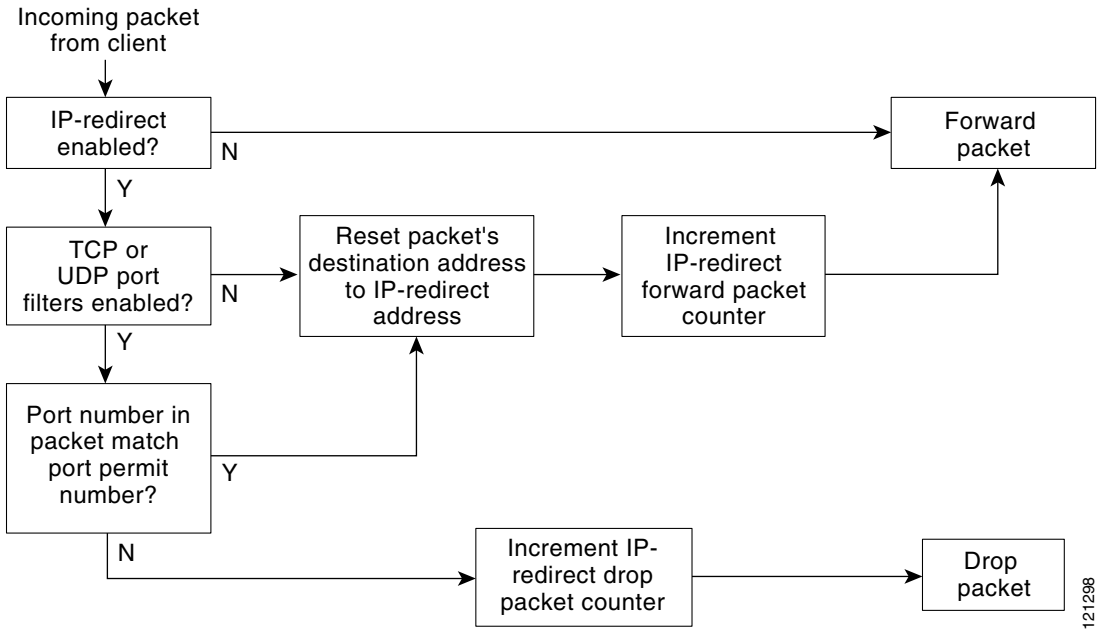
When you configure IP redirection for an SSID, the access point redirects all packets sent from client devices associated to that SSID to a specific IP address. IP redirection is used mainly on wireless LANs serving handheld devices that use a central software application and are statically configured 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



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	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface.
Step 3	**ssid** *ssid-string*	Enter configuration mode for a specific SSID.
Step 4	**ip redirection host** *ip-address*	Enter IP redirect configuration mode for the IP address. Enter the IP address with decimals, as in this 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 5	**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 access point's incoming 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)# interface dot11radio 0
AP(config-if)# ssid batman
AP(config-if-ssid)# ip redirection host 10.91.104.91
AP(config-if-ssid-redirect)# end
```

This example shows how to configure IP redirection only for packets sent to the specific TCP and UDP ports specified in an ACL. When the access point receives packets from client devices associated using the SSID *robin*, it redirects packets sent to the specified ports and discards all other packets:

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid robin
AP(config-if-ssid)# ip redirection host 10.91.104.91 access-group redirect-acl in
AP(config-if-ssid)# end
```

Including an SSID in an SSIDL IE

The access point beacon can advertise only one broadcast SSID. However, you can use SSIDL information elements (SSIDL IEs) in the access point beacon to alert client devices of additional SSIDs on the access point. When you designate an SSID to be included in an SSIDL IE, client devices detect that the SSID is available, and they also detect the security settings required to associate using that SSID.

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 SSID in an SSIDL IE:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dot11radio** { **0** | **1** }	Enter interface configuration mode for the radio interface.
Step 3	**ssid** *ssid-string*	Enter configuration mode for a specific SSID.
Step 4	**information-element ssidl** [**advertisement**] [**wps**]	Include an SSIDL IE in the access point beacon that advertises the access point's extended capabilities, 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.

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 FastEthernet0 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’s 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:

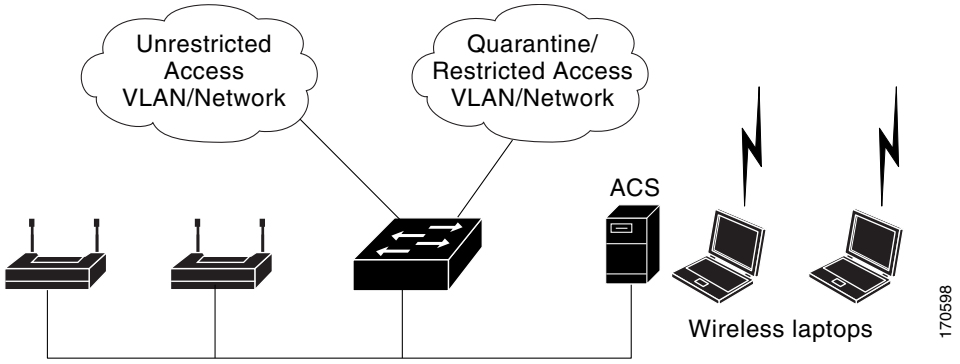
```
vlan <name>|<id> [backup <name>|<id>, <name>|<id>, <name>|<id>
```

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 3 shows a typical network setup.

Figure 3 Typical NAC Network Setup



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 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. This chapter contains these sections:

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.

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 points 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 supports both per-VLAN spanning tree (PVST) and a single 802.1q spanning tree without VLANs. The access point cannot run 802.1s MST or 802.1d Common Spanning Tree, which maps multiple VLANs into a one-instance spanning tree.

The access point 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 MAC address, is associated with each instance. For each VLAN, the access point with the lowest access point ID becomes the spanning-tree root for that VLAN.

350 Series Bridge Interoperability

Cisco Aironet 1300 and 350 Series Bridges are interoperable when STP is enabled and no VLANs are configured. This configuration is the only one available for the following reasons:

- When STP is disabled, the 350 series bridge acts as a 350 series access point and disallows association of non-root bridges, including non-root 350, 1200, and 1240 series access points.
- The 350 series bridge supports only a single instance of STP in both non-VLAN and VLAN configurations, while the 1300 series bridge has a single instance of STP in non-VLAN configurations and multiple instances of STP in VLAN configurations.
- Incompatibilities between single and multiple instances of STP can cause inconsistent blocking of traffic when VLANs are configured. When the native VLAN is blocked, you can experience bridge flapping.

Therefore, the best configuration for STP interoperability is when the 350 and 1300 series access point STP feature is enabled and VLANs are not configured.

Note When the 350 and 1300 series access points are configured as workgroup bridges, they can operate with STP disabled and allow for associations with access points. However, this configuration is not technically a bridge-to-bridge scenario.

Access Point/Bridge Protocol Data Units

The stable, active spanning-tree topology of your network is determined by these elements:

- The unique access point ID (wireless access point priority and MAC address) associated with each VLAN on each wireless access point
- 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 points in a network are powered up, each access point functions as the STP root. The access points 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 ID of the wireless access point that the sending access point identifies as the spanning-tree root
- The spanning-tree path cost to the root
- The access point ID of the sending access point
- Message age
- The identifier of the sending interface
- Values for the hello, forward delay, and max-age protocol timers

When a access point receives a configuration BPDU that contains *superior* information (lower access point 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, the access point also forwards it with an updated message to all attached LANs for which it is the designated access point.

If a access point receives a configuration BPDU that contains *inferior* information to that currently stored for that port, it discards the BPDU. If the access point is a designated access point 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 is elected as the spanning-tree root.
- A root port is selected for each access point (except the spanning-tree root). This port provides the best path (lowest cost) when the access point forwards packets to the spanning-tree root.
- The shortest distance to the spanning-tree root is calculated for each access point based on the path cost.
- A designated access point for each LAN segment is selected. The designated access point incurs the lowest path cost when forwarding packets from that LAN to the spanning-tree root. The port through which the designated access point 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 points in the Layer 2 network participating in STP gather information about other access points 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 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 with the highest access point priority (the lowest numerical priority value) is elected as the spanning-tree root. If all access points are configured with the default priority (32768), the access point with the lowest MAC address in the VLAN becomes the spanning-tree root. The access point priority value occupies the most significant bits of the access point ID.

When you change the access point priority value, you change the probability that the access point will be elected as the root access point. 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 and its ports, including access point and MAC addresses, access point 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.

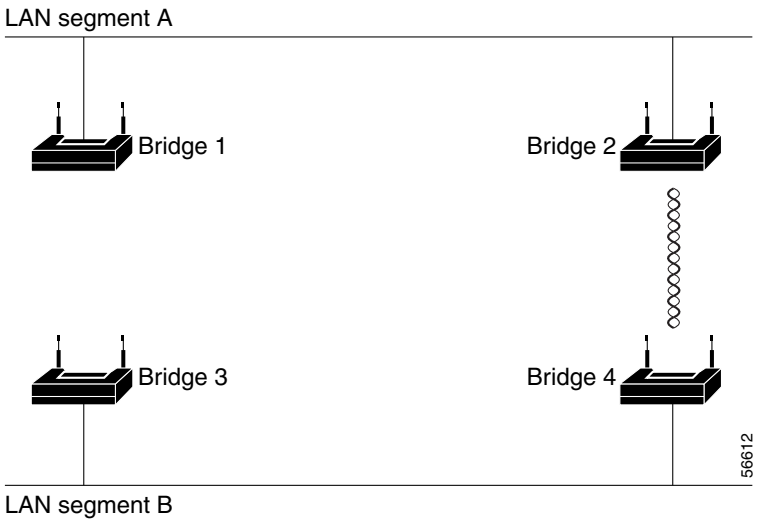
Table 8-1 Spanning-Tree Timers

Variable	Description
Hello timer	Determines how often the access point broadcasts hello messages to other access points.
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 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 points 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 using spanning tree exists in one of these states:

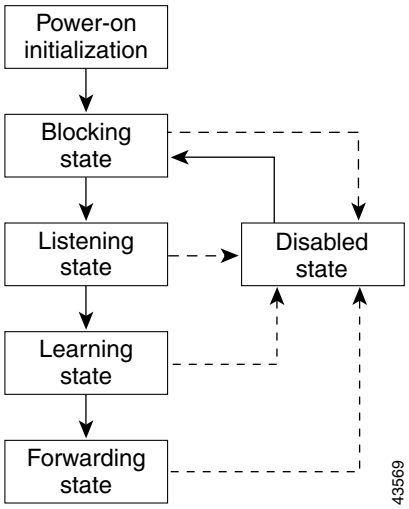
- Blocking—The interface does not participate in frame forwarding.
- Listening—The first transitional state after the blocking state when the spanning tree determines that the interface should participate in frame forwarding.
- Learning—The interface prepares to participate in frame forwarding.
- Forwarding—The 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, 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 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's Ethernet and radio ports. A access point initially functions as the spanning-tree root until it exchanges BPDUs with other access points. This exchange establishes which access point in the network is the spanning-tree root. If there is only one access point 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 port is blocked, some broadcast or multicast packets can reach a forwarding port on the access point 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:

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

Table 8-2 Default STP Values When STP is Enabled (continued)

Setting	Default Value
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 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:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface { dot11radio** *number* **| fastethernet** *number* }	Enter interface configuration mode for radio or Ethernet interfaces or sub-interfaces.
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 points with and without VLANs:

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
ip subnet-zero
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
ssid tsunami
authentication open
guest-mode
!
speed basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 2312
station-role root
no cdp enable
infrastructure-client
bridge-group 1
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1
!
interface BVI1
ip address 1.4.64.23 255.255.0.0
no ip route-cache
!
ip default-gateway 1.4.0.1
bridge 1 protocol ieee
bridge 1 route ip
bridge 1 priority 9000
!
line con 0
exec-timeout 0 0
line vty 0 4
login
line vty 5 15
login
!
```

```
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
ip subnet-zero
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
ssid tsunami
authentication open
guest-mode
!
speed basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 2312
station-role non-root
no cdp enable
bridge-group 1
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
bridge-group 1 path-cost 40
!
interface BVI1
ip address 1.4.64.24 255.255.0.0
no ip route-cache
!
bridge 1 protocol ieee
bridge 1 route ip
bridge 1 priority 10000
!
line con 0
line vty 0 4
login
line vty 5 15
login
!
end
```

Root Bridge with VLANs

This example shows the configuration of a root bridge with VLANs configured with STP enabled:

```
hostname master-bridge-hq
!
ip subnet-zero
!
ip ssh time-out 120
```

```
ip ssh authentication-retries 3
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
ssid vlan1
vlan 1
infrastructure-ssid
authentication open
!
speed basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 2312
station-role root
no cdp enable
infrastructure-client
!
interface Dot11Radio0.1
encapsulation dot1Q 1 native
no ip route-cache
no cdp enable
bridge-group 1
!
interface Dot11Radio0.2
encapsulation dot1Q 2
no ip route-cache
no cdp enable
bridge-group 2
!
interface Dot11Radio0.3
encapsulation dot1Q 3
no ip route-cache
bridge-group 3
bridge-group 3 path-cost 500
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
!
interface FastEthernet0.1
encapsulation dot1Q 1 native
no ip route-cache
bridge-group 1
!
interface FastEthernet0.2
encapsulation dot1Q 2
no ip route-cache
bridge-group 2
!
interface FastEthernet0.3
encapsulation dot1Q 3
no ip route-cache
bridge-group 3
!
interface BVI1
ip address 1.4.64.23 255.255.0.0
no ip route-cache
!
ip default-gateway 1.4.0.1
bridge 1 protocol ieee
```

```
bridge 1 route ip
bridge 1 priority 9000
bridge 2 protocol ieee
bridge 2 priority 10000
bridge 3 protocol ieee
bridge 3 priority 3100
!
line con 0
exec-timeout 0 0
line vty 5 15
!
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
!
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
bridge irb
!
interface Dot11Radio0
no ip address
no ip route-cache
!
ssid vlan1
vlan 1
authentication open
infrastructure-ssid
!
speed basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
rts threshold 2312
station-role non-root
no cdp enable
!
interface Dot11Radio0.1
encapsulation dot1Q 1 native
no ip route-cache
no cdp enable
bridge-group 1
!
interface Dot11Radio0.2
encapsulation dot1Q 2
no ip route-cache
no cdp enable
bridge-group 2
!
interface Dot11Radio0.3
encapsulation dot1Q 3
no ip route-cache
no cdp enable
bridge-group 3
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
```

```
speed auto
!
interface FastEthernet0.1
encapsulation dot1Q 1 native
no ip route-cache
bridge-group 1
!
interface FastEthernet0.2
encapsulation dot1Q 2
no ip route-cache
bridge-group 2
!
interface FastEthernet0.3
encapsulation dot1Q 3
no ip route-cache
bridge-group 3
bridge-group 3 path-cost 400
!
interface BVI1
ip address 1.4.64.24 255.255.0.0
no ip route-cache
!
bridge 1 protocol ieee
bridge 1 route ip
bridge 1 priority 10000
bridge 2 protocol ieee
bridge 2 priority 12000
bridge 3 protocol ieee
bridge 3 priority 2900
!
line con 0
line vty 5 15
!
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. This chapter contains these sections:

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

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 AAA.

	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 20 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)# 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** as the authentication port and **1813** 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 host 172.20.0.1 auth-port 1000 acct-port 1001 key 77654
AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646 key 77654
AP(config)# radius-server host 10.91.6.151 auth-port 1812 acct-port 1813 key 110337
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 host** ***hostname | ip-address*** 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 use the Aironet Client Utility to import the PAC file.

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** *filename username* [**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 **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
Router#sh radius local-server statistics
Successes              : 1           Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 0
Unknown NAS            : 0           Invalid packet from NAS: 0

NAS : 100.0.0.53
Successes              : 1           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

Username                  Successes  Failures  Blocks
clients_aaa                           1        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 thirdsecond 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 Cipher Suites and WEP

This chapter describes how to configure the cipher suites required to use WPA and CCKM authenticated key management, Wired Equivalent Privacy (WEP), WEP features including AES, Message Integrity Check (MIC), Temporal Key Integrity Protocol (TKIP), and broadcast key rotation. This chapter contains these sections:

Understanding Cipher Suites and WEP

This section describes how WEP and cipher suites protect traffic on your wireless LAN.

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 WEP is the first line of defense against intruders, Cisco recommends that you use full encryption on your wireless network.

WEP encryption scrambles the communication between the access point and client devices to keep the communication private. 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.

Extensible Authentication Protocol (EAP) authentication, also called 802.1x authentication, provides dynamic WEP keys to wireless users. 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 to enable Wi-Fi Protected Access (WPA) or Cisco Centralized Key Management (CCKM). Because cipher suites provide the protection of WEP while also allowing use of authenticated 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 menu in the web-browser interface. Cipher suites that contain TKIP provide the best security for your wireless LAN, and cipher suites that contain only WEP are the least secure.

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 Cisco Aironet 1130 and 1230 series access points support WPA2. Cisco Aironet 1100, 1200, and 1300 series 802.11g radios support WPA2 with a Cisco IOS software upgrade to Release 12.3(2)JA or later.

Note Cisco Aironet 1200 series radio modules having part numbers AIR-RM21A or AIR-RM22A support WPA2 or AES.

- 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.
- CMIC (Cisco Message Integrity Check)—Like TKIP's *Michael*, Cisco's message integrity check mechanism is designed to detect forgery attacks.
- 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. When you enable broadcast key rotation, only wireless client devices using 802.1x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point.

Configuring Cipher Suites and WEP

These sections describe how to configure cipher suites, WEP and additional WEP features such as MIC, TKIP, and broadcast key rotation:

Note WEP, TKIP, MIC, and broadcast key rotation are disabled by default.

Creating 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 is radio 0, and the 5-GHz radio is radio 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. Up to 16 VLANs can be assigned. You can assign up to 4 WEP keys for each VLAN4 WEP keys to one of the VLANs. • 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 is encrypted (**7**) or unencrypted (**0**). • (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 or CMIC, 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** Using security features such as authenticated key management can limit WEP key configurations. See the "WEP Key Restrictions" section on page 10-5 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 or CMIC	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. When you enable broadcast key rotation, only wireless client devices using 802.1x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point.

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
3	—	not set	—	not set
4	—	not set	—	FEDCBA0987654321123456789 0

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 and WEP

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.
Step 3	**encryption** [**vlan** *vlan-id*] **mode ciphers** {[**aes-ccm** | **ckip** | **cmic** | **ckip-cmic** | **tkip**]} {[**wep128** | **wep40**]}	Enable a cipher suite containing the WEP 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 WEP and WEP features. • Set the cipher options and WEP level. You can combine TKIP with 128-bit or 40-bit WEP. **Note** If you enable a cipher suite with two elements (such as TKIP and 128-bit WEP), the second cipher becomes the group cipher. **Note** If you configure **ckip**, **cmic**, or **ckip-cmic**, 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.
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.

This example sets up a cipher suite for VLAN 22 that enables CKIP (unsupported), CMIC (unsupported), and 128-bit WEP.

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# encryption vlan 22 mode ciphers ckip-cmic wep128
ap1200(config-if)# exit
```

Matching Cipher Suites with WPA and 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
WPA	• encryption mode ciphers tkip • encryption mode ciphers tkip wep128 • encryption mode ciphers tkip wep40

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 CCKM and instructions for configuring authenticated key management, see the "Using CCKM for Authenticated Clients" section on page 11-6 and the "Using WPA Key Management" section on page 11-7.

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. When you enable broadcast key rotation, only wireless client devices using 802.1x authentication (such as LEAP, EAP-TLS, or PEAP) can use the access point.

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 is radio 0, and the 5-GHz radio is radio 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 pointwireless device. This chapter contains these sections:

Understanding Authentication Types

This section describes 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. 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, authentication types that rely on an authentication server on your network.

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. Changing the service-type attribute to login-only ensures that Microsoft IAS servers recognize reauthentication requests from the access point. Use the **dot11 aaa authentication attributes service-type login-only** global configuration command to set the service-type attribute in reauthentication requests to login-only.

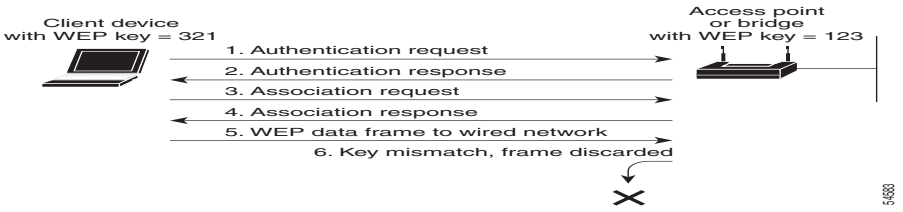
The access point uses several authentication mechanisms or types and can use more than one at the same time. These sections explain each authentication type:

Open Authentication to the Access Point

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, but the device can communicate only if its WEP keys match the access point's. Devices not using WEP do not attempt to authenticate with an access point that is using WEP. Open authentication does not rely on a RADIUS server on your network.

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



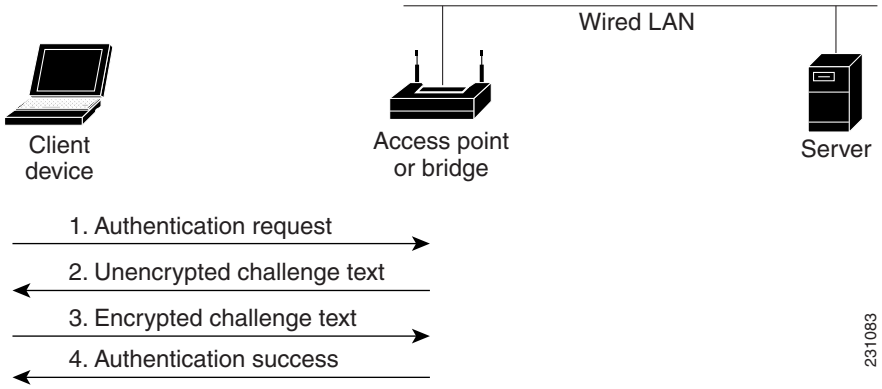
Shared Key Authentication to the Access Point

Cisco provides shared key authentication to comply with the IEEE 802.11b standard. However, because of shared key's security flaws, Cisco recommends 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

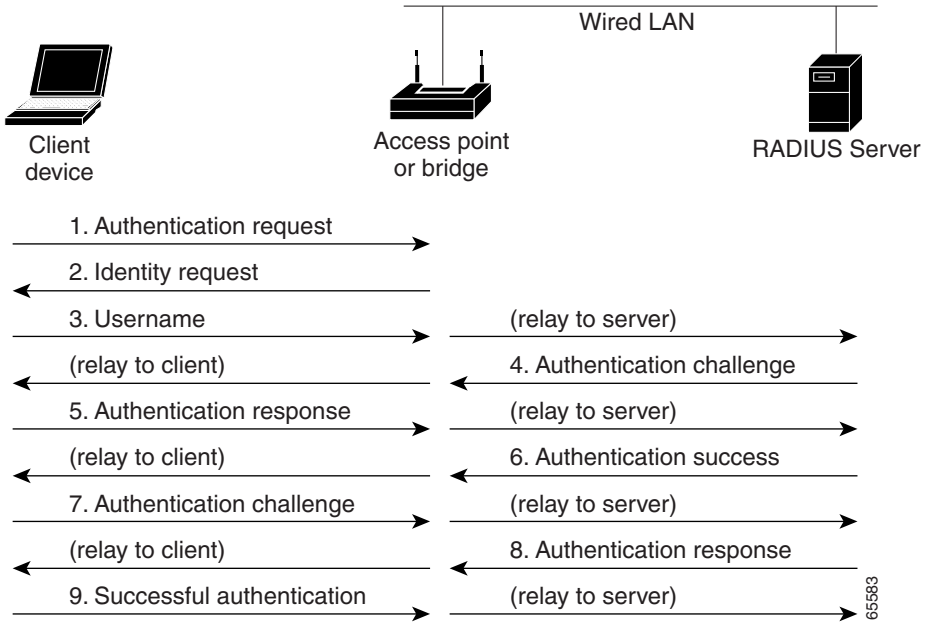


EAP Authentication to the Network

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 WEP key. The RADIUS server sends the WEP 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 WEP key (entered in the access point's WEP key slot 1) with the client's unicast key and sends it to 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 password 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 WEP key 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, called a *session key*, over the wired LAN to the access point. The access point encrypts its broadcast key with the session key and sends the encrypted broadcast key to the client, which uses the session key to decrypt it. The client and access point activate WEP and use the session and broadcast WEP 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 11-10 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 don't have to. EAP authentication controls authentication both to your access point and to your network.

MAC Address Authentication to the Network

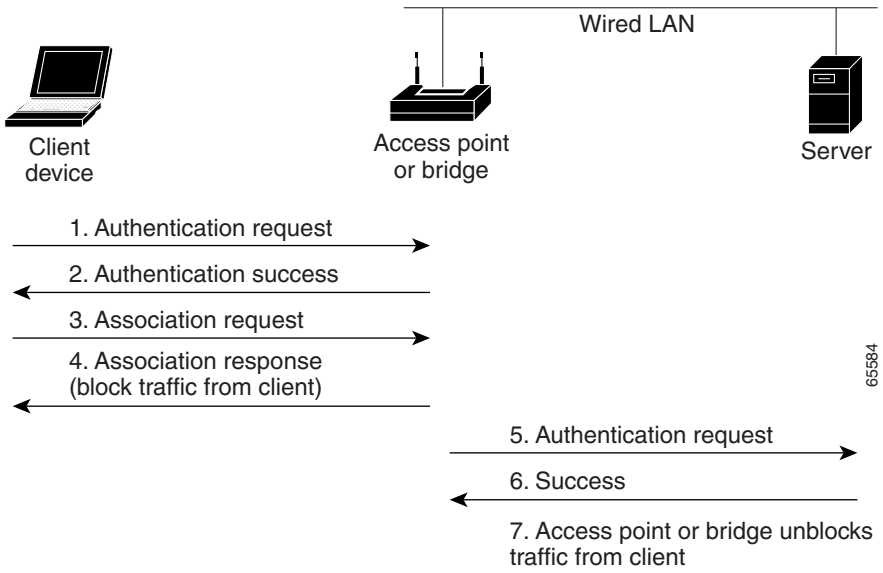
The access point relays the wireless client device's MAC address to a RADIUS server on your network, and the server checks the address against a list of allowed MAC addresses. Intruders can create counterfeit MAC addresses, so MAC-based authentication is less secure than EAP authentication. However, 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 11-10 for instructions on enabling MAC-based authentication.

Tip If you don't 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



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 11-10 for instructions on setting up this combination of authentications.

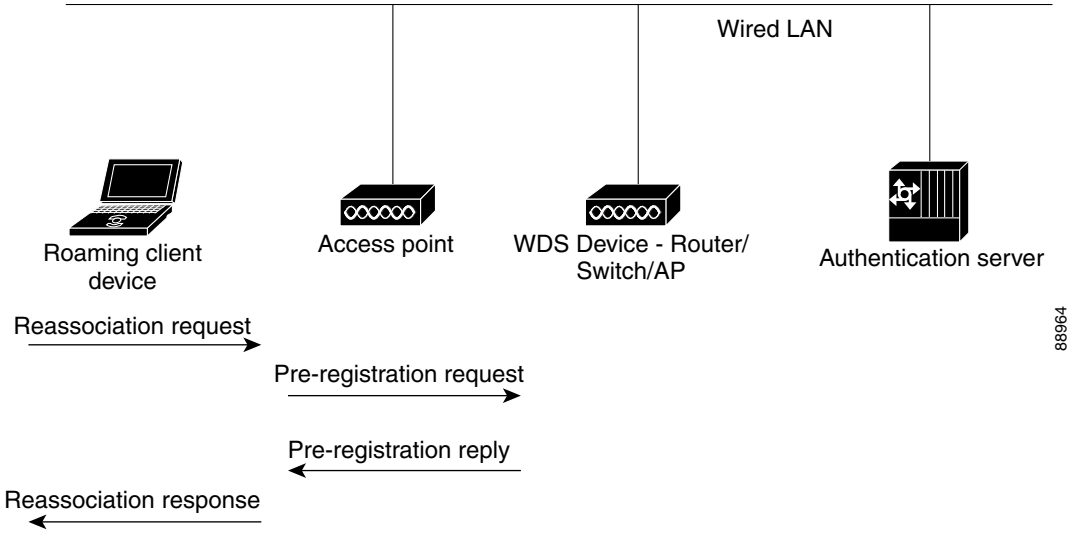
Using CCKM for Authenticated Clients

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 11-10 for instructions on enabling CCKM on your access point. See the "Configuring Access Points as Potential WDS Devices" section on page 12-9 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

Wi-Fi Protected Access is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.

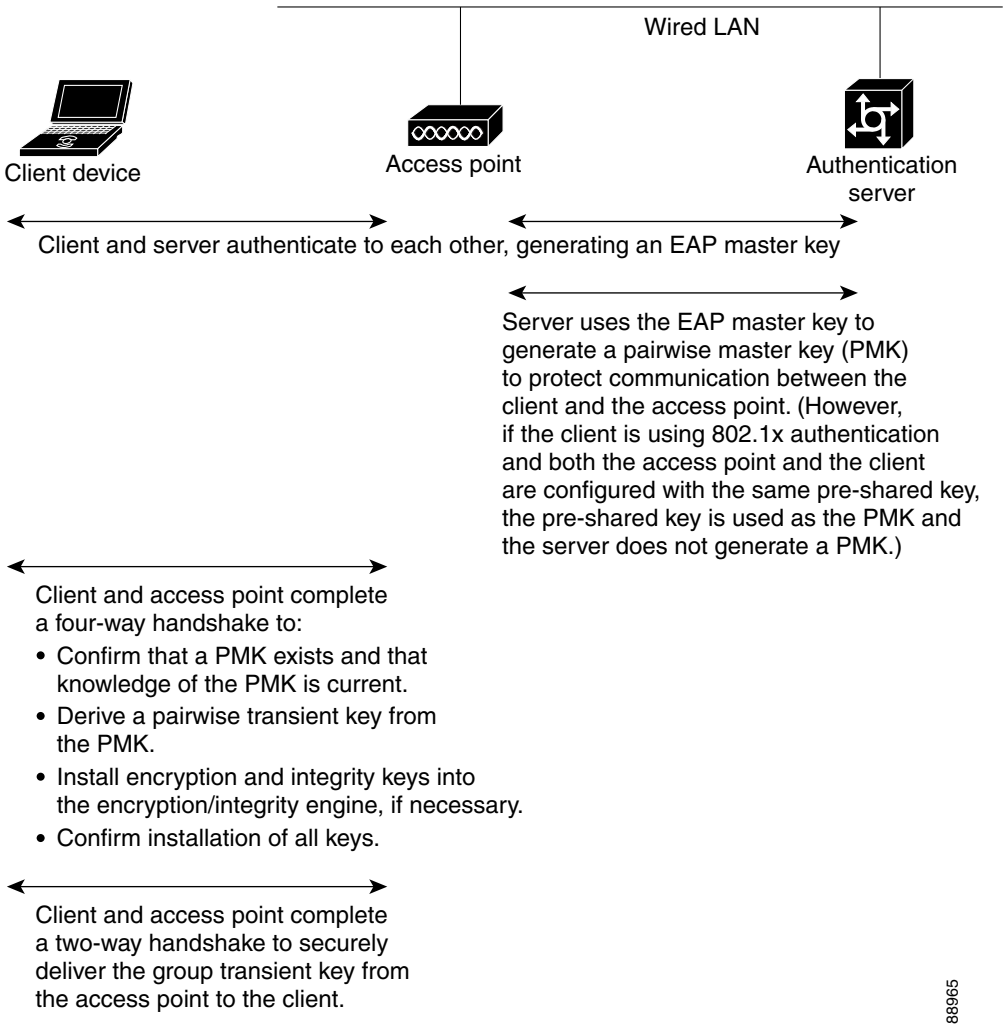
WPA key management supports two mutually exclusive management types: WPA and WPA-Pre-shared key (WPA-PSK). Using WPA key management, clients and the authentication server authenticate to each other using an EAP authentication method, and the client and server generate a pairwise master key (PMK). Using 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 11-10 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



Software and Firmware Requirements for WPA, CCKM, CKIP, and WPA-TKIP

Table 11-1 lists the firmware and software requirements required on access points and Cisco Aironet client devices to support WPA and CCKM key management and CKIP and WPA-TKIP encryption protocols.

To support the security combinations in Table 11-1, your Cisco Aironet access points and Cisco Aironet client devices must run the following software and firmware versions:

- Cisco IOS Release 12.2(13)JA or later on access points
- Install Wizard version 1.2 for 340, 350, and CB20A client devices, which includes these components:
  - PC, LM, and PCI card driver version 8.4
  - Mini PCI and PC-cardbus card driver version 3.7
  - Aironet Client Utility (ACU) version 6.2
  - Client firmware version 5.30.13

Table 11-1 Software and Firmware Requirements for WPA, CCKM, CKIP, and WPA-TKIP

Key Management and Encryption Protocol	Third Party Host Supplicant[1] Required?	Supported Platform Operating Systems
LEAP with CKIP **Note** This security combination requires 12.2(11)JA or later.	No	Windows 95/98, Me, NT, 2000, XP, Windows CE, Mac OS X, Linux, DOS
LEAP with CCKM and CKIP **Note** This security combination requires 12.2(11)JA or later.	No	Windows 98, Me, NT, 2000, XP, Windows CE
LEAP with CCKM and WPA-TKIP	No	Windows XP and 2000
LEAP with WPA (no CCKM)	No	Windows XP and 2000
Host-based EAP (such as PEAP, EAP-SIM, and EAP-TLS) with WPA (no CCKM)	No[2]	Windows XP
Host-based EAP (such as PEAP, EAP-SIM, and EAP-TLS) with WPA (no CCKM)	Yes	Windows 2000
WPA-PSK Mode	No[2]	Windows XP
WPA-PSK Mode	Yes	Windows 2000

1. Such as Funk Odyssey Client supplicant version 2.2 or Meetinghouse Data Communications Aegis Client version 2.1.
2. Windows XP does not require a third-party supplicant, but you must install Windows XP Service Pack 1 and Microsoft support patch 815485.

Refer to the *Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows* for complete instructions on configuring security settings on Cisco Aironet client devices. Click this URL to browse to the *Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows*:

http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guides_list.html

Note When you configure **TKIP**-only cipher encryption (not **TKIP + WEP 128** or **TKIP + WEP 40**) on any radio interface or VLAN, every SSID on that radio or VLAN must be set to use WPA or CCKM key management. If you configure TKIP on a radio or VLAN but you do not configure key management on the SSIDs, client authentication fails on the SSIDs.

Configuring Authentication Types

This section describes how to configure authentication types. You attach configuration types to the access point's SSIDs. See Chapter 7, "Configuring Multiple SSIDs," for details on setting up multiple SSIDs. This section contains these topics:

Note There are no default authentication SSIDs for the wireless router.

Assigning Authentication Types to an SSID

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. The SSID can consist of up to 32 alphanumeric, case-sensitive, characters. The first character cannot 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

	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. Click this link for more information on method lists: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2 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 shared key's security flaws, Cisco recommends that you avoid using it. **Note** You can assign shared key authentication to only one SSID. • (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.

	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, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. However, the access point does not force all client devices to perform EAP authentication. • (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.
Step 6	**authentication key-management** { [**wpa**] [**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 and CCKM clients can use this SSID. If you do not use the **optional** keyword, only WPA or CCKM client devices are allowed to use the SSID. To enable CCKM for an SSID, you must also enable Network-EAP authentication. When CCKM and Network EAP are enabled for an SSID, client devices using LEAP, EAP-FAST, PEAP/GTC, MSPEAP, EAP-TLS, and EAP-FAST can authenticate using the SSID. To enable WPA for an SSID, you must also enable Open authentication or Network-EAP or both. **Note** When you enable both WPA and CCKM for an SSID, you must enter **wpa** first and **cckm** second. 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. To enable both CCKM and WPA, you must set the encryption mode to a cipher suite that includes TKIP. See the "Configuring Cipher Suites and WEP" section on page 10-3 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" section on page 11-14 for instructions on configuring a pre-shared key. See Chapter 12, "Configuring WDS, Fast Secure Roaming, Radio Management, and Wireless Intrusion Detection Services," for detailed instructions on setting up your wireless LAN to use CCKM and a subnet context manager.

	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.

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

WPA migration mode allows these client device types to associate to the access point using the same SSID:

- 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 on a wireless LAN where 802.1X-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 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.

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 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 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.
Step 4	**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.
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.

	Command	Purpose
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 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 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 mac-authen filter-cache** [*address*]	Clear all entries in the cache. Include client MAC addresses to clear specific clients from the cache.
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 **no** form of the **dot11 aaa mac-authen filter-cache** command to disable MAC authentication caching. This example shows how to enable MAC authentication caching with a one-hour timeout:

```
ap# configure terminal
ap(config)# dot11 aaa mac-authen filter-cache timeout 3600
ap(config)# end
```

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 is radio 0, and the 5-GHz radio is radio 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. If the access point detects two MIC failures within 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.

Note The 8021X supplicant is available on 1130AG, 1240AG, and 1300 series access points. It is not available on 1100 and 1200 series access points.

See Creating a Credentials Profile, page 4-31 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**	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.

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 root access points. 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 fastethernet 0**	Enter the interface configuration mode for the access point's Fast Ethernet port. You can also use **interface fa0** 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. 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 is radio 0, and the 5-GHz radio is radio 1.
Step 3	**ssid** *ssid*	Assign the uplink SSID to the radio interface.
Step 4	**exit**	Return to the configure terminal mode.
Step 5	**eap profile** *profile*	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 the *Cisco Aironet Wireless LAN Client Adapters Installation and Configuration Guide for Windows* for instructions on setting authentication types on wireless client adapters. Refer to Chapter 10, "Configuring Cipher Suites and WEP," for instructions on configuring cipher suites and WEP on the access point.

Table 11-2 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**.
Likewise, to allow both Cisco Aironet 802.11a/b/g client adapters (CB21AG and PI21AG) running EAP-FAST and non-Cisco Aironet clients using EAP-FAST or 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 11-2 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

Table 11-2 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
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 don't 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.
802.1X authentication and CCKM	Enable LEAP	Select a cipher suite and enable 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.

Table 11-2 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
802.1X authentication and WPA	Enable any 802.1X authentication method	Select a cipher suite and enable Open authentication and WPA for the SSID (you can also enable Network-EAP authentication in addition to or instead of Open authentication) **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 and WPA for the SSID (you can also enable Network-EAP authentication in addition to or instead of Open authentication). Enter a WPA pre-shared key. **Note** To allow both WPA clients and non-WPA clients to use the SSID, enable optional WPA.
EAP-TLS authentication		
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and select Enable network access control using IEEE 802.1X and Smart Card or Other Certificate as the EAP Type in Windows 2000 (with Service Pack 3) or Windows XP	Set up and enable WEP and enable EAP and Open authentication for the SSID
If using Windows XP 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 Authentication for the SSID
EAP-MD5 authentication		
If using ACU to configure card	Create a WEP key, enable Host Based EAP, and enable Use Static WEP Keys in ACU and select Enable network access control using IEEE 802.1X and MD5-Challenge as the EAP Type in Windows 2000 (with Service Pack 3) or Windows XP	Set up and enable WEP and enable EAP and Open authentication for the SSID
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 11-2 Client and Access Point Security Settings (continued)

Security Feature	Client Setting	Access Point Setting
PEAP authentication		
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and select Enable network access control using IEEE 802.1X and PEAP as the EAP Type in Windows 2000 (with Service Pack 3) or Windows XP	Set up and enable WEP and enable EAP and Open authentication for the SSID
If using Windows XP 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 Authentication for the SSID
EAP-SIM authentication		
If using ACU to configure card	Enable Host Based EAP and Use Dynamic WEP Keys in ACU and select Enable network access control using IEEE 802.1X and SIM Authentication as the EAP Type in Windows 2000 (with Service Pack 3) or Windows XP	Set up and enable WEP with full encryption and enable EAP and Open authentication for the SSID
If using Windows XP 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 Authentication 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**. Likewise, to allow both Cisco Aironet 802.11a/b/g client adapters (CB21AG and PI21AG) running EAP-FAST and non-Cisco Aironet clients using EAP-FAST or LEAP to associate using the same SSID, you might need to configure the SSID for both **Network EAP** authentication and **Open authentication with EAP**.

CHAPTER 12

Configuring WDS, Fast Secure Roaming, Radio Management, and Wireless Intrusion Detection Services

This chapter describes how to configure your access points for wireless domain services (WDS), fast, secure roaming of client devices, radio management, and wireless intrusion detection services (WIDS). This chapter contains these sections:

For instructions on configuring WDS on a switch's Wireless LAN Services Module (WLSM), refer to the *Catalyst 6500 Series Wireless LAN Services Module Installation and Configuration Note*.

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, or a switch configured as the WDS device) to provide fast, secure roaming for client devices and to participate in radio management. If you use a switch as the WDS device, the switch must be equipped with a Wireless LAN Services Module (WLSM). 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, and a WLSM-equipped switch supports up to 600 participating access points and up to 240 mobility groups.

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, 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. The WDS device aggregates the information and forwards it to a wireless LAN solution engine (WLSE) device on your network.

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.
- Collects radio data from access points in the subnet, aggregates the data, and forwards it to the WLSE device on your network.
- 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, 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, or a WLSM-equipped switch.

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

Table 12-1 Participating Access Points Supported by WDS Devices (continued)

Unit Configured as WDS Device	Participating Access Points Supported
Integrated Services Router (ISR)	100 (depending on ISR platform)
WLSM-equipped switch	600

Role of Access Points Using the WDS Device

The access points on your wireless LAN interact with the WDS device in these activities:

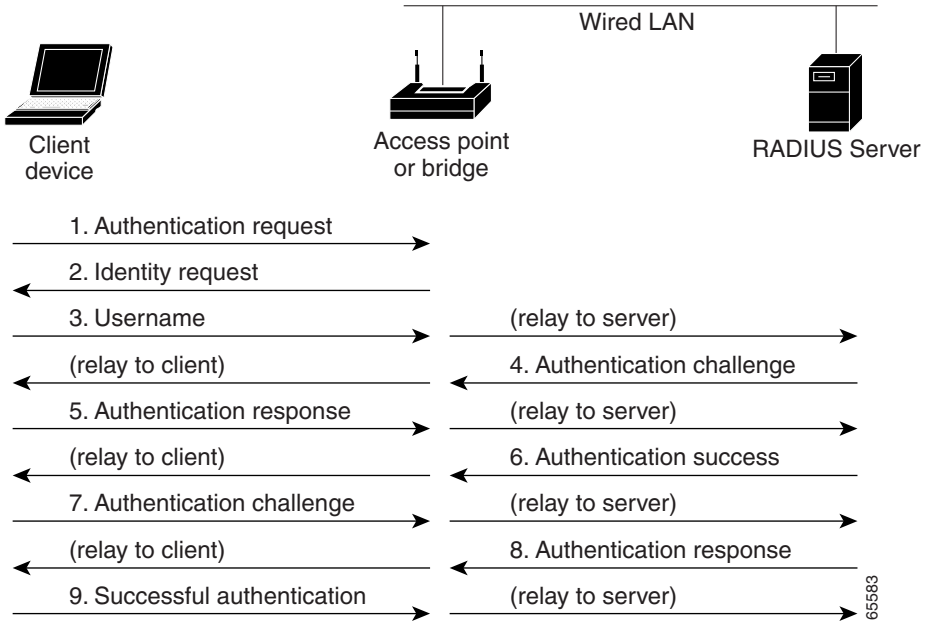
- Discover and track the current WDS device and relay WDS advertisements to the wireless LAN.
- Authenticate with the WDS device and establish a secure communication channel to the WDS device.
- Register associated client devices with the WDS device.
- Report radio data to the WDS device.

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.

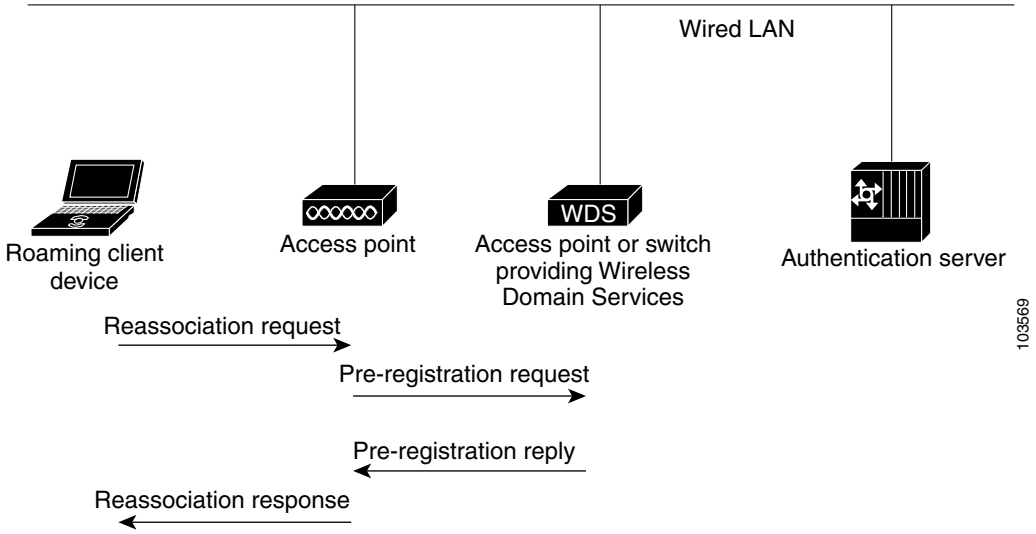
During normal operation, LEAP-enabled client devices mutually authenticate with a new access point by performing a complete LEAP authentication, including communication with the main RADIUS server, as in Figure 12-1.

Figure 12-1 Client Authentication Using a RADIUS Server



When you configure your wireless LAN for fast, secure roaming, however, LEAP-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 12-22 for instructions on configuring access points to support fast, secure roaming.

Understanding Radio Management

Access points participating in radio management scan the radio environment and send reports to the WDS device on such radio information as potential rogue access points, associated clients, client signal strengths, and the radio signals from other access points. The WDS device forwards the aggregated radio data to the WLSE device on your network. Access points participating in radio management also assist with the self-healing wireless LAN, automatically adjusting settings to provide coverage in case a nearby access point fails. Refer to the "Configuring Radio Management" section on page 12-29 for instructions on configuring radio management.

Click this URL to browse to the WLSE documentation:

http://www.cisco.com/en/US/products/sw/cscowork/ps3915/index.html

Understanding Layer 3 Mobility

When you use a WLSM as the WDS device on your network, you can install access points anywhere in a large Layer 3 network without configuring one specific subnet or VLAN throughout the wired switch infrastructure. Client devices use multipoint GRE (mGRE) tunnels to roam to access points that reside on different Layer 3 subnets. The roaming clients stay connected to your network without changing IP addresses.

For instructions on configuring WDS on a switch equipped with a Wireless LAN Services Module (WLSM), refer to the *Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM) Deployment Guide.*

The Layer 3 mobility wireless LAN solution consists of these hardware and software components:

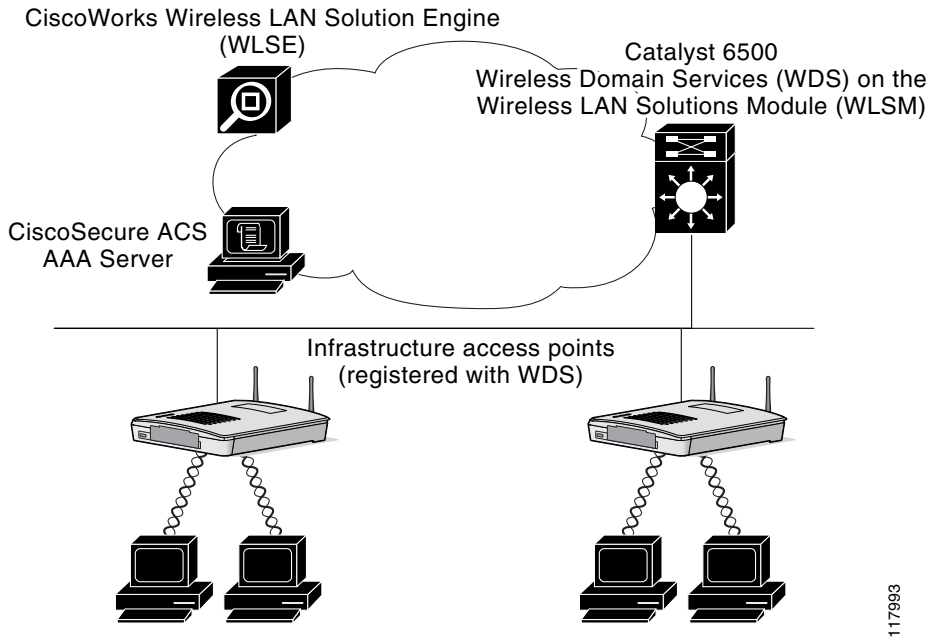
- 1100 or 1200 series access points participating in WDS
- Catalyst 6500 switch with Supervisor Module and WLSM configured as the WDS device

Note You must use a WLSM as your WDS device to properly configure Layer 3 mobility. Layer 3 mobility is not supported when you use an access point as your WDS device.

- Client devices

Figure 12-3 shows the components that interact to perform Layer 3 mobility.

Figure 12-3 Required Components for Layer 3 Mobility



Click this link to browse to the information pages for the Cisco Structured Wireless-Aware Network (SWAN):

http://www.cisco.com/en/US/netsol/ns340/networking_solutions_large_enterprise_home.html

Note If you enable Layer 3 mobility for an SSID and your WDS device does not support Layer 3 mobility, client devices cannot associate using that SSID.

Note Repeater access points and access points in workgroup bridge mode cannot associate to an SSID on which Layer 3 mobility is enabled.

Understanding Wireless Intrusion Detection Services

When you implement Wireless Intrusion Detection Services (WIDS) on your wireless LAN, your access points, WLSE, 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 WLSE, 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 WLSE derives a wired-side MAC address from the wireless MAC address and uses it to search the switch's BRIDGE MIB. When one or more searchable MAC addresses are available, the WLSE uses CDP to discover any switches connected up to two hops away from the detecting

access points. The WLSE examines the BRIDGE MIB of each CDP-discovered switch to determine if they contain any of the target MAC addresses. If CDP finds any of the MAC addresses, WLSE suppresses the corresponding switch port number.

- 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 WLSE.
- 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 12-31 for instructions on configuring the access point to participate in WIDS and Configuring Management Frame Protection, page 12-25 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.

Note MFP requires WLSE for reporting intrusion events.

Note MFP is available only on 32 Mb platforms: 1130 and 1240 series access points, and 1300 series access points in AP mode.

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.
- You cannot configure a 350 series access point as your main WDS device. However, you can configure 350 series access points to participate in WDS.

Requirements for WDS

To configure WDS, you must have these items on your wireless LAN:

- At least one access point, Integrated Services Router (ISR), or switch (equipped with a Wireless LAN Services Module) that you can configure as the WDS device
- An authentication server (or an access point or ISR configured as a local authenticator)

Note The 1300 access point/bridge cannot be configured as a WDS master, but can participate in a WDS network. This functionality is not supported on the 1300 access point/bridge.

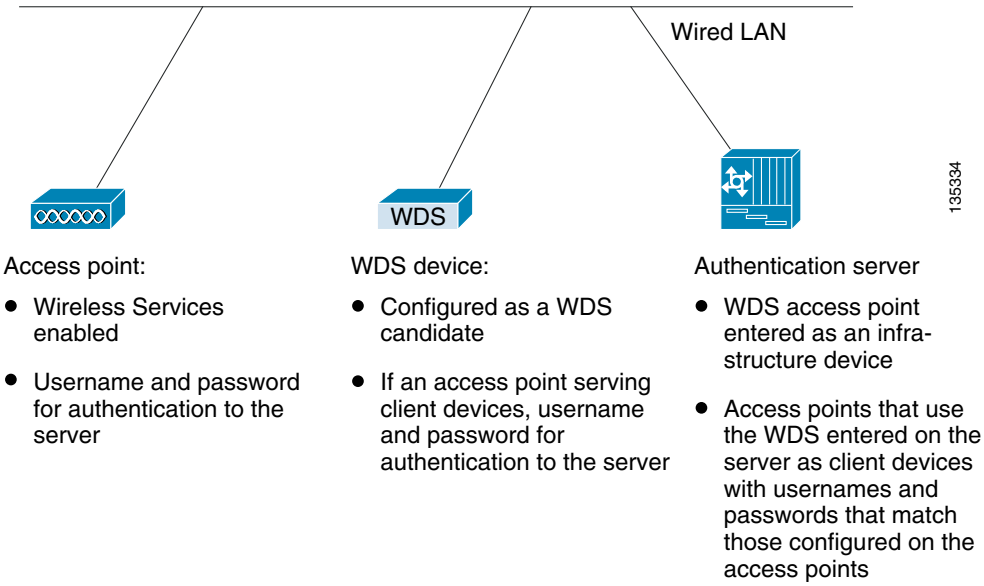
Configuration Overview

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. For instructions on configuring WDS on a switch equipped with a Wireless LAN Services Module (WLSM), refer to the *Cisco Catalyst 6500 Series Wireless LAN Services Module (WLSM) Deployment Guide.*
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 12-4 shows the required configuration for each device that participates in WDS.

Figure 12-4 Configurations on Devices Participating in WDS



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.

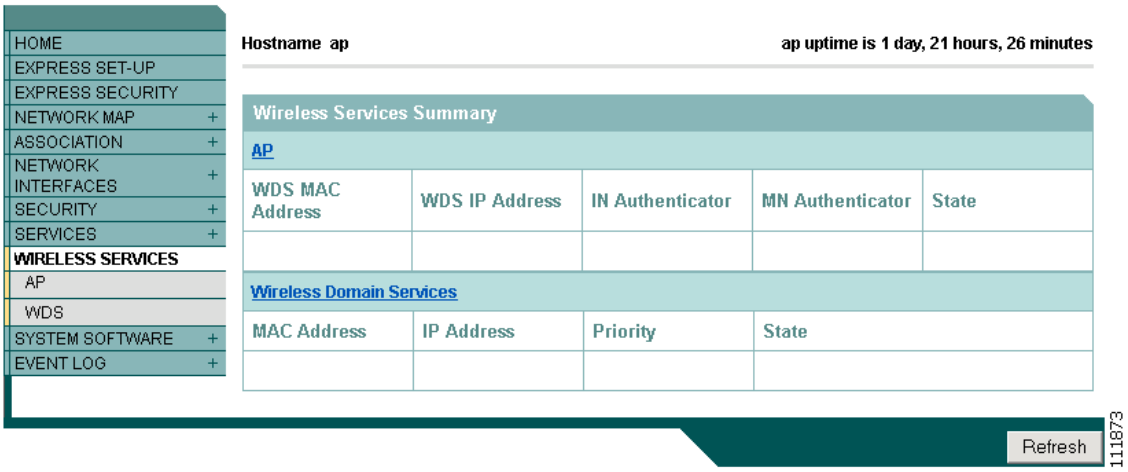
Note When WDS is enabled, the WDS access point performs and tracks all authentications. Therefore, you must configure EAP security settings on the WDS access point. See Chapter 11, "Configuring Authentication Types," for instructions on configuring EAP on the access point.

Note You cannot configure a 350 series access point as your main WDS device. However, you can configure 350 series access points to participate in WDS.

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 Browse to the Wireless Services Summary page. Figure 12-5 shows the Wireless Services Summary page.

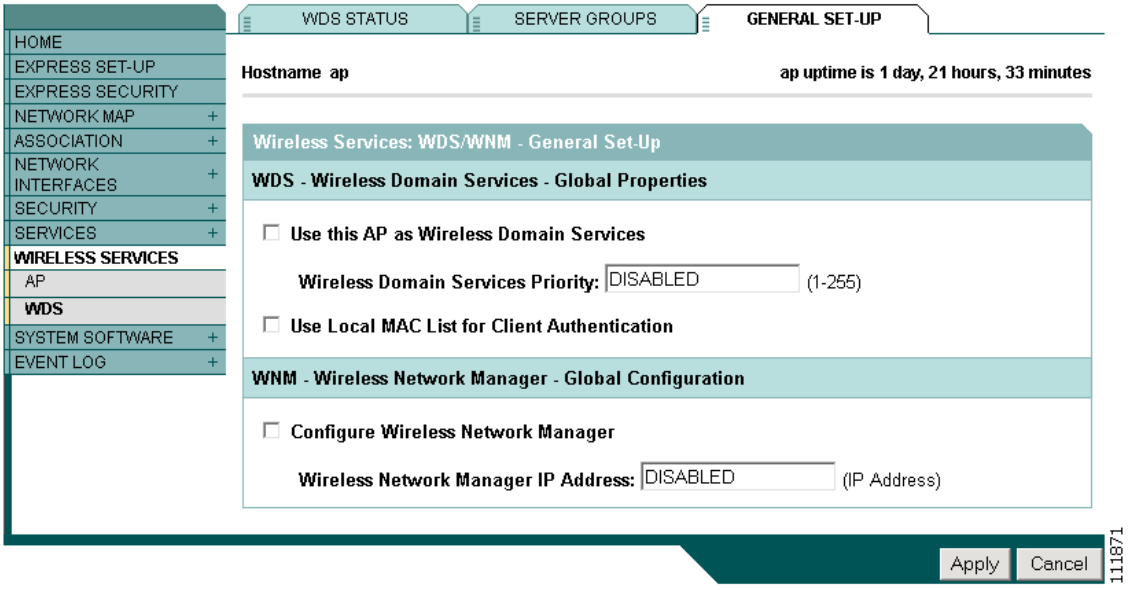
Figure 12-5 Wireless Services Summary Page



Step 2 Click **WDS** to browse to the WDS/WNM Summary page.

Step 3 On the WDS/WNM Summary page, click **General Setup** to browse to the WDS/WNM General Setup page. Figure 12-6 shows the General Setup page.

Figure 12-6 WDS/WNM General Setup Page



Step 4 Check the *Use this AP as Wireless Domain Services* check box.

Step 5 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 6 (Optional) Select the *Use Local MAC List for Client Authentication* check box to authenticate client devices using MAC addresses in the local list of addresses configured on the WDS device. If you do not select 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.

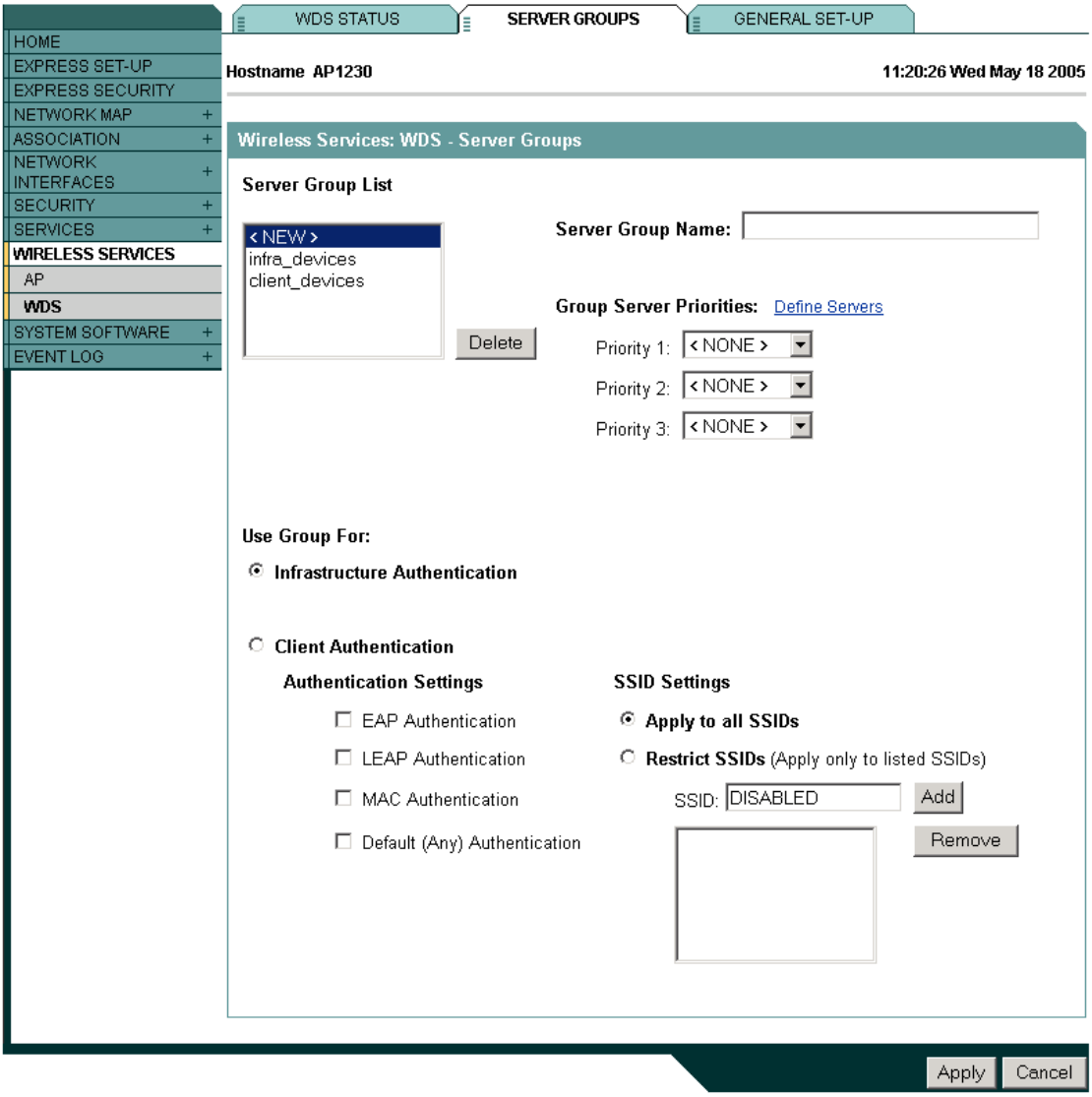
Note Selecting the *Use Local MAC List for Client Authentication* check box does not force client devices to perform MAC-based authentication. It provides a local alternative to server-based MAC-address authentication.

Step 7 (Optional) If you use a Wireless LAN Solutions Engine (WLSE) on your network, check the *Configure Wireless Network Manager* check box and enter the IP address of the WLSE device in the *Wireless Network Manager IP Address* field. The WDS access point collects radio measurement information from access points and client devices and sends the aggregated data to the WLSE device.

Step 8 Click **Apply**.

Step 9 Click **Server Groups** to browse to the WDS Server Groups page. Figure 12-7 shows the WDS Server Groups page.

Figure 12-7 WDS Server Groups Page



Step 10 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 11 Select the primary server from the Priority 1 drop-down menu. (If a server that you need to add to the group does not appear in the Priority drop-down menus, 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 don't 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 12 (Optional) Select backup servers from the Priority 2 and 3 drop-down menus.

Step 13 Click **Apply**.

Step 14 Configure the list of servers to be used for 802.1x authentication for client devices. You can specify a separate list for clients using a certain type of authentication, such as EAP, LEAP, PEAP, 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 checkbox is present specifically for the Cisco clients identified below:

- Cisco Aironet 350 series cards using LEAP and EAP-FAST
- Cisco 7920, 7921, and 7925 phones using LEAP, EAP-FAST, PEAP, & EAP-TLS
- ADU using LEAP

Unchecking the LEAP Authentication checkbox prevents these client devices from connecting to a wireless network, but does not prevent other client cards or supplicant combinations from connecting because these clients use network-EAP for authentication under the various EAP types identified above. All other clients use the 802.1x standard for open authentication.

The information above does not apply to non-Cisco clients.

Step 15 Select the primary server from the Priority 1 drop-down menu. (If a server that you need to add to the group does not appear in the Priority drop-down menus, click **Define Servers** to browse to the Server Manager page. Configure the server there, and then return to the WDS Server Groups page.)

Step 16 (Optional) Select backup servers from the Priority 2 and 3 drop-down menus.

Step 17 (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 18 Click **Apply**.

Step 19 Configure the WDS access point for LEAP authentication. See Chapter 11, "Configuring Authentication Types," for instructions on configuring LEAP.

Note If your WDS access point serves client devices, follow the instructions in the "Configuring Access Points to use the WDS Device" section on page 12-14 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 12-9:

```
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*.

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

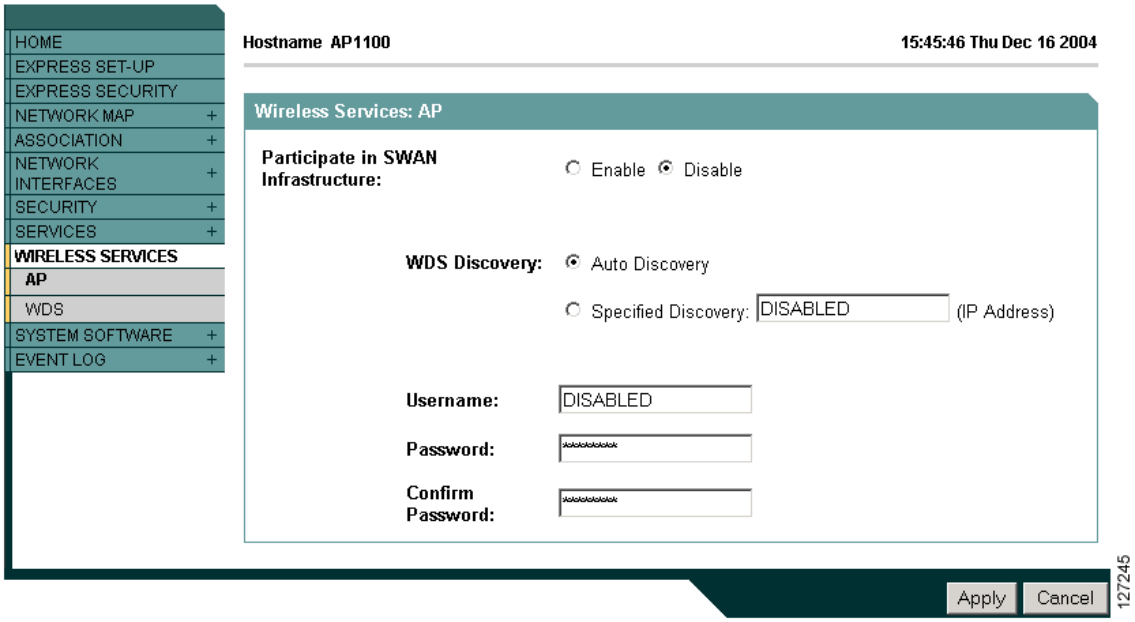
Follow these steps to configure an access point to authenticate through the WDS device and participate in WDS:

Note To participate in WDS, infrastructure access points should run the same version of IOS as the one that WDS runs.

Step 1 Browse to the Wireless Services Summary page.

Step 2 Click **AP** to browse to the Wireless Services AP page. Figure 12-8 shows the Wireless Services AP page.

Figure 12-8 Wireless Services AP Page



Step 3 Click **Enable** for the *Participate in SWAN Infrastructure* setting.

Step 4 (Optional) If you use a WLSM switch module as the WDS device on your network, select **Specified Discovery** and enter the IP address of the WLSM 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 5 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 6 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.

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 12-14:

```
AP# configure terminal
AP(config)# wlccp ap username APWestWing password 7 wes7win8
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. 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*.

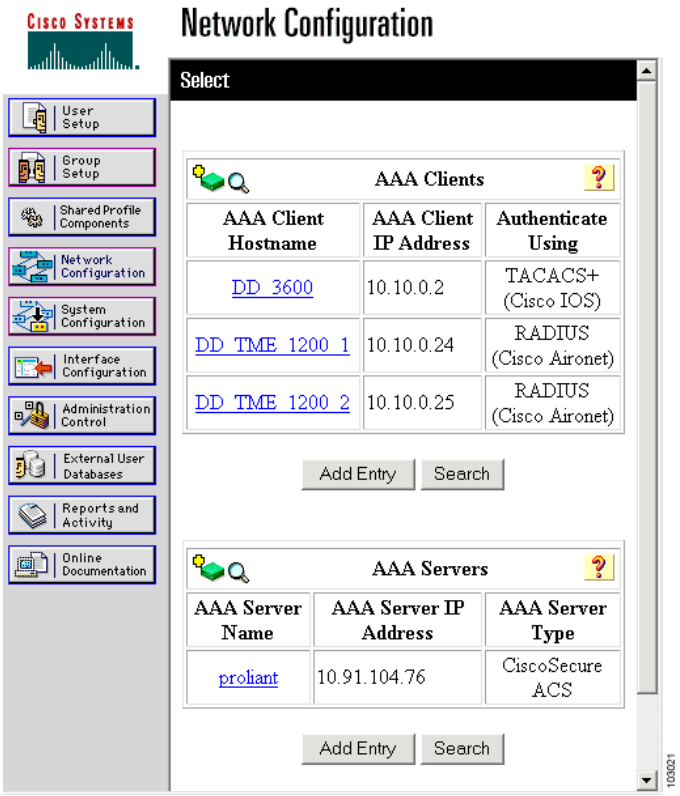
Configuring the Authentication Server to Support WDS

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:

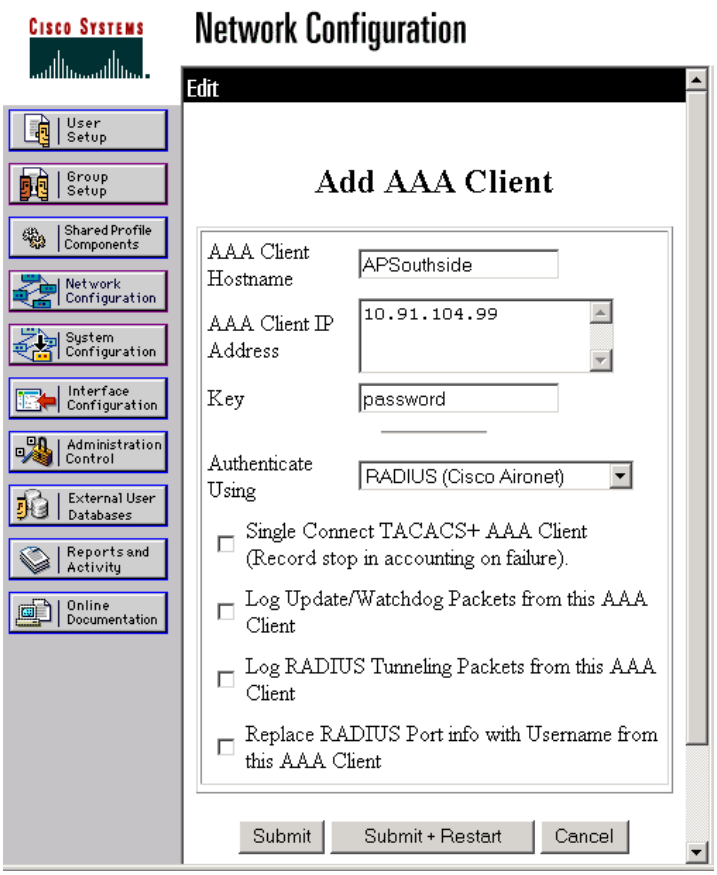
Step 1 Log into Cisco Secure ACS and click **Network Configuration** to browse to the Network Configuration page. You must use the Network Configuration page to create an entry for the WDS device. Figure 12-9 shows the Network Configuration page.

Figure 12-9 Network Configuration Page



Step 2 Click **Add Entry** under the AAA Clients table. The Add AAA Client page appears. Figure 12-10 shows the Add AAA Client page.

Figure 12-10 Add AAA Client Page



Step 3 In the AAA Client Hostname field, enter the name of the WDS device.

Step 4 In the AAA Client IP Address field, enter the IP address of the WDS device.

Step 5 In the Key field, enter exactly the same password that is configured on the WDS device.

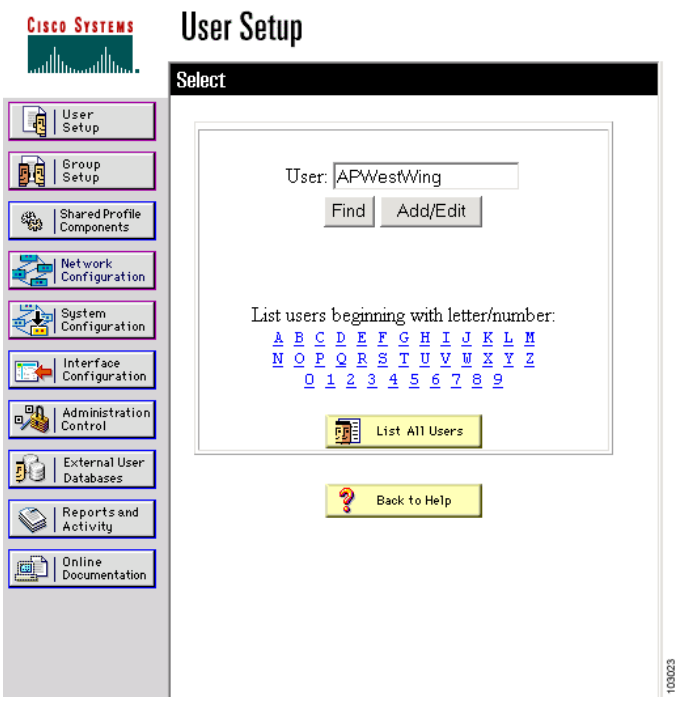
Step 6 From the Authenticate Using drop-down menu, select **RADIUS (Cisco Aironet)**.

Step 7 Click **Submit**.

Step 8 Repeat Step 2 through Step 7 for each WDS device candidate.

Step 9 Click **User Setup** to browse to the User Setup page. You must use the User Setup page to create entries for the access points that use the WDS device. Figure 12-11 shows the User Setup page.

Figure 12-11 User Setup Page

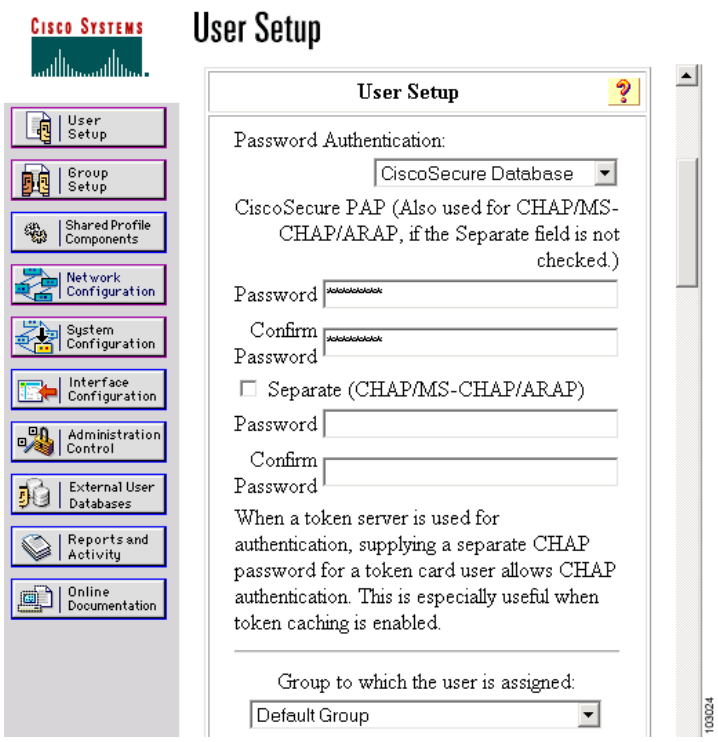


Step 10 Enter the name of the access point in the User field.

Step 11 Click **Add/Edit**.

Step 12 Scroll down to the User Setup box. Figure 12-12 shows the User Setup box.

Figure 12-12 ACS User Setup Box



Step 13 Select **CiscoSecure Database** from the Password Authentication drop-down menu.

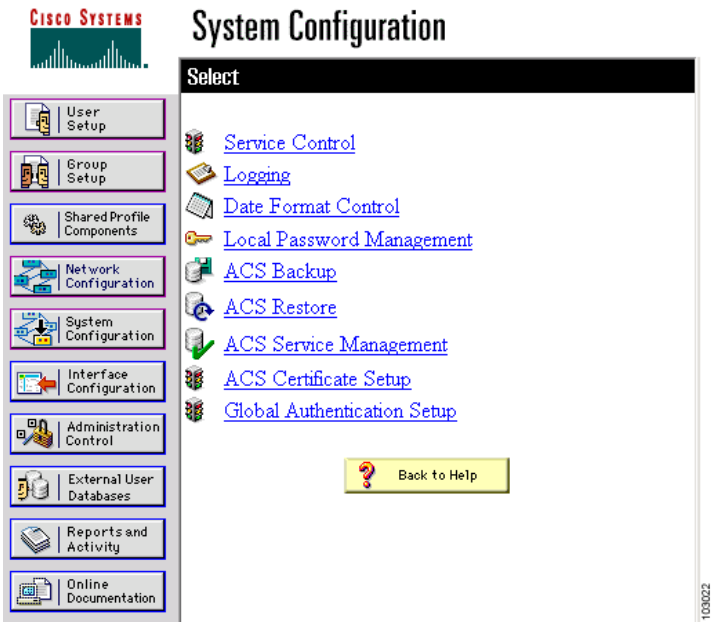
Step 14 In the Password and Confirm Password fields, enter exactly the same password that you entered on the access point on the Wireless Services AP page.

Step 15 Click **Submit**.

Step 16 Repeat Step 10 through Step 15 for each access point that uses the WDS device.

Step 17 Browse to the System Configuration page, click **Service Control**, and restart ACS to apply your entries. Figure 12-13 shows the System Configuration page.

Figure 12-13 ACS System Configuration Page



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** command to turn off WDS onlly 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 reloadss, the dot11 radio subsytems 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** | **mn** } [**detail**] [**mac-addr** *mac-address*]	On the WDS device only, use this command to display cached information about access points and client devices. • **ap**—Use this option to display access points participating in CCKM. The command displays each access point's MAC address, IP address, state (authenticating, authenticated, or registered), and lifetime (seconds remaining before the access point must reauthenticate). Use the **mac-addr** option to display information about a specific access point. • **mn**—Use this option 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-addr** option to display information about a specific client device. If you only enter **show wlccp wds**, the command displays 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. If the state is WDS-only, the command displays the device's MAC address, IP address, interface state, access point count, and mobile node count.

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** | **wds-discovery** | **state**}	Use this command to turn on display of debug messages related to client devices (**mn**), 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 wds [**aggregator** | **authenticator** | **nm** | **state** | **statistics**]	Use this command and its options to turn on display of WDS debug messages. 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, or switch (equipped with a WLSM) 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, or switch 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

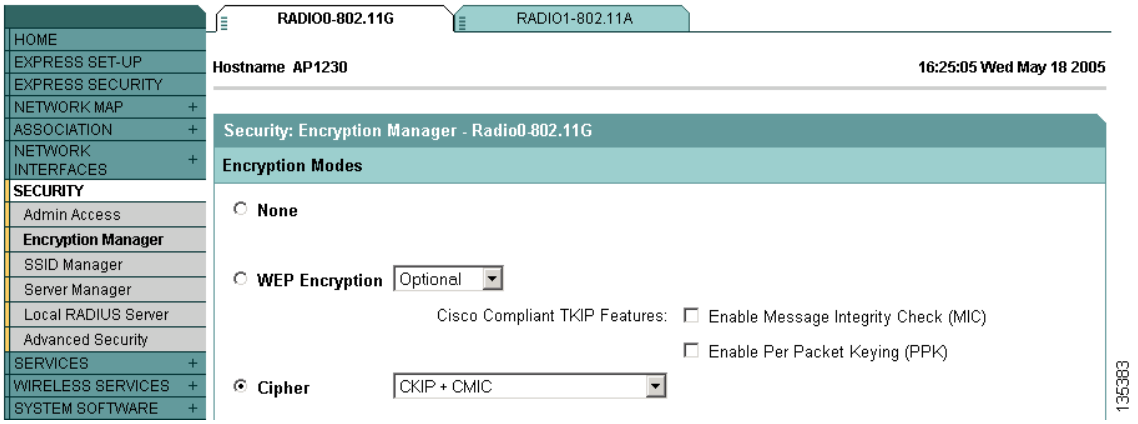
For instructions on configuring WDS, refer to the "Configuring WDS" section on page 12-7.

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 at least one SSID. Follow these steps to configure CCKM for an SSID:

Step 1 Browse to the Encryption Manager page on the access point GUI. Figure 12-14 shows the top section of the Encryption Manager page.

Figure 12-14 Encryption Manager Page



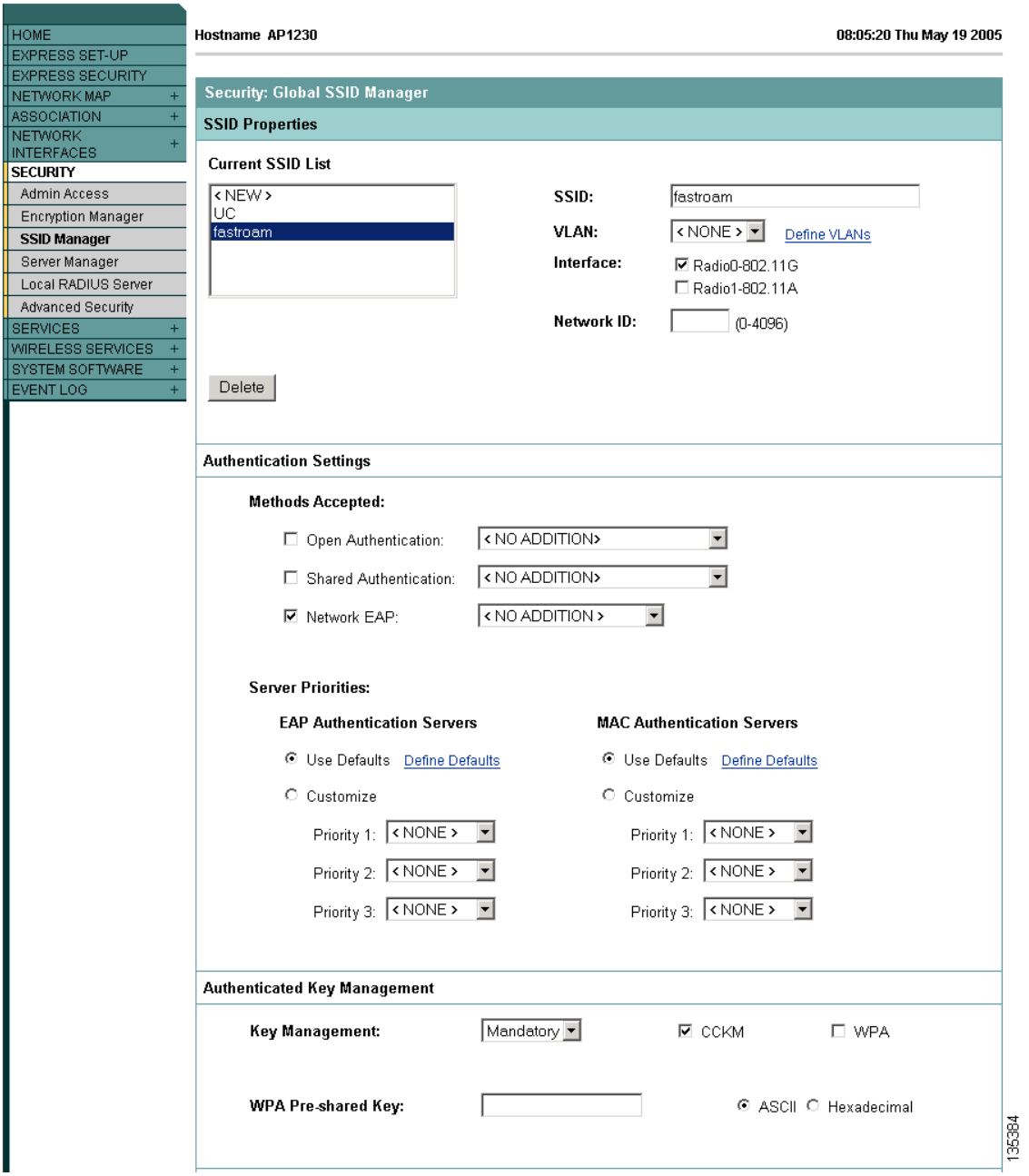
Step 2 Click the **Cipher** button.

Step 3 Select **CKIP + CMIC** from the Cipher drop-down menu.

Step 4 Click **Apply**.

Step 5 Browse to the Global SSID Manager page. Figure 12-15 shows the top sections of the Global SSID Manager page.

Figure 12-15 Global SSID Manager Page



Step 6 On the SSID that supports CCKM, select these settings:

b. If your access point contains multiple radio interfaces, select the interfaces on which the SSID applies.

c. Select **Network EAP** under Authentication Settings. When you enable CCKM, you must enable Network EAP as the authentication type.

d. Select **Mandatory** or **Optional** under Authenticated Key Management. 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.

e. Check the **CCKM** check box.

Step 7 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 12-23:

```
AP# configure terminal
AP(config)# dot11 ssid fastroam
AP(config-ssid)# authentication network-eap eap_methods
AP(config-ssid)# authentication key-management cckm
AP(config-ssid)# exit
AP(config)# interface dot11radio0
AP(config-if)# encryption mode ciphers ckip-cmic
AP(config-if)# ssid fastroam
AP(config-if)# exit
AP(config)# end
```

In this example, the SSID *fastroam* is configured to support Network EAP and CCKM, the CKIP-CMIC cipher suite is enabled on the 2.4-GHz radio interface, and the SSID *fastroam* 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*.

Configuring Management Frame Protection

Management Frame Protection operation requires a WDS and is available on 32 Mb platforms only (s: 1130 and 1240 series access points, and 1300 series access points in AP mode.). MFP is configured at the WLSE, but you can configure MFP on an access point and WDS manually.

Note If a WLSE is not present, then MFP cannot report detected intrusions and so has limited effectiveness. If a WLSE is present, you should perform the configuration from the WLSE.

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.

Management Frame Protection operation requires a WDS and is available on 32 Mb platforms only (1130 and 1240 series access points, and 1300 series access points in AP mode.). MFP is configured at the WLSE, but you can configure MFP on an access point and WDS manually.

Note If a WLSE is not present, then MFP cannot report detected intrusions and so has limited effectiveness. If a WLSE is present, you should perform the configuration from the WLSE.

For complete protection, you should also configure an MFP access point for Simple Network Transfer Protocol (SNTP).

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.

Protection of Unicast Management Frames

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.

Protection of Broadcast Management Frames

In order to prevent attacks using broadcast frames, access points supporting CCXv5 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.

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

The following CLI commands are used to configure Client MFP for access points in root mode.

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.

no ids mfp client

This ssid configuration 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.

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.

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.

	Command	Description
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ids mfp generator**	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.

	Command	Description
Step 3	**dot11 ids mfp detector**	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.
Step 4	**sntp server** *server IP address*	Enter the name or ip address of the SNTP server.
Step 5	**end**	Return to the privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Beginning in privileged EXEC mode, follow these steps to configure the WDS:

	Command	Description
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**dot11 ids mfp distributor**	Configures 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.
Step 3	**end**	Return to the privileged EXEC mode.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

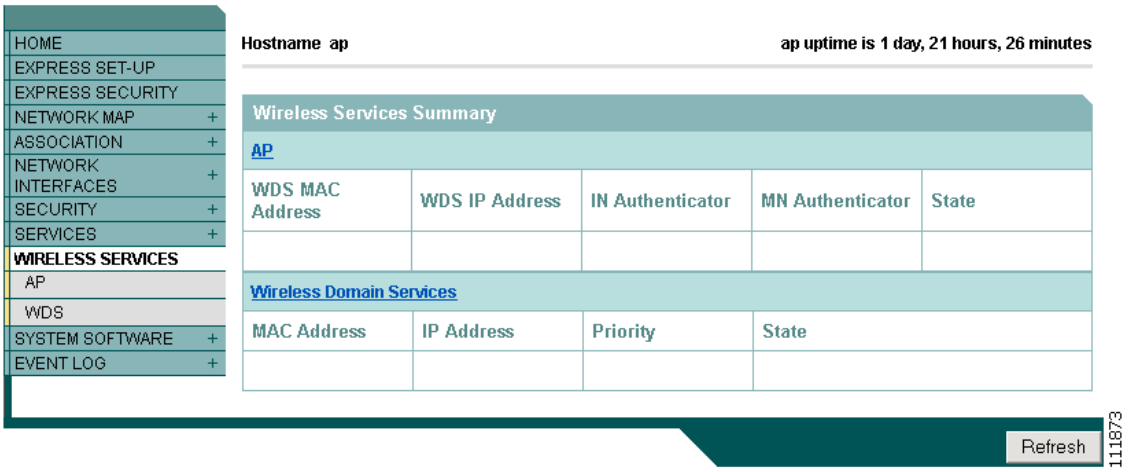
Configuring Radio Management

*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 WLSE device 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. Figure 12-16 shows the Wireless Services Summary page.

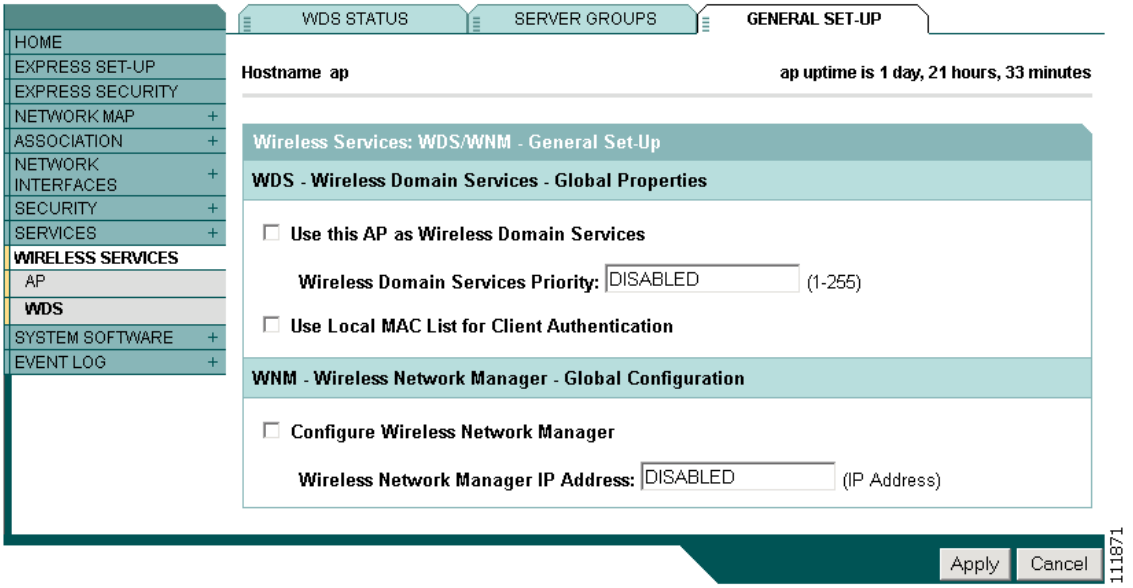
Figure 12-16 Wireless Services Summary Page



Step 2 Click **WDS** to browse to the General Setup page.

Step 3 On the WDS/WNM Summary page, click **Settings** to browse to the General Setup page. Figure 12-17 shows the General Setup page.

Figure 12-17 WDS/WNM General Setup Page



Step 4 Check the *Configure Wireless Network Manager* check box.

Step 5 In the *Wireless Network Manager IP Address* field, enter the IP address of the WLSE device on your network.

Step 6 Click **Apply**. The WDS access point is configured to interact with your WLSE device.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Configuring Radio Management" section on page 12-29:

```
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 WLSE device 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 12-14 and in the "Configuring Radio Management" section on page 12-29 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 is radio 0, and the 5-GHz radio is radio 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 is radio 0, and the 5-GHz radio is radio 1.

	Command	Purpose
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 WLSM Failover

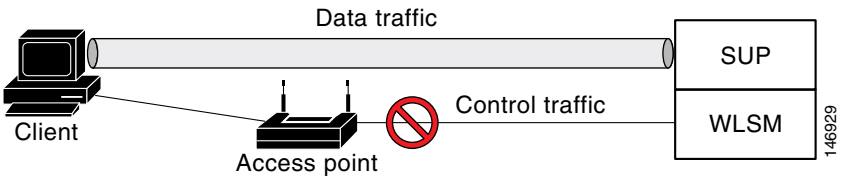
To ensure near hot standby in cases of WLSM failure, the WLSM Version 2.13 Release supports resilient tunnel recovery and active and standby WLSMs.

Resilient Tunnel Recovery

In the case of a single chassis scenario (only one WLSM per chassis), if the WLSM software fails, existing access point clients connected to the SUP continue to be connected to the SUP and won't notice any interruption in service. When an access point detects a WLSM failure, it doesn't tear down the active

tunnels, which keeps data traffic going between client and SUP. But because of the WLSM failure, the control traffic going between the access point and the WLSM is disrupted (as shown in Figure 12-18), which prevents the access points from accepting new client connections until the WLSM software is back online. Resilient tunnel recovery is automatic and does not require any configuration.

Figure 12-18 Resilient Tunnel Recovery



Active/Standby WLSM Failover

In addition to resilient tunnel recovery, WLSM supports another level of resiliency by allowing you to deploy two WLSMs per chassis: an active WLSM and a standby WLSM. If the active WLSM fails, the standby WLSM becomes active and takes over the control traffic for existing and new access point clients without interrupting data traffic. This feature in addition to resilient tunnel recovery provide near-hot standby in case of WLSM failure.

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 is 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*.

This chapter contains these sections:

Configuring and Enabling RADIUS

This section describes how to configure and enable RADIUS. These sections describe RADIUS configuration:

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 Secure Access Control Server version 3.0), Livingston, Merit, 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. In one case, RADIUS has been used with Enigma's security cards to validate users and to grant access to network resources.
- 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.

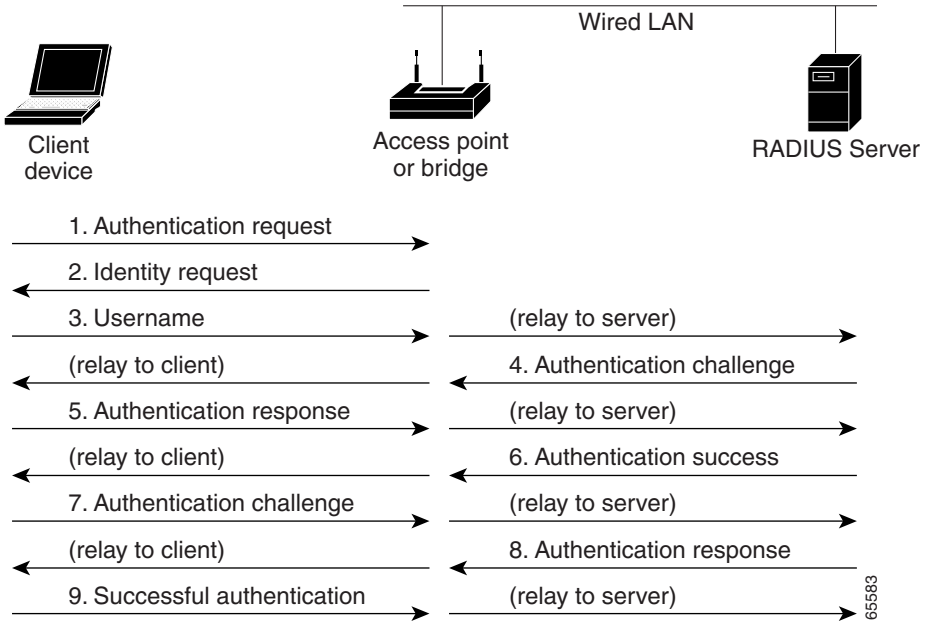
RADIUS is not suitable in these network security situations:

- Multiprotocol access environments. RADIUS does not support AppleTalk Remote Access (ARA), NetBIOS Frame Control Protocol (NBFCP), NetWare Asynchronous Services Interface (NASI), or X.25 PAD connections.
- Switch-to-switch or router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one device to a non-Cisco device if the non-Cisco device requires authentication.
- 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



In Steps 1 through 9 in Figure 13-1, 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 password 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 WEP key 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, called a *session key*, over the wired LAN to the access point. The access point encrypts its broadcast key with the session key and sends the encrypted broadcast key to the client, which uses the session key to decrypt it. The client and access point activate WEP and use the session and broadcast WEP 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 11-10 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 a minimum, you must identify the host or hosts 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:

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 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. The default port number is 1645 if this parameter is not present. • (Optional) For **acct-port** *port-number*, specify the UDP destination port for accounting requests. The default port number is 1646 if this parameter is not present. • (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.

	Command	Purpose
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/en/US/docs/ios/12_2/security/configuration/guide/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: http://www.cisco.com/en/US/docs/ios/wlan/command/reference/wl_book.html
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.
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/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsaaa/scfathen.htm#xtocid2 • 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**	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 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
```

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.

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. This may be needed in at least two situations:

- Detection of fraudulent use, which cannot be performed before accepting the call.
- Disconnecting hot spot users when their prepaid access time has expired.

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.

Note PoD is supported on the Cisco CNS Access Registrar (CAR) RADIUS server, but not on the Cisco Secure ACS Server, v4.0 and earlier.

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.

Starting RADIUS Accounting m

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.

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. 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
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.

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 and a local authenticator with a server deadtime of 10 minutes:

```
AP(config)# aaa new-model

AP(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001 key 77654

AP(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646 key 77654

AP(config)# radius-server host 10.91.6.151 auth-port 1812 acct-port 1813 key 110337

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

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, refer to the "RADIUS Attributes" appendix in the *Cisco IOS Security Configuration Guide for Release 12.2*.

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 host 172.20.30.15 nonstandard
AP(config)# radius-server key rad124
```

Configuring WISPr RADIUS Attributes

The Wi-Fi Alliance's *WISPr Best Current Practices for Wireless Internet Service Provider (WISP) Roaming* document 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 Best Current Practices for Wireless Internet Service Provider (WISP) Roaming* 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 Best Current Practices for Wireless Internet Service Provider (WISP) Roaming* 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. Changing the service-type attribute to login-only ensures that Microsoft IAS servers recognize reauthentication requests from the access point. Use the **dot11 aaa authentication attributes service-type login-only** global configuration command to set the service-type attribute in reauthentication requests to login-only.

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 client devices associated to the access point.

TACACS+ services are maintained in a database on a TACACS+ daemon typically running on a UNIX or Windows NT workstation. 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 (such as PPP), 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 the user's mother's maiden name.

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

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.

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.

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.
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.

	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 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 in the following sections:. These sections describe how to configure your access point to support VLANs:

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 802.11Q tag awareness to the access point. Frames destined for different VLANs are transmitted by the access point wirelessly on different SSIDs with different WEP keys. Only the clients associated with that VLAN receive those packets. Conversely, packets coming from a client associated with a certain VLAN are 802.11Q tagged before they are forwarded onto the wired network.

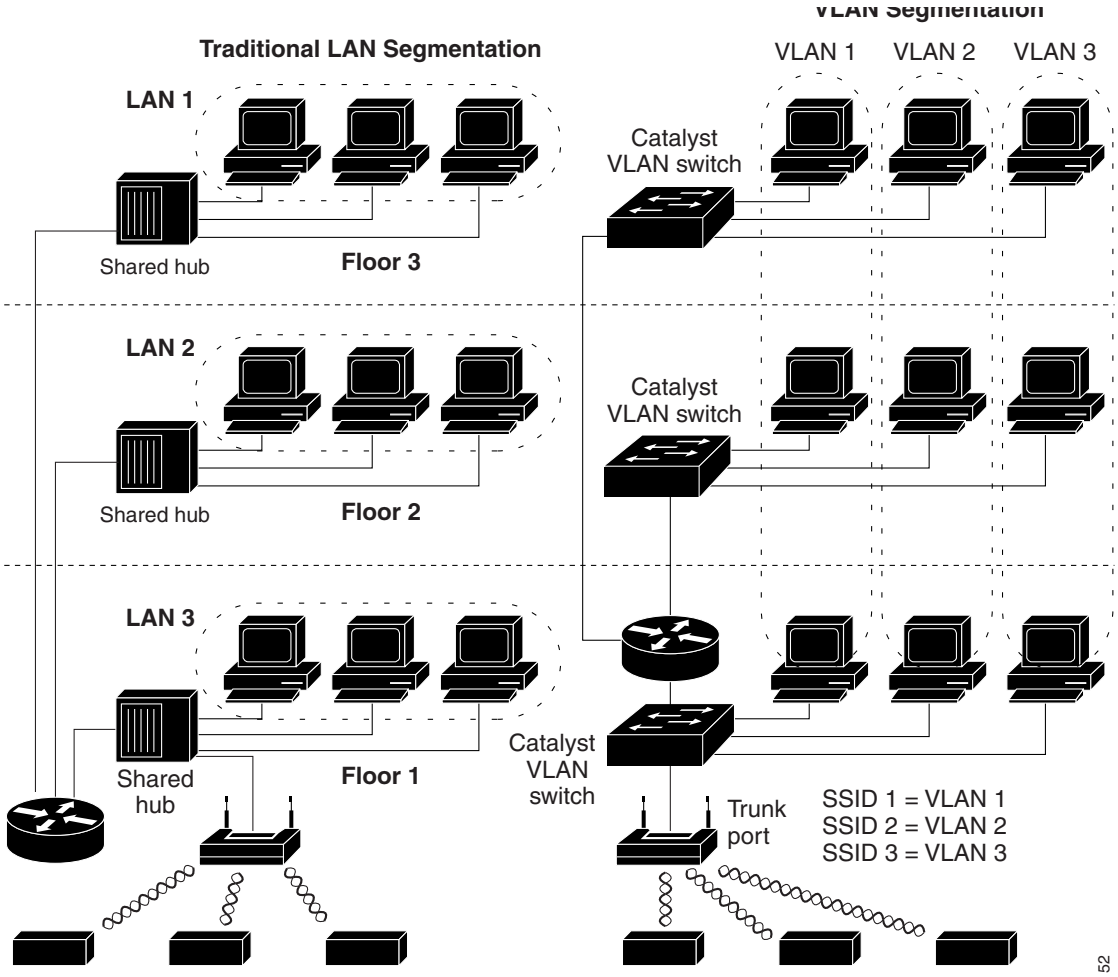
If 802.1q is configured on the FastEthernet interface of an access point, the access point always sends keepalives on VLAN1 even if VLAN 1 is not defined on the access point. As a result, the Ethernet switch connects to the access point and generates a warning message. There is no loss of function on both the access point and the switch. However, the switch log contains meaningless messages that may cause more important messages to be wrapped and not be seen.

This behavior creates a problem when all SSIDs on an access point are associated to mobility networks. If all SSIDs are associated to mobility networks, the Ethernet switch port the access point is connected to can be configured as an access port. The access port is normally assigned to the native VLAN of the access point, which is not necessarily VLAN1, which causes the Ethernet switch to generate warning messages saying that traffic with an 802.1q tag is sent from the access point.

You can eliminate the excessive messages on the switch by disabling the keepalive function.

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



Related Documents

These documents provide more detailed information pertaining to VLAN design and configuration:

- *Cisco IOS Switching Services Configuration Guide.* Click this link to browse to this document: http://www.cisco.com/en/US/docs/ios/12_2/switch/configuration/guide/fswtch_c.html
- *Cisco Internetwork Design Guide.* Click this link to browse to this document: http://www.cisco.com/en/US/docs/internetworking/design/guide/idg4.html
- *Cisco Internetworking Technology Handbook.* Click this link to browse to this document: http://www.cisco.com/en/US/docs/internetworking/technology/handbook/ito_doc.html
- *Cisco Internetworking Troubleshooting Guide.* Click this link to browse to this document: http://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1901.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 the VLAN is 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 only one SSID to a VLAN.

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 static WEP, and some wireless users might have more sophisticated devices using dynamic WEP. You can group and isolate these devices into separate VLANs.

Note You cannot configure multiple VLANs on repeater access points. Repeater access points support only the native VLAN.

Configuring VLANs

These sections describe how to configure VLANs on your access point:

- Configuring a VLAN, page 14-5
- Assigning Names to VLANs, page 14-7
- Using a RADIUS Server to Assign Users to VLANs, page 14-8
- Viewing VLANs Configured on the Access Point, page 14-9

Configuring a VLAN

Note When you configure VLANs on access points, the Native VLAN must be VLAN1. In a single architecture, client traffic received by the access point is tunneled through an IP-GRE tunnel, which is established on the access point's Ethernet interface native VLAN. Because of the IP-GRE tunnel, some users may configure another switch port as VLAN1. This misconfiguration causes errors on the switch port.

Configuring your access point to support VLANs is a three-step process:

1. Enable the VLAN on the radio and Ethernet ports.
2. Assign SSIDs to VLANs.
3. Assign authentication settings to SSIDs.

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.

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 | 1***slot/port*	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	**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. 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 **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 4	**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 SSID to a VLAN. **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 5	**exit**	Return to interface configuration mode for the radio interface.
Step 6	**interface dot11radio 0.x** | **1.x***slot/port.x*	Enter interface configuration mode for the radio VLAN sub interface.
Step 7	**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 8	**exit**	Return to global configuration mode.
Step 9	**interface fastEthernet0.x**	Enter interface configuration mode for the Ethernet VLAN subinterface.
Step 10	**encapsulation dot1q** *vlan-id* [**native**]	Enable a VLAN on the Ethernet interface. (Optional) Designate the VLAN as the native VLAN. On many networks, the native VLAN is VLAN 1.

	Command	Purpose
Step 11	**end**	Return to privileged EXEC mode.
Step 12	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to:

- Name an SSID
- Assign the SSID to a VLAN
- Enable the VLAN on the radio and Ethernet ports as the native VLAN

```
ap1200Router# configure terminal
ap1200Router(config)# interface dot11radio0
ap1200Router(config-if)# ssid batman
ap1200Router(config-ssid)# vlan 1
ap1200Router(config-ssid)# exit
ap1200Router(config)# interface dot11radio0.1
ap1200Router(config-subif)# encapsulation dot1q 1 native
ap1200Router(config-subif)# exit
ap1200Router(config)# interface fastEthernet0.1
ap1200Router(config-subif)# encapsulation dot1q 1 native
ap1200Router(config-subif)# exit
ap1200Router(config)# 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, Cisco recommends 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.
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 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 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*

Using a RADIUS Server for Dynamic Mobility Group Assignment

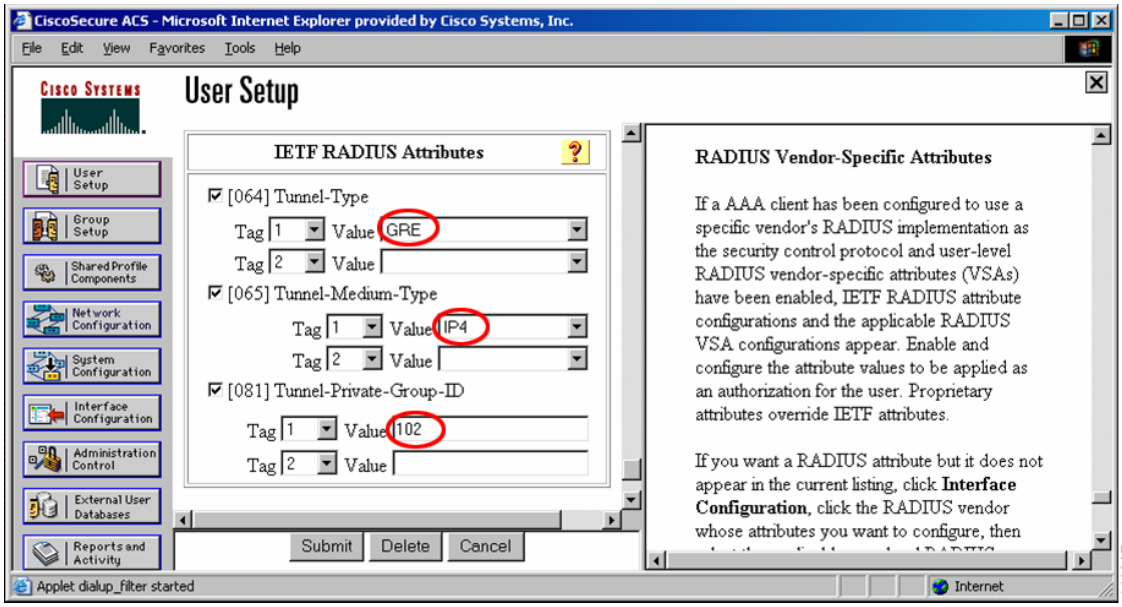
You can configure a RADIUS server to dynamically assign mobility groups to users or user groups. This eliminates the need to configure multiple SSIDs on the access point. Instead, you need to configure only one SSID per access point.

When users associate to the SSID, the access point passes their login information to WLSM, which passes the information to the RADIUS server. Based on the login information, the RADIUS server assigns the users to the appropriate mobility group and sends their credentials back.

To enable dynamic mobility group assignment, you need to configure the following attributes on the RADIUS server:

- Tunnel-Type (64)
- Tunnel-Medium-Type(65)
- Tunnel-Private-Group-ID (81)

Figure 14-2 Dynamic Mobility Group Assignment



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
FastEthernet0
Virtual-Dot11Radio0

 This is configured as native Vlan for the following interface(s) :
Dot11Radio0
FastEthernet0
```

```
Virtual-Dot11Radio0

   Protocols Configured:   Address:              Received:        Transmitted:
        Bridging        Bridge Group 1             201688                  0
        Bridging        Bridge Group 1             201688                  0
        Bridging        Bridge Group 1             201688                  0

Virtual LAN ID:  2 (IEEE 802.1Q Encapsulation)

   vLAN Trunk Interfaces:  Dot11Radio0.2
FastEthernet0.2
Virtual-Dot11Radio0.2

   Protocols Configured:   Address:              Received:        Transmitted:
```

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 LEAP.
- 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 LEAP.
- 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 WEP.

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	boss	01
Faculty	teach	02
Student	learn	03

Managers configure their wireless client adapters to use SSID boss, 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 fastEthernet and dot11radio interfaces on the access point. You should make this VLAN the native VLAN.
5. Configure VLANs 2 and 3 on both the fastEthernet 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
ap1200Router# **configure terminal** ap1200Router(config)# **interface dot11radio 0/0** ap1200Router(config-if)# **ssid boss** ap1200Router(config-ssid)# **vlan 01** ap1200Router(config-ssid)# **end**	ap1200Router# **configure terminal** ap1200Router(config)# **interface dot11radio 0/0** ap1200Router(config-if)# **ssid teach** ap1200Router(config-ssid)# **vlan 02** ap1200Router(config-ssid)# **end**	ap1200Router# **configure terminal** ap1200Router(config)# **interface dot11radio 0/0** ap1200Router(config-if)# **ssid learn** ap1200Router(config-ssid)# **vlan 03** ap1200Router(config-ssid)# **end**
ap1200Router **configure terminal** ap1200Router(config) **interface FastEthernet0.1** ap1200Router(config-subif) **encapsulation dot1Q 1 native** ap1200Router(config-subif) **exit**	ap1200Router(config) **interface FastEthernet0.2** ap1200Router(config-subif) **encapsulation dot1Q 2** ap1200Router(config-subif) **bridge-group 2** ap1200Router(config-subif) **exit**	ap1200Router(config) **interface FastEthernet0.3** ap1200Router(config-subif) **encapsulation dot1Q 3** ap1200Router(config-subif) **bridge-group 3** ap1200Router(config-subif) **exit**
ap1200Router(config)# **interface Dot11Radio 0/0.1** ap1200Router(config-subif)# **encapsulation dot1Q 1 native** ap1200Router(config-subif)# **exit** **Note** You do not need to configure a bridge group on the subinterface that you set up as the native VLAN. This bridge group is moved to the native subinterface automatically to maintain the link to BVI 1, which represents both the radio and Ethernet interfaces.	ap1200Router(config) **interface Dot11Radio 0/0.2** ap1200Router(config-subif) **encapsulation dot1Q 2** ap1200Router(config-subif) **bridge-group 2** ap1200Router(config-subif) **exit**	ap1200Router(config) **interface Dot11Radio 0/0.3** ap1200Router(config-subif) **encapsulation dot1Q 3** ap1200Router(config-subif) **bridge-group 3** ap1200Router(config-subif) **exit**

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**0/0**.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**0/0**.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**0/0**.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 FastEthernet0.1 encapsulation dot1Q 1 native no ip route-cache bridge-group 1 no bridge-group 1 source-learning bridge-group 1 spanning-disabled	interface FastEthernet0.2 encapsulation dot1Q 2 no ip route-cache bridge-group 2 no bridge-group 2 source-learning bridge-group 2 spanning-disabled	interface FastEthernet0.3 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 FastEthernet 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.

This chapter consists of these sections:

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 LANs differs from QoS implementations on other Cisco devices. With QoS enabled, access points perform the following:

- 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 EDCF like queuing on the radio egress port only.
- They do only FIFO queueing 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 Symbol 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

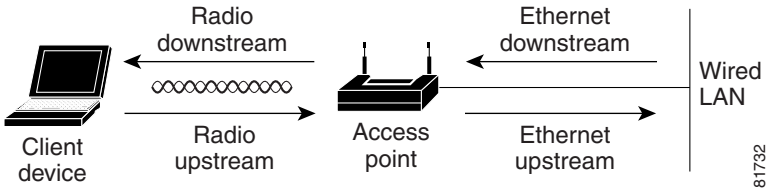
Impact of QoS on a Wireless LAN

Wireless LAN QoS features are a subset of the proposed 802.11e draft. QoS on wireless LANs provides prioritization of traffic from the access point over the WLAN based on traffic classification.

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. QoS for wireless LANs does not affect this traffic.
- 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.

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.

2. *QoS Element for Wireless Phones* setting—If you enable the *QoS Element for Wireless Phones* setting, dynamic voice classifiers are created for some of the wireless phone vendor clients, 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 the future upgrade of the 7920 Wireless Phone firmware to support the standard QBSS Load IE. The new 7920 Wireless Phone firmware will be announced at a later date.

Note This release continues to support existing 7920 wireless phone firmware. Do not attempt to use the new standard (IEEE 802.11e draft 13) QBSS Load IE with the 7920 Wireless Phone until new phone firmware is available for you to upgrade your phones.

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 draft 13) 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 replay detection is done per access class on the receiver. Like 802.11 sequence numbering, WPA replay detection allows high-priority packets to interrupt lower priority retries without signalling 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.

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

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.

Configuring QoS Using the Web-Browser Interface

This section describes configuring QoS using the web-browser interface.

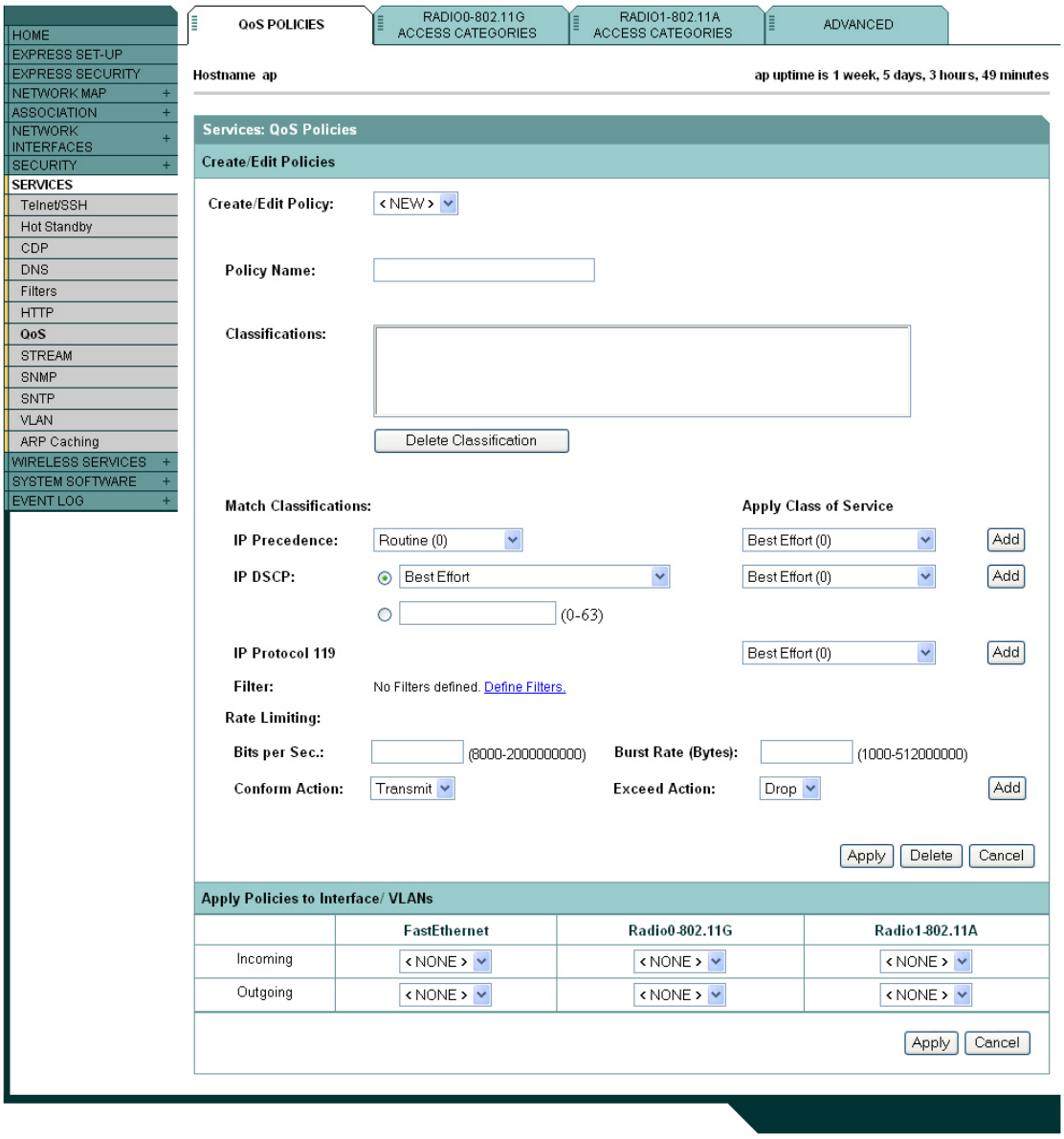
For a list of Cisco IOS commands for configuring QoS using the CLI, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

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 task menu on the left side of any page in the web-browser interface. When the list of Services expands, click **QoS**. The QoS Policies page appears. Figure 15-2 shows the QoS Policies page.

Figure 15-2 QoS Policies Page



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 menu. 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 Use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to packets of the type that you selected from the IP Precedence menu. The access point matches your IP Precedence selection with your class of service selection. Settings in the Apply Class of Service menu include:

- 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 precedence information in the IP header TOS field, select an IP DSCP classification from the IP DSCP drop-down menu. 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 menu to select the class of service 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 menu 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 menu 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 menu.) 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 does not affect the access points' packet forwarding decisions.

Step 13 Use the Apply Class of Service drop-down menu 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 If you want to set a default classification for all packets on a VLAN, use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to all packets on a VLAN. The access point matches all packets with your class of service selection.

Step 16 Click the **Add** button beside the Class of Service menu for *Default classification for packets on the VLAN*. The classification appears in the Classifications field.

Step 17 When you finish adding classifications to the policy, click the **Apply** button under the Apply Class of Service drop-down menus. To cancel the policy and reset all fields to defaults, click the **Cancel** button under the Apply Class of Service drop-down menus. To delete the entire policy, click the **Delete** button under the Apply Class of Service drop-down menus.

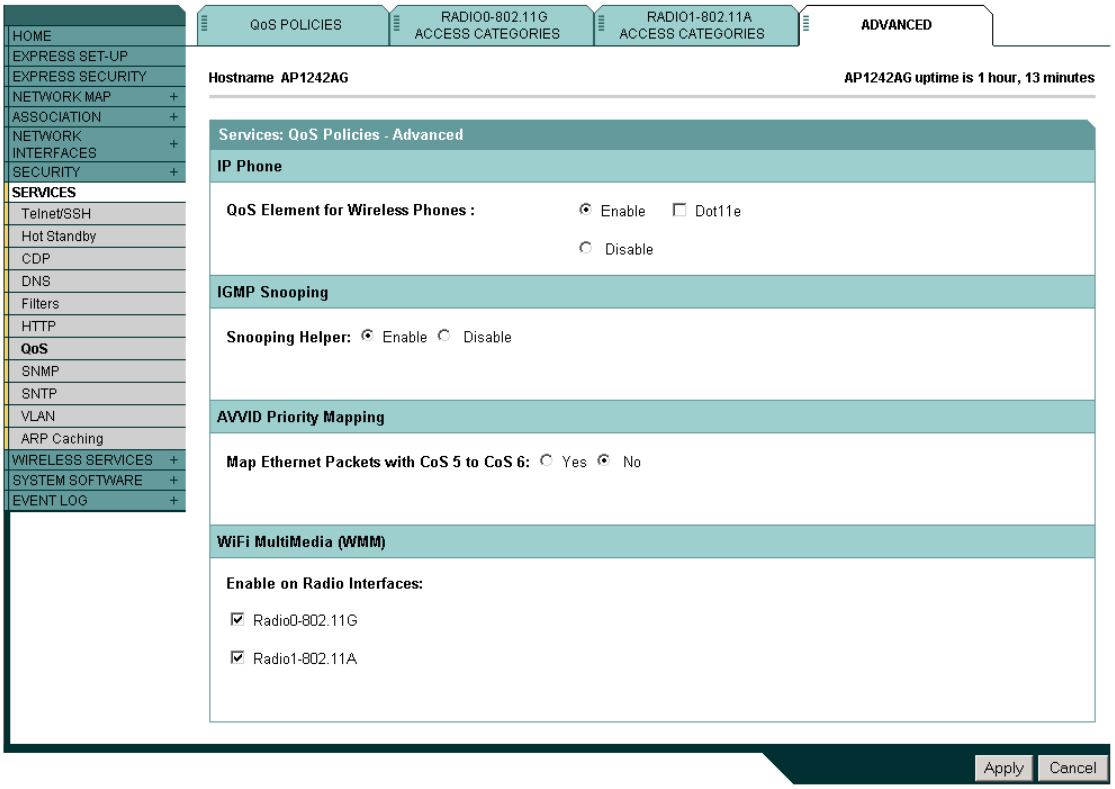
Step 18 Use the Apply Policies to Interface/VLANs drop-down menus to apply policies to the access point Ethernet and radio ports. If VLANs are configured on the access point, drop-down menus for each VLANs' virtual ports appear in this section. If VLANs are not configured on the access point, drop-down menus for each interface appear.

Step 19 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



Select **Enable** or 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 latest version of QBSS Load IE. If you leave this selection blank, the previous version QBSS Load IE is used.

IGMP Snooping

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

AVVID priority mapping maps Ethernet packets tagged as class of service 5 to class of service 6. 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 WMM on the access point's radio interface. When you enable admission control, clients associated to the access point must complete the WMM admission control procedure before they can use that access category.

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 Draft Standard 802.11e. For detailed information on these values, consult that standard.

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

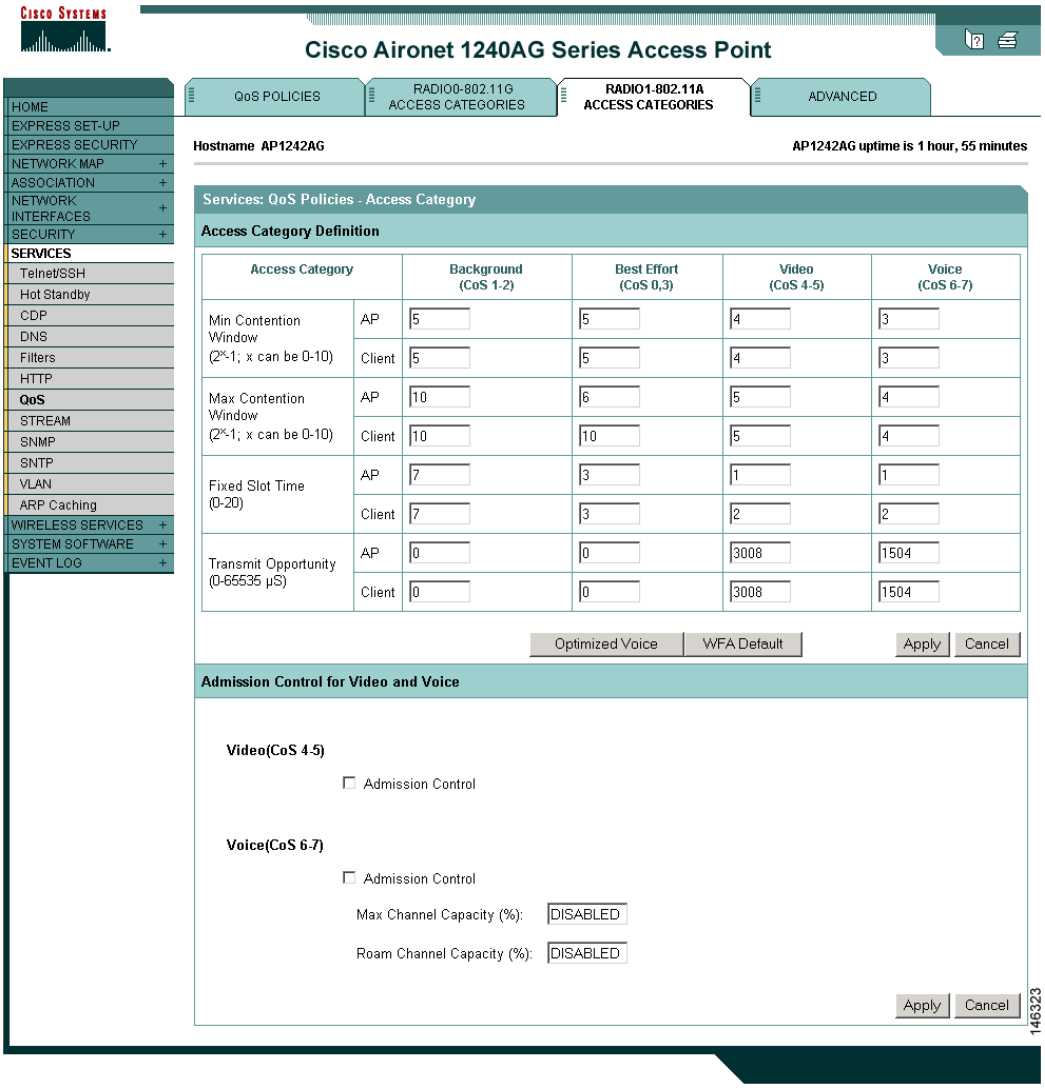
where X is the value from Table 15-1.

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



Note In this release, clients are blocked from using an access category when you select **Enable** for Admission Control.

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.

Step 5 To use video access category (AC = 2) for signaling, select the **Admission Control** check box under **Video(CoS 4-5)**.

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

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
  ```

QoS Configuration Examples

These sections describe two common uses for QoS:

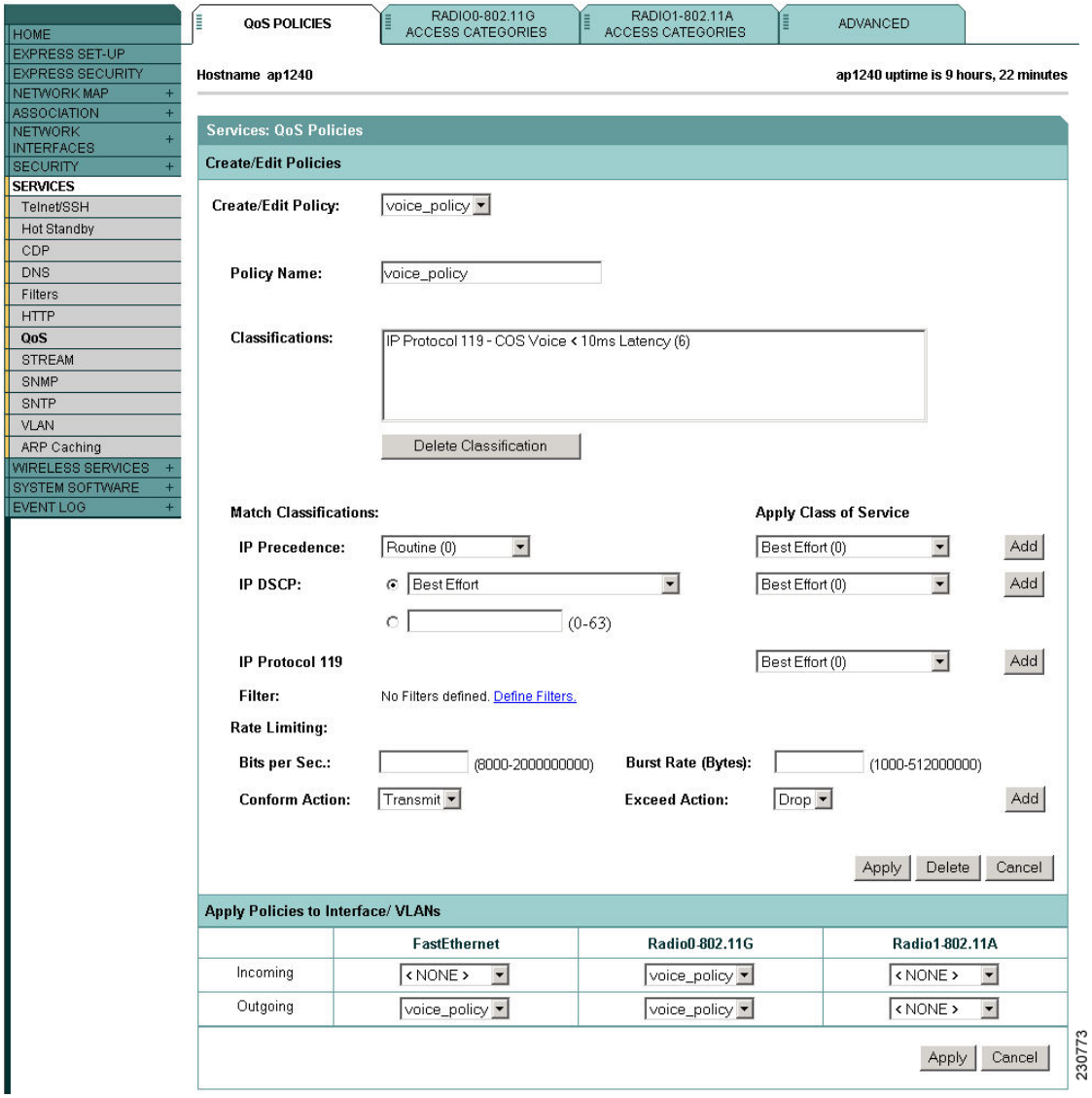
- Giving Priority to Voice Traffic, page 15-13
- Giving Priority to Video Traffic, page 15-14

Giving Priority to Voice Traffic

This section demonstrates how you can apply a QoS policy to your wireless networks' voice VLAN to give priority to wireless phone traffic.

In this example, the network administrator creates a policy named *voice_policy* that applies voice class of service to traffic from Spectralink phones (protocol 119 packets). The user applies the voice_policy to the incoming and outgoing radio ports and to the outgoing Ethernet port. Figure 15-5 shows the administrator's QoS Policies page.

Figure 15-5 QoS Policies Page for Voice Example



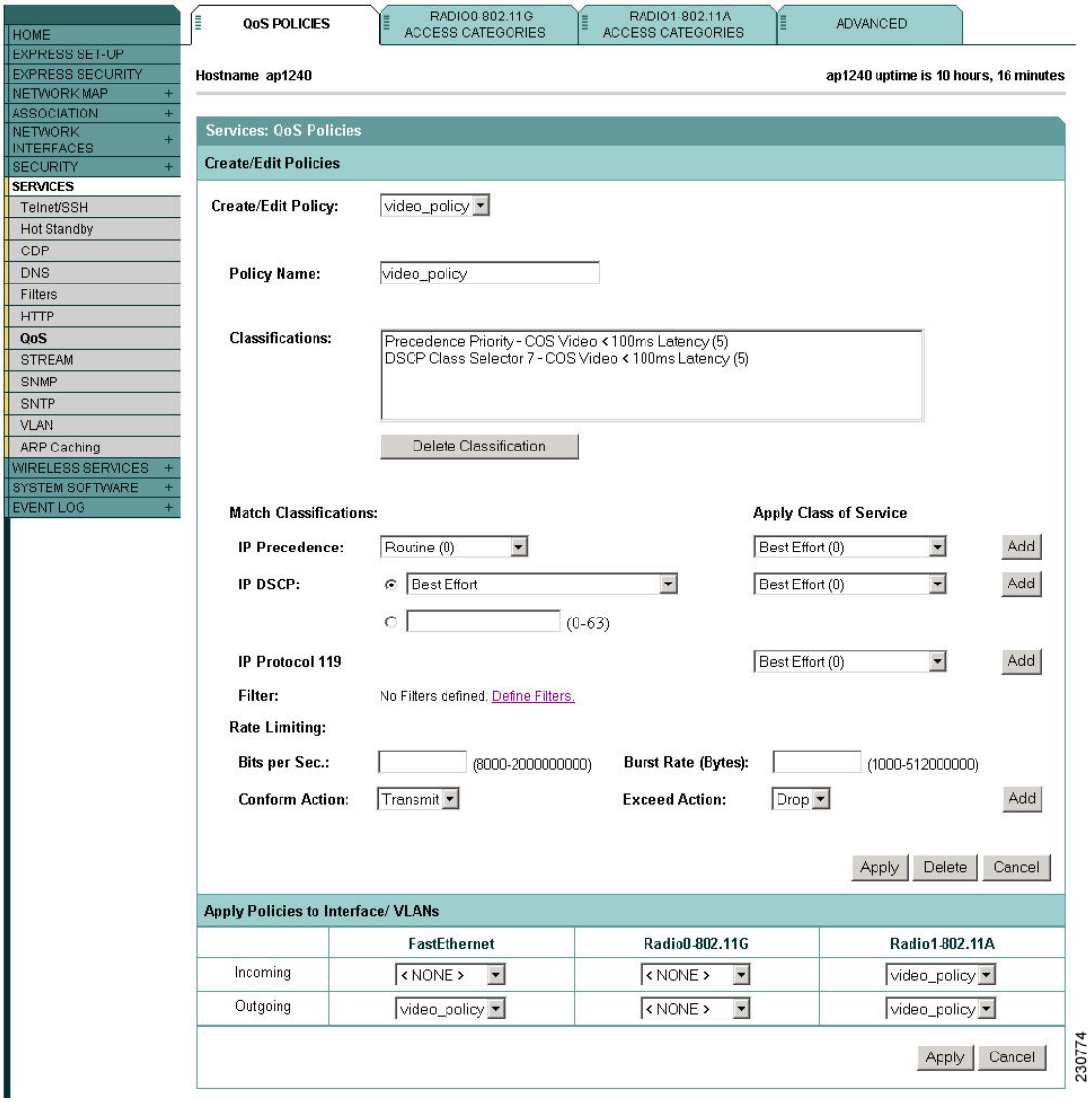
The network administrator also enables the *QoS element for wireless phones* setting on the QoS Policies - Advanced page. This setting gives priority to all voice traffic regardless of VLAN.

Giving Priority to Video Traffic

This section demonstrates how you could apply a QoS policy to a VLAN on your network dedicated to video traffic.

In this example, the network administrator creates a policy named *video_policy* that applies video class of service to video traffic. The user applies the video_policy to the incoming and outgoing radio ports and to the outgoing Ethernet port. Figure 15-6 shows the administrator's QoS Policies page.

Figure 15-6 QoS Policies Page for Video Example



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. This chapter contains these sections:

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 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. You can find explanations of these concepts and instructions for implementing them in these documents:

- *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
- *Catalyst 4908G-L3 Cisco IOS Release 12.0(10)W5(18e) Software Feature and Configuration Guide*. Click this link to browse to the "Command Reference" chapter: http://www.cisco.com/univercd/cc/td/doc/product/l3sw/4908g_l3/ios_12/10w518e/config/cmd_ref.htm

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.

These sections describe setting up and enabling three filter types:

- Configuring and Enabling MAC Address Filters, page 16-3
- Configuring and Enabling IP Filters, page 16-8
- Configuring and Enabling Ethertype Filters, page 16-11

Configuring and Enabling MAC Address Filters

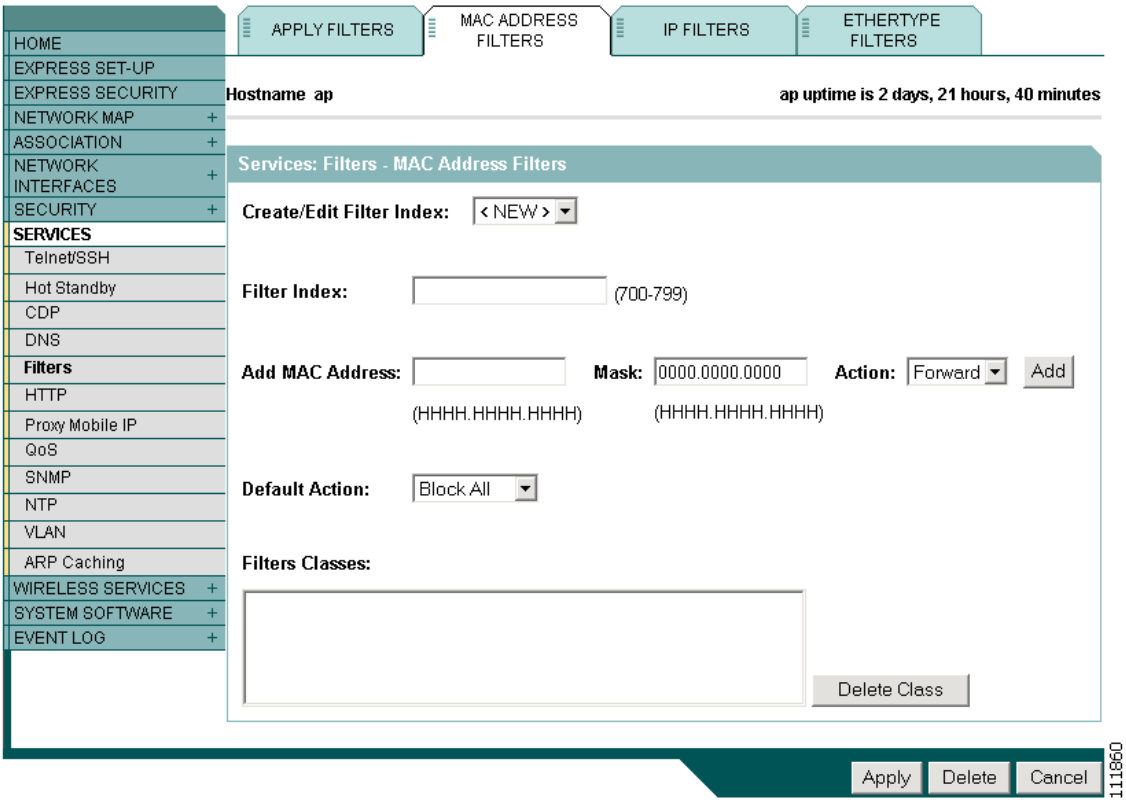
MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific MAC addresses. You can create a filter that passes traffic to all MAC addresses except those you specify, or you can create a filter that blocks traffic to all MAC addresses 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 you can lock yourself out of the access point if you make a mistake setting up the filters. If you accidentally lock yourself out of your access point, use the CLI 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



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 4 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.

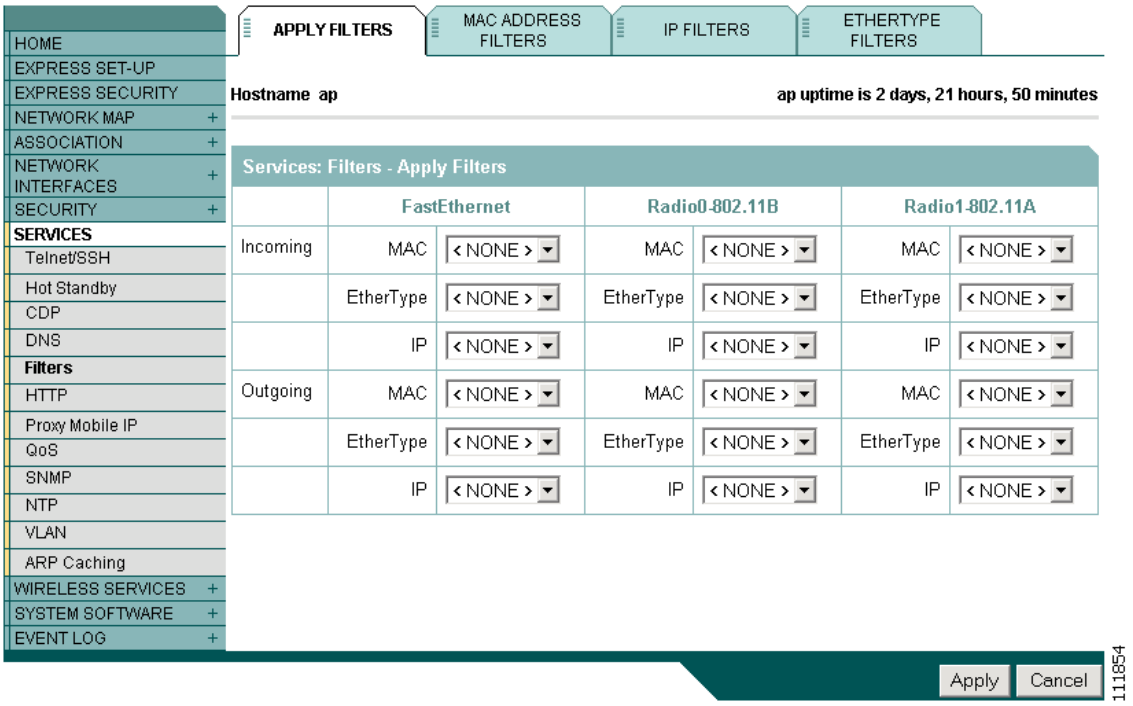
Step 9 Select **Forward All** or **Block All** from the Default Action menu. The filter's default action must be the opposite of the action for at least one of the addresses in the filter. For example, if you enter several addresses and you select **Block** as the action for all of them, you must choose **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 11-10 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



Step 12 Select the filter number from one of the MAC drop-down menus. 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 **System 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.

Using MAC Address ACLs to Block or Allow Client Association to the Access Point

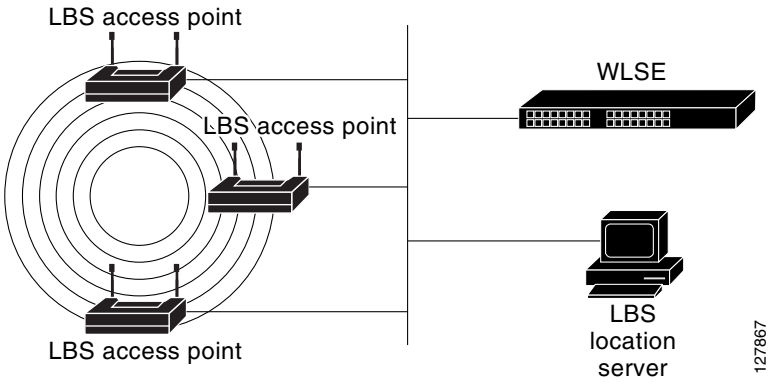
You can use MAC address ACLs to block or allow association to the access point. Instead of filtering traffic across an interface, you use the ACL to filter associations to the access point radio.

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.

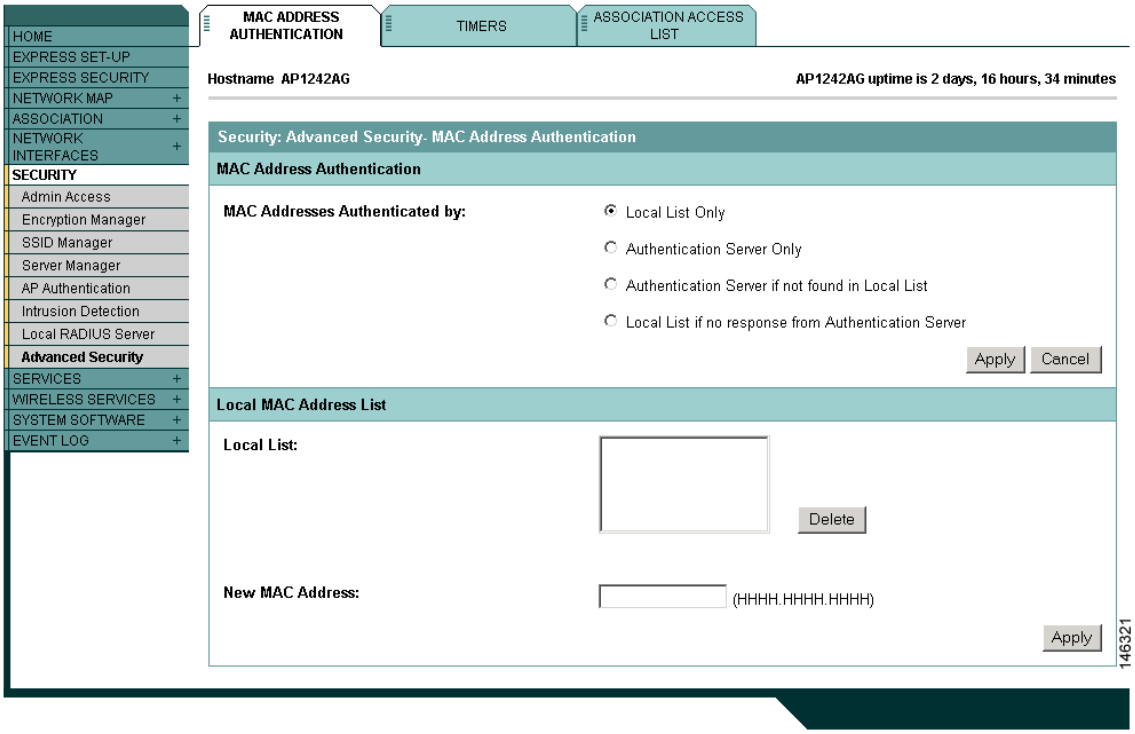
Step 2 Click **Security** to browse to the Security Summary page. Figure 16-3 shows the Security Summary page.

Figure 16-3 Security Summary Page



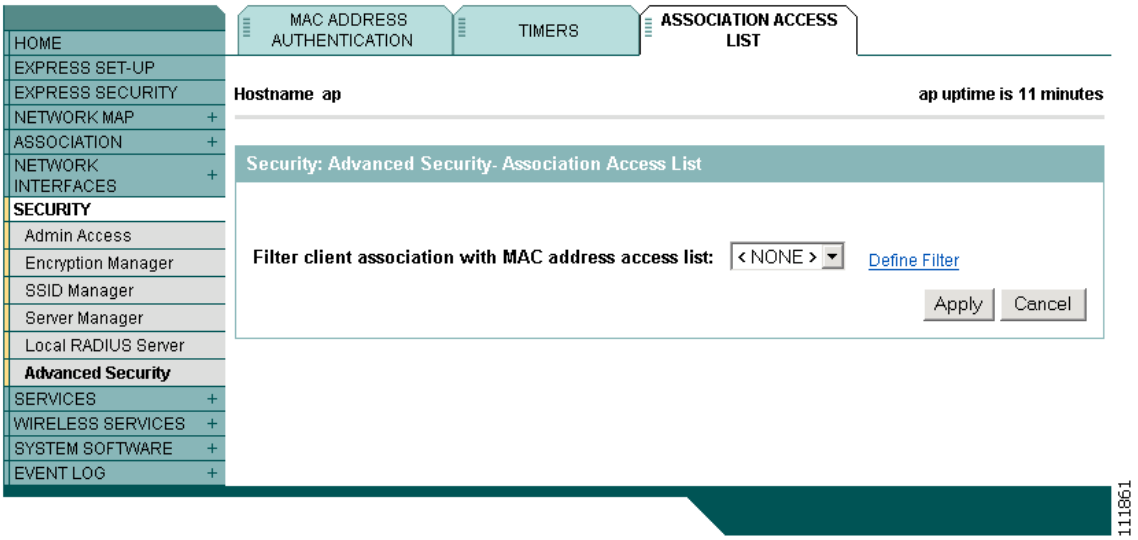
Step 3 Click **Advanced Security** to browse to the Advanced Security: MAC Address Authentication page. Figure 16-4 shows the MAC Address Authentication page.

Figure 16-4 Advanced Security: MAC Address Authentication Page



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



Step 5 Select your MAC address ACL from the drop-down menu.

Step 6 Click **Apply**.

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.

CLI Configuration Example

This example shows the CLI commands that are equivalent to the steps listed in the "Using MAC Address ACLs to Block or Allow Client Association to the Access Point" section on page 16-6:

```
AP# configure terminal
AP(config)# dot11 association access-list 777
AP(config)# end
```

In this example, only client devices with MAC addresses listed in access list 777 are allowed to associate to the access point. The access point blocks associations from all other MAC addresses.

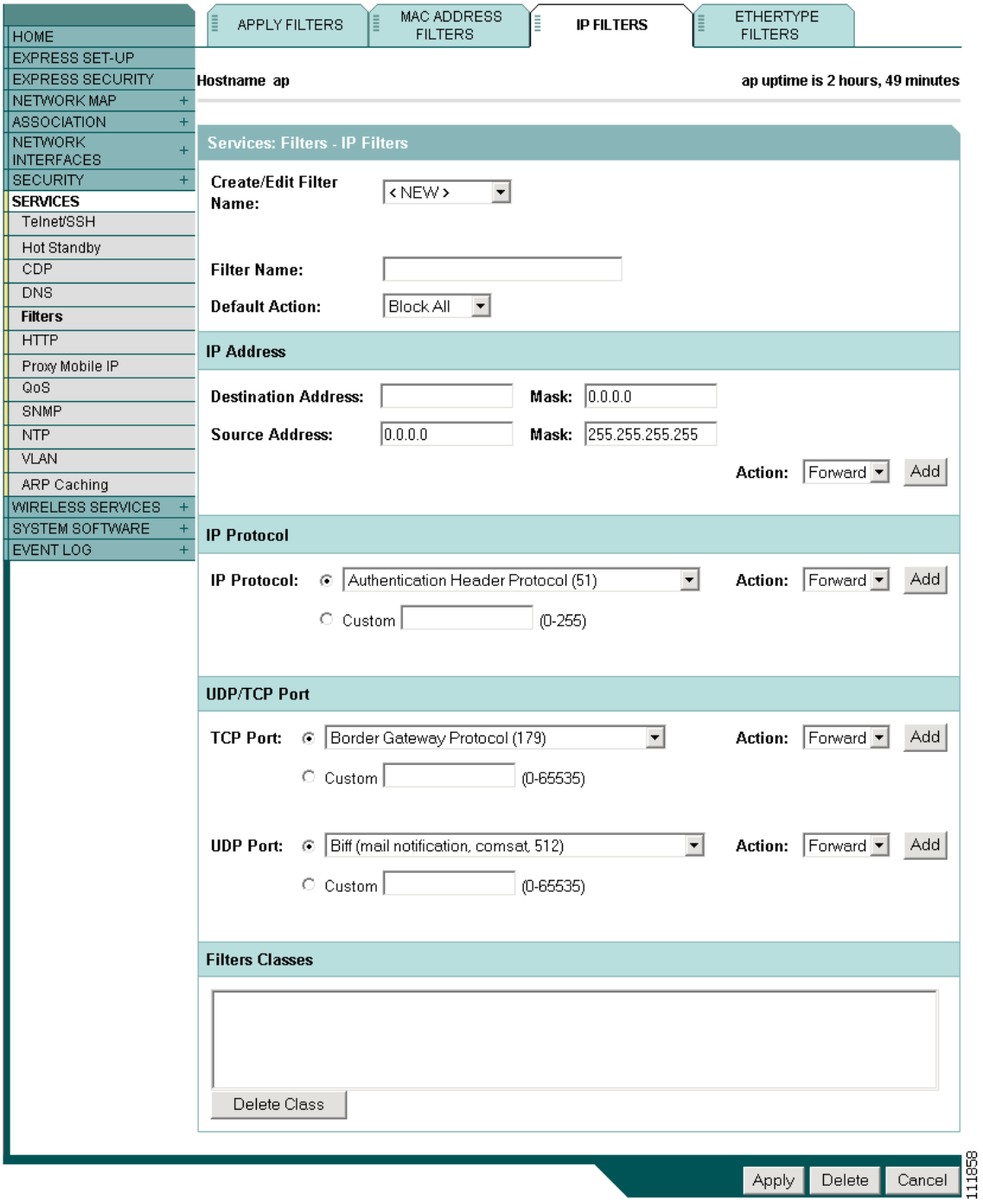
For complete descriptions of the commands used in this example, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

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



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 (112.334.556.778, 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 menu, 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 menus, 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.

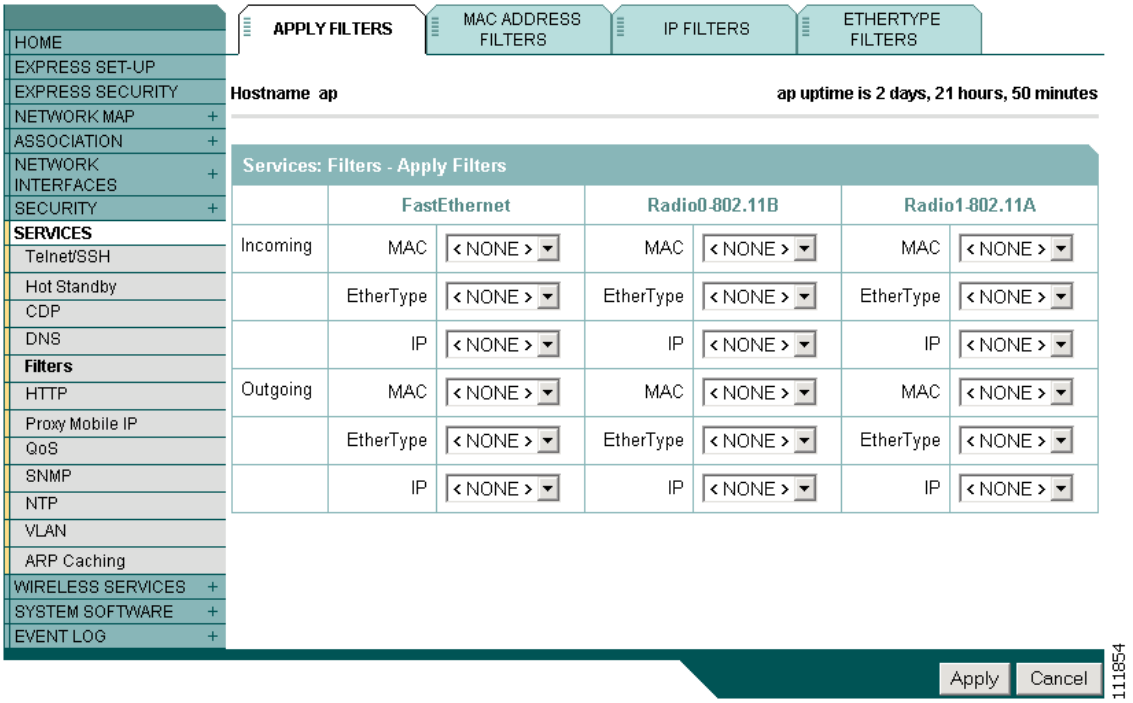
Step 13 Select **Forward** or **Block** from the Action menu.

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



Step 17 Select the filter name from one of the IP drop-down menus. You can apply the filter to either or both the Ethernet and radio ports, and to either or both incoming and outgoing packets.

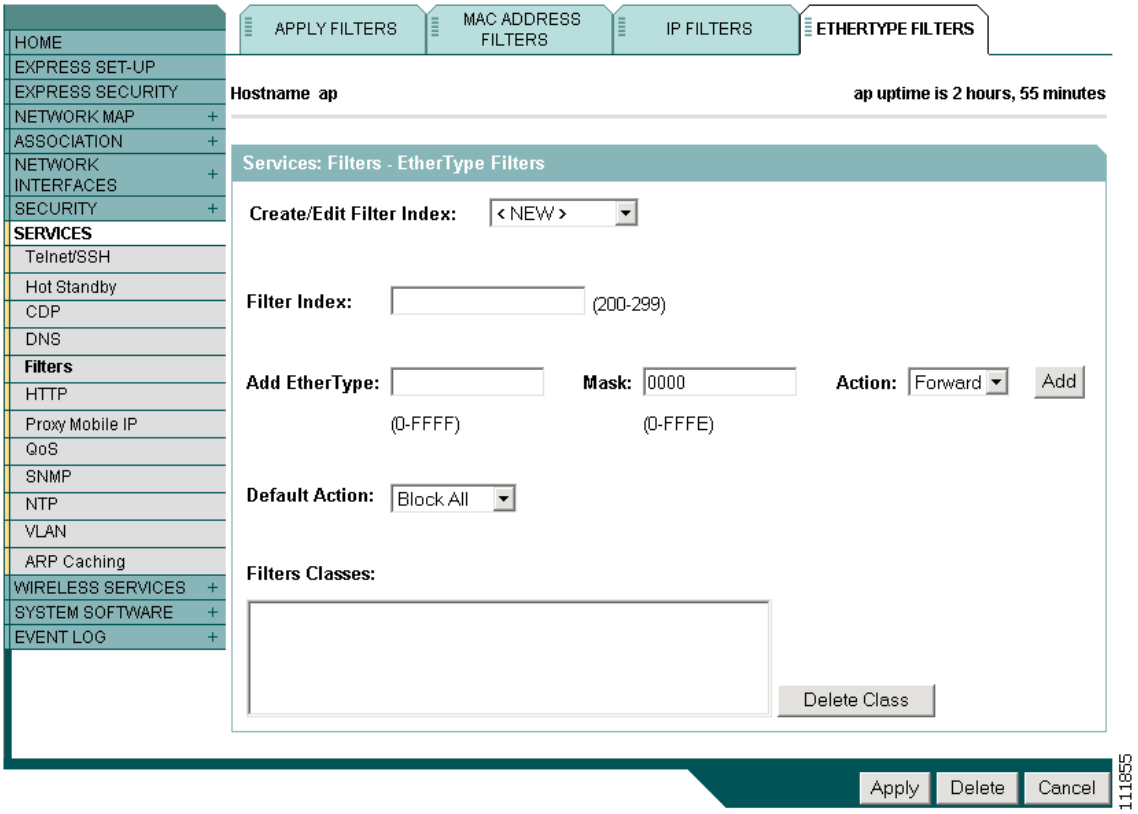
Step 18 Click **Apply**. The filter is enabled on the selected ports.

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



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.

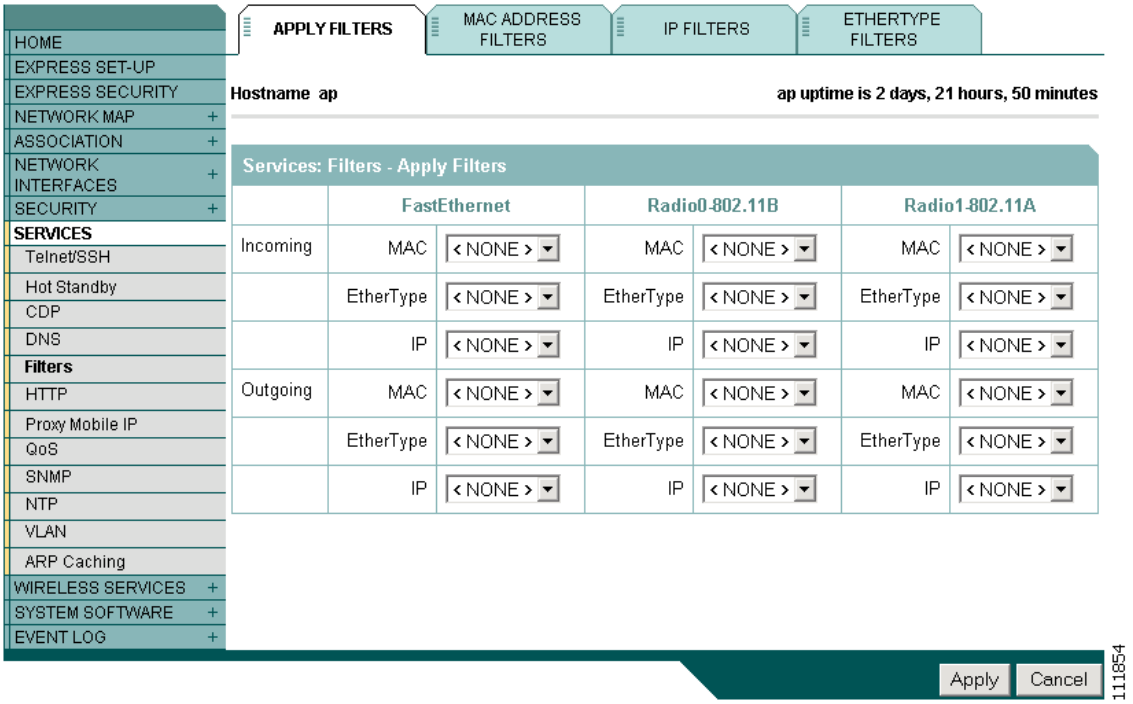
Step 7 Click **Add**. The Ethertype appears in the Filters Classes field. To remove the Ethertype from the Filters Classes list, select it and click **Delete Class**. Repeat Step 4 through Step 7 to add Ethertypes to the filter.

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. Figure 16-9 shows the Apply Filters page.

Figure 16-9 Apply Filters Page



Step 11 Select the filter number from one of the Ethertype drop-down menus. 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 1200 Series Access Point Command Reference* for this release and the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.2*.

This chapter contains these sections:

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 CiscoWorks2000.

CDP is enabled on the access point Ethernet port by default. However, 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, Cisco recommends 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

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	**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 17-4.

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.
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.

Command	Description
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
0FFFFFFFF010221FF0000000000000000024B293A00FF0000
VTP Management Domain: ''
Duplex: full

-------------------------
```

```
Device ID: idf2-1-lab-13.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
0FFFFFFFF010101FF0000000000000000142EFA400FF
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
```

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 and Bridges* for this release and to the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.3*.

This chapter consists of these sections:

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 CiscoWorks. 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

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

For detailed information on SNMPv3, click this link to browse to the *New Feature Documentation* for Cisco IOS Release 12.0(3)T:

http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html

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.

A community string can have one of these attributes:

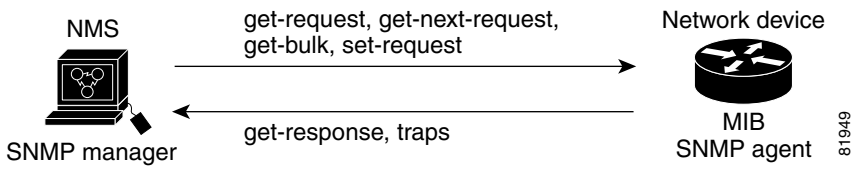
- Read-only—Gives read access to authorized management stations to all objects in the MIB except the community strings, but does not allow write access
- Read-write—Gives read and write access to authorized management stations to all objects in the MIB, but does not allow access to the community strings

Using SNMP to Access MIB Variables

An example of an NMS is the CiscoWorks network management software. CiscoWorks 2000 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 as a graph 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

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 18-10 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.

	Command	Purpose
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 non-IEEE802dot11-MIB objects and *ieee* is the community string for queries on IEEE802dot11-mib objects:

```
ap(config)# snmp-server view dot11view ieee802dot11 included
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
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.

Table 18-4 Notification Types (continued)

Notification Type	Description
syslog	Enable syslog traps.
wlan-wep	Enable WEP traps.

Some notification types cannot be controlled with the **snmp-server enable** global configuration command, such as **tty** and **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, Cisco recommends 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 18-8.
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 18-8. 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.

	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 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 for Release 12.3*.

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. This chapter contains these sections:

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 configured as a root 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.

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:

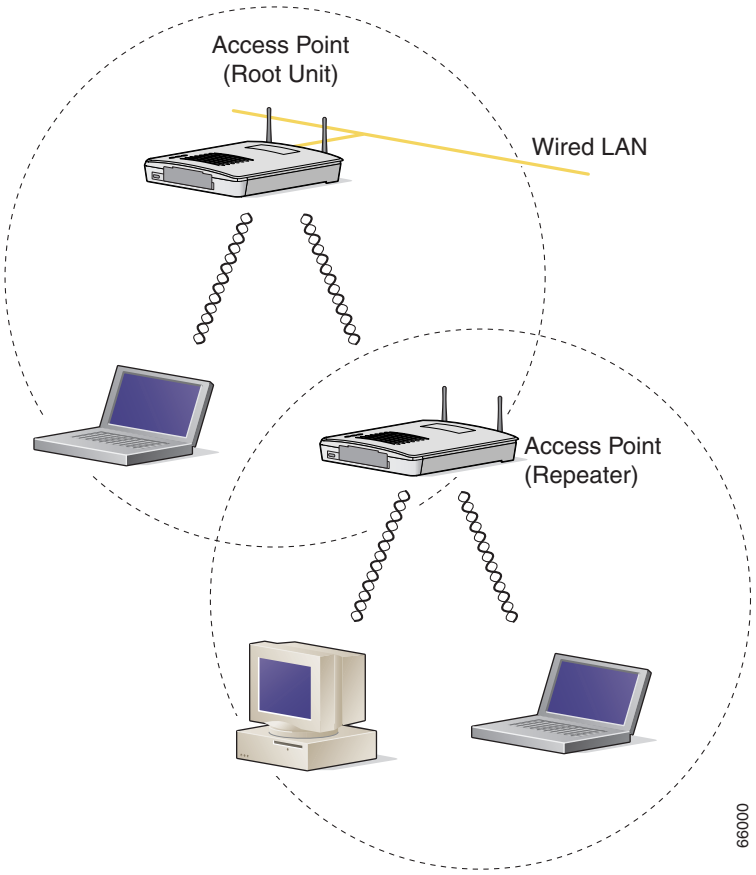
```
SSID [xxx] must be configured as native-vlan before enabling infrastructure-ssid
```

Note Because access points create a virtual interface for each radio interface, repeater access points associate to the root access point twice: once for the actual interface and once for the virtual interface.

Note You cannot configure multiple VLANs on repeater access points. Repeater access points support only the native VLAN.

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

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. Non-Cisco client devices sometimes have trouble communicating with repeater access points.
- 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 6-7.
- Repeater access points support only the native VLAN. You cannot configure multiple VLANs on a repeater access point.

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.

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 is radio 0, and the 5-GHz radio is radio 1.
Step 3	**ssid** *ssid-string*	Create 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.
Step 4	**infrastructure-ssid** [**optional**]	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 5	**exit**	Exit SSID configuration mode and return to radio interface configuration mode.
Step 6	**station-role repeater**	Set the access point's role in the wireless LAN to repeater.
Step 7	**dot11 extensions aironet**	If Aironet extensions are disabled, enable Aironet extensions.
Step 8	**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. The repeater attempts to associate to MAC address 1 first; if that access point does not respond, the repeater tries the next access point in its parent list. **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 also enter a timeout value in seconds that determines how long the repeater attempts to associate to a parent access point before trying the next parent in the list. Enter a timeout value from 0 to 65535 seconds.
Step 9	**end**	Return to privileged EXEC mode.
Step 10	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to set up a repeater access point with three potential parents:

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid chicago
AP(config-ssid)# infrastructure-ssid
AP(config-ssid)# exit
AP(config-if)# station-role repeater
AP(config-if)# dot11 extensions aironet
AP(config-if)# parent 1 0987.1234.h345 900
AP(config-if)# parent 2 7809.b123.c345 900
AP(config-if)# parent 3 6543.a456.7421 900
AP(config-if)# end
```

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** }	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	**antenna-alignment** *timeout*	Establish 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, check the LEDs on top of the repeater access point. If your repeater is functioning correctly, the LEDs on the repeater and the root access point to which it is associated behave like this:

- The status LED on the root access point is steady green, indicating that at least one client device is associated with it (in this case, the repeater).
- The status LED on the repeater access point is steady green when it is associated with the root access point and the repeater has client devices associated to it. The repeater's status LED flashes (steady green for 7/8 of a second and off for 1/8 of a second) when it is associated with the root access point but the repeater has no client devices associated to it.

The repeater access point should also appear as associated with the root access point in the root access point's Association Table.

Setting Up a Repeater As a LEAP 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 authenticates to your network using LEAP, Cisco's wireless authentication method, and receives and uses dynamic WEP keys.

Setting up a repeater as a LEAP client requires three major steps:

1. Create an authentication username and password for the repeater on your authentication server.
2. Configure LEAP authentication 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 LEAP client. Beginning in Privileged Exec mode, follow these instructions to set up the repeater as a LEAP client:

	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.
Step 3	**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 4	**authentication network-eap** *list-name*	Enable LEAP authentication on the repeater so that LEAP-enabled client devices can authenticate through the repeater. For list-name, specify the list name you want to use for EAP authentication. You define list names for EAP and for MAC addresses using the **aaa authentication login** command. These lists define the authentication methods activated when a user logs in and indirectly identify the location where the authentication information is stored.
Step 5	**authentication client username** *username* **password** *password*	Configure the username and password that the repeater uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the repeater on the authentication server.
Step 6	**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.

	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.

Setting Up a Repeater As a WPA 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 WPA-enabled client devices.

Beginning in Privileged Exec mode, follow these steps to set up the repeater as a WPA client:

	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.
Step 3	**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.
Step 4	**authentication open**	Enable open authentication for the SSID.
Step 5	**authentication key-management wpa**	Enable WPA authenticated key management for the SSID.
Step 6	**infrastructure ssid**	Designate the SSID as the SSID that the repeater uses to associate to other access points.
Step 7	**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 8	**end**	Return to privileged EXEC mode.
Step 9	**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.

Configuring a Hot Standby Access Point

When you set up the standby access point, you must enter the MAC address of the access point that the standby unit will monitor. 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
- WEP settings
- Authentication types and authentication servers

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 the "Working with Configuration Files" section on page 20-8 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 a 1200 Series access point with two radios to monitor a 1200 Series 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.
Step 3	**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.
Step 4	**ssid** *ssid-string*	Create the SSID that the standby access point uses to associate to the monitored access point; in the next step designate this SSID as an infrastructure SSID. If you created an infrastructure SSID on the monitored access point, create the same SSID on the standby access point, also.
Step 5	**infrastructure-ssid** [**optional**]	Designate the SSID as an infrastructure SSID. The standby uses this SSID to associate to the monitored access point. If the standby access point takes the place of the monitored access point, infrastructure devices must associate to the standby access point using this SSID unless you also enter the **optional** keyword.
Step 6	**authentication client username** *username* **password** *password*	If the monitored access point is configured to require LEAP authentication, configure the username and password that the standby access point uses when it performs LEAP authentication. This username and password must match the username and password that you set up for the standby access point on the authentication server.
Step 7	**exit**	Exit SSID configuration mode and return to radio interface configuration mode.

	Command	Purpose
Step 8	**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 9	**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 10	**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.
Step 11	**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 12	**end**	Return to privileged EXEC mode.
Step 13	**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 1100, 1130, 1200, 1230, and 1240 series 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 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 interface the other remains up.

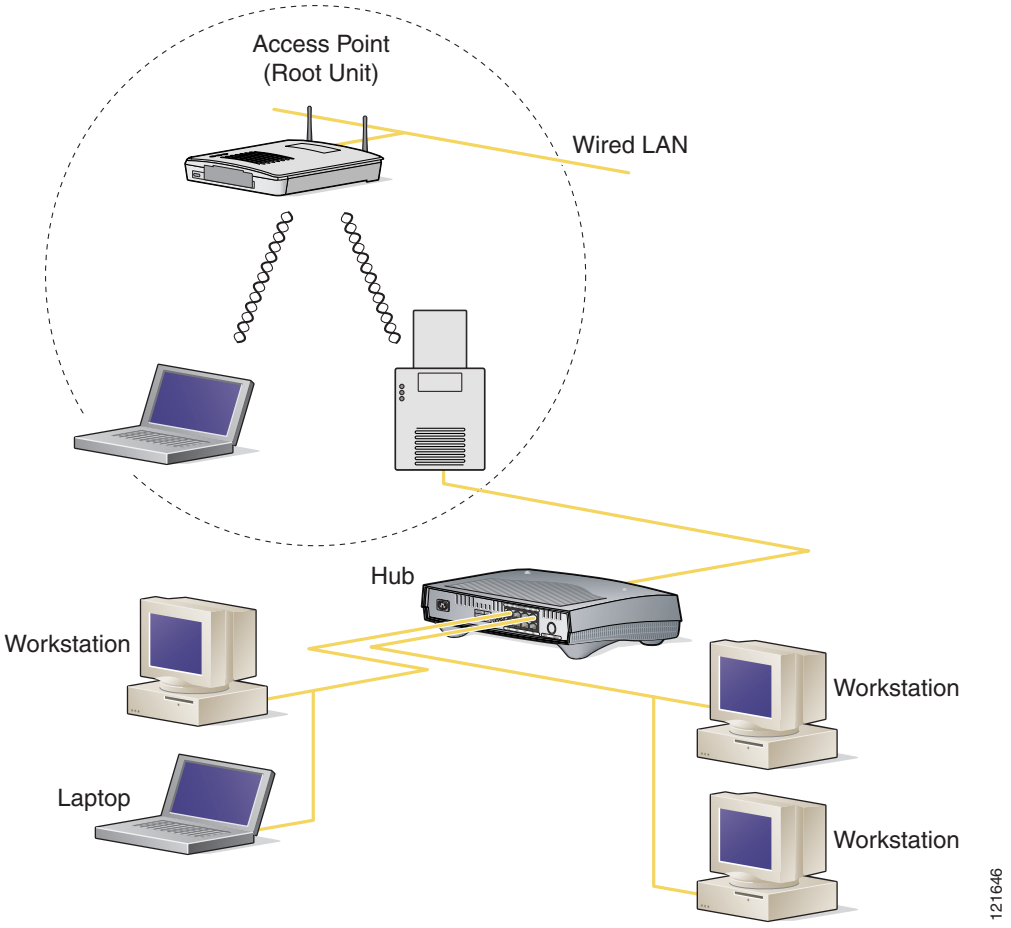
Caution An access point in workgroup bridge mode can introduce a bridge loop if you connect its Ethernet port to your wired LAN. To avoid a bridge loop on your network, disconnect the workgroup bridge from your wired LAN before or soon after you configure it as a workgroup bridge.

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 workgroup bridges at the edge of the access point's coverage area might lose IP connectivity. 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

Configuring a Workgroup Bridge for Roaming

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.

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.

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**	Set the radio role to workgroup bridge. If your access point contains two radios, the radio not set to workgroup bridge mode is automatically disabled.
Step 4	**ssid** *ssid-string*	Create the SSID that the workgroup bridge uses to associate to a parent access point or bridge.
Step 5	**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 6	**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 7	**exit**	Exit SSID configuration mode and return to radio interface configuration mode.
Step 8	**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. The workgroup bridge attempts to associate to MAC address 1 first; if that access point does not respond, the workgroup bridge tries the next access point in its parent list. **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 also enter a timeout value in seconds that determines how long the workgroup bridge attempts to associate to a parent access point before trying the next parent in the list. Enter a timeout value from 0 to 65535 seconds.
Step 9	**exit**	Exit radio configuration mode and return to global configuration mode.
Step 10	**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 11	**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 12	**end**	Return to privileged EXEC mode.
Step 13	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

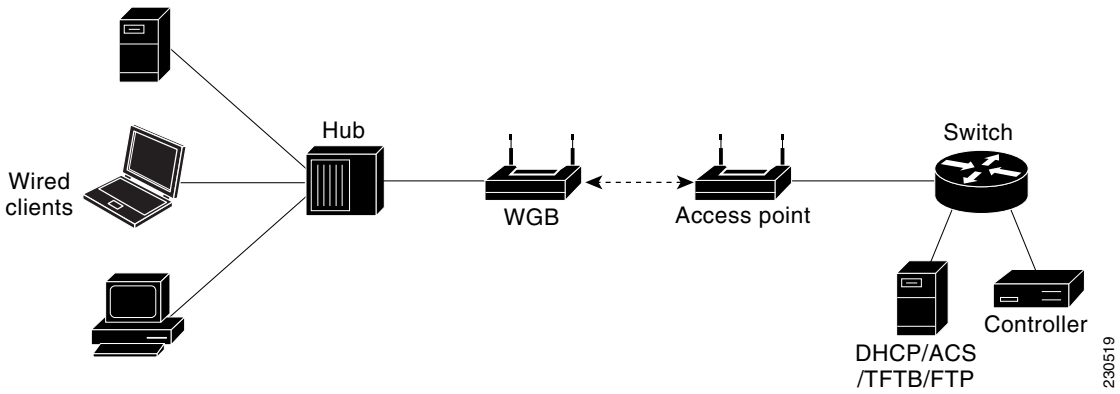
This example shows how to configure an 1100 series access point as a workgroup bridge. In this example, the workgroup bridge uses the configured username and password to perform LEAP authentication, and the devices attached to its Ethernet port are assigned to VLAN 22:

```
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
```

The Workgroup Bridge 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 clients. See the example in

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 12.4(3g)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 AP1121, AP1130, AP1231, AP1240, and AP1310. Cisco IOS Releases prior to 12.4(eg)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. Cisco recommends 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 Settings > Network Interfaces page.
- On the workgroup bridge access point CLI, enter this command: **station-role workgroup-bridge**
- The workgroup bridge can associate only to lightweight access points (except the Cisco Airespace AP1000 series access points, which are not supported).
- Only workgroup bridge in client mode (which is the default value) are supported. Those in infrastructure mode are not supported. Perform one of the following to enable client mode on the workgroup bridge:
  - On the workgroup bridge access point GUI, choose **Disabled** for the Reliable Multicast to workgroup bridge parameter.
  - On the workgroup bridge access point CLI, enter this command: **no infrastructure client**.

Note VLANs are not supported for use with workgroup bridges.

- 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, Cisco recommends that you physically secure the wired side of the workgroup bridge.
- With Layer 3 roaming, if you plug 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 Configuration

Here is a sample configuration of a workgroup bridge access point using static WEP with a 40-bit WEP key:

```
ap#confure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ap(config)#dot11 ssid WGB_with_static_WEP
ap(config-ssid)#authentication open
ap(config-ssid)#guest-mode
ap(config-ssid)#exit
ap(config)#interface dot11Radio 0
ap(config)#station-role workgroup-bridge
ap(config-if)#encry mode wep 40
ap(config-if)#encry key 1 size 40 0 1234567890
ap(config-if)#WGB_with_static_WEP
ap(config-if)#end
```

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. Cisco recommends configuring the seconds parameter to a value greater than the wired client's idle period.

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 Aironet 1200 Series Access Point Command Reference* for this release and the *Cisco IOS Configuration Fundamentals Command Reference for Release 12.3*.

This chapter consists of these sections:

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
*   16128000    11118592     flash     rw   flash:
    16128000    11118592   unknown     rw   zflash:
       32768       26363     nvram     rw   nvram:
           -           -   network     rw   tftp:
           -           -    opaque     rw   null:
           -           -    opaque     rw   system:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
           -           -   network     rw   rcp:
           -           -   network     rw   ftp:
```

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.

Table 20-1 show file systems Field Descriptions (continued)

Field	Value
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.
Flags	Permission for file system. **ro**—read-only. **rw**—read/write. **wo**—write-only.
Prefixes	Alias for file system. **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 new_configs**	Change to the directory of interest. The command example shows how to change to the directory named *new_configs*.
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 old_configs**	Create a new directory. The command example shows how to create the directory named *old_configs*. 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.

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 20-8.

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 20-18.

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 the *c1200-k9w7-mx.122-8.JA.tar* file that is in Flash memory:

```
ap# archive tar /table flash:c1200-k9w7-mx.122-8.JA.tar
info (219 bytes)
c1200-k9w7-mx.122-8.JA/ (directory)
c1200-k9w7-mx.122-8.JA/html/ (directory)
c1200-k9w7-mx.122-8.JA/html/foo.html (0 bytes)
c1200-k9w7-mx.122-8.JA/c1200-k9w7-mx.122-8.JA.bin (610856 bytes)
c1200-k9w7-mx.122-8.JA/info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the *c1200-k9w7-mx.122-8.JA/html* directory and its contents:

```
ap# archive tar /table flash:c1200-k9w7-mx.122-8.JA/html
c1200-k9w7-mx.122-8.JA/html/ (directory)
c1200-k9w7-mx.122-8.JA/html/foo.html (0 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

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. On a Sun workstation, make sure that the /etc/inetd.conf file contains this line:

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  Make sure that the /etc/services file contains this line:

  ```
  tftp 69/udp
  ```

  Note You must restart the inetd daemon after modifying the /etc/inetd.conf and /etc/services files. To restart the daemon, either stop the inetd process and restart it, or enter a **fastboot** command (on the SunOS 4.x) or a **reboot** command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, refer to the documentation for your workstation.

- 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 (usually /tftpboot on a UNIX workstation).
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- Before uploading the configuration file, you might need to create an empty file on the TFTP server. To create an empty file, enter the **touch** *filename* command, where *filename* is the name of the file you will use when uploading it to the server.
- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) 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 20-10.

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 20-10.

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 (see Steps 4, 5, and 6).
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 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 (see Steps 4, 5, and 6).
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 (see Steps 4 and 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	**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-config 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 (see Steps 4 and 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	**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-confg
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 for Release 12.1*.

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:

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.

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

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. On a Sun workstation, make sure that the /etc/inetd.conf file contains this line:

  ```
  tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
  ```

  Make sure that the /etc/services file contains this line:

  ```
  tftp 69/udp
  ```

  Note You must restart the inetd daemon after modifying the /etc/inetd.conf and /etc/services files. To restart the daemon, either stop the inetd process and restart it, or enter a **fastboot** command (on the SunOS 4.x) or a **reboot** command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, refer to the documentation for your workstation.

- 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 (usually */*tftpboot on a UNIX workstation).
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- Before uploading the image file, you might need to create an empty file on the TFTP server. To create an empty file, enter the **touch** *filename* command, where *filename* is the name of the file you will use when uploading the image to the server.

- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) 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 20-20
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 20-20.

	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 20-23
- Downloading an Image File by Using FTP, page 20-24
- Uploading an Image File by Using FTP, page 20-26

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 Steps 1 through 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 20-23.
Step 2		Log into the access point through a Telnet session.

	Command	Purpose
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).
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 20-23. • 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 20-23. • 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 (see Steps 4, 5, and 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 20-23. • 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

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 20-27.
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 (see Steps 4 and 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 20-27. • 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 20-27. • 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 20-27.
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 (see Steps 4 and 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 20-27. • 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. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

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 User Name field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click the **System Software** tab and then click **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. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.x).

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 User Name field.

Step 4 Enter the access point password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click the **System 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 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.

CHAPTER 21

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 for Release 12.3*.

This chapter consists of these sections:

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 UNIX syslog server, depending on your configuration. The process also sends messages to the console.

Note The syslog format is compatible with 4.3 BSD UNIX.

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

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 21-1 describes the elements of syslog messages.

Table 21-1 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 21-6.
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 21-6.
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 21-3 on page 21-8.
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:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
00:00:47: %LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to up
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
00:00:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to down 2
*Mar  1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
*Mar  1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)
```

Default System Message Logging Configuration

Table 21-2 shows the default system message logging configuration.

Table 21-2 Default System Message Logging Configuration

Feature	Default Setting
System message logging to the console	Enabled
Console severity	Debugging (and numerically lower levels; see Table 21-3 on page 21-8)
Logging buffer size	4096 bytes
Logging history size	1 message

Table 21-2 Default System Message Logging Configuration (continued)

Feature	Default Setting
Timestamps	Disabled
Synchronous logging	Disabled
Logging server	Disabled
Syslog server IP address	None configured
Server facility	Local7 (see Table 21-4 on page 21-11)
Server severity	Informational (and numerically lower levels; see Table 21-3 on page 21-8)

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 21-6.

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 UNIX 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 UNIX Syslog Servers" section on page 21-10.
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. To disable logging to a file, use the **no logging file** [*severity-level-number* | *type*] 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:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

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 21-3.

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 21-3 on page 21-8).
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 21-3 on page 21-8).
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 21-3 on page 21-8). For complete syslog server configuration steps, see the "Configuring UNIX Syslog Servers" section on page 21-10.
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 21-3 describes the *level* keywords. It also lists the corresponding UNIX syslog definitions from the most severe level to the least severe level.

Table 21-3 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. Debug commands are typically used only by the Technical Assistance Center (TAC).
- 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 21-3 on page 21-8) 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 21-3 on page 21-8 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 21-3 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 UNIX Syslog Servers

The next sections describe how to configure the 4.3 BSD UNIX server syslog daemon and define the UNIX system logging facility.

Logging Messages to a UNIX Syslog Daemon

Before you can send system log messages to a UNIX syslog server, you must configure the syslog daemon on a UNIX server. Log in as root, and perform these steps:

Note Some recent versions of UNIX syslog daemons no longer accept by default syslog packets from the network. If this is the case with your system, use the UNIX **man syslogd** command to determine what options must be added to or removed from the syslog command line to enable logging of remote syslog messages.

Step 1 Add a line such as the following to the file /etc/syslog.conf:

```
local7.debug /usr/adm/logs/cisco.log
```

The **local7** keyword specifies the logging facility to be used; see Table 21-4 on page 21-11 for information on the facilities. The **debug** keyword specifies the syslog level; see Table 21-3 on page 21-8 for information on the severity levels. The syslog daemon sends messages at this level or at a more severe level to the file specified in the next field. The file must already exist, and the syslog daemon must have permission to write to it.

Step 2 Create the log file by entering these commands at the UNIX shell prompt:

```
$ touch /usr/adm/log/cisco.log
$ chmod 666 /usr/adm/log/cisco.log
```

Step 3 Make sure the syslog daemon reads the new changes by entering this command:

```
$ kill -HUP `cat /etc/syslog.pid`
```

For more information, see the **man syslog.conf** and **man syslogd** commands on your UNIX system.

Configuring the UNIX 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 UNIX syslog facilities.

Beginning in privileged EXEC mode, follow these steps to configure UNIX system facility message logging:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**logging** *host*	Log messages to a UNIX 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.

	Command	Purpose
Step 3	**logging trap** *level*	Limit messages logged to the syslog servers. Be default, syslog servers receive informational messages and lower. See Table 21-3 on page 21-8 for *level* keywords.
Step 4	**logging facility** *facility-type*	Configure the syslog facility. See Table 21-4 on page 21-11 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 21-4 lists the 4.3 BSD UNIX system facilities supported by the Cisco IOS software. For more information about these facilities, consult the operator's manual for your UNIX operating system.

Table 21-4 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
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 for Release 12.2.*

To display the logging history file, use the **show logging history** privileged EXEC command.

CHAPTER 22

Wireless Device 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

Sections in this chapter include:

Checking the Top Panel Indicators

If your wireless device is not communicating, check the three LED indicators on the top panel to quickly assess the device's status. Figure 22-1 shows the indicators on the 1200 series access point. Figure 22-2 shows the indicators on the 1100 series access point. Figure 22-3 and Figure 22-4 show the indicators on the 350 series access point.

Note The 1130 series access point has a status LED on the top of the unit and two LEDs inside the protective cover. See the "Indicators on 1130 Series Access Points" section on page 22-6 for information on 1130 series access point indicators.

Figure 22-1 Indicators on the 1200 Series Access Point

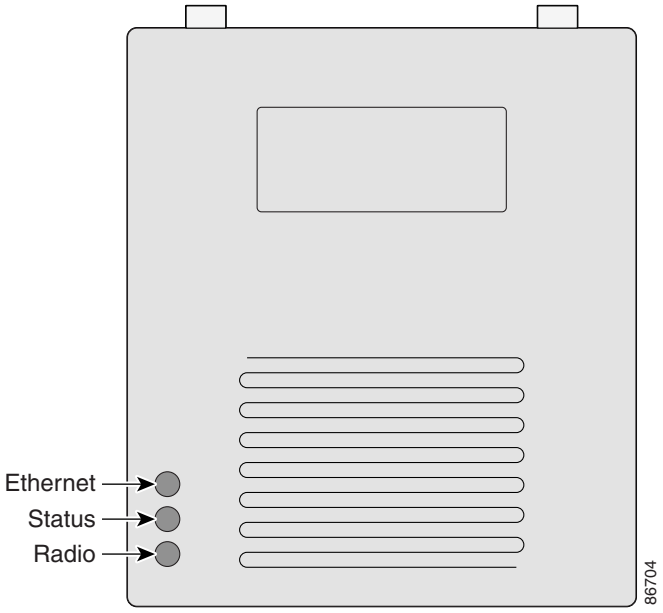


Figure 22-2 Indicators on the 1100 Series Access Point

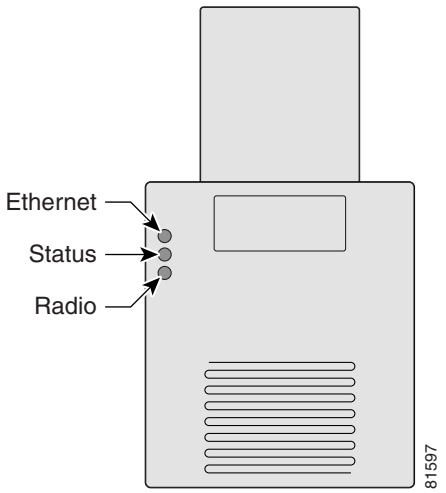


Figure 22-3 Indicators on the 350 Series Access Point (Plastic Case)

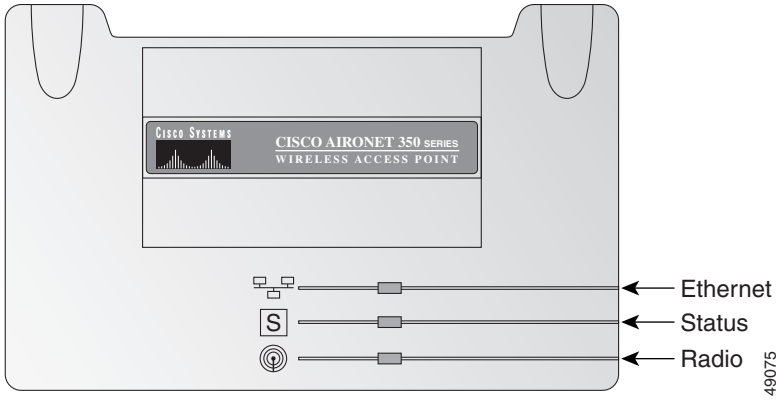
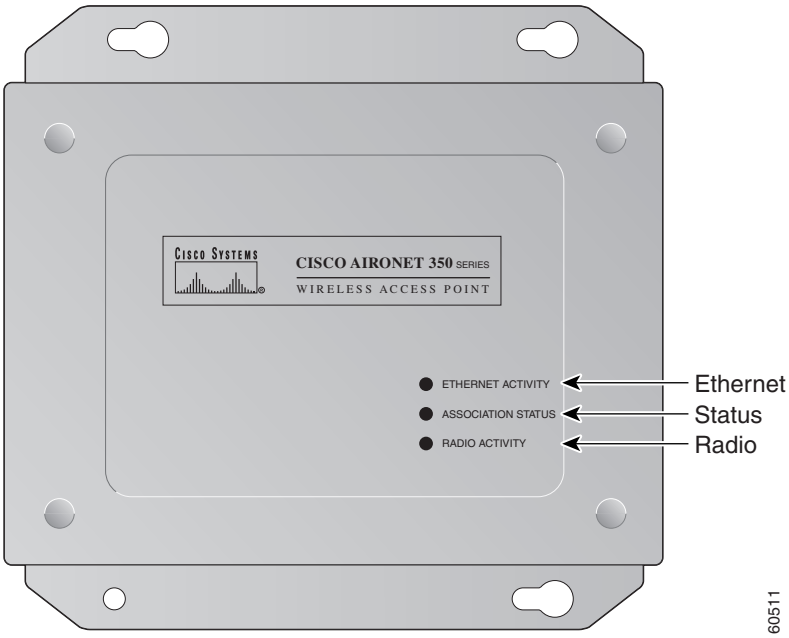


Figure 22-4 Indicators on the 350 Series Access Point (Metal Case)



The indicator signals on the wireless device have the following meanings (for additional details refer to Table 22-1):

- The Ethernet indicator signals traffic on the wired LAN. This indicator is normally green when an Ethernet cable is connected, and blinks green when a packet is received or transmitted over the Ethernet infrastructure. The indicator is off when the Ethernet cable is not connected.
- The status indicator signals operational status. Steady green indicates that the wireless device is associated with at least one wireless client. Blinking green indicates that the wireless device is operating normally but is not associated with any wireless devices.
- The radio indicator blinks green to indicate radio traffic activity. The light is normally off, but it blinks whenever a packet is received or transmitted over the wireless device's radio.

Table 22-1 Top Panel Indicator Signals

Message type	Ethernet indicator	Status indicator	Radio indicator	Meaning
Boot loader status	Green	–	Green	DRAM memory test.
	–	Amber	Red	Board initialization test.
	–	Blinking green	Blinking green	Flash memory test.
	Amber	Green	–	Ethernet initialization test.
	Green	Green	Green	Starting Cisco IOS software.
Association status	–	Green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the wireless device's SSID and WEP settings.

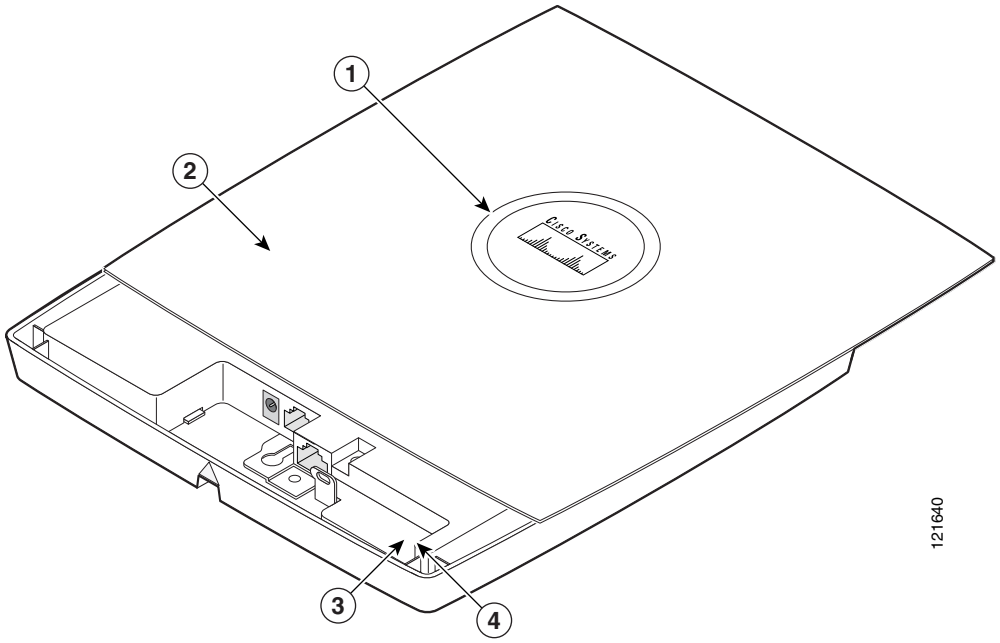
Table 22-1 Top Panel Indicator Signals (continued)

Message type	Ethernet indicator	Status indicator	Radio indicator	Meaning
Operating status	–	Green	Blinking green	Transmitting/receiving radio packets.
	Green	–	–	Ethernet link is operational.
	Blinking green	–	–	Transmitting/receiving Ethernet packets.
Boot Loader Errors	Red	–	Red	DRAM memory test failure.
	–	Red	Red	File system failure.
	Red	Red	–	Ethernet failure during image recovery.
	Amber	Green	Amber	Boot environment error.
	Red	Green	Red	No Cisco IOS image file.
	Amber	Amber	Amber	Boot failure.
Operation Errors	–	Green	Blinking amber	Maximum retries or buffer full occurred on the radio.
	Blinking amber	–	–	Transmit/receive Ethernet errors.
	–	Blinking amber	–	General warning.
Configuration Reset	–	Amber	–	Resetting the configuration options to factory defaults.
Failures	Red	Red	Red	Firmware failure; try disconnecting and reconnecting unit power.
	Blinking red	–	–	Hardware failure. The wireless device must be replaced.
Firmware Upgrade	–	Red	–	Loading new firmware image.

Indicators on 1130 Series Access Points

If your access point is not working properly, check the LED ring on the top panel or the Ethernet and Radio LEDs in the cable bay area. You can use the LED indications to quickly assess the unit's status. Figure 22-5 shows the access point LEDs.

Figure 22-5 1130 Series Access Point LEDs



1	Status LED	**3**	Ethernet LED
2	Access point cover	**4**	Radio LED

Note To view the Ethernet and Radio LEDs you must open the access point cover.

The LED signals are listed in Table 22-2.

Table 22-2 LED Signals

	Cable Bay Area		Top of Unit	
Message type	**Ethernet LED**	**Radio LED**	**Status LED**	**Meaning**
Boot loader status	Green	Green	Green	DRAM memory test ok.
	Off	Blinking green	Light blue	Initialize Flash file system.
	Off	Green	Pink	Flash memory test ok.
	Green	Off	Blue	Ethernet test ok.
	Green	Green	Green	Starting Cisco IOS.
Association status	n/a	n/a	Light green	Normal operating condition, but no wireless client devices are associated with the unit.
	n/a	n/a	Light blue	Normal operating condition, at least one wireless client device is associated with the unit.
Operating status	Green	n/a	n/a	Ethernet link is operational.
	Blinking green	n/a	n/a	Transmitting or receiving Ethernet packets.
	n/a	Blinking green	n/a	Transmitting or receiving radio packets.
	n/a	n/a	Blinking dark blue	Software upgrade in progress
Boot loader warnings	Off	Off	Yellow	Ethernet link not operational.
	Red	Off	Yellow	Ethernet failure.
	Amber	Off	Yellow	Configuration recovery in progress (Mode button pressed for 2 to 3 seconds).
	Off	Red	Pink	Image recovery (Mode button pressed for 20 to 30 seconds)
	Blinking green	Red	Blinking pink and off	Image recovery in progress and Mode button is released.

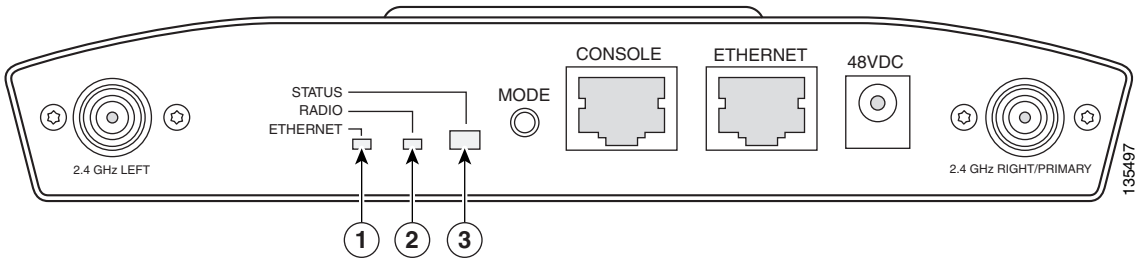
Table 22-2 LED Signals (continued)

Message type	Cable Bay Area		Top of Unit	Meaning
	Ethernet LED	Radio LED	Status LED	
Boot loader errors	Red	Red	Red	DRAM memory test failure.
	Off	Red	Blinking red and blue	Flash file system failure.
	Off	Amber	Blinking red and light blue	Environment variable (ENVAR) failure.
	Amber	Off	Blinking red and yellow	Bad MAC address.
	Red	Off	Blinking red and off	Ethernet failure during image recovery.
	Amber	Amber	Blinking red and off	Boot environment error.
	Red	Amber	Blinking red and off	No Cisco IOS image file.
	Amber	Amber	Blinking red and off	Boot failure.
Cisco IOS errors	Blinking amber	n/a	n/a	Transmit or receive Ethernet errors.
	n/a	Blinking amber	n/a	Maximum retries or buffer full occurred on the radio.
	Red	Red	Orange	Software failure; try disconnecting and reconnecting unit power.
	n/a	n/a	Orange	General warning, insufficient inline power.
	Blinking green	Blinking green	Blinking green	User activation of location indicator.

Indicators on 1240 Series Access Points

If your access point is not working properly, check the Status, Ethernet, and Radio LEDs on the 2.4 GHz end of the unit. You can use the LED indications to quickly assess the unit's status. Figure 22-6 shows the access point LEDs (for additional information refer to the Event Log using the access point browser interface).

Figure 22-6 1240 Series Access Point LEDs



1	Ethernet LED	**3**	Radio LED
2	Radio LED		

The LED signals are listed in Table 22-3.

Table 22-3 LED Signals

Message type	Ethernet LED	Radio LED	Status LED	Meaning
Boot loader status	Green	Green	Green	DRAM memory test ok.
	Off	Blinking green	Blue-green	Initialize Flash file system.
	Off	Green	Pink	Flash memory test ok.
	Green	Off	Dark blue	Ethernet test ok.
	Green	Green	Green	Starting Cisco IOS.
Association status	—	—	Light green	Normal operating condition, but no wireless client devices are associated with the unit.
	—	—	Blue	Normal operating condition, at least one wireless client device is associated with the unit.
Operating status	Green	—	—	Ethernet link is operational.
	Blinking green	—	—	Transmitting or receiving Ethernet packets.
	—	Blinking green	—	Transmitting or receiving radio packets.
	—	—	Blinking dark blue	Software upgrade in progress

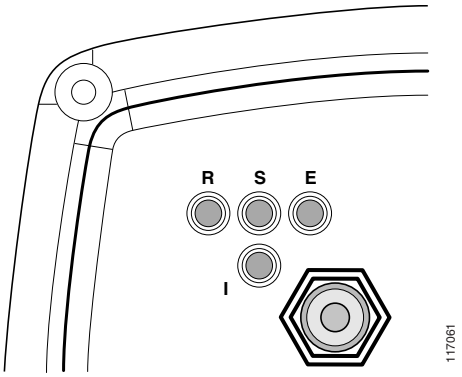
Message type	Ethernet LED	Radio LED	Status LED	Meaning
Boot loader warnings	Off	Off	Yellow	Ethernet link not operational.
	Red	Off	Yellow	Ethernet failure.
	Amber	Off	Yellow	Configuration recovery in progress (Mode button pressed for 2 to 3 seconds).
	Off	Red	Pink	Image recovery (Mode button pressed for 20 to 30 seconds)
	Blinking green	Red	Blinking pink and off	Image recovery in progress and Mode button is released.
Boot loader errors	Red	Red	Red	DRAM memory test failure.
	Off	Red	Blinking red and blue	Flash file system failure.
	Off	Amber	Blinking red and blue-green	Environment variable (ENVAR) failure.
	Amber	Off	Blinking red and yellow	Bad MAC address.
	Red	Off	Blinking red and off	Ethernet failure during image recovery.
	Amber	Amber	Blinking red and off	Boot environment error.
	Red	Amber	Blinking red and off	No Cisco IOS image file.
	Amber	Amber	Blinking red and off	Boot failure.
Cisco IOS errors	Blinking amber	—	—	Transmit or receive Ethernet errors.
	—	Blinking amber	—	Maximum retries or buffer full occurred on the radio.
	Red	Red	Amber	Software failure; try disconnecting and reconnecting unit power.
	—	—	Amber	General warning, insufficient inline power (see the Low Power Condition section).

Indicators on 1300 Outdoor Access Point/Bridges

If your access point/bridge is not associating with a remote bridge or access point, check the four LEDs on the back panel. You can use them to quickly assess the unit's status. For information on using the LEDs during the installation and alignment of the access point/bridge antenna, refer to the *Cisco Aironet 1300 Series Outdoor Access Point/Bridge Mounting Instructions* that shipped with your access point/bridge.

Figure 22-7 shows the access point/bridge LEDs.

Figure 22-7 LEDs



R	Radio LED	**E**	Ethernet LED
S	Status LED	**I**	Install LED

Normal Mode LED Indications

During access point/bridge operation the LEDs provide status information as shown in Table 22-4.

Table 22-4 LED Indications

Ethernet LED	Status LED	Radio LED	Install LED	Meaning
Off	—	—	—	Ethernet link is down or disabled.
Blinking green	—	—	—	Transmitting and receiving Ethernet packets.
Blinking amber	—	—	—	Transmitting and receiving Ethernet errors.
amber	—	—	—	Firmware error—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.
—	Blinking green	—	—	Root bridge mode—no remote bridges are associated. Non-root bridge mode—not associated to the root bridge. If all bridges are powered up, this could be caused by incorrect SSID and security settings or improper antenna alignment. You should check the SSID and security settings of all bridges and verify antenna alignment. If the problem continues, contact technical support for assistance.
—	Green	—	—	Root mode—associated to at least one remote bridge. Non-root mode—associated to the root bridge. This is normal operation.
—	Blinking amber	—	—	General warning—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.
—	Amber	—	—	Loading firmware.

Table 22-4 LED Indications (continued)

Ethernet LED	Status LED	Radio LED	Install LED	Meaning
Red	Amber	Red	—	Loading Firmware error—disconnect and reconnect the power injector power. If the problem continues, contact technical support for assistance.
—	—	Off	—	Normal operation.
—	—	Blinking green	—	Transmitting and receiving radio packets—normal operation.
—	—	Blinking amber	—	Maximum retries or buffer full occurred on the radio interface—disconnect and reconnect the power injector power jack. If the problem continues, contact technical support for assistance.
—	—	Amber	—	Radio firmware error—disconnect and reconnect power injector power.If the problem continues, contact technical support for assistance.
—	—	—	Amber blinking	Not associated (non-root mode). The access point/bridge attempts to associate with a root bridge for 60 seconds[1].
—	—	—	Amber	Associated (non-root mode).
—	—	—	Green blinking	Not associated (root mode). The access point/bridge attempts to associate with a non-root bridge indefinitely.
—	—	—	Green	Associated (root mode).
—	—	—	Red	Overcurrent or overvoltage error—disconnect power to the power injector, check all coax cable connections, wait approximately 1 minute, and reconnect power. If error continues, contact technical support.

1. Preconfigured bridges search indefinitely.

The access point/bridge uses a blinking code to identify various error conditions. The code sequence uses a two-digit diagnostic code that starts with a long pause to delimit the code, followed by the LED flashing red to count out the first digit, then a short pause, followed by the LED flashing red to count out the second digit.

The LED blinking error codes are described in Table 22-5.

Table 22-5 LED Blinking Error Codes

LED	Blinking Codes		Description
	First Digit	Second Digit	
Ethernet	2	1	Ethernet cable problem—verify that the cable is properly connected and not defective. This error might also indicate a problem with the Ethernet link. If the cable is connected properly and not defective, contact technical support for assistance.

Table 22-5 LED Blinking Error Codes (continued)

LED	Blinking Codes		Description
	First Digit	Second Digit	
Radio	1	2	Radio not detected—contact technical support for assistance.
	1	3	Radio not ready—contact technical support for assistance.
	1	4	Radio did not start—contact technical support for assistance.
	1	5	Radio failure—contact technical support for assistance.
	1	6	Radio did not flash its firmware—contact technical support for assistance.

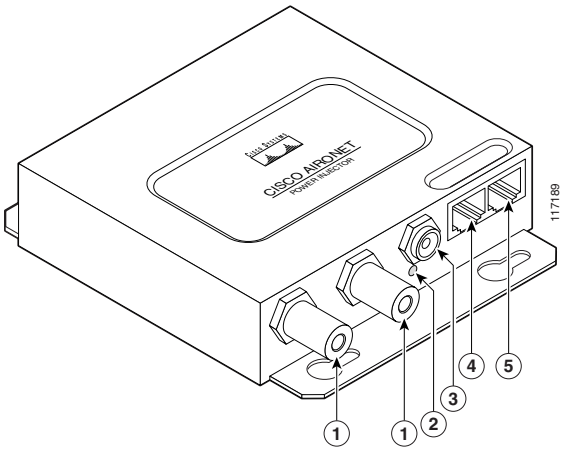
Power Injector

When the power injector is powered up, it applies 48-VDC to the dual-coax cables to the access point/bridge.

When power is applied to the access point/bridge, the unit activates the bootloader and begins the POST operations. The access point/bridge begins to load the IOS image when the Post operations are successfully completed. Upon successfully loading the IOS image, the unit initializes and tests the radio.

The power injector LED is shown in Figure 22-8.

Figure 22-8 Power Injector



1	Dual-coax Ethernet ports (F-Type connectors)	**4**	Ethernet LAN port (RJ-45 connector)
2	Power LED	**5**	Console serial port (RJ-45 connector)
3	Power jack		

The power injector is available in two models:

- Cisco Aironet Power Injector LR2—standard version (included with the bridge)
  - 48-VDC input power
  - Uses the 48-VDC power module (included with the bridge)

- Cisco Aironet Power Injector LR2T—optional transportation version
  - 12- to 40-VDC input power
  - Uses 12 to 40 VDC from a vehicle battery

Checking Power

You can verify the availability of power to the access point/bridge by checking the power injector LED (see Figure 22-8):

- Power LED
  - 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. The 1130 and 1240 access points support the IEEE 802.3af power standard, Cisco Pre-Standard PoE protocol, and Cisco Intelligent Power Management for in-line power sources.

For full operation, the 1130 and 1240 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.

Note An 802.3af compliant switch (Cisco or non-Cisco) is capable of supplying sufficient power for full operation.

On power up, the 1130 and 1240 series 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 Cipher Suites and WEP," 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.

Note The wireless device MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the wireless device radio. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

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 1100 and 1200 series 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 You cannot use the mode button to reset the configuration to defaults on 350 series access points. To reset the configuration on 350 series access points, follow the instructions in the "Using the Web Browser Interface" section on page 22-16, or in the "Using the CLI" section on page 22-17.

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.

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. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.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 User Name field.

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

Step 5 Click **System 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 **reload** command to reboot the wireless device.

```
ap: reload
System configuration has been modified. Save (y/n)?y
Building configuration.
[OK]
Proceed with reload? [confirm]
Connection with host lost.
```

Step 8 When the access point has finished reloading 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 1100 and 1200 series 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. On 350 series access points, you cannot use the MODE button to reload the image file, but you can use the CLI through a Telnet or console port connection.

Using the MODE button

You can use the MODE button on 1100 and 1200 series 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.

Note You cannot use the mode button to reload the image file on 350 series access points. To reload the image file on 350 series access points, follow the instructions in the "Using the CLI" section on page 22-20.

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, WEP keys, 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 *c1100-k9w7-tar.123-8.JA.tar* for an 1100 series access point or *c1200-k9w7-tar.123-8.JA.tar* for a 1200 series access point) 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 **c1100-k9w7-tar.123-8.JA.tar** for an 1100 series access point, rename the file to **c1100-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 (version 5.x or later) or Netscape Navigator (version 4.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 User Name field.

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

Step 5 Click the **System 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. You must use Microsoft Internet Explorer (version 5.x or later) or Netscape Navigator (version 4.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 User Name field.

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

Step 5 Click the **System 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.

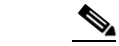
Step 1 Open the CLI using a Telnet session or a connection to the wireless device console port.

Step 2 Reboot the wireless device by removing power and reapplying power.

Step 3 Let the wireless device boot until 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/c350-k9w7-tar.122-13.JA1 flash:
```

Step 7 When the display becomes full, the CLI pauses and displays `--MORE--`. Press the spacebar to continue.

```
extracting info (229 bytes)
c350-k9w7-mx.122-13.JA1/ (directory) 0 (bytes)
c350-k9w7-mx.122-13.JA1/html/ (directory) 0 (bytes)
c350-k9w7-mx.122-13.JA1/html/level1/ (directory) 0 (bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/appsui.js (558 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/back.htm (205 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/cookies.js (5027 bytes).
extracting c350-k9w7-mx.122-13.JA1/html/level1/forms.js (15704 bytes)...
extracting c350-k9w7-mx.122-13.JA1/html/level1/sitewide.js (14621 bytes)...
extracting c350-k9w7-mx.122-13.JA1/html/level1/config.js (2554 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/stylesheet.css (3215 bytes)
c350-k9w7-mx.122-13.JA1/html/level1/images/ (directory) 0 (bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/ap_title_appname.gif (1422 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_1st.gif (1171 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_cbottom.gif (318 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_current.gif (348 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last.gif (386 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last_filler.gif (327
bytes)
```

```
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last_flat.gif (318
bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_nth.gif (1177 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_leftnav_dkgreen.gif (869 bytes)
 -- MORE --
```

Note If you do not press the spacebar to continue, the process eventually times out and the wireless device stops inflating the image.

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:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
```

Step 9 Enter the **set** command to check your bootloader entries.

```
ap: set
BOOT=flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
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 Tools and Resources Downloads page at the following URL:

http://www.cisco.com/cisco/software/navigator.html

Step 2 Expand the Wireless LAN Access folder.

Step 3 Expand the appropriate access point folder.

Step 4 Select the appropriate access point.

Step 5 Enter your CCO login and password. The Select Software page appears.

Step 6 Click **IOS**. A list of available Cisco IOS versions appears.

Step 7 Choose the version you wish to download. The download page for the version you chose appears.

Step 8 Click **WIRELESS LAN**.

Step 9 If prompted, enter your login and password. The Encryption Software Export Distribution Authorization page appears.

Step 10 Answer the questions on the page and click **Submit**. The Download page appears.

Step 11 Click **DOWNLOAD**. The Software Download Rules page appears.

Step 12 Read the Software Download Rules carefully and click **Agree**.

Step 13 If prompted, enter your login and password. A File Download window appears.

Step 14 Save the file to a director on your hard drive.

Obtaining TFTP Server Software

You can download TFTP server software from several websites. Cisco recommends the shareware TFTP utility available at this URL:

http://tftpd32.jounin.net

Follow the instructions on the website for installing and using the utility.

APPENDIX A

Protocol Filters

The tables in this appendix list some of the protocols that you can filter on the access point. The tables include:

- Table A-1, Ethertype Protocols
- Table A-2, IP Protocols
- Table A-3, IP Port Protocols

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 0-1 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 0-2 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 0-3 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 0-3 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 0-3 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. This appendix contains these sections:

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. The appendix contains the following sections:

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.

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, MSGDEF_LIMIT_MEDIUM."`

Explanation The indicated station disassociated from the access point on the indicated interface.

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.

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.

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 AP. Attempt to alleviate any unwanted noise. 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 "Working with Software Images" section on page 20-18.

If the IOS on the access point is corrupt, reload the access point image using the Mode button method.

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: [chars]`

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.

Recommended Action

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 `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.

Explanation 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.

Error Message Reconfigure or replace the source of inline power.

External Radius Server Error Messages

Error Message `RADIUS: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.

GLOSSARY

802.11 The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) wireless LANs operating in the 2.4-GHz band.

802.11a The IEEE standard that specifies carrier sense media access control and physical layer specifications for wireless LANs operating in the 5-GHz frequency band.

802.11b The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps wireless LANs operating in the 2.4-GHz frequency band.

802.11g The IEEE standard that specifies carrier sense media across control and physical layer specifications for 6, 9, 12, 18, 24, 36, 48, and 54 Mbps LANs operating in the 2.4-GHz frequency band.

802.3af The IEEE standard that specifies a mechanism for Power over Ethernet (PoE). The standard provides the capability to deliver both power and data over standard Ethernet cabling.

A

access point A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.

ad hoc network A wireless network composed of stations without Access Points.

antenna gain The gain of an antenna is a measure of the antenna's ability to direct or focus radio energy over a region of space. High gain antennas have a more focused radiation pattern in a specific direction.

associated A station is configured properly to allow it to wirelessly communicate with an Access Point.

B

backoff time The random length of time that a station waits before sending a packet on the LAN. Backoff time is a multiple of slot time, so a decrease in slot time ultimately decreases the backoff time, which increases throughput.

beacon A wireless LAN packet that signals the availability and presence of the wireless device. Beacon packets are sent by access points and base stations; however, client radio cards send beacons when operating in computer to computer (Ad Hoc) mode.

BOOTP Boot Protocol. A protocol used for the static assignment of IP addresses to devices on the network.

BPSK A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 1 Mbps.

broadcast packet A single data message (packet) sent to all addresses on the same subnet.

C

CCK Complementary code keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.

CCKM Cisco Centralized Key Management. Using 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.

cell The area of radio range or coverage in which the wireless devices can communicate with the base station. The size of the cell depends upon the speed of the transmission, the type of antenna used, and the physical environment, as well as other factors.

client A radio device that uses the services of an Access Point to communicate wirelessly with other devices on a local area network.

CSMA Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.

D

data rates The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).

dBi A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain, and the more acute the angle of coverage.

DHCP Dynamic host configuration protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.

dipole A type of low-gain (2.2-dBi) antenna consisting of two (often internal) elements.

domain name The text name that refers to a grouping of networks or network resources based on organization-type or geography; for example: name.com—commercial; name.edu—educational; name.gov—government; ISPname.net—network provider (such as an ISP); name.ar—Argentina; name.au—Australia; and so on.

DNS Domain Name System server. A server that translates text names into IP addresses. The server maintains a database of host alphanumeric names and their corresponding IP addresses.

DSSS Direct sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

E

EAP Extensible Authentication Protocol. An optional IEEE 802.1x security feature ideal for organizations with a large user base and access to an EAP-enabled Remote Authentication Dial-In User Service (RADIUS) server.

Ethernet The most widely used wired local area network. Ethernet uses carrier sense multiple access (CSMA) to allow computers to share a network and operates at 10, 100, or 1000 Mbps, depending on the physical layer used.

F

file server A repository for files so that a local area network can share files, mail, and programs.

firmware Software that is programmed on a memory chip.

G

gateway A device that connects two otherwise incompatible networks together.

GHz Gigahertz. One billion cycles per second. A unit of measure for frequency.

I

IEEE Institute of Electrical and Electronic Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.

infrastructure The wired Ethernet network.

IP address The Internet Protocol (IP) address of a station.

IP subnet mask The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway. This number is expressed in a form similar to an IP address; for example: 255.255.255.0.

isotropic An antenna that radiates its signal in a spherical pattern.

M

MAC Media Access Control address. A unique 48-bit number used in Ethernet data packets to identify an Ethernet device, such as an access point or your client adapter.

modulation Any of several techniques for combining user information with a transmitter's carrier signal.

multipath The echoes created as a radio signal bounces off of physical objects.

multicast packet A single data message (packet) sent to multiple addresses.

O

omni-directional This typically refers to a primarily circular antenna radiation pattern.

Orthogonal Frequency Division Multiplex (OFDM) A modulation technique used by IEEE 802.11a-compliant wireless LANs for transmission at 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

P

packet A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

Q

Quadruple Phase Shift Keying A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 2 Mbps.

R

range A linear measure of the distance that a transmitter can send a signal.

receiver sensitivity A measurement of the weakest signal a receiver can receive and still correctly translate it into data.

RF Radio frequency. A generic term for radio-based technology.

roaming A feature of some Access Points that allows users to move through a facility while maintaining an unbroken connection to the LAN.

RP-TNC A connector type unique to Cisco Aironet radios and antennas. Part 15.203 of the FCC rules covering spread spectrum devices limits the types of antennas that may be used with transmission equipment. In compliance with this rule, Cisco Aironet, like all other wireless LAN providers, equips its radios and antennas with a unique connector to prevent attachment of non-approved antennas to radios.

S

slot time The amount of time a device waits after a collision before retransmitting a packet. Short slot times decrease the backoff time, which increases throughput.

spread spectrum A radio transmission technology that spreads the user information over a much wider bandwidth than otherwise required in order to gain benefits such as improved interference tolerance and unlicensed operation.

SSID Service Set Identifier (also referred to as Radio Network Name). A unique identifier used to identify a radio network and which stations must use to be able to communicate with each other or to an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

T

transmit power The power level of radio transmission.

U

UNII Unlicensed National Information Infrastructure—regulations for UNII devices operating in the 5.15 to 5.35 GHz and 5.725 to 5.825 GHz frequency bands.

UNII-1 Regulations for UNII devices operating in the 5.15 to 5.25 GHz frequency band.

UNII-2 Regulations for UNII devices operating in the 5.25 to 5.35 GHz frequency band.

UNII-3 Regulations for UNII devices operating in the 5.725 to 5.825 GHz frequency band.

unicast packet A single data message (packet) sent to a specific IP address.

W

WDS Wireless Domain Services (WDS). An access point providing WDS on your wireless LAN 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 WDS access point forwards the client's credentials to the new access point with the multicast key. Only two packets pass between the client and the new access point, greatly shortening the reassociation time.

WEP Wired Equivalent Privacy. An optional security mechanism defined within the 802.11 standard designed to make the link integrity of wireless devices equal to that of a cable.

WLSE Wireless LAN Solutions Engine. The WLSE is a specialized appliance for managing Cisco Aironet wireless LAN infrastructures. It centrally identifies and configures access points in customer-defined groups and reports on throughput and client associations. WLSE's centralized management capabilities are further enhanced with an integrated template-based configuration tool for added configuration ease and improved productivity.

WNM Wireless Network Manager.

workstation A computing device with an installed client adapter.

WPA Wi-Fi Protected Access (WPA) is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP (Temporal Key Integrity Protocol) for data protection and 802.1X for authenticated key management.

INDEX

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W