Cisco 880 Series Integrated Services Router Software Configuration Guide

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

Text Part Number: OL-22206-02

Cisco 880 Series Integrated Services Router Software Configuration Guide

CONTENTS

Preface

This preface describes the objectives, audience, organization, and conventions used in this guide and describes related documents that have additional information. It contains the following sections:

Objective

This guide provides an overview and explains how to configure the various features for the Cisco 880 series Integrated Services Router (ISR). Some information may not apply to your particular router model.

For warranty, service, and support information, see the “Cisco One-Year Limited Hardware Warranty Terms” section in *Readme First for the Cisco 800 Series Integrated Services Routers* that was shipped with your router.

Audience

This guide is intended for Cisco equipment providers who are technically knowledgeable and familiar with Cisco routers and Cisco IOS software and features.

Organization

This guide is organized into the following parts, chapters, and appendixes.

Chapters	
Product Overview	Provides a brief description of the router models and the available software features.
Wireless Device Overview	Provides an introduction to the wireless device on the router and its use in network configurations.
Basic Router Configuration	Provides procedures for configuring the basic parameters of the router.
Basic Wireless Device Configuration	Provides procedures for initial configuration of the wireless device.
Configuring Radio Settings	Provides procedures for configuring the radio settings.

Conventions

Table 1 lists the conventions used in this document.

Table 1 Command Conventions

Convention	Description
boldface font	Commands and keywords.
italic font	Variables for which you supply values.
[ ]	Optional keywords or arguments appear in square brackets.
{**x** | **y** | **z**}	A choice of required keywords appears in braces separated by vertical bars. You must select one.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information you must enter.
< >	Nonprinting characters, for example, passwords, appear in angle brackets in contexts where italics are not available.
[ ]	Default responses to system prompts appear in square brackets.

Note Means *reader take note*. Notes contain helpful suggestions or references to additional information and material.

Caution This symbol means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

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

Related Documentation

In addition to *Cisco 880 Series ISR Software Configuration Guide* (this document), the Cisco 880 series ISR documentation set includes the following documents:

- *Readme First for the Cisco 800 Series Integrated Services Routers*
- *Regulatory Compliance and Safety Information for Cisco 800 Series and SOHO Series Routers*
- *Declarations of Conformity and Regulatory Information for Cisco Access Products with 802.11n Radios*
- *Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2*
- *Cisco IOS Release Notes* for Cisco IOS Release 15.1.4 (M)

You may also need to refer to the following documents:

- *Cisco System Manager Quick Start Guide*
- *Cisco IOS Release 12.4 Quality of Service Solutions Configuration Guide*
- *Cisco IOS Security Configuration Guide, Release 12.4*
- *Cisco IOS Security Configuration Guide, Release 12.4T*
- *Cisco IOS Security Command Reference, Release 12.4*
- *Cisco IOS Security Command Reference, Release 12.4T*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, versions 12.4(10b) JA and 12.3(8) JEC*
- *Cisco Aironet 1240AG Access Point Support Documentation*
- *Cisco 4400 Series Wireless LAN Controllers Support Documentation*
- *LWAPP Wireless LAN Controllers*
- *LWAPP Wireless LAN Access Points*
- *Cisco IOS Release 12.4 Voice Port Configuration Guide*
- *SCCP Controlled Analog (FXS) Ports with Supplementary Features in Cisco IOS Gateways*
- *Cisco Software Activation Conceptual Overview*
- *Cisco Software Activation Tasks and Commands*

Searching Cisco Documents

To search an HTML document using a web browser, use the **Ctrl+F** (Windows) or **Cmd+F** (Apple) sequences. In most browsers, the option to search whole words only, invoke case sensitivity, or search forward and backward are also available.

To search a PDF document in Adobe Reader, use the basic Find toolbar **(Ctrl+F)** or the Full Reader Search window **(Shift+Ctrl+F)**. Use the Find toolbar to find words or phrases within one specific document. Use the Full Reader Search window to search multiple PDF files simultaneously, as well as change case sensitivity and other options. Adobe Reader comes with an online help with more information regarding searching PDF documents.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

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

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

CHAPTER 1

Product Overview

This chapter provides an overview of the features available for the Cisco 880 series Integrated Service Router (ISR), and contains the following sections:

General Description

The Cisco 880 ISR provides Internet, VPN, data, and backup capability to corporate teleworkers and remote and small offices of fewer than 20 users. These routers are capable of bridging and multiprotocol routing between LAN and WAN ports and provide advanced features such as antivirus protection. In addition, the Cisco 880W series ISR incorporates an 802.11b/g/n wireless radio that allows the ISR to act as a wireless access point.

Cisco 880 Series ISR

The Cisco 880 series ISRs are a family of fixed-configuration data routers as described in the following sections:

In addition, this family of fixed-configuration data routers utilizes a dual-core infrastructure. The host router software runs on the first core while the WLAN AP software runs on the second core.

Models of the Cisco 880 Series ISRs

The Cisco 880 series ISRs have data capabilities. Each router has one WAN port. Data backup ports are also available on most of the routers. The 802.11a/n or 802.11b/g/n option is available on all models.

Table 1-1 gives the port configurations and supported WLAN radios of the Cisco 880 series data routers.

Table 1-1 Port Configurations and Supported WLAN Radios of the Cisco 880 Series Data ISRs

Model	WAN Port	Supported WLAN Radios
C886VA-W-E-K9	ADSL2+ UR2	2.4 GHz
C887VAM-W-E-K9	ADSL2+ Annex M	2.4 GHz
C887VA-W-A-K9	ADSL2+ Annex A	2.4 GHz
C887VA-W-E-K9	ADSL2+ Annex A	2.4 GHz
C887VAGW+7-A-K9	VDSL2/ADSL2	2.4 GHz and 5 GHz
C887VAGW+7-E-K9	VDSL2/ADSL2	2.4 GHz and 5 GHz
C887VA-WD-A-K9	VDSL2/ADSL2	2.4 GHz and 5 GHz
C887VA-WD-E-K9	VDSL2/ADSL2	2.4 GHz and 5 GHz
C881W-A-K9	FE	2.4 GHz
C881W-E-K9	FE	2.4 GHz
C881W-P-K9	FE	2.4 GHz
C881GW+7-A-K9	FE	2.4 GHz and 5 GHz
C881GW+7-E-K9	FE	2.4 GHz and 5 GHz
C881WD-A-K9	FE	2.4 GHz and 5 GHz
C881WD-E-K9	FE	2.4 GHz and 5 GHz
C881GW-S-A-K9	FE	2.4 GHz and 5 GHz
C881GW-V-A-K9	FE	2.4 GHz and 5 GHz

For 3G-related product descriptions, see *Configuring Cisco EHWIC and 880G for 3G (EV-DO Rev A)* and *Configuring Cisco EHWIC and 880G for 3.7G (HSPA+)/3.5G (HSPA)*.

Common Features

Cisco 880 series ISRs support the following features:

4-port 10/100 FE LAN Switch

This switch provides four ports for connecting to 10/100BASE-T FE LANs, access points, or IP phones. A factory-installed upgrade is available that gives Power over Ethernet (PoE) on two of the ports to provide power to access points or phones.

802.11b/g/n Wireless LAN

The Cisco 880W series ISRs have an integrated 802.11b/g/n radio module for wireless LAN connectivity. With this module, the router can act as an access point in the local infrastructure.

For more information on supported WLAN radio modules, see Table 1-1.

Battery-backed-up Real-Time Clock

A battery-backed-up real-time clock (RTC) provides the date and time when the system is powered on. The RTC is used to verify the validity of the Certification Authority stored on the router.

Cisco CleanAir Technology

The Cisco CleanAir technology is a system-wide feature of the Cisco Unified Wireless Network that improves air quality by detecting RF interference that other systems cannot recognize, identifying the source, locating it on a map, and then making automatic adjustments to optimize wireless coverage.

Cisco access points with the CleanAir technology provide the highest-performance 802.11n connectivity for mission-critical mobility. By intelligently avoiding interference, the access points offer performance protection for 802.11n networks to help ensure reliable application delivery.

Note The Cisco CleanAir technology is supported on dual-radio access points only.

For more information, see *Cisco CleanAir Technology.*

Dynamic Frequency Selection

Access points with 5-GHz radios configured at the factory for use in the United States and Europe 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 point detects a radar on a certain channel, it avoids using that channel for 30 minutes.

The DFS functionality is disabled on Cisco 880 series ISRs with pending Federal Communications Commission (FCC) certification.

Note The DFS functionality is supported on dual-radio access points only.

For more information, see *Dynamic Frequency Selection and IEEE 802.11h Transmit Power Control*.

Dual-Radio Wireless LAN

With the dual-radio/dual-band IEEE 802.11n access point, the Cisco 880 Series ISRs offer a secure, integrated access point in a single device. The ISRs support both autonomous and unified modes and are backward-compatible with 802.11a/b/g.

The routers support IEEE 802.11n draft 2.0 and use multiple-input, multiple-output (MIMO) technology that provides increased throughput, reliability, and predictability.

For information on configuring the Cisco 880 series ISRs, see the "Basic Router Configuration" section on page 3-1.

Security Features

The Cisco 880 platforms provide the following security features:

- Intrusion Prevention System (IPS)
- Dynamic Multipoint VPN (DMVPN)
- IP security (IPsec)
- Quality of service (QoS)
- Firewall
- URL filtering

Licensing

The Cisco 880 ISR is shipped with licensed software installed. Software features may be upgraded and the software licenses may be managed through the *Cisco License Manager.* See *Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2* for details.

When you order a new router, you can specify the software image and feature set. The image and feature set are installed on your router before you receive it, so you do not need to purchase a software license. The router stores the software license file on the flash memory.

Selecting Feature Sets

Some feature sets are bundled and offered with a software license that is installed on the hardware platforms. For a list of features available with a software license on the Cisco 880, see *Cisco 880 Series Integrated Services Routers Data Sheet.* See *Software Activation Configuration Guide* on Cisco.com for details about how to activate and manage the software licenses.

880 SKUs for next generation Cisco 880 Series ISR platforms

The following lists the SKUs particular for Next generation Cisco 880 Series ISR platforms.

C881W and C881WD

- 512 MB memory
- 256 MB Flash
- 4-port 10/100 Switch
- 2-port PoE is a factory-configurable option
- 10/100 FE WAN
- 1-port console/aux
- 1-port external USB 2.0
- Real-time clock
- Embedded WLAN antenna on wireless models

C886VA-W

- 512 MB memory
- 256 MB Flash
- 4-port 10/100 Switch
- 2-port PoE is a factory-configurable option
- 1-port console/aux
- 1-port external USB 2.0
- ADSL2+ Annex B
- ISDN backup WAN
- Real-time clock
- Embedded WLAN antenna on wireless models

C887VAM-W

- 512 MB memory
- 256 MB Flash
- 4-port 10/100 Switch
- 2-port PoE is a factory-configurable option
- 1-port console/aux
- 1-port external USB 2.0

- ADSL2+ Annex M
- Real-time clock
- Embedded WLAN antenna on wireless model

C887VA-W and C887VA-WD

- 512 MB memory
- 256 MB Flash
- 4-port 10/100 Switch
- 2 port PoE is a factory-configurable option
- 1-port console/aux
- 1-port external USB 2.0
- ADSL2+ Annex A
- Real-time clock
- Embedded WLAN antenna on wireless model

C887VAGW

- 512 MB memory
- 256 MB Flash
- 4-port 10/100 Switch
- 2-port PoE is a factory-configurable option
- 1-port console/aux
- 1-port external USB 2.0
- ADSL2+ Annex A
- Real-time clock
- Embedded WLAN antenna on wireless model
- 3G modem with dual SIM card slots

C881GW

- 512 MB memory
- 256 MB Flash
- 4-port 10/100 Switch
- 2-port PoE is a factory-configurable option
- 10/100 FE WAN
- 3G modem with Dual SIMM card slots
- 1-port console/aux

- 1-port external USB 2.0
- Real-time clock
- Embedded WLAN antenna on wireless models

C887GW

- 512 MB memory
- 256 MB Flash
- 4-port 10/100 Switch
- 2-port PoE is a factory-configurable option
- 1-port console/aux
- 1-port external USB 2.0
- ADSL2+ Annex A
- 3G modem with Dual SIMM card slots
- Real-time clock
- Embedded WLAN antenna on wireless models

For more 3G-related product descriptions, see *Configuring Cisco EHWIC and 880G for 3G (EV-DO Rev A)* and *Configuring Cisco EHWIC and 880G for 3.7G (HSPA+)/3.5G (HSPA)*.

Memory

Table 1-2 illustrates the onboard memory and flash size for the first and second core. The total memory installed is 512 MB + 256 MB flash, and they are partitioned as shown in the following table.

Table 1-2 Memory Specifications

Onboard Memory	**1st core**	**2nd core**
512 MB	384 MB	128 MB
Flash size		
256	192	64

LED Overview

Table 1-3 shows all LEDs that are visible on the front of the chassis (bezel side). No LEDs are mounted on the I/O side.

Table 1-3 LED Definition Summary by Interface

LED	Color	Description	Indication
PWR Ok	Green	Power On OK, Router Operational	Off=no power Steady on=normal operation Blink=boot up phase in ROM Monitor mode
Ethernet Switch and FE/GE LAN/WAN ports	Green	Ethernet Switch	Off= No link Steady on= link Blink= TXD/RXD data
PoE	Green/Amber	PoE Status	Off= no device powered, PoE administratively disabled Steady on green= PD connected and powered Steady on amber= PD denied power, power delivery fault
xDSL	Green	CD	Steady on= connected Blink= training
	Green	Data	Blink= TXD/RXD data
ISDN data	Green	Link	Off= no connection Steady on= BRI S/T connection established
	Green	B1 channel data	Off= No data Blin= TXD/RXD data
	Green	B2 channel data	Off= No data Blink= TXD/RXD data

Table 1-3 LED Definition Summary by Interface (continued)

LED	Color	Description	Indication
Wireless/LAN	Green	2.4 GHz Radio	Off= Radio is down (no SSID configured) Steady on= Radio is up, SSID configured, beacons being send, client is associated, no data traffic being sent/received Slow blink= Radio is up (SSID configured and sending beacon) Fast Blink= Radio is up, client is associated, radio is sending/receiving data traffic
	Green	If 5 GHz radio is supported	
	Green	Autonomous Mode	Off= Ethernet link down On= Ethernet link up, no traffic Blink= Ethernet link up with data traffic
		Unified Mode	Off= Ethernet link down On= Ethernet link up, connected to controller Blink= AP not communicating with controller
VPN_OK			Off= no tunnel Steady on= at least one tunnel is up
PPP_OK			Off=no PPP session Steady on= at least one PPP established

Power Supply

The following power supplies are used across Next-generation Cisco 880 ISR platforms depending on SKU:

External 12 VDC Power Supply Adapter

A new and grounded 12 VDC 30 W external desktop adapter is available for all 86x and 88x models. Connection to the chassis is through a single barrel connector..

Onboard 12 VDC Power supply

PoE ports are powered from 12 VDC on the motherboard.

Power over Ethernet Inline Power Option

Inline power is a configurable option. PoE-configured boxes are supplied with a 12 VDC 60 W adapter in lieu of the 30 W.

Images Supported

c800-universalk9-mz

This image offers all IOS features supported by c8xx platforms.

c800-universalk9_npe-mz

This image does not support VPN payload and secure voice functionality and satisfies import considerations for CIS countries.

Licenses for Each Image:

For universalk9 image:

Technology Package licenses:

- Advipservices
- advsecurityk9

Feature licenses:

- ios-ips-update
- SSL_VPN

For universalk9_npe image:

Technology Package licenses:

- advipservices_npe
- advsecurity_npe

Feature licenses:

- ios-ips-ipdate

Images Supported for AP802

Table 1-4 Images Supported for AP802

Mode	Image
Autonomous	ap802-k9w7-tar
Unified	ap802-k9w8-tar
Recovery	a802-rcvk9w8-tar

Minimum Software Version Needed to Support AP802

Table 1-5 lists the minimum software version needed to support AP802.

Table 1-5 Minimum Software Version Needed for AP802

Software	AP802 Single Radio	AP802 Dual Radio
Router IOS	15.1(4) M1	15.2(4)M1
AP IOS (Autonomous mode)	12.4(25d)JAX	12.4(25d)JAX1
AP IOS (Unified mode)	12.4(23c)JA2	15.2(2)JA
AP IOS (Recovery mode)	12.4(23c)JA2	15.2(2)JA
WLC	7.0.116.0	7.3.101.0
WCS	7.0.172.0	—
NCS	—	1.2.0.103

CHAPTER 2

Wireless Device Overview

Wireless devices (commonly configured as *access points*) 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. When configured as an access point, the wireless 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 can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

With a management system based on Cisco IOS software, wireless devices are Wi-Fi CERTIFIED™, 802.11b-compliant, 802.11g-compliant, and 802.11n-compliant wireless LAN transceivers.

Software Modes

The access point is shipped with an autonomous image and a recovery image on the access point's flash. The default mode is autonomous; however, the access point can be upgraded to operate in Cisco Unified Wireless mode.

Each mode is described below:

- **Autonomous mode—**Supports standalone network configurations, where all configuration settings are maintained locally on the wireless device. Each autonomous device can load its starting configuration independently and still operate in a cohesive fashion on the network.
- **Cisco Unified Wireless mode—**Operates in conjunction with a Cisco Unified Wireless LAN controller, where all configuration information is maintained within the controller. In the Cisco Unified Wireless LAN architecture, wireless devices operate in the lightweight mode using Lightweight Access Point Protocol (LWAPP), as opposed to autonomous mode. The lightweight access point, or wireless device, has no configuration until it associates to a controller. The configuration on the wireless device can be modified by the controller only when the networking is up and running. The controller manages the wireless device configuration, firmware, and control transactions such as 802.1x authentication. All wireless traffic is tunneled through the controller.

  For more information about this network architecture design, see *Why Migrate to a Cisco Unified Wireless Network?* on Cisco.com.

Management Options

The wireless device runs its own version of Cisco IOS software that is separate from the Cisco IOS software operating on the router. You can configure and monitor the access point with several different tools:

- Cisco IOS software CLI
- Simple Network Management Protocol (SNMP)
- Web-browser interface: http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap2-gui.html

Note 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.

Note Avoid using the CLI and the web-browser tools concurrently to configure the wireless device. If you configure the wireless device using the CLI, the web-browser interface may display an inaccurate interpretation of the configuration. This inappropriate display of information does not necessarily mean the wireless device is misconfigured.

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

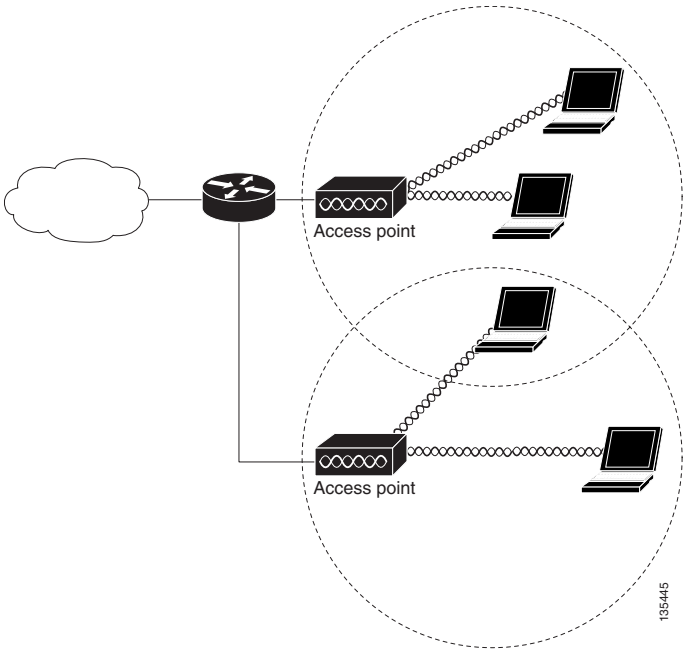
Network Configuration Examples

Set up the access point role in any of these common wireless network configurations. The access point default configuration can either be as a root unit connected to a wired LAN or as a central unit in an all-wireless network. Access points can also be configured as bridges and workgroup bridges. These roles require specific configurations, as defined in the following examples.

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 2-1 shows access points acting as root units on a wired LAN.

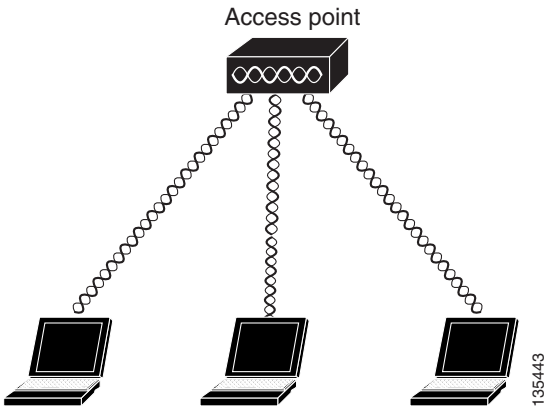
Figure 2-1 Access Point as Root Unit on a Wired LAN



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 2-2 shows an access point in an all-wireless network.

Figure 2-2 Access Point as Central Unit in All-Wireless Network



CHAPTER 3

Basic Router Configuration

This chapter provides procedures for configuring the basic parameters of your Cisco router, including global parameter settings, routing protocols, interfaces, and command-line access. It also describes the default configuration on startup.

Note Individual router models may not support every feature described in this guide. Features that are not supported by a particular router are indicated whenever possible.

This chapter includes configuration examples and verification steps, as available.

Interface Ports

Table 3-1 lists the interfaces that are supported for each router and their associated port labels on the equipment.

Table 3-1 Supported Interfaces and Associated Port Labels by Cisco Router

Router	Interface	Port Label
Cisco 880	Fast Ethernet LAN	LAN, FE0–FE3
	Wireless LAN	(no label)
Cisco 881, 881W, 881G, 881GW	Fast Ethernet WAN	WAN, FE4
Cisco 886, 886W, 886G, 886GW	ADSLoverISDN	ADSLoPOTS
Cisco 887, 887W	ADSL2oPOTS WAN	ADSLoPOTS
Cisco 887V, 887VW, 887VG, 887VGW	VDSL2oPOTS WAN	VDSLoPOTS
Cisco 888, 888W	G.SHDSL WAN	G.SHDSL

Default Configuration

When you first boot up your Cisco router, some basic configuration has already been performed. All of the LAN and WAN interfaces have been created, console and vty ports are configured, and the inside interface for Network Address Translation (NAT) has been assigned. Use the **show running-config** command to view the initial configuration, as shown in the following example for a Cisco 881W:

```
Router# show running-config


User Access Verification

Password:
Router> en
Password:
Router# show running-config
Building configuration...

Current configuration : 986 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$g4y5$NxDeM.0hON6YA51bcfGvN1
enable password ciscocisco
!
```

```
no aaa new-model
!
!
!
!
no ip routing
no ip cef
!
!
!
!
!
multilink bundle-name authe
!
!
archive
 log config
  hidekeys
!
!
!
!
!
interface FastEthernet0
!
interface FastEthernet1
 shutdown
!
interface FastEthernet2
 shutdown
!
interface FastEthernet3
 shutdown
!
interface FastEthernet4
 ip address 10.1.1.1 255.255.255.0
 no ip route-cache
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface wlan-ap0
 description Service Module interface to manage the embedded AP
 ip unnumbered Vlan1
 no cdp enable
 arp timeout 0
!
ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
```

```
line con 0
 no modem enable
line aux 0
line vty 0 4
 password cisco
 login
 transport input telnet ssh
!
scheduler max-task-time 5000

!
webvpn cef
end

Router#
```

Information Needed for Configuration

You need to gather some or all of the following information, depending on your planned network scenario, before configuring your network:

- If you are setting up an Internet connection, gather the following information:
  - PPP client name that is assigned as your login name
  - PPP authentication type: Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP)
  - PPP password to access your ISP account
  - DNS server IP address and default gateways
- If you are setting up a connection to a corporate network, you and the network administrator must generate and share the following information for the WAN interfaces of the routers:
  - PPP authentication type: CHAP or PAP
  - PPP client name to access the router
  - PPP password to access the router
- If you are setting up IP routing:
  - Generate the addressing scheme for your IP network.
  - Determine the IP routing parameter information, including IP address and ATM permanent virtual circuits (PVCs). These PVC parameters are typically virtual path identifier (VPI), virtual circuit identifier (VCI), and traffic-shaping parameters.
  - Determine the number of PVCs that your service provider has given you, along with their VPIs and VCIs.
  - For each PVC, determine the type of AAL5 encapsulation supported. It can be one of the following:

    AAL5SNAP—This can be either routed RFC 1483 or bridged RFC 1483. For routed RFC 1483, the service provider must provide you with a static IP address. For bridged RFC 1483, you may use DHCP to obtain your IP address, or you may obtain a static IP address from your service provider.

    AAL5MUX PPP—With this type of encapsulation, you need to determine the PPP-related configuration items.

- If you plan to connect over an ADSL or G.SHDSL line:
  - Order the appropriate line from your public telephone service provider.

    For ADSL lines—Ensure that the ADSL signaling type is DMT (also known as ANSI T1.413) or DMT Issue 2.

    For G.SHDSL lines—Verify that the G.SHDSL line conforms to the ITU G.991.2 standard and supports Annex A (North America) or Annex B (Europe).

After you have collected the appropriate information, you can perform a full configuration on your router, beginning with the tasks in the "Configuring Command-Line Access" section on page 3-5.

To obtain or change software licenses, see *Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2*.

Configuring Command-Line Access

To configure parameters to control access to the router, follow these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **line** [**aux** | **console** | **tty** | **vty**] *line-number*
2. **password** *password*
3. **login**
4. **exec-timeout** *minutes* [*seconds*]
5. **line** [**aux** | **console** | **tty** | **vty**] *line-number*
6. **password** *password*
7. **login**
8. **end**

DETAILED STEPS

	Command	Purpose

Step 1	**line** [**aux** | **console** | **tty** | **vty**] *line-number*
	
	Example:
	`Router(config)# line console 0`
	`Router(config-line)#`
		Enters line configuration mode, and specifies the type of line.
		
		This example specifies a console terminal for access.

Step 2	**password** *password*
	
	Example:
	`Router(config)# password 5dr4Hepw3`
	`Router(config-line)#`
		Specifies a unique password for the console terminal line.

Step 3	**login**
	
	Example:
	`Router(config-line)# login`
	`Router(config-line)#`
		Enables password checking at terminal session login.

	Command	Purpose

Step 4	**exec-timeout** *minutes* [*seconds*]
	
	Example:
	`Router(config-line)# exec-timeout 5 30`
	`Router(config-line)#`
		Sets the interval that the EXEC command interpreter waits until user input is detected. The default is 10 minutes. Optionally, add seconds to the interval value.
		
		This example shows a timeout of 5 minutes and 30 seconds. Entering a timeout of 0 0 specifies never to time out.

Step 5	**line** [**aux** | **console** | **tty** | **vty**] *line-number*
	
	Example:
	`Router(config-line)# line vty 0 4`
	`Router(config-line)#`
		Specifies a virtual terminal for remote console access.

Step 6	**password** *password*
	
	Example:
	`Router(config-line)# password aldf2ad1`
	`Router(config-line)#`
		Specifies a unique password for the virtual terminal line.

Step 7	**login**
	
	Example:
	`Router(config-line)# login`
	`Router(config-line)#`
		Enables password checking at the virtual terminal session login.

Step 8	**end**
	
	Example:
	`Router(config-line)# end`
	`Router#`
		Exits line configuration mode, and returns to privileged EXEC mode.

Example

The following configuration shows the command-line access commands.

You do not need to input the commands marked “default.” These commands appear automatically in the configuration file generated when you use the **show running-config** command.

```
!
line con 0
exec-timeout 10 0
password 4youreyesonly
login
transport input none (default)
stopbits 1 (default)
line vty 0 4
password secret
login
!
```

Configuring Global Parameters

To configure selected global parameters for your router, follow these steps:

SUMMARY STEPS

1. **configure terminal**
2. **hostname** *name*
3. **enable secret** *password*
4. **no ip domain-lookup**

DETAILED STEPS

	Command	Purpose

Step 1	**configure terminal**
	
	Example:
	`Router> enable`
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode, when using the console port.
		
		If you are connecting to the router using a remote terminal, use the following:
		`telnet router name or address`
		`Login: login id`
		`Password: *********`
		`Router> enable`

Step 2	**hostname** *name*
	
	Example:
	`Router(config)# hostname Router`
	`Router(config)#`
		Specifies the name for the router.

Step 3	**enable secret** *password*
	
	Example:
	`Router(config)# enable secret cr1ny5ho`
	`Router(config)#`
		Specifies an encrypted password to prevent unauthorized access to the router.

Step 4	**no ip domain-lookup**
	
	Example:
	`Router(config)# no ip domain-lookup`
	`Router(config)#`
		Disables the router from translating unfamiliar words (typos) into IP addresses.

Configuring WAN Interfaces

Configure the WAN interface for your router using one of the following as appropriate:

- Configuring a Fast Ethernet WAN Interface, page 3-8
- Configuring a VDSL2 WAN Interface, page 3-8
- Configuring ADSL or VDSL on Cisco Multi Mode 886VA and 887VA ISRs, page 3-9
- Configuring ADSL Mode, page 3-10

Configuring a Fast Ethernet WAN Interface

To configure the Fast Ethernet interface on a Cisco 861 or 881 ISR, follow these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **interface** *type number*
2. **ip address** *ip-address mask*
3. **no shutdown**
4. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**interface** *type number*
	
	Example:
	`Router(config)# interface fastethernet 4`
	`Router(config-if)#`
		Enters the configuration mode for a Fast Ethernet WAN interface on the router.

Step 2	**ip address** *ip-address mask*
	
	Example:
	`Router(config-if)# ip address 192.168.12.2 255.255.255.0`
	`Router(config-if)#`
		Sets the IP address and subnet mask for the specified Fast Ethernet interface.

Step 3	**no shutdown**
	
	Example:
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
		Enables the Ethernet interface, changing its state from administratively down to administratively up.

Step 4	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits configuration mode for the Fast Ethernet interface and returns to global configuration mode.

Configuring a VDSL2 WAN Interface

The VDSL2 WAN interface is used on the Cisco 887V ISR platforms.

Note The VDSL2 WAN interface uses Ethernet as the Layer 2 transport mechanism.

To configure VDSL2 on the Cisco 887V ISR, follow these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **controller** *vdsl 0*
2. **interface** *type number*

3. **ip address** *ip-address mask*
4. **shutdown**
5. **no shutdown**
6. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**controller** *vdsl 0*
	
	Example:
	`Router# config t`
	`Router(config)# controller vdsl 0`
		Enters controller configuration mode and the controller number.
		
		Note There is no need to configure any VDSL2 parameters from the CPE side. Any specific VDSL2 settings should be set on the DSLAM side.

Step 2	**interface** *type number*
	
	Example:
	`Router(config)# interface ethernet 0`
	`Router(config-if)#`
		Enters the configuration mode for Ethernet Layer 2 transport on the VDSL WAN interface on the router.

Step 3	**ip address** *ip-address mask*
	
	Example:
	`Router(config-if)# ip address 192.168.12.2 255.255.255.0`
	`Router(config-if)#`
		Sets the IP address and subnet mask for the interface.

Step 4	**shutdown**
	
	Example:
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
		Disables the interface, changing its state from administratively up to administratively down.

Step 5	**no shutdown**
	
	Example:
	`Router(config-if)# no shutdown`
	`Router(config-if)#`
		Enables the interface, changing its state from administratively down to administratively up.

Step 6	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits configuration mode and returns to global configuration mode.

Configuring ADSL or VDSL on Cisco Multi Mode 886VA and 887VA ISRs

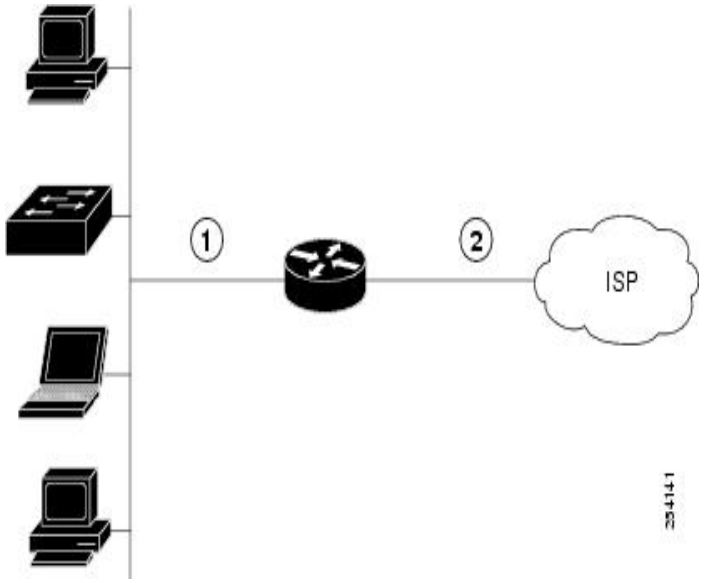
The Cisco customer premise equipment (CPE) 886VA and 887VA Integrated Services Routers (ISRs) support asymmetric digital subscriber line (ADSL) 1/2/2+ and very high-speed digital subscriber line 2 (VDSL2) transmission modes, also called multi mode. The 886VA supports xDSL over ISDN and the 887VA supports xDSL over a plain old telephone system (POTS).

The default CPE operating mode is auto. Auto mode means that the CPE trains up to the mode configured on the digital subscriber line access multiplexer (DSLAM), ADSL1/2/2+ or VDSL2.

The following examples assume the DSLAM is configured in either ADSL2+ mode or VDSL2, and the CPE is configured in auto mode.

Figure 3-1 shows an ATM WAN or Ethernet WAN network topography.

Figure 3-1 Example Topology



1	Fast Ethernet LAN interface	2	ATM WAN interface—ADSL1/2/2+ mode or Ethernet WAN Interface—VDSL2 mode

Note A DSLAM in Layer 1 mode may be configured for auto mode. A DSLAM in Layer 2 mode must be configured for ATM mode or packet transfer mode (PTM).

Note Cisco 886VA and 887VA allow a maximum of four permanent virtual circuits (PVCs).

Configuring ADSL Mode

To configure ADSL mode, follow these tasks:

- Configuring ADSL Auto Mode, page 3-11
- Configuring CPE and Peer for ADSL Mode, page 3-11
- ADSL Configuration Example, page 3-13
- Verifying ADSL Configuration, page 3-14
- Verifying CPE to Peer Connection for ADSL, page 3-16

Configuring ADSL Auto Mode

To configure the DSL controller to auto mode, follow these steps, beginning in global configuration mode:

Note Configure the DSLAM in ADSL 1/2//2+ mode prior to configuring the router.

SUMMARY STEPS

1. **controller vdsl** *slot*
2. **operating mode {auto | adsl1 | adsl2 | adsl2+ | vdsl2 | ansl}**
3. **end**

DETAILED STEPS

	Command	Purpose

Step 1	**controller vdsl** *slot*
	Example:
	`Router (config) #`
	`Controller vdsl 0`
		Enters config mode for the VDSL controller.

Step 2	**operating mode {auto|adsl1|adsl2|adsl2+|vdsl2|ansl}**
	Example:
	`Router (config-controller) #`
	`operating mode`
	`auto`
		Configures the operating mode. The default is auto and is recommended.

Step 3	**end**
	Example:
	`Router (config-conroller) #`
	`end`
	`Router`
		Exits the configuration mode and enters EXEC mode.

When configured in auto, the operating mode does not appear in the **show running** command.

Configuring CPE and Peer for ADSL Mode

When configuring for ADSL, the ATM main interface or ATM sub-interface must be configured with a PVC and an IP address. Perform a **no shutdown** command on the interface, if needed.

Configuring the ATM CPE Side

To configure the ATM CPE side, follow these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **interface** *type number*
2. **no shutdown**
3. **interface atm0.1 point-to-point**

4. **ip address** *ip-address mask*
5. **pvc [name] vpi/vci**
6. **protocol** *protocol* {*protocol-address* [**virtual-template**] | **inarp**} [[**no**] **broadcast** | **disable-check-subnet** | [**no**] **enable-check-subnet**]
7. **end**

DETAILED STEPS

	Command	Purpose
Step 1	**interface** *type number* **Example:** `Router (config) # interface atm0`	Enters configuration mode for the ATM WAN interface (ATM0).

Step 2	**no shutdown**
	Example:
	`Router (config-if) # no shutdown`
	`Router (config-if) #`
		Enables the configuration changes to the ATM interface.

Step 3	**interface atm0.1 point-to-point**
	Example:
	`Router (config-if) # interface ATM0.1`
	`point-to-point`
	`Router (config-subif) #`
		Enables the ATM0.1 point-to-point interface.

Step 4	**ip address** *ip-address mask* **Example:** `Router (config-subif)# ip address 30.0.0.1 255.255.255.0`	Enters IP address and subnet mask.

Step 5	**pvc [name] vpi/vci**
	Example:
	`Router (config-subif) # pvc 13/32`
	`Router (config-if-atm-vc) #`
		Creates or assigns a name to an ATM PVC and enters the ATM virtual circuit configuration mode.

Step 6	**protocol** *protocol* {*protocol-address* [**virtual-template**] | **inarp**} [[**no**] **broadcast** | **disable-check-subnet** | [**no**] **enable-check-subnet**]
	Example:
	`Router (config-if-atm-vc) #`
	`protocol ip 30.0.0.2 broadcast`
		Configures a static map for an ATM PVC.

Step 7	**end**
	Example:
	`Router (config-if-atm-vc) # end`
	`Router #`
		Exits the configuration mode and enters EXEC mode.

ADSL Configuration Example

The following example shows a typical ADSL2+ configuration set to auto mode. Outputs in **bold** are critical.

```
Router# show running
Building configuration...

Current configuration  :    1250 bytes
!
! Last configuration change at 02:07:09 UTC Tue Mar 16 2010
!
version 15.1
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 10
ip source-route
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO887-V2-K9 sn FHK1313227E
license boot module c880-data level adviperservices
!
!
vtp domain cisco
vtp mode transparet
!
!
controller VDSL 0
!
vlan 2-4
!
!
!
!
!
interface Ethernet 0
 no ip address
 shutdown
 no fair-queue
!
interface BRI0
 no ip address
 encapsulation hdlc
 shutdown
```

```
 isdn termintation multidrop
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
!
interface ATM0.1 point-to-point
 ip address 30.0.0.1 255.255.255.0
 pvc 15/32
  protocol ip 30.0.0.2 broadcast
!
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
!
!
!
!
control-palne
!
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 login
 transport input all
!
exception data-corruption buffer truncate
end
```

Verifying ADSL Configuration

Verify that the configuration is set properly by using the **show controller vdsl 0** command in the privileged EXEC mode. Outputs in **bold** are critical.

```
Router# show controller vdsl 0
Controller VDSL 0 is UP


Daemon Status:               Up
                           XTU-R (DS)            XTU-C (US)
chip Vendor ID:             'BDM'                 'BDCM'
Chip Vendor Specific:       0x0000                0x6110
Chip Vendor Country:        0xB500                0xB500
```

```
Modem Vendor ID:              'csco'                 'BDCM'
Modem Vendor Specific:        0x4602                 0x6110
Modem Vendor Country:         0xB500                 0xB500
Serial Number Near:           FHK1313227E 887-V2-K 15.1(20100
Serial Number Far:
Modem Version Nead:           15.1(20100426:193435) [changahn
Modem Version Far:            0x6110


Modem Status:                 TC Sync (Showtime!)
DSL Config Mode:              AUTO
Trained Mode:                 G.992.5 (ADSL2+) Annex A
TC Mode:                      ATM
Selftest Result:              0x00
DELT configuration:           disabled
DELT state:                   not running
Trellis:                      ON                     ON
Line Attenuation:             1.0 dB                 1.4 dB
Signal Attenuation:           1.0 dB                 0.0 dB
Noise Margin:                 6.8 dB                 13.6 dB
Atteinable Rate:              25036 kbits/s          1253 kbits/s
Actual Power:                 13.7 dBm               12.3 dBM
Total FECS:                   0                      0
Total ES:                     0                      0
Total SES:                    0                      0
Total LOSS:                   0                      0
Total UAS:                    0                      0
Total LPRS:                   0                      0
Total LOFS:                   0                      0
Total LOLS:                   0                      0
Bit swap:                     163                    7

Full inits:                   32
Failed Full inits:            0
Short inits:                  0
Failed short inits:           0


Firmware          Source          Filename (version)
--------          ------          ------------------
VDSL              embedded        VDSL_LINUX_DEV_01212008 (1)


Modem FW Version:         100426_1053-4.02L.03.A2pv6C030f.d22j
Modem PHY Version:        A2pv6C030f.d22j


                DS Channel1   DS Channel0  US Channel1  US channel0
Speed (kbps):             0          24184            0         1047
Previous Speed:           0          24176            0         1047
Total Cells:              0      317070460            0     13723742
User Cells:               0              0            0            0
Reed-solomon EC:          0              0            0            0
CRC Errors:               0              0            0            0
Header Errors:            0              0            0            0
Interleave (ms):      0.00           0.08         0.00        13.56
Actual INP:           0.00           0.00         0.00         1.80


Training Log:   Stopped
Training Log Filename:  flash:vdsllog.bin
```

Verifying CPE to Peer Connection for ADSL

Ping the peer to confirm that CPE to peer configuration is setup correctly.

```
Router# ping 30.0.0.2 rep 20

Type escape sequence to abort.
Sending 20, 100-byte ICMP Echos to 30.0.0.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (20/20), round-trip min/avg/max = 20/22/28 ms
Router#
```

Configuring the Fast Ethernet LAN Interfaces

The Fast Ethernet LAN interfaces on your router are automatically configured as part of the default VLAN and are not configured with individual addresses. Access is provided through the VLAN. You may assign the interfaces to other VLANs.

Configuring the Wireless LAN Interface

The Cisco 880 series wireless routers have an integrated 802.11n module for wireless LAN connectivity. The router can then act as an access point in the local infrastructure. For more information about configuring a wireless connection, see the "Basic Wireless Device Configuration" section on page 4-1.

Configuring a Loopback Interface

The loopback interface acts as a placeholder for the static IP address and provides default routing information.

To configure a loopback interface, follow these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **interface** *type number*
2. **ip address** *ip-address mask*
3. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**interface** *type number*
	
	Example:
	`Router(config)# interface Loopback 0`
	`Router(config-if)#`
		Enters configuration mode for the loopback interface.

Step 2	**ip address** *ip-address mask*
	
	Example:
	`Router(config-if)# ip address 10.108.1.1 255.255.255.0`
	`Router(config-if)#`
		Sets the IP address and subnet mask for the loopback interface.

Step 3	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits configuration mode for the loopback interface and returns to global configuration mode.

Example

The loopback interface in this sample configuration is used to support Network Address Translation (NAT) on the virtual-template interface. This configuration example shows the loopback interface configured on the Fast Ethernet interface with an IP address of 200.200.100.1/24, which acts as a static IP address. The loopback interface points back to virtual-template1, which has a negotiated IP address.

```
!
interface loopback 0
ip address 200.200.100.1 255.255.255.0 (static IP address)
ip nat outside
!
interface Virtual-Template1
ip unnumbered loopback0
no ip directed-broadcast
ip nat outside
!
```

Verifying Configuration

To verify that you have properly configured the loopback interface, enter the **show interface loopback** command. You should see a verification output similar to the following example:

```
Router# show interface loopback 0
Loopback0 is up, line protocol is up
  Hardware is Loopback
  Internet address is 200.200.100.1/24
  MTU 1514 bytes, BW 8000000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
```

```
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Another way to verify the loopback interface is to ping it.

```
Router# ping 200.200.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.200.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Configuring Static Routes

Static routes provide fixed routing paths through the network. They are manually configured on the router. If the network topology changes, the static route must be updated with a new route. Static routes are private routes unless they are redistributed by a routing protocol.

To configure static routes, follow these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
2. **end**

DETAILED STEPS

	Command	Purpose

Step 1	**ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]}
	
	Example:
	`Router(config)# ip route 192.168.1.0 255.255.0.0 10.10.10.2`
	`Router(config)#`
		Specifies the static route for the IP packets.
		
		For details about this command and about additional parameters that can be set, see *Cisco IOS IP Routing Protocols Command Reference*.

Step 2	**end**
	
	Example:
	`Router(config)# end`
	`Router#`
		Exits router configuration mode and enters privileged EXEC mode.

Example

In the following configuration example, the static route sends out all IP packets with a destination IP address of 192.168.1.0 and a subnet mask of 255.255.255.0 on the Fast Ethernet interface to another device with an IP address of 10.10.10.2. Specifically, the packets are sent to the configured PVC.

You do not need to enter the command marked "(**default**)." This command appears automatically in the configuration file generated when you use the **show running-config** command.

```
!
ip classless (default)
ip route 192.168.1.0 255.255.255.0 10.10.10.2!
```

Verifying Configuration

To verify that you have properly configured static routing, enter the **show ip route** command and look for static routes signified by the "S."

You should see a verification output similar to the following:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
S* 0.0.0.0/0 is directly connected, FastEthernet0
```

Configuring Dynamic Routes

In dynamic routing, the network protocol adjusts the path automatically, based on network traffic or topology. Changes in dynamic routes are shared with other routers in the network.

The Cisco routers can use IP routing protocols, such as Routing Information Protocol (RIP) or Enhanced Interior Gateway Routing Protocol (EIGRP), to learn routes dynamically. You can configure either of these routing protocols on your router.

- Configuring Routing Information Protocol, page 3-20
- Configuring Enhanced Interior Gateway Routing Protocol, page 3-21

Configuring Routing Information Protocol

To configure the RIP routing protocol on the router, follow these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **router rip**
2. **version** {**1** | **2**}
3. **network** *ip-address*
4. **no auto-summary**
5. **end**

DETAILED STEPS

	Command	Task

Step 1	**router rip**
	
	Example:
	`Router> configure terminal`
	`Router(config)# router rip`
	`Router(config-router)#`
		Enters router configuration mode, and enables RIP on the router.

Step 2	**version** {**1**	**2**}
		
		Example:
		`Router(config-router)# version 2`
		`Router(config-router)#`
			Specifies use of RIP version 1 or 2.

Step 3	**network** *ip-address*
	
	Example:
	`Router(config-router)# network 192.168.1.1`
	`Router(config-router)# network 10.10.7.1`
	`Router(config-router)#`
		Specifies a list of networks on which RIP is to be applied, using the address of the network of each directly connected network.

Step 4	**no auto-summary**
	
	Example:
	`Router(config-router)# no auto-summary`
	`Router(config-router)#`
		Disables automatic summarization of subnet routes into network-level routes. This allows subprefix routing information to pass across classful network boundaries.

Step 5	**end**
	
	Example:
	`Router(config-router)# end`
	`Router#`
		Exits router configuration mode and enters privileged EXEC mode.

Example

The following configuration example shows RIP version 2 enabled in IP network 10.0.0.0 and 192.168.1.0.

To see this configuration, use the **show running-config** command from privileged EXEC mode.

```
!
Router# show running-config
router rip
 version 2
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
!
```

Verifying Configuration

To verify that you have properly configured RIP, enter the **show ip route** command and look for RIP routes signified by "R." You should see a verification output like in the following example:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
R    3.0.0.0/8 [120/1] via 2.2.2.1, 00:00:02, Ethernet0/0
```

Configuring Enhanced Interior Gateway Routing Protocol

To configure the Enhanced Interior Gateway Routing Protocol (EIGRP), follow these steps, beginning in global configuration mode:

SUMMARY STEPS

1. **router eigrp** *as-number*
2. **network** *ip-address*
3. **end**

DETAILED STEPS

	Command	Purpose

Step 1	**router eigrp** *as-number*
	
	Example:
	`Router(config)# router eigrp 109`
	`Router(config)#`
		Enters router configuration mode, and enables EIGRP on the router. The autonomous-system number identifies the route to other EIGRP routers and is used to tag the EIGRP information.

Step 2	**network** *ip-address*
	
	Example:
	`Router(config)# network 192.145.1.0`
	`Router(config)# network 10.10.12.115`
	`Router(config)#`
		Specifies a list of networks on which EIGRP is to be applied, using the IP address of the network of directly connected networks.

Step 3	**end**
	
	Example:
	`Router(config-router)# end`
	`Router#`
		Exits router configuration mode and enters privileged EXEC mode.

Example

The following configuration example shows the EIGRP routing protocol enabled in IP networks 192.145.1.0 and 10.10.12.115. The EIGRP autonomous system number is 109.

To see this configuration, use the **show running-config** command, beginning in privileged EXEC mode.

```
!
router eigrp 109
    network 192.145.1.0
        network 10.10.12.115
!
```

Verifying Configuration

To verify that you have properly configured IP EIGRP, enter the **show ip route** command, and look for EIGRP routes indicated by "D." You should see a verification output similar to the following:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 1 subnets
C       10.108.1.0 is directly connected, Loopback0
D    3.0.0.0/8 [90/409600] via 2.2.2.1, 00:00:02, Ethernet0/0
```

CHAPTER 4

Basic Wireless Device Configuration

This chapter describes how to configure the autonomous wireless device on the Cisco 880 Series Integrated Services Router (ISR).

Note To upgrade the autonomous software to Cisco Unified software on the embedded wireless device, see the "Upgrading to Cisco Unified Software" section on page 4-9 for instructions.

The wireless device is embedded and does not have an external console port for connections. To configure the wireless device, use a console cable to connect a personal computer to the host router's console port, and perform these procedures to establish connectivity and configure the wireless settings.

Starting a Wireless Configuration Session

Note *Before* you configure the wireless settings in the router's setup, you must follow these steps to open a session between the router and the access point.

Enter the following commands in global configuration mode on the router's Cisco IOS CLI.

SUMMARY STEPS

1. **interface wlan-ap0**
2. **ip address** *subnet mask*
3. **no shutdown**
4. **interface vlan1**
5. **ip address** *subnet mask*
6. **exit**
7. **exit**
8. **service-module wlan-ap 0 session**

DETAILED STEPS

	Command	Purpose

Step 1	**interface wlan-ap0**
	
	Example:
	`router(config)# interface wlan-ap0`
	`router(config-if)#`
		Defines the router's console interface to the wireless device. The interface is used for communication between the router's console and the wireless device.
		Always use port 0.
		The following message appears:
		
		`The wlan-ap 0 interface is used for managing the embedded AP. Please use the` **`service-module wlan-ap 0 session`** `command to console into the embedded AP.`

Step 2	**ip address** *subnet mask*
	
	Example:
	`router(config-if)# ip address 10.21.0.20 255.255.255.0`
	
	`or`
	`router(config-if)# ip unnumbered vlan1`
		Specifies the interface IP address and subnet mask.
		Note The IP address can be shared with the IP address assigned to the Cisco Integrated Services Router by using the **ip unnumbered vlan1** command.

Step 3	**no shutdown** **Example:** `router(config-if)# no shutdown`	Specifies that the internal interface connection remains open.

	Command	Purpose
Step 4	**interface vlan1** **Example:** `router(config-if)# interface vlan1`	Specifies the virtual LAN interface for data communication on the internal Gigabit Ethernet 0 (GE0) port to other interfaces. • All the switch ports inherit the default vlan1 interface on the Cisco 880 Series ISR.
Step 5	**ip address** *subnet mask* **Example:** `router(config-if)# ip address 10.10.0.30 255.255.255.0`	Specifies the interface IP address and subnet mask.

Step 6	**exit**
	
	Example:
	`router(config-if)# exit`
	`router(config)#`
		Exits the interface configuration mode.

Step 7	**exit**
	
	Example:
	`router(config)# exit`
	`router#`
		Exits the global configuration mode.

Step 8	**service-module wlan-ap 0 session**
	
	Example:
	`router# service-module wlan-ap0 session`
	`Trying 10.21.0.20, 2002 ... Open`
	
	`ap>`
		Opens the connection between the wireless device and the router's console.

Tip To create a Cisco IOS software alias for the console to session into the wireless device, enter the **alias exec dot11radio service-module wlan-ap 0 session** command at the EXEC prompt.

Closing the Session

To close the session between the wireless device and the router's console, follow these steps:

Wireless Device

1. **Control-Shift-6 x**

Router

1. Type the **disconnect** command.
2. Press **Enter.**

Configuring Wireless Settings

Note If you are configuring the wireless device for the first time, you must start a configuration session between the access point and the router before you attempt to configure the basic wireless settings. See the "Starting a Wireless Configuration Session" section on page 4-2.

Configure the wireless device with the tool that matches the software on the device.

- Cisco Express Setup, page 4-4—Unified Software
- Cisco IOS Command Line Interface, page 4-5—Autonomous software

Note If you are running the wireless device in autonomous mode and would like to upgrade to Unified mode, see the "Upgrading to Cisco Unified Software" section on page 4-9 for upgrade instructions.

After upgrading to Cisco Unified Wireless software, use the web-browser interface to configure the device at the following URL:
http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap2-gui.html

Cisco Express Setup

To configure the autonomous wireless device, use the web-browser tool:

Step 1 Establish a console connection to the wireless device and get the Bridge-Group Virtual Interface (BVI) IP address by entering the **show interface bvi1** Cisco IOS command.

Step 2 Open a browser window, and enter the BVI IP address in the browser-window address line. Press **Enter**. An Enter Network Password window appears.

Step 3 Enter your username. *Cisco* is the default username.

Step 4 Enter the wireless device password. *Cisco* is the default password. The Summary Status page appears. For details about using the web-browser configuration page, see the following URL:
http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap4-first.html#wp1103336

Cisco IOS Command Line Interface

To configure the autonomous wireless device, use the Cisco IOS CLI tool to perform the following tasks:

- Configuring the Radio, page 4-5
- Configuring Wireless Security Settings, page 4-5
- Configuring Wireless Quality of Service, page 4-8 (Optional)

Configuring the Radio

Configure the radio parameters on the wireless device to transmit signals in autonomous or Cisco Unified mode. For specific configuration procedures, see the "Configuring Radio Settings" section on page 5-1.

Configuring Wireless Security Settings

- Configuring Authentication, page 4-5
- Configuring Access Point as Local Authenticator, page 4-6
- Configuring WEP and Cipher Suites, page 4-6
- Configuring Wireless VLANs, page 4-6
- Assigning SSIDs, page 4-7

Configuring Authentication

Authentication types are tied to the Service Set Identifiers (SSIDs) that are configured for the access point. To serve different types of client devices with the same access point, configure multiple SSIDs.

Before a wireless client device can communicate on your network through the access point, the client device must authenticate to the access point by using open or shared-key authentication. For maximum security, client devices should also authenticate to your network using MAC address or Extensible Authentication Protocol (EAP) authentication. Both authentication types rely on an authentication server on your network.

To select an authentication type, see *Authentication Types for Wireless Devices* at http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html.

To set up a maximum security environment, see *RADIUS and TACACS+ Servers in a Wireless Environment* at http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html.

Configuring Access Point as Local Authenticator

To provide local authentication service or backup authentication service for a WAN link failure 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 Lightweight Extensible Authentication Protocol (LEAP), Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), or MAC-based authentication. The access point performs up to five authentications per second.

You configure the local authenticator access point manually with client usernames and passwords because it does not synchronize its database with RADIUS servers. You can specify a VLAN and a list of SSIDs that a client is allowed to use.

For details about setting up the wireless device in this role, see *Using the Access Point as a Local Authenticator* at http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html.

Configuring WEP and Cipher Suites

Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between wireless devices to keep the communication private. Wireless devices and their wireless client devices use the same WEP key to encrypt and decrypt data. WEP keys encrypt both unicast and multicast messages. Unicast messages are addressed to one device on the network. Multicast messages are addressed to multiple devices on the network.

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).

Cipher suites that contain Temporal Key Integrity Protocol (TKIP) provide the greatest security for your wireless LAN. Cipher suites that contain only WEP are the least secure.

For encryption procedures, see *Configuring WEP and Cipher Suites* at http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html.

Configuring Wireless VLANs

If you use VLANs on your wireless LAN and assign SSIDs to VLANs, you can create multiple SSIDs by using any of the four security settings defined in the "Security Types" section on page 4-7. 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), that are 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 of protocols for each VLAN.

For more information about wireless VLAN architecture, see *Configuring Wireless VLANs* at http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html.

Note If you do *not* use VLANs on your wireless LAN, the security options that you can assign to SSIDs are limited because the encryption settings and authentication types are linked on the Express Security page.

Assigning SSIDs

You can configure up to 16 SSIDs on a wireless device in the role of an access point, and you can configure a unique set of parameters for each SSID. For example, you might use one SSID to allow guests limited access to the network and another SSID to allow authorized users access to secure data.

For more about creating multiple SSIDs, see *Service Set Identifiers* at http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html.

Note 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 the SSIDs use different encryption settings. If you find that the security setting for an SSID conflicts with the settings for another SSID, you can delete one or more SSIDs to eliminate the conflict.

Security Types

Table 4-1 describes the four security types that you can assign to an SSID.

Table 4-1 Types of SSID Security

Security Type	Description	Security Features Enabled
No security	This is the least secure option. You should use this option only for SSIDs in a public space and you should assign it to a VLAN that restricts access to your network.	—
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 the MAC address. For more information, see C*ipher Suites and WEP* at http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html. Or If your network does not have a RADIUS server, consider using an access point as a local authentication server. For instructions, see *Using the Access Point as a Local Authenticator* at http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html.	Mandatory WEP. Client devices cannot associate using this SSID without a WEP key that matches the wireless device key.

Table 4-1 Types of SSID Security (continued)

Security Type	Description	Security Features Enabled
EAP[1] authentication	This option enables 802.1X authentication (such as LEAP[2], PEAP[3], EAP-TLS[4], EAP-FAST[5], EAP-TTLS[6], EAP-GTC[7], EAP-SIM[8], and other 802.1X/EAP-based products) This setting uses mandatory encryption, WEP, open authentication plus EAP, network EAP authentication, no key management, and RADIUS server authentication port 1645. You are required to enter the IP address and shared secret key for an authentication server on your network (server authentication port 1645). Because 802.1X authentication provides dynamic encryption keys, you do not need to enter a WEP key.	Mandatory 802.1X authentication. Client devices that associate using this SSID must perform 802.1X authentication. If radio clients are configured to authenticate using EAP-FAST, open authentication with EAP should also be configured. If you do not configure open authentication with EAP, the following warning message appears: `SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.`
WPA[9]	This option permits wireless access to users who are authenticated against a database. Access is through the services of an authentication server. Users' IP traffic is then encrypted with stronger algorithms than those used in WEP. This setting uses encryption ciphers, TKIP[10], open authentication plus 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 key for an authentication server on your network (server authentication port 1645).	Mandatory WPA authentication. Client devices that associate using this SSID must be WPA capable. If radio clients are configured to authenticate using EAP-FAST, open authentication with EAP should also be configured. If you do not configure open authentication with EAP, the following warning message appears: `SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.`

1. EAP = Extensible Authentication Protocol.
2. LEAP = Lightweight Extensible Authentication Protocol.
3. PEAP = Protected Extensible Authentication Protocol.
4. EAP-TLS = Extensible Authentication Protocol—Transport Layer Security.
5. EAP-FAST = Extensible Authentication Protocol—Flexible Authentication via Secure Tunneling.
6. EAP-TTLS = Extensible Authentication Protocol—Tunneled Transport Layer Security.
7. EAP-GTC = Extensible Authentication Protocol—Generic Token Card.
8. EAP-SIM = Extensible Authentication Protocol—Subscriber Identity Module.
9. WPA = Wi-Fi Protected Access.
10. TKIP = Temporal Key Integrity Protocol.

Configuring Wireless Quality of Service

Configuring quality of service (QoS) can provide preferential treatment to certain traffic at the expense of other traffic. Without QoS, the device 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. To configure QoS for your wireless device, see *Quality of Service in a Wireless Environment* at http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html.

Configuring the Access Point in Hot Standby Mode

In hot standby mode, an access point is designated as a backup for another access point. The standby access point is placed near the access point that it monitors and is configured exactly like the monitored access point. The standby access point associates with the monitored access point as a client and sends Internet Access Point Protocol (IAPP) queries to the monitored access point through the Ethernet and 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 ensure that client devices can switch easily to the standby access point. For more information, see *Hot Standby Access Points* at http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html.

Upgrading to Cisco Unified Software

To run the access point in Cisco Unified mode, upgrade the software by performing the following procedures:

- Preparing for the Upgrade, page 4-9
- Performing the Upgrade, page 4-11
- Upgrading AP bootloader, page 4-12
- Downgrading the Software on the Access Point, page 4-12
- Recovering Software on the Access Point, page 4-13

Software Prerequisites

- Cisco 880 Series ISRs with embedded access points are eligible to upgrade from autonomous software to Cisco Unified software if the router is running the advipservices feature set and Cisco IOS Release15.2(4)M1 or later versions.
- To use the embedded access point in a Cisco Unified Architecture, the Cisco Wireless LAN Configuration (WLC) must be running the minimum versions for single radio (Cisco IOS Release 7.0.116.0 or later versions) and dual radio (Cisco IOS Release 7.2.110.0 or later versions).

Preparing for the Upgrade

To prepare for the upgrade, peform the following tasks:

- Secure an IP Address on the Access Point, page 4-10
- Confirm that the Mode Setting is Enabled, page 4-10

Secure an IP Address on the Access Point

Secure an IP address on the access point so it that can communicate with the WLC and download the Unified image upon bootup. The host router provides the access point DHCP server functionality through the DHCP pool. The access point communicates with the WLC and setup option 43 for the controller IP address in the DHCP pool configuration. The following is a sample configuration:

```
ip dhcp pool embedded-ap-pool
network 60.0.0.0 255.255.255.0
dns-server 171.70.168.183
default-router 60.0.0.1
option 43 hex  f104.0a0a.0a0f   (single WLC IP address(10.10.10.15) in hex format)
int vlan1
ip address 60.0.0.1 255.255.255.0
```

For more information about the WLC discovery process, see *Cisco Wireless LAN Configuration Guide* at http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ccfig40.html.

Confirm that the Mode Setting is Enabled

To confirm that the mode setting is enabled, follow these steps:

Step 1 Ping the WLC from the router to confirm IP connectivity.

Step 2 Enter the **service-module wlan-ap 0 session** command to establish a session into the access point.

Step 3 Confirm that the access point is running an autonomous boot image.

Step 4 Enter the **show boot** command on the access point to confirm that the mode setting is enabled. The following is a sample output for the command:

```
# show boot
BOOT path-list:      flash:ap802-k9w7-mx.124/ap802-k9w7-mx.124
Config file:         flash:/config.txt
Private Config file: flash:/private-config
Enable Break:          no
Manual Boot:         yes
HELPER path-list:    no
NVRAM/Config file
buffer size:   32768
Mode Button:    on
Radio Core TFTP:
ap#
```

Performing the Upgrade

To upgrade the autonomous software to Cisco Unified software, follow these steps:

Step 1 To change the access point boot image to a Cisco Unified upgrade image (also known as a *recovery image*), issue the **service-module wlan-ap 0 bootimage unified** command in global configuration mode.

```
Router# configure terminal
Router(config)# service-module wlan-ap 0 bootimage unified
Router(config)# end
```

Note If the **service-module wlan-ap 0 bootimage unified** command does not work, check whether the advipservices or advipsevices_npe software license is enabled or not.

To identify the access point's boot image path, use the **show boot** command in privileged EXEC mode on the access point console:

```
autonomous-AP# show boot
BOOT path-list: flash:/ap802-rcvk9w8-mx/ap802-rcvk9w8-mx
```

Step 2 To perform a graceful shutdown and reboot of the access point to complete the upgrade process, issue the **service-module wlan-ap 0 reload** command in privileged EXEC mode. Establish a session into the access point and monitor the upgrade process.

Troubleshooting an Upgrade or Reverting the AP to Autonomous Mode

Q. My access point failed to upgrade from autonomous software to Cisco Unified software, and it appears to be stuck in the recovery mode. What is my next step?

A. If the access point fails to upgrade from autonomous to Unified software, perform the following actions:

- Check to ensure the autonomous access point does not have the static IP address configured on the BVI interface before you boot the recovery image.
- Issue a ping between the router/access point and the WLC to confirm communication.
- Check that the access point and WLC clock (time and date) are set correctly.

Q. My access point is attempting to boot, but it keeps failing. Why?
My access point is stuck in the recovery image and does not upgrade to the Unified software. Why?

A. The access point may attempt to boot and fail or may become stuck in the recovery mode and fail to upgrade to the Unified software. If either occurs, use the **service-module wlan-ap0 reset bootloader** command to return the access point to the bootloader for manual image recovery.

Upgrading AP bootloader

For AP802, the bootloader is available as part of the host router image. To upgrade the bootloader, perform the following steps:

Step 1 Verify the WLAN AP bootloader bundled with the host router image running on the first core using the **show platform version** command.

```
Router# show platform version
Platform Revisions/Versions :
.
WLAN AP Boot loader (bundled):
AP802 Boot Loader (AP802-BOOT-M) Version 12.4(25e)JA1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Compiled Wed 30-May-12 03:46 by prod_rel_team
```

Step 2 Open a session between the router and the WLAN AP.

For information on how to open a session between a router and an access point, see the "Starting a Wireless Configuration Session" section on page 4-2.

Step 3 Verify the version of the WLAN AP bootloader.

At the WLAN AP bootloader, use the **version** command.

```
ap: version
AP802 Boot Loader (AP802-BOOT-M) Version 12.4(25e)JA1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Compiled Wed 30-May-12 03:46 by prod_rel_team
```

At the WLAN AP IOS, use the show version command.

```
ap# show version
.
BOOTLDR: AP802 Boot Loader (AP802-BOOT-M) Version 12.4(25e)JA1, RELEASE SOFTWARE (fc1)
<snip>
Configuration register is 0xF
```

Step 4 Upgrade the bootloader using the following commands:

```
Router# service-module wlan-ap 0 upgrade bootloader
Router# service-module wlan-ap 0 reset
```

Downgrading the Software on the Access Point

To reset the access point boot to the last autonomous image, use the **service-module wlan-ap0 bootimage autonomous** command in privileged EXEC mode on the host router running on the first core. To reload the access point with the autonomous software image, use the **service-module wlan-ap 0 reload** command.

```
Router# configure terminal
Router(config)# service-module wlan-ap 0 bootimage autonomous
Router(config)# end
Router# write
Router# service-module wlan-ap 0 reload
```

Recovering Software on the Access Point

To recover the image on the access point, use the **service-module wlan-ap0 reset bootloader** command in privileged EXEC mode. This command returns the access point to the bootloader for manual image recovery.

Caution Use this command with caution. It does *not* provide an orderly shutdown and consequently may impact file operations that are in progress. Use this command only to recover from a shutdown or a failed state.

Images Supported

For information on images supported on the Cisco 880 Series ISRs, see the "Images Supported" section on page 1-11.

Related Documentation

See the following documentation for additional autonomous and unified configuration procedures:

- Autonomous Mode Documentation—Table 4-2
- Unified Mode Documentation—Table 4-3

Table 4-2 Autonomous Mode Documentation

Autonomous Mode	Links	Description
Network Design		
Wireless Overview	Wireless Device Overview	Describes the roles of the wireless device on the network.
Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges Versions 12.4(25d)JA and 12.3(8)JEE	http://www.cisco.com/en/US/docs/wireless/access_point/12.4.25d.JA/Command/reference/cr12425d-preface.html	Describes the Cisco IOS Release 12.4(25d)JA and Cisco IOS Release 12.3(8)JEE commands for configuring Cisco Aironet access points and bridges.
Configuration		
Configuring the Radio	Configuring Radio Settings	Describes how to configure the wireless radio.
Security		
Authentication Types for Wireless Devices	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html	Describes the authentication types that are configured on the access point.

Table 4-2 Autonomous Mode Documentation (continued)

Autonomous Mode	Links	Description
RADIUS and TACACS+ Servers in a Wireless Environment	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html	Describes how to enable and configure the RADIUS[1] and TACACS+[2] and provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS and TACACS+ are facilitated through AAA[3] and can be enabled only through AAA commands.
Using the Access Point as a Local Authenticator	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html	Describes how to use a wireless device in the role of an access point as a local authenticator, serving as a standalone authenticator for a small wireless LAN or providing backup authentication service. As a local authenticator, the access point performs LEAP, EAP-FAST, and MAC-based authentication for up to 50 client devices.
Cipher Suites and WEP	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html	Describes how to configure the cipher suites required when using WPA[4] and CCKM[5]; WEP[6]; and WEP features including AES[7], MIC[8], TKIP[9], and broadcast key rotation.
Hot Standby Access Points	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html	Describes how to configure your wireless device as a hot standby unit.
Configuring Wireless VLANs	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html	Describes how to configure an access point to operate with the VLANs set up on a wired LAN.
Service Set Identifiers	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html	In the role of an access point, a wireless device can support up to 16 SSIDs[10]. This document describes how to configure and manage SSIDs on the wireless device.
Administering		
Quality of Service	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html	Describes how to configure QoS[11] on your Cisco wireless interface. With this feature, you can provide preferential treatment to certain traffic at the expense of other traffic. Without QoS, the device 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.
Regulatory Domains and Channels	http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/scg_chanels.html	Lists the radio channels supported by Cisco access products in the regulatory domains of the world.
System Message Logging	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SysMsgLogging.html	Describes how to configure system message logging on your wireless device.

1. RADIUS = Remote Authentication Dial-In User Service.
2. TACACS+ = Terminal Access Controller Access Control System Plus.

3. AAA = Authentication, Authorization, and Accounting.
4. WPA = Wireless Protected Access.
5. CCKM = Cisco Centralized Key Management.
6. WEP = Wired Equivalent Privacy.
7. AES = Advanced Encryption Standard.
8. MIC = Message Integrity Check.
9. TKIP = Temporal Key Integrity Protocol.
10. SSID = service set identifiers.
11. QoS = quality of service.

Table 4-3 Unified Mode Documentation

Network Design	Links
Why Migrate to the Cisco Unified Wireless Network?	http://www.cisco.com/en/US/solutions/ns175/networking_solutions_products_genericcontent0900aecd805299ff.html
Wireless LAN Controller (WLC) FAQ	http://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a008064a991.shtml
Single-Radio AP802	
Cisco Wireles LAN Controller Configuration Guide, Release 7.0.116.0	http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/cg_controller_setting.html
Dual-Radio AP802	
Cisco Unified Wireless Network Software Release 7.2.110.0 (7.2 Maintenance Release 1)	http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps10315/product_bulletin_c25-707629.html

CHAPTER 5

Configuring Radio Settings

This module describes how to configure radio settings for the wireless device in the following sections:

Enabling the Radio Interface

The wireless device radios are disabled by default.

Note You must create a service set identifier (SSID) before you can enable the radio interface.

To enable the access point radio, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **dot11 ssid** *ssid*
3. **interface dot11radio** {**0**}
4. **ssid** *ssid*
5. **no shutdown**
6. **end**
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**dot11 ssid** *ssid*	Enters the SSID. **Note** The SSID consists of up to 32 alphanumeric characters. SSIDs are case sensitive.
Step 3	**interface dot11radio** {**0**}	Enters interface configuration mode for the radio interface. • The 2.4-GHz and 802.11g/n 2.4-GHz radios are radio 0.
Step 4	**ssid** *ssid*	Assigns the SSID that you created in Step 2 to the appropriate radio interface.
Step 5	**no shutdown**	Enables the radio port.
Step 6	**end**	Returns to privileged EXEC mode.
Step 7	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

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

Configuring the Role in the Radio Network

The radio performs the following roles in the wireless network:

- Access point
- Access point (fallback to radio shutdown)
- Root bridge
- Non-root bridge
- Root bridge with wireless clients
- Non-root bridge without wireless clients

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. The default fallback role for Cisco ISR wireless devices is as follows:

Shutdown—the wireless device shuts down its radio and disassociates all client devices.

To set the wireless device's radio network role and fallback role, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **station-role non-root** {**bridge | wireless-clients**} **root** {**access-point | ap-only | [bridge | wireless-clients] | [fallback | repeater | shutdown]**} **workgroup-bridge** {**multicast | mode** <*client* | *infrastructure*>**| universal** <*Ethernet client MAC address*>}
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0**}	Enters interface configuration mode for the radio interface. • The 2.4-GHz and 802.11g/n 2.4-GHz radios are radio 0.
Step 3	**station-role** **non-root** {**bridge** | **wireless-clients**} **root** {**access-point** | **ap-only** | **[bridge** | **wireless-clients]** | **[fallback** | **repeater** | **shutdown]**} **workgroup-bridge** {**multicast** | **mode** <*client* | *infrastructure*>| **universal** <*Ethernet client MAC address*>}	Sets the wireless device role. • Sets the role to non-root bridge with or without wireless clients, to root access point or bridge, or to workgroup bridge. **Note** The **bridge** mode radio supports point-to-point configuration only. **Note** The **repeater** and **wireless-clients** commands are not supported on Cisco 860 Series and Cisco 880 Series Integrated Services Routers. **Note** The **scanner** command is not supported on Cisco 860 Series and Cisco 880 Series Integrated Services Routers. • 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. A workgroup bridge can have a maximum of 25 clients, presuming that no other wireless clients are associated to the root bridge or access point.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

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

Radio Tracking

You can configure the access point to track or monitor the status of one of its radios. If 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
```

Fast Ethernet Tracking

You can configure the access point for fallback when its Ethernet port is disabled or disconnected from the wired LAN. For guidance on configuring the access point for Fast Ethernet tracking, see the "Configuring the Role in the Radio Network" section on page 5-3.

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 come up or go 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
```

Configuring Radio Data Rates

You use the data rate settings to choose the data rates that the wireless device uses for data transmission. The rates are expressed in megabits per second (Mb/s). The wireless device always attempts to transmit at the highest data rate set to **basic**, also known as **required** 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 data rates of the wireless device 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 Mb/s service only, set the 11-Mb/s 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 Mb/s, 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-Mb/s service only, set the 54-Mb/s 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-Mb/s rate to **basic** and sets 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 cannot connect to the access point although other clients can, the client might not be within the coverage area of the access point. In such a case, using the range option will help extend 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 renegotiate in order to maintain the link (but at a lower data rate). A link that is configured for a higher throughput simply drops when the signal degrades enough that it no longer sustains a configured high data rate, or the link roams to another access point with sufficient coverage, if one is available. The balance between the two (throughput vs. range) is a design decision that must be made based on resources available to the wireless project, the type of traffic the users will be passing, the 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 Mb/s are set to **required** (**basic**) and that all other data rates are set to **enable**. The 802.11b adapters do not recognize the 54 Mb/s data rate and do not operate if data rates higher than 11 Mb/s are set to **required** on the connecting access point.

To configure the radio data rates, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **speed**
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0**}	Enters interface configuration mode for the radio interface. • The 2.4-GHz and the 802.11g/n 2.4-GHz radios are radio 0.

	Command or Action	Purpose
Step 3	**speed** 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**} 802.11g, 2.4-GHz radio: {[**1.0**] [**2.0**] [**5.5**] [**6.0**] [**9.0**] [**11.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**basic-1.0**] [**basic-2.0**] [**basic-5.5**] [**basic-6.0**] [**basic-9.0**] [**basic-11.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] | **range** | **throughput** [**ofdm**] | **default**} 802.11a 5-GHz radio: {[**6.0**] [**9.0**] [**12.0**] [**18.0**] [**24.0**] [**36.0**] [**48.0**] [**54.0**] [**basic-6.0**] [**basic-9.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-54.0**] | **range** | **throughput** | **ofdm-throughput** | **default**} 802.11n 2.4-GHz radio: {[**1.0**] [**11.0**] [**12.0**] [**18.0**] [**2.0**] [**24.0**] [**36.0**] [**48.0**] [**5.5**] [**54.0**] [**6.0**] [**9.0**] [**basic-1.0**] [**basic-11.0**] [**basic-12.0**] [**basic-18.0**] [**basic-24.0**] [**basic-36.0**] [**basic-48.0**] [**basic-5.5**] [**basic-54.0**] [**basic-6.0**] [**basic-9.0**] [**default**] [**m0-7**] [**m0.**] [**m1.**] [**m10.**] [**m11.**] [**m12.**] [**m13.**] [**m14.**] [**m15.**] [**m2.**] [**m3.**] [**m4.**] [**m5.**] [**m6.**] [**m7.**] [**m8-15**] [**m8.**] [**m9.**] [**ofdm**] [**only-ofdm**] | **range** | **throughput**}	Sets each data rate to **basic** or **enabled**, or enters **range** to optimize range or enters **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** If the client must support the basic rate that you select, it cannot associate to the wireless device. If you select 12-Mb/s or higher for the basic data rate on the 802.11g radio, 802.11b client devices cannot associate to the wireless device 802.11g radio. Enter **basic-6.0**, **basic-9.0**, **basic-12.0**, **basic-18.0**, **basic-24.0**, **basic-36.0**, **basic-48.0**, and **basic-54.0** to set these data rates to **basic** on the 5-GHz radio. • (Optional) 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 sets 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 to 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 stes rates 6, 9, 12, 18, 24, 36, 48, and 54 to **enabled**. These rate settings allow both 802.11b and 802.11g client devices to associate to the wireless device 802.11g radio.

	Command or Action	Purpose
	speed (continued)	On the 5-GHz radio, the **default** option sets rates 6.0, 12.0, and 24.0 to **basic**, and stes rates 9.0, 18.0, 36.0, 48.0, and 54.0 to **enabled**. On the 802.11g/n 2.4-GHz radio, the **default** option sets rates 1.0, 2.0, 5.5, and 11.0 to **enabled**. On the 802.11g/n 5-GHz radio, the **default** option sets rates to 6.0, 12.0, and 24.0 to **enabled**. The modulation coding scheme (MCS) index range for both 802.11g/n radios is 0 to 15.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves 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 MCS Rates

Modulation coding scheme (MCS) is a specification of PHY parameters consisting of modulation order (binary phase shift keying [BPSK], quaternary phase shift keying [QPSK], 16-quadrature amplitude modulation [16-QAM], 64-QAM) and forward error correction (FEC) code rate (1/2, 2/3, 3/4, 5/6). MCS is used in the wireless device 802.11n radios, which define 32 symmetrical settings (8 per spatial stream):

- MCS 0–7
- MCS 8–15
- MCS 16–23
- MCS 24–31

The wireless device supports MCS 0–15. High-throughput clients support at least MCS 0–7.

MCS is an important setting because it provides for potentially greater throughput. High-throughput data rates are a function of *MCS*, *bandwidth*, and *guard interval*. The 802.11a, b, and g radios use 20-MHz channel widths. Table 5-1 shows potential data rated based on MCS, guard interval, and channel width.

Table 5-1 Data Rates Based on MCS Settings, Guard Interval, and Channel Width

MCS Index	Guard Interval = 800 ns		Guard Interval = 400 ns	
	20-MHz Channel Width Data Rate (Mb/s)	40-MHz Channel Width Data Rate (Mb/s)	20-MHz Channel Width Data Rate (Mb/s)	40-MHz Channel Width Data Rate (Mb/s)
0	6.5	13.5	7 2/9	15
1	13	27	14 4/9	30

Table 5-1 Data Rates Based on MCS Settings, Guard Interval, and Channel Width (continued)

MCS Index	Guard Interval = 800 ns		Guard Interval = 400 ns	
2	19.5	40.5	21 2/3	45
3	26	54	28 8/9	60
4	39	81	43 1/3	90
5	52	109	57 5/9	120
6	58.5	121.5	65	135
7	65	135	72 2/9	152.5
8	13	27	14 4/9	30
9	26	54	28 8/9	60
10	39	81	43 1/3	90
11	52	108	57 7/9	120
12	78	162	86 2/3	180
13	104	216	115 5/9	240
14	117	243	130	270
15	130	270	144 4/9	300
The legacy rates are as follows:				
5 GHz: 6, 9, 12, 18, 24, 36, 48, and 54 Mb/s				
2.4 GHz: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mb/s				

MCS rates are configured using the **speed** command. The following example shows a **speed** setting for an 802.11g/n 2.4-GHz radio:

```
interface Dot11Radio0
    no ip address
    no ip route-cache
    !
    ssid 800test
    !
    speed basic-1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0 m0. m1. m2. m3. m4.
    m8. m9. m10. m11. m12. m13. m14. m15.
```

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 set the transmit power on access point radios, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **power local**
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface dot11radio** {**0**}	Enters interface configuration mode for the radio interface. • The 2.4-GHz and the 802.11g/n 2.4-GHz radios are radio 0.
Step 3	**power local** These options are available for the 2.4-GHz 802.11n radio (in dBm): {**8** | **9**| **11** | **14** | **15** | **17** | **maximum**}	Sets the transmit power for the 2.4-GHz radio so that the power level is allowed in your regulatory domain.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Use the **no** form of the **power local** 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 (DPC) to refer to limiting the power level on associated client devices.

To specify a maximum allowed power setting on all client devices that associate to the wireless device, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **power client**
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0**}	Enters interface configuration mode for the radio interface. • The 2.4-GHz and 802.11g/n 2.4-GHz radios are radio 0.
Step 3	**power client** These options are available for 802.11n 2.4-GHz clients (in dBm): {**local** | **8** | **9** | **11** | **14** | **15** | **17** | **maximum**}	Sets the maximum power level allowed on client devices that associate to the wireless device. • Setting the power level to **local** sets the client power level to that of the access point. • Setting the power level to **maximum** sets the client power to the allowed maximum. **Note** The settings allowed in your regulatory domain might differ from the settings listed here.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Use the **no** form of the **power client** command to disable the maximum power level for associated clients.

Note Aironet extensions must be enabled to limit the power level on associated client devices. Aironet extensions are enabled by default.

Configuring Radio Channel Settings

The default channel setting for the wireless device radios is least congested. At startup, the wireless device scans for and selects the least-congested channel. For the most consistent performance after a site survey, however, we recommend that you assign a static channel setting for each access point. The channel settings on the wireless device correspond to the frequencies available in your regulatory domain. See the access point hardware installation guide for the frequencies allowed in your domain.

Each 2.4-GHz channel covers 22 MHz. Because the bands for channels 1, 6, and 11 do not overlap, you can set up multiple access points in the same vicinity without causing interference. The 802.11b and 802.11g 2.4-GHz radios use the same channels and frequencies.

The 5-GHz radio operates on 8 channels from 5180 to 5320 MHz, up to 27 channels from 5170 to 5850 MHz depending on regulatory domain. Each channel covers 20 MHz, and the bands for the channels overlap slightly. For best performance, use channels that are not adjacent (use channels 44 and 46, for example) for radios that are close to each other.

Note The presence of too many access points in the same vicinity can create radio congestion that can reduce throughput. A careful site survey can determine the best placement of access points for maximum radio coverage and throughput.

802.11n Channel Widths

The 802.11n standard allows both 20-MHz and 40-Mhz channel widths consisting of two contiguous non-overlapping channels (for example, 2.4-GHz channels 1 and 6).

One of the 20-MHz channels is called the *control channel*. Legacy clients and 20-MHz high-throughput clients use the control channel. Only beacons can be sent on this channel. The other 20-MHz channel is called the *extension channel.* The 40-MHz stations may use this channel and the control channel simultaneously.

A 40-MHz channel is specified as a channel and extension, such as 1,1. In this example, the control channel is channel 1 and the extension channel is above it.

To set the wireless device channel width, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0** }
3. **channel** {*frequency* | **least-congested** | **width** [**20** | **40-above** | **40-below**] | **dfs**}
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0** }	Enters interface configuration mode for the radio interface. • The 802.11g/n 2.4-GHz radio is radio 0.
Step 3	**channel** {*frequency* | **least-congested** | **width** [**20** | **40-above** | **40-below**] | **dfs**}	Sets the default channel for the wireless device radio.To search for the least-congested channel on startup, enter **least-congested**. • Use the **width** option to specify a bandwidth to use. This option is available for the Cisco 800 series ISR wireless devices and consists of three available settings: **20**, **40-above**, and **40-below:** – Choosing **20** sets the channel width to 20 MHz. – Choosing **40-above** sets the channel width to 40 MHz with the extension channel above the control channel. – Choosing **40-below** sets the channel width to 40 MHz with the extension channel below the control channel. **Note** The **channel** command is disabled for 5-GHz radios that comply with European Union regulations on dynamic frequency selection (DFS). See the "Enabling and Disabling World Mode" section on page 5-14 for more information.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Enabling and Disabling World Mode

You can configure the wireless device to support 802.11d world mode, Cisco legacy world mode, or world mode roaming. When you enable world mode, the 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 detect whether the wireless device is using 802.11d or Cisco legacy world mode and automatically use the 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 and changes its settings as required.

World mode is disabled by default.

To enable world mode, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **world-mode** {**dot11d country_code** *code* {**both** | **indoor** | **outdoor**}| **world-mode roaming** | **legacy**}
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0**}	Enters interface configuration mode for the radio interface.
Step 3	**world-mode** {**dot11d country_code** *code* {**both** | **indoor** | **outdoor**} | **world-mode roaming** | **legacy**}	Enables 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** option 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**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Use the **no** form of the **world-mode** 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.
- Long—A long preamble ensures compatibility between the wireless device and all early models of Cisco Aironet Wireless LAN Adapters. 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.

To disable short radio preambles, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0** }
3. **no preamble-short**
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0** }	Enters interface configuration mode for the 2.4-GHz radio interface.
Step 3	**no preamble-short**	Disables short preambles and enables long preambles.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves 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 that the wireless device uses to receive and transmit data. There are three options for both the receive antenna and the transmit antenna:

- Gain—Sets the resultant antenna gain in decibels (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.

To select the antennas that the wireless device uses to receive and transmit data, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **gain** *dB*
4. **antenna receive** {**diversity | left | right**}
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0**}	Enters interface configuration mode for the radio interface. • The 802.11g/n 2.4-GHz radio is radio 0.
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** The Cisco 860 and Cisco 880 ISRs are shipped with a fixed antenna that cannot be removed. The antenna gain cannot be configured on these models.
Step 4	**antenna receive** {**diversity** | **left** | **right**}	Sets 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	**end**	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

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 on the basis of such factors 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 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 is based on an early algorithm presented by the IEEE 802.11i security task group. The standards-based algorithm, Temporal Key Integrity Protocol (TKIP), does not require Aironet extensions to be enabled.
- 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. To disable Aironet extensions, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **no dot11 extension aironet**
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0**}	Enters interface configuration mode for the radio interface. The 802.11g/n 2.4-GHz radio is radio 0.
Step 3	**no dot11 extension aironet**	Disables Aironet extensions.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves 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 by using an encapsulation transformation method. These are the two transformation methods:

- 802.1H—This method provides optimum performance for Cisco wireless products.
- RFC 1042—Use this setting to ensure interoperability with non-Cisco wireless equipment. RFC1042 does not provide the interoperability advantages of 802.1H but is used by other manufacturers of wireless equipment.

To configure the encapsulation transformation method, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **payload-encapsulation** {**snap** | **dot1h**}
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0**}	Enters interface configuration mode for the radio interface. • The 802.11g/n 2.4-GHz radio is radio 0.
Step 3	**payload-encapsulation** {**snap** | **dot1h**}	Sets the encapsulation transformation method to RFC 1042 (**snap**) or 802.1h (**dot1h**, the default setting).
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Enabling and Disabling Public Secure Packet Forwarding

Public Secure Packet Forwarding (PSPF) prevents client devices that are associated to an access point from inadvertently sharing files or communicating with other client devices that are associated to the access point. PSPF 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 5-21 for instructions on setting up protected ports.

To enable and disable PSPF using CLI commands on the wireless device, you use bridge groups. For a detailed explanation on bridge groups and instructions for implementing them, see the Configuring Transparent Bridging chapter of *Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2* at the following link:

http://www.cisco.com/en/US/docs/ios/12_2/ibm/configuration/guide/bcftb_ps1835_TSD_Products_Configuration_Guide_Chapter.html

PSPF is disabled by default. To enable PSPF, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **bridge-group** *group* **port-protected**
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0**}	Enters interface configuration mode for the radio interface. • The 802.11g/n 2.4-GHz radio is radio 0.
Step 3	**bridge-group** *group* **port-protected**	Enables PSPF.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Use the **no** form of the **bridge group** command to disable PSPF.

Configuring Protected Ports

To prevent communication between client devices that are 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.

To define a port on your switch as a protected port, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **switchport protected**
4. **end**
5. **show interfaces** *interface-id* **switchport**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id*	Enters interface configuration mode. • Enter the type and number of the switch port interface to configure, such as **wlan-gigabitethernet0**.
Step 3	**switchport protected**	Configures the interface to be a protected port.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**show interfaces** *interface-id* **switchport**	Verifies your entries.
Step 6	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

To disable protected port, use the **no switchport protected** command.

For detailed information on protected ports and port blocking, see the "Configuring Port-Based Traffic Control" chapter in *Catalyst 3550 Multilayer Switch Software Configuration Guide, 12.1(12c)EA1* at the following URL*:*

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 (Kmicrosecs). One Kmicrosec 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 if the data beacon rate is set at 2, its default setting, then the wireless device sends a beacon containing a DTIM every 200 Kmicrosecs.

The default beacon period is 100, and the default DTIM is 2. To configure the beacon period and the DTIM, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **beacon period** *value*
4. **beacon dtim-period** *value*
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0**}	Enters interface configuration mode for the radio interface. • The 802.11g/n 2.4-GHz radio is radio 0.
Step 3	**beacon period** *value*	Sets the beacon period. • Enter a value in kilomicroseconds.
Step 4	**beacon dtim-period** *value*	Sets the DTIM. • Enter a value in kilomicroseconds.
Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Configure RTS Threshold and Retries

The request to send (RTS) threshold determines the packet size at which the wireless device issues an 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 detect each other. You can enter a setting ranging from 0 to 2347 bytes.

The 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 32.

To configure the RTS threshold and maximum RTS retries, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **rts threshold** *value*
4. **rts retries** *value*
5. **end**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0**}	Enters interface configuration mode for the radio interface. • The 2.4-GHz and the 802.11g/n 2.4-GHz radios are radio 0.
Step 3	**rts threshold** *value*	Sets the RTS threshold. • Enter an RTS threshold from 0 to 2347.
Step 4	**rts retries** *value*	Sets the maximum RTS retries. • Enter a setting from 1 to 128.
Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Use the **no** form of the **rts** command to reset the RTS settings to defaults.

Configuring the Maximum Data Retries

The maximum data retries setting determines the number of attempts that the wireless device makes to send a packet before it drops the packet. The default setting is 32.

To configure the maximum data retries, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **packet retries** *value*
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0**}	Enters interface configuration mode for the radio interface. • The 802.11g/n 2.4-GHz radio is radio 0.
Step 3	**packet retries** *value*	Sets the maximum data retries. • Enter a setting from 1 to 128.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Use the **no** form of the **packet retries** command to reset the setting to the default.

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 2346 bytes.

To configure the fragmentation threshold, follow these steps, beginning in privileged EXEC mode:

SUMMARY STEPS

1. **configure terminal**
2. **interface dot11radio** {**0**}
3. **fragment-threshold** *value*
4. **end**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface dot11radio** {**0**}	Enters interface configuration mode for the radio interface. • The 802.11g/n 2.4-GHz and 5-GHz radios are radio 0.
Step 3	**fragment-threshold** *value*	Sets the fragmentation threshold. • Enter a setting from 256 to 2346 bytes for the 2.4-GHz radio. • Enter a setting from 256 to 2346 bytes for the 5-GHz radio.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Use the **no** form of the **fragment-threshold** command to reset the setting to the default.

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 the **short-slot-time** command to enable short slot time:

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

Use the **no** form of the **short-slot-time** command 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.

Use the **show dot11 carrier busy** command to redisplay 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 class of service (CoS) 5 (Video) and CoS 6 (Voice) user priorities.

To configure VoIP packet handling on an access point, follow these steps:

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**.

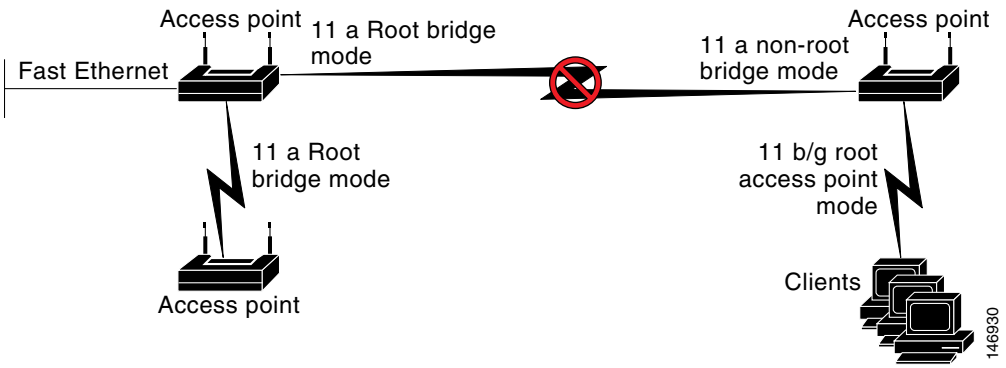
The Stream page appears.

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 5-1). This value indicates how many times the access point will try to retrieve a lost packet before discarding it.

Figure 5-1 Packet Handling Configuration



Note You may also configure the CoS 4 (Controlled Load) user priority and its maximum retries value.

Step 6 Click **Apply**.

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 *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.